Hacking Ético: Taxonomía de un Ataque

Henry Alexander Diaz Mongua, *Consultor Seguridad Informática, CEO Hackers Colombianos*

***Resumen*—No hay metodología clara propuesta para entender "el cómo?" se realiza un ataque, ya sea a un sistema informático, una red, al hardware o algún proceso o procedimiento establecido, por personas mal llamadas hackers, crackers y phreakings; este documento busca exponer una clasificación y ordenar las piezas del rompecabezas que conforman un ataque, para entender su proceder y así mismo gracias a este análisis crear una línea base de seguridad y defensa, para aprender a proteger nuestros activos informáticos. El artículo describe la taxonomía del ataque perpetuados por los hackers y crackers; entender la manera de cómo actúan y mostrar la metodología en general de acuerdo a la investigación realizada.**

***Palabras Claves*--. Hackers, cracker, amenaza, ataque, vulnerabilidad, riesgo, incidente, impacto, confidencialidad, disponibilidad, integridad, footprinting.**

***Abstract*- No clear methodology proposed to understand "how?" Is carried out an attack, either on a computer system, a network, hardware or any process or procedure established by people misnamed hackers, crackers and phreakings; this document seeks to expose a classification and sort the pieces of the puzzle that make up an attack, to understand their actions and also thanks to this analysis establish a baseline of security and defence, to learn how to protect our IT assets. The article describes the taxonomy of the attack perpetuated by hackers and crackers; understand how to act and show how the methodology generally according to research carried out.**

Key words -. Hackers, crackers, threat, attack, vulnerability, risk, incident, impact, confidentiality, availability, integrity, footprinting.

I. INTRODUCCION

LA seguridad informática en este tiempo ha tomado un lugar muy privilegiado en el área informática, ya que las personas ya están tomando conciencia de los posibles riesgos expuestos por estar conectado a la gran autopista llamada la red de redes es decir el Internet, la gran mayoría de las empresas están cambiando, la forma de realizar sus negocios, todo gracias al apoyo de la tecnología, el desarrollo del software y la interconexión hace imaginable el hasta donde se puede llegar gracias a los computadores, servidores, las telecomunicaciones, los servicios prestados, pero hey!!, algo pasa, como aseguro mis sistemas, mis redes, mi información confidencial?. Como se que toda la tecnología adquirida y adoptada es segura?. Como evito irme a la quiebra por la información sustraída ya sea por cualquier técnica hacker o medio humano como por ejemplo ingeniería social?, estas personas inescrupulosas o expertas contratadas por terceros para hacerme daño, o divulgar información confidencial robada, que viendo desde otro ángulo puede afectar un gobierno, una organización, una empresa, una familia, una persona, o que tal esta información sustraída ayude o sirva como una prueba fehaciente para incriminar a cualquier ente que este obrando fuera de la ley. La información es un activo muy valioso, y hay que protegerla, y que mejor manera entendiendo como se perpetúa un ataque, entender los pasos, las formas, aprender a estudiar a estas personas que con malas intenciones puede penetrar en nuestros sistemas abruptamente, sin nuestro consentimiento, sin nuestro permiso y afectarnos de una manera o otra. Para tener una buena defensa, dicen por allí: "conoce a tu enemigo o únetele". Teniendo esto claro estamos entendiendo el "modus operandi" de estas personas que sin importar la ideología, razón, motivos o circunstancias logre penetrar a nuestros sistemas y así evitarles el éxito, ya que estaríamos un paso adelante de ellos, claro está que la tecnología cambia a diario, entonces debemos siempre pensar en la protección proactiva, es decir estar anunciando lo nuevo, así evitaremos ser atacados.

II. QUE ES UN ATAQUE

Según la escuela de Hackers de Argentina es: "Método por el cual, valiéndose de una vulnerabilidad y sin tener el permiso correspondiente, o sin validarse o identificarse, se puede realizar una negación de servicio, ejecutar código arbitrario, obtener información confidencial, escalar privilegios, administrar el sistema, tomar el control del mismo, o simplemente detener o dañar el sistema informático" [1], es una de las mejores definiciones que encontré en la web gracias a Google.

A. *Tipos de ataques*

Los ataques se dividen en dos tipos: Ataque Activo que altera el sistema o red atacado y ataque pasivo que es simplemente obtener información del sistema o red; y puede provenir desde dos sitios: Interno es decir dentro la red, los empleados descontentos, terceros dentro de la organización y Externo o refiérase a ataques fuera del perímetro de la red o otras redes, Internet, proveedores y hackers maliciosos.

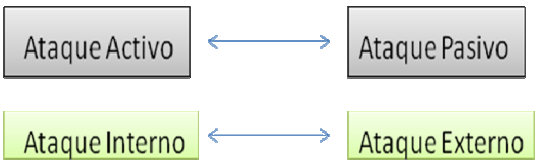


Figura 1. Tipos de Ataques

Ahora bien teniendo la definición y los tipos de ataque claros, se expone las ocho fases del ataque, la clasificación o taxonomía propuesta de acuerdo a la teoría del CEH [2] y los complementos agregados de acuerdo a mi criterio y experiencia de 5 anos en el medio de la seguridad Informática.

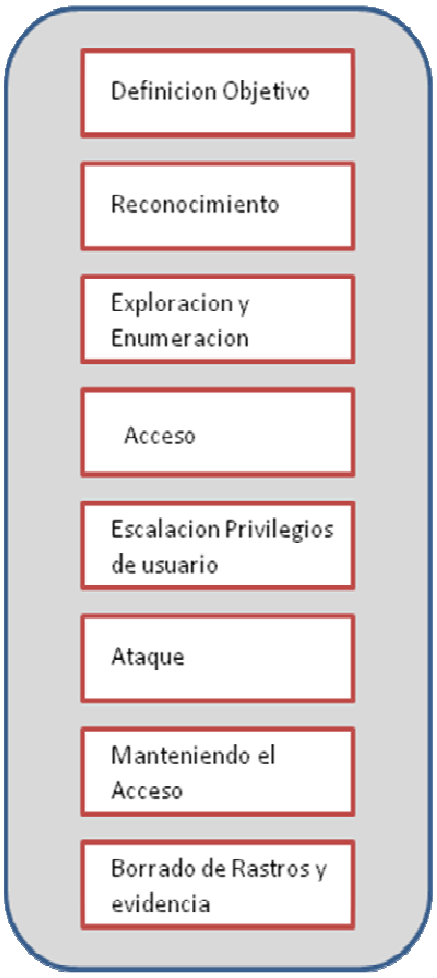


Figura 2. Ocho Fases de Ataque

B. *Fase 1: Definicion del Objetivo*

Esta es la primera fase del ataque o hacking, en el cual se define el objetivo a atacar, sea una red, un servidor remoto, una página web, una aplicación cliente/servidor, hardware, un proceso o procedimiento, una compañía, una organización, etc. En esta primera fase el hacker tiene el reto en su mente y visualiza su objetivo.

C. *Fase 2: Reconocimiento*

Esta fase se divide en dos: Reconocimiento Pasivo el cual se recolecta información del objetivo sin que este conozca o se de cuenta, por ejemplo mirar la entrada y salida de los empleados al edificio, también se realiza la búsqueda por google, para obtener la mayor recopilación de información posible. La ingeniería social y el sniffing también son métodos de reconocimiento pasivo. El Reconocimiento Activo es la exploración de la red, equipos y servicios, también indica al hacker las medidas de seguridad implementadas, pero el proceso aumenta la posibilidad de ser capturado o elevar la sospecha. Una técnica utilizada en esta fase es el Footprinting: que significa construir el mapa de red y sistemas del objetivo a atacar, por medio de los datos adquiridos del ambiente y arquitectura, también identifica vulnerabilidades, servicios, identifica medios por donde se podría ingresar para atacar el objetivo. Algunas técnicas para realizar footprinting es utilizar herramientas como el whois (ver figura 3), traceroute, e-mail tracking, nslookup, sam spade [3], web spiders a la IP o Dominio del objetivo.

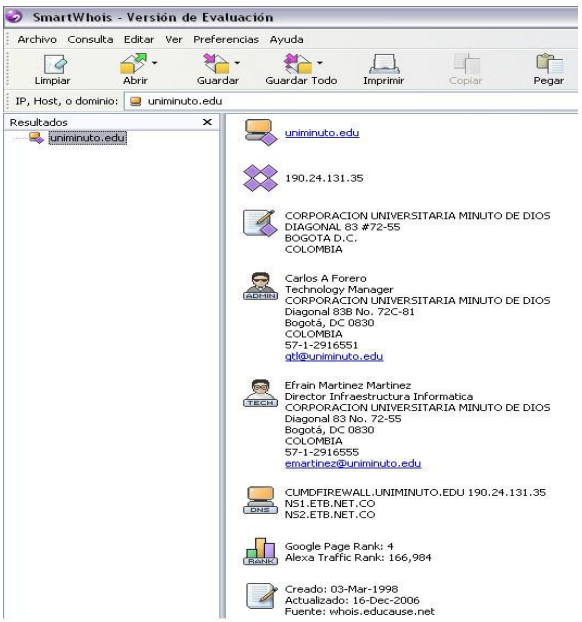
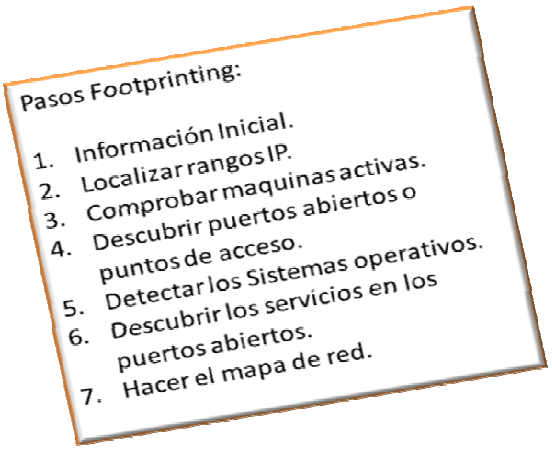


Figura 3. Footprinting con Smartwhois

Pasos para realizar el Footprinting son los siguientes:

TABLA I
Pasos para realizar con éxito Footprinting



De acuerdo a la tabla I nos muestra muy resumido los pasos para tener en cuenta y realizar un correcto footprinting, entre más lo realices, se va obteniendo la habilidad para leer solo la información más relevante y la que se necesita para el ataque.

D. Exploración y Enumeración

Los tipos de exploración o Scanning se dividen como lo muestra la siguiente tabla:

TABLA 2
TIPOS DE SCANNING

Tipo de Scanning	Proposito
Scan de Puertos	TCP/UDP y Servicios
Scan de Red	Rangos IP
Scan de Vulnerabilidades	Aplicaciones y sistema operativo

Las técnicas de scanning de red referidas más utilizadas son las siguientes: Ping sweep, SYN, Stealh, Xmas, NULL, Idle, FIN, war dialing, Banner grabbing, finger printing, anonymizer, HTTP tunneling e IP spoofing, con las herramientas NMAP, IPeye y SocksChain se realizar estas técnicas.

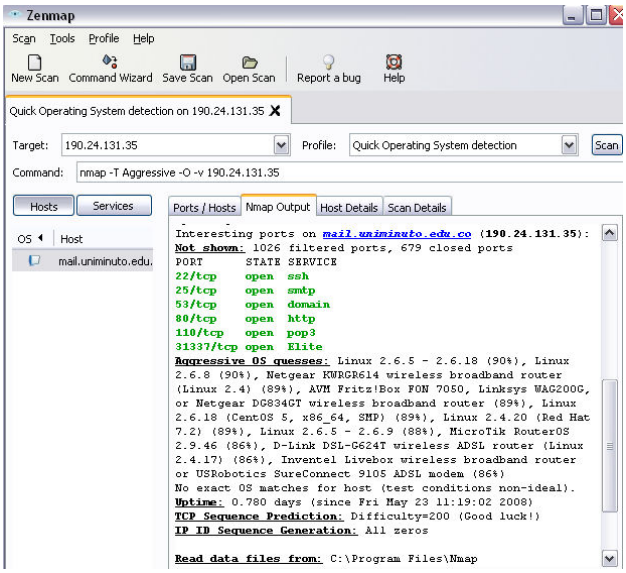


Figura 4. Scanning con Zenmap, versión grafica de nmap

Que es la Enumeracion? El objetivo es identificar las cuentas de usuarios administrativos y normales del sistema para luego obtener escalada de privilegios en caso de tomar un usuario normal, existe una herramienta muy útil llamada DumpSec, que permite la enumeración de usuarios, grupos, permisos, también la herramienta Hyena logra esta enumeración muy rápido en un entorno de dominio o grupo de trabajo.

E. *Acceso*

Esta se inicia con las técnicas de crackeo de passwords o contraseñas, las cuales se pueden realizar online, es decir realizando los test en vivo con una herramienta especial llamada Hydra el cual usa la técnica de diccionario, también hay la posibilidad de realizar el ataque offline, obteniendo los archivos donde se almacenan las contraseñas encriptadas y correrle técnicas de diccionario, fuerza bruta o criptoanálisis, para ello hay una herramienta muy eficaz llamada Cain y Abel (figura 5) en su última versión, lo cual con una copia del archivo de la SAM de Windows, puede descifrar las contraseñas, lo malo es que el tiempo que tarda es proporcional a complejidad de la contraseña.

Figura 5. Ataque online contraseña diccionario con hydra

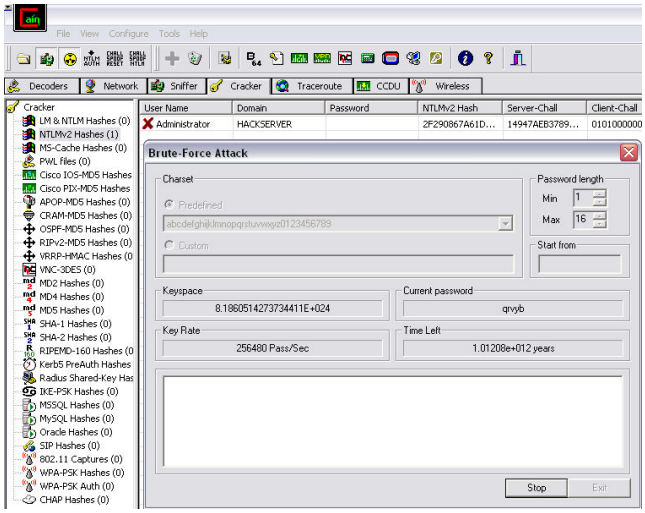


Figura 6. Ataque offline contraseña fuerza bruta con Cain.

Se debe estudiar bastante criptografía y por lo menos conocer de los algoritmos más usados: MD5, SHA, RC4, RC5, Blowfish, etc.

Es esta fase de acceso es complicada, ya que se tiene que evadir los Firewalls, realizar evasión de IDS/IPS y los Honeypots para realizar la penetración, se usan unas herramientas tales como 007 Shell, ICMP Shell, AckCmd, y framework (figura 7), para tener éxito.

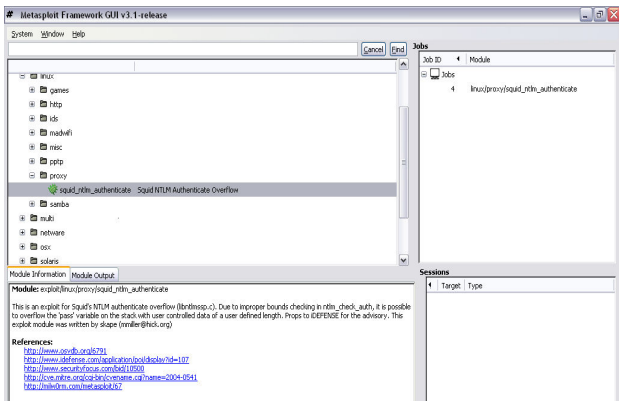


Figura 7. Ataque con metasploit Framework en Windows.

F. *Escalacion de Privilegios*

En esta etapa ya se tiene un usuario valido en el sistema, el cual puede tener permisos mínimos por esta razón se debe realizar una escalación de privilegios que simplemente es añadir mas permisos o derechos a la cuenta de usuario que se tiene, la idea es volverlo administrador del sistema para instalar y ejecutar aplicaciones, para realizar esto existe un troyano llamado GetAdmin.exe [4], lo cual realiza esto en los sistemas Windows NT, pero es detectable por la mayoría de Antivirus.

Ejecutando aplicaciones: Ya con los derechos de administrador se tiene control del sistema atacado, entonces se instala un back door, para mantener el acceso y un keystroke logger [6] para obtener información confidencial; copiar y ejecutar archivos con una herramienta llamada PsExec [5] y causar daño en el sistema, una vez esto cumplido el sistema ya no es nuestro es del hacker.

Buffer Overflows: Son intentos de hacking que explotan una falla en el código de una aplicación, se hace mediante consola o Shell.

Spyware: Son programas espías que recopilan información del usuario sin su conocimiento y envían la información a un servidor remoto para analizar su comportamiento, tendencia y características en la navegación de Internet, a nivel de hacking nos sirve para conocer a la víctima y engañarla más fácilmente haciéndola creer cosas que él necesita así instalar más fácilmente las aplicaciones que se necesitan para el ataque.

Rootkits: Es un programa utilizado para ocultar los servicios publicados en un sistema comprometido, los cuales pueden incluir llamadas a puertas traseras, esconder aplicaciones que abren puertos específicos para el hacker para garantizar el control absoluto del sistema.

Figura 8. Tipos de Rootkits.

G. *Ataques*

Esta es la parte más emocionante de un hacker, realizar el ataque del sistema, ya que su ego y su capacidad de lograrlo es lo que lo motiva mas para realizar ataques más sofisticados, He aquí la fórmula secreta de un ataque [7]:

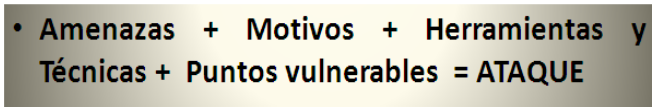


Figura 9. Formula de un Ataque

A nivel de ataques la Denegación de Servicio (DoS), hacen a un sistema inservible o retardan significativamente por sobrecarga de recurso, esto impide que los usuarios legítimos puedan acceder al sistema. Existen dos categorías de ataques DoS, que puede ser enviado por un sistema único (simple DoS) o enviarse por muchos sistemas a un solo objetivo (DDoS) distribuido.

Los ataques DDos pueden ser perpetrados por Bots y Botnets, que traducen equipo zombi y red de equipos zombis,

que son programas robots muy inteligentes, que son esclavos de un Master o servidor central, que les ordena en que momento realizar el ataque a la víctima, o enviar correos masivos o realizar un ataque distribuido.

Otro ataque es el Smurf, que envía una gran cantidad de ICMP (ping) trafico a broadcast con la IP origen falsificada de la víctima, lo cual la maquina trata de responder y se inundaría de tráfico y dejaría a la maquina con un DoS de ping.

El ataque SYN Flooding, es un ataque de inundación de peticiones SYN es decir peticiones de conexión TCP, El atacante crea una dirección de origen aleatoria falsa para cada paquete y fija la bandera SYN, la victima responde a la dirección IP falsa y luego de esperar el TCP de confirmación que nunca llega, en consecuencia se queda esperando las respuestas de todas las conexiones, produciendo un DoS de red y los usuarios legítimos se quedan sin el servicio.

Session Hijacking o secuestro de sesión es otro ataque común el cual un hacker toma el control de una sesión de usuario después de que el usuario ha tenido éxito contra la autentificación con un servidor. Esto implica la identificación de un ataque de IDS de sesión, comunicación entre cliente y servidor, periodo de sesiones y calculo de numero de secuencia utilizando unas herramientas de cálculo para ello.

El ataque Spoofing o el uso de técnicas de suplantación de identidad como IPs, ARPs, DNS, WEB, correo electrónico, también son muy usados para engañar un sistema lograr validación.

Ataques a Nivel de Aplicaciones, lo más común es encontrar las vulnerabilidades a nivel de sistema operativo, como las configuraciones por defecto, el código de programación, instalación por defecto, falta de actualización de parches de seguridad y falta de políticas de seguridad adecuadas.

Los ataques contra los web server, llamados defacement o reemplazos, lo realizan al explotar las vulnerabilidades del sistema operativo o del programa webserver que se este usando, como por ejemplo IIS, Apache, TomCat, etc. A continuación los ataques usados para alterar un sitio web:

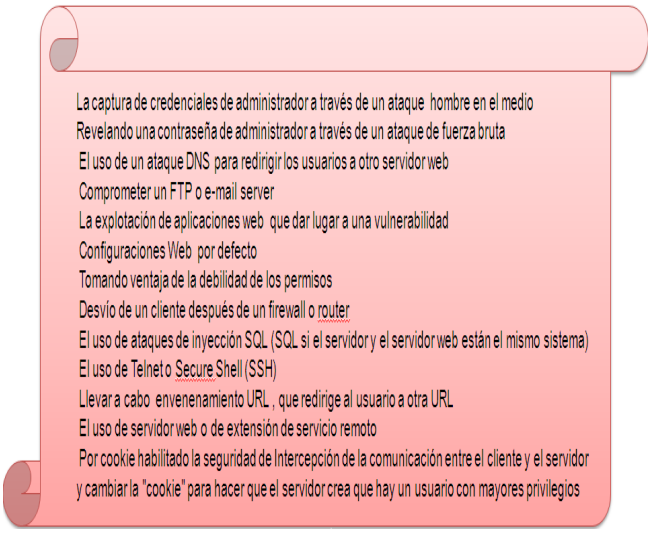


Figura 10. Técnicas de Ataques a sitios Web.

Anatomía de un Ataque de aplicaciones Web: es similar a otros sistemas, primero se debe realizar un escaneo, obtener información de la aplicación web, realizar una prueba, planificar el ataque y realizar el ataque. Las principales amenazas de las aplicaciones web son el Cross-site scripting, SQL injection, Command injection, envenenamiento de cookies, Buffer overflow, autenticación hijacking y directorio de recorrido/Unicode.

El ataque Google Hacking [8] se refiere al uso del fuerte buscador o motor para localizar o buscar información valiosa, como contraseñas o datos directamente de base de datos.

Wifi hacking: para realizar esto se debe conocer a profundidad todos los mecanismos de autenticación (WEP,WPA), los hackers escanean el SSIDs, para obtener el trafico la información de autenticación, esto se hace con una herramienta llamada Aircrack [9], realizan un ataque de fuerza bruta para obtener el password de conexión, también aplica ataques de MAC spoofing o falsificación de MAC , otro ataque bien conocido es colocar un AP o Access Point falso, para que los usuarios se conecten allí y poderlos atacar más fácilmente, aplica también el DoS.

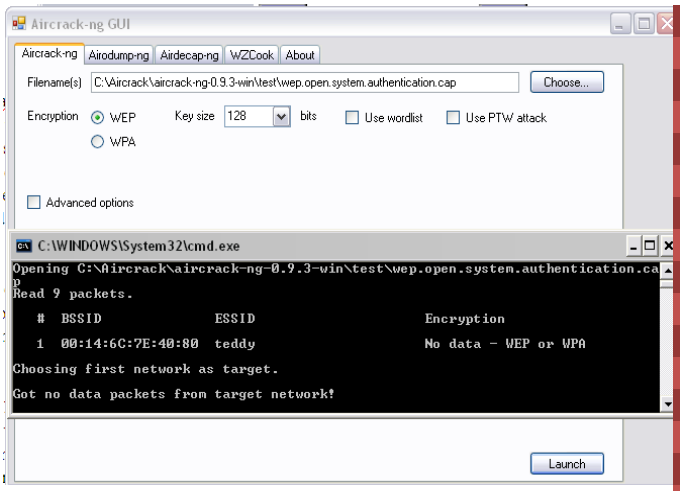


Figura 11. Hacking Wifi con Aircrack

Los ataques más usados por los hackers maliciosos con sus respectivas herramientas son los siguientes:

TABLA II
Ataques y herramientas

ATAQUES	HERRAMIENTAS
Footprinting	Google hacking
	Sam Spade
	Smart whois
	eMailTracking Pro
Ingenieria Social	Shoulder surfing
	Dumpster diving
Scanning	Pinger
	Friendly Pinger
	Ipeye
	IPSecscan
	Solarwinds
	Netcraft
	Sockschain
Enumeration	Dumpsec
	Hyena
	smb auditing tool
	netbios aditing tool
Enumeration Users	User2SID
	GetAcct
	SMBBF
Cracker de contrasenas	Legion
	LOphtCrack
	John the Ripper
	KerbCrack
	Offline NT Password Resetter
Ataque Netbios	SMBRelay
	pwddump
	Samdump
	C2myazz
	SMBGrind
Elevacion de privilegios	Getadmin.exe
	Hk.exe
Ejecutar aplicaciones remotas	Psexec
	Remoxec
Esteganografia	ImageHide
	Blindside
	MP3Stego
	Stealth
Borrar pistas	Audipol
	elsave.exe
	Winzapper
	Evidence Eliminator
Troyanos famosos	Tini
	Netbus
	Backorifice 2000
	Computer spy key logger
	CyberSpy
Sniffers	Ethereal
	Snort
	windump
	Iris
Tool hacking	Cain & Abel
	The Metasploit framework
Denegacion de Servicio DoS	Ssping
	CPU hog
	Winnuke
	Targa
	Bubonic
Hijahacking	Juggernaut
	Hunt
	TTYWatcher
	IP Watcher
	T-Sight
Scanner Webs	N-Stalker web application
	Core Impact
	SAINT Vulnerability Scanner

H. *Manteniendo el Acceso*

Ya teniendo control del sistema atacado por el hacker proceden a instalar troyanos para permitir el acceso por puertas traseras, contagiar el sistema con código malicioso o virus, y esto se hace con los Wrapping, que son programas para construir un troyano y con la envoltura de un archivo legitimo, es decir lo esconden tras una instalador de una aplicación dada, por ejemplo un juego animado llamado Graffiti, Silk Rope 2000, EliteWraps y IconPlus, etc. Tambien con virus y gusanos de red pueden crear entradas fijas al sistema (abriendo puertos) y tener monitoreo del sistema comprometido.

I. *Borrando rastros*

Como todo un buen hacker después de realizar el ataque, debe borrar los rastros del crimen realizado, para evitar ser culpado y que nadie descifre las técnicas utilizadas para perpetuar el ataque al sistema, por tal motivo los pasos que realizan son los siguientes:

A. Deshabilitar la Auditoria del sistema en caso que este activa.
B. Realizar el borrado de todos los logs posibles en el sistema y aplicaciones comprometidas.
C. Borrar la evidencia o pistas de las herramientas utilizadas, o posibles programas instalados, según el ataque realizado para que no puedan rastrearlo ni dejar ninguna pista, se puede usar la esteganografia [10] para ocultar los archivos usados.

III. CONCLUSIONES

El anterior artículo genera las siguientes conclusiones:

A. Ningún sistema es 100% seguro, siempre habrá alguna técnica, proceso o procedimiento para violar la seguridad y obtener un acceso no autorizado, por tal motivo la conciencia es la de minimizar las amenazas, los riesgos y tener una clara gestión de seguridad en todos los sistemas a proteger.

B. Las técnicas hackers cada día son más sofisticadas y cambian de acuerdo a la tecnología del momento, por eso siempre se debe estar un paso adelante.

C. Estas son las técnicas generales más usadas para apropiarse de un sistema, se realizo un análisis de las técnicas y herramientas usadas y conocidas según la documentación del CEH [11], que es la certificación oficial de Etical Hacker.

D. Tanto desde Windows como Linux se puede realizar los ataques, existen herramientas equivalentes para cada sistema operativo, entonces no importa el sistema operativo del hacker, lo que realmente importa es la habilidad lógica y mental para descubrir las vulnerabilidades y explotarlas.

E. La anterior taxonomía nos abre el mundo de posibilidades y nos permite estudiar y analizar cuál sería la mejor defensa para evitar los ataques y desarrollar una línea base de seguridad para minimizar el riesgo.

IV. AGRADECIMIENTOS

A todos los docentes del Diplomado de Seguridad Informática dictado en la corporación universitaria Minuto de Dios y a esas personas que me han ayudado con su gran experiencia y apoyo en el campo de seguridad informática.

V. REFERENCIAS

Estas son las referencias de consulta, para profundizar más en los temas mencionados en este articulo.

[1] http://www.escuelahacker.com.ar/biblioteca/glosario.php
[2] PDF. Official Certified Ethical Hacker. Kimberly Graves. 2007.
[3] http://samspade.org
[4] http://toolshacker.blogspot.com/2006/12/tools-dari-yogya-free.html.
[5] http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx
[6] http://www.kmint21.com/download.html.
[7] http://www.geocities.com/Baja/1762/winnt.html
[8] http://johnny.ihackstuff.com/ghdb.php
[9] http://www.aircrack-ng.org/doku.php
[10] http://es.wikipedia.org/wiki/Esteganograf%C3%ADa
[11] http://www.eccouncil.org/CEH.htm

VI. BIOGRAFIA AUTOR

Henry Alexander Diaz Mongua

Consultor independiente especializado en seguridad informática, amplia experiencia en productos y servicios informáticos, tecnólogo en Informática y diplomado en seguridad informática de la Corporación Universitaria Minuto de Dios, actualmente desempeña el cargo de oficial de seguridad de la Información en un Datacenter, CEO hackerscolombianos.org. Logro el 6 puesto a nivel nacional en el ECADES (ICFES), examen de conocimientos en tecnología informática del año 2005; amplio conocimiento de redes, plataforma Linux y Windows, infraestructura, ético hacking, ISO 17779, análisis de riesgos y gestión de vulnerabilidades, ha diseñado, implementado y soportado gran cantidad de proyectos de seguridad informática con varios fabricantes y en grandes empresas públicas y privadas Colombianas.
(pilo.dx@hackerscolombianos.com).