NPROS
NETWORK PROFESSIONAL
SECURITY PERU S.A.C.

Hacking Ético

Fundamentos

Alonso Eduardo Caballero Quezada
Consultor de NPROS Perú S.A.C.
Sitio Web: http://www.npros.com.pe
Correo electrónico: cursos@npros.com.pe
Correo personal: reydes@gmail.com

Sobre NPROS Perú SAC

Network Professional Security Perú - NPROS Perú S.A.C se creó en Enero del año 2008 para ofrecer servicios de capacitación especializada en Perú y orientarse en el dictado de cursos de Seguridad en Tecnologías de la Información.

Tenemos cuatro años de experiencia en el dictado de cursos a diferentes instituciones y empresas tanto públicas como privadas, como por ejemplo: Universidades, Sector Financiero: Bancos, Cajas; Sector Gobierno y Municipios, entre otras instituciones del sector privado y público.

Servicios NPROS Perú

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Cursos:

Modalidades: Presencial (Lima, Trujillo) & Online (Virtual).
Duración: 20 Horas

- Curso de Hacking Ético **(CNHE)**.
- Curso de Cómputo Forense **(CNCF)**.
- Curso de Hacking Aplicaciones Web **(CNHAW)**.
- Otros cursos: Hacking Windows, Hacking GNU/Linux, Antiforense.

Webminars Gratuitos:

Duración 1 Hora.

Otros Servicios:

- Análisis de Vulnerabilidades.
- Pruebas de Penetración.
- Análisis Forense de Computadoras.

Contacto NPROS Perú

Correo electrónico: cursos@npros.com.pe

Teléfono: 948351218
RPM: #948891476
RPC: 980715946

Página Web:
http://www.npros.com.pe

Twitter:

http://twitter.com/#!/NPROSPeru

FaceBook:

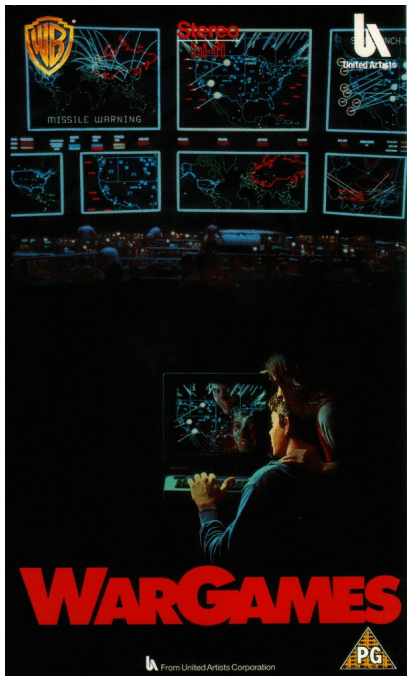
http://www.facebook.com/pages/NPROS-Per%C3%BA/215242575183641

LinkedIn:
http://pe.linkedin.com/pub/npros-per%C3%BA-sac/37/235/3a5

Agenda

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

- Terminología del Hacking Ético
- Diferentes tipos en Tecnologías de Hacking
- Fases involucradas en el Hacking Ético
- ¿Qué es el Hacktivismo?
- Diferentes tipos de Hackers
- Conocimientos para ser un Hacker Ético
- ¿Qué es la investigación de vulnerabilidades?
- Procedimiento para realizar un Hacking Ético



Definición de un Hacker Ético

Es una persona que se encarga de realizar Pruebas de Penetración.

Es contratado por una organización para intentar penetrar en los sistemas o redes de computadoras, utilizando los mismos métodos de un Hacker “Malicioso”, con el propósito de encontrar y solucionar vulnerabilidades en seguridad en las computadoras.

Las Pruebas de Penetración son realizadas por solicitud del propietario de los sistemas o redes objetivos, y son totalmente legales.


Terminología del Hacking Ético

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

1. Amenaza: Es un entorno o situación que deriva en una potencial brecha de seguridad.

2. Exploit: Pieza de software que se aprovecha de una falla, error o vulnerabilidad, permitiendo el acceso no autorizado, realizar una escalado de privilegios o un Negación de Servicio (DoS) en un sistema de cómputo.

2.1 Exploit remoto: Funciona sobre la red y explota vulnerabilidades de seguridad sin tener un acceso previo en el sistema vulnerable.

2.2 Exploit local: Requiere de un acceso previo en el sistema vulnerable para poder proceder con la elevación de los privilegios.

Un Exploit es una forma definida de violar la seguridad de un Sistema de Tecnologías de Información mediante una vulnerabilidad.

Terminología del Hacking Ético (Cont.)

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

3. Vulnerabilidad: Es la existencia de una imperfección en el software, diseño lógico o error de implementación que deriva en un evento inesperado, con la ejecución de instrucciones dañinas o indeseadas en el sistema.

4. Objetivo de Evaluación (ToE): Es un sistema, programa, o red de computadoras que está sujeto a un análisis de seguridad o un ataque.

Un ataque ocurre cuando se compromete un sistema en base a un vulnerabilidad. La mayoría de ataques utilizan un exploit.

Los Hackers Éticos utilizan herramientas para encontrar sistemas que puedan ser vulnerables a un exploit para un sistema operativo, configuración de red, o aplicaciones instaladas en el sistema, y prevenir que el ataque sea realizado por otras entidades “maliciosas”.

Diferentes Tipos en Tecnologías de Hacking

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Existen muchos métodos y herramientas para encontrar vulnerabilidades, ejecutar exploits, y comprometer sistemas. Algunos de estos son los troyanos, puertas traseras (backdoors), rootkits, husmeadores (sniffers), exploits, desbordamientos de buffer, inyección SQL (SQL Injection), etc

Todas estas herramientas explotan debilidades en alguna de las siguientes áreas:

1. Sistema Operativo: Las configuraciones por defecto en los Sistemas Operativos traen como consecuencia potenciales vulnerabilidades.

2. Aplicaciones: Generalmente no se detectan vulnerabilidades en el código de las aplicación, lo cual genera y deja muchas imperfecciones.

3. Código “retráctil”: Muchos programas vienen con “añadidos” que no son evidentes para el usuario y que pueden utilizarse para explotar el sistema.

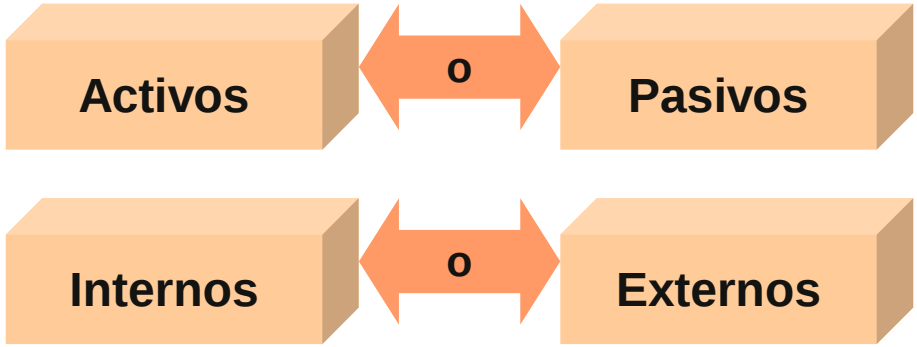
4. Desconfiguraciones: Una situación donde se define una configuración con una seguridad baja.

Diferentes Tipos en Tecnologías de Hacking (Cont.)

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Además de los tipos de tecnologías, existen diferentes tipos de ataques. Estos pueden ser Activos o Pasivos. Ambos ataques son utilizados contra la infraestructura de seguridad de red y servidores.

Los Activos alteran los sistemas o redes, los Pasivos obtienen información del sistema. Los ataques Activos afectan la Disponibilidad, Integridad y Autenticidad de los datos; los ataques Pasivos violan la Confidencialidad.

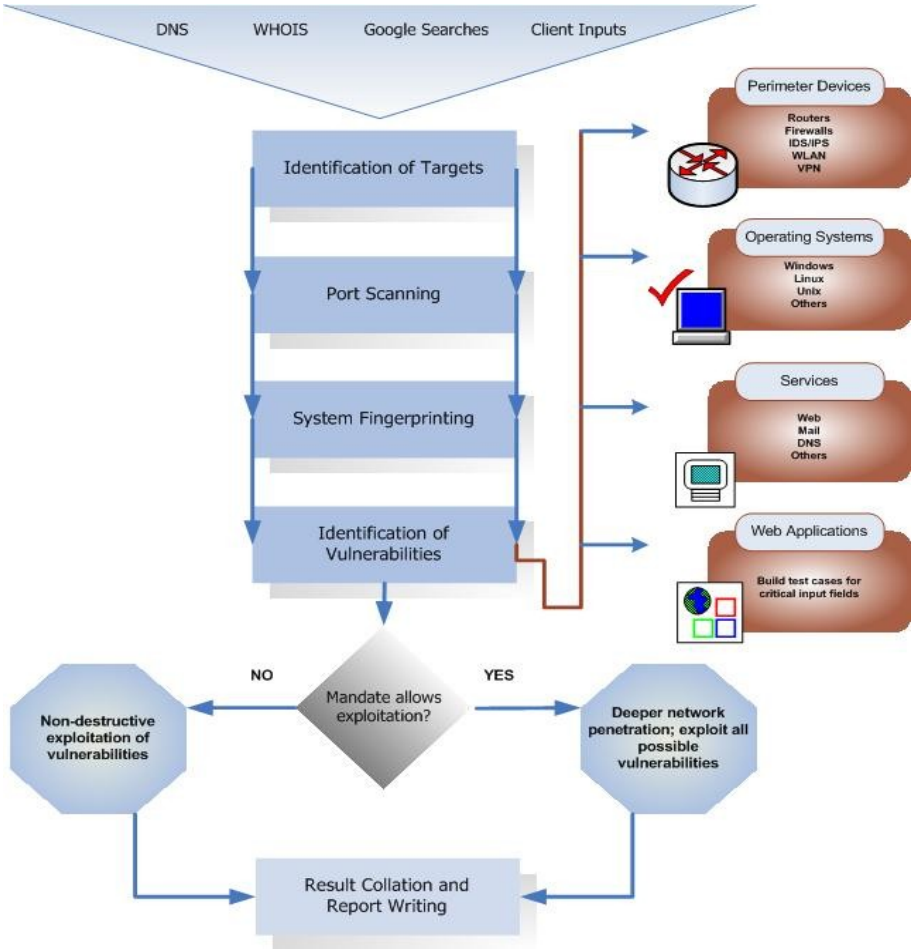


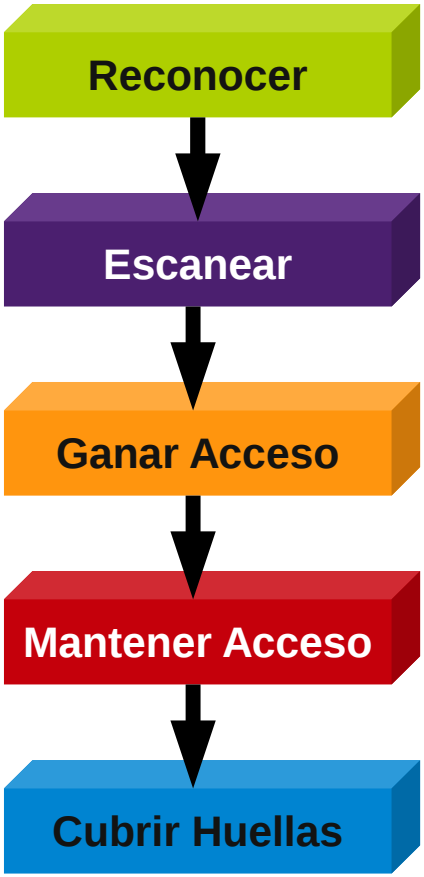
Los ataques se categorizan en Internos y Externos. Un Interno se origina dentro del perímetro de seguridad y es causado por un “insider”. Un Externo se origina fuera del perímetro de seguridad, como internet o una conexión de acceso remoto.

Fases involucradas en el Hacking Ético

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Un Hacker Ético sigue una metodología similar a la utilizada por un Hacker "Malicioso". Los fases o etapas del Hacking Ético son iguales, aquí no interesan las intenciones del Hacker.





Fases involucradas en el Hacking Ético (Cont.)

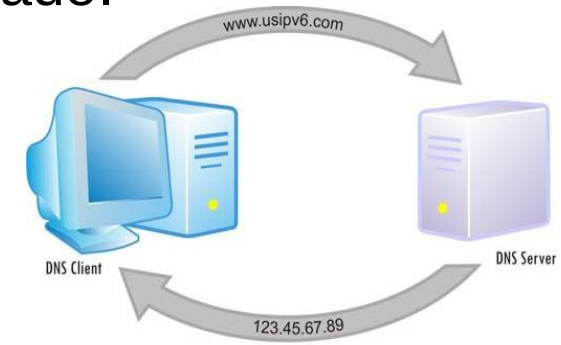
NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Reconocimiento

1. Reconocimiento Pasivo: Captura información relacionada al objetivo sin conocimiento del individuo o empresa objetivo. Este proceso se denomina captura de información. Algunos métodos utilizados son; la búsqueda de basura e ingeniería social. El Sniffing (Humeo) en la red es también un mecanismo utilizado en este tipo de reconocimiento.

2. Reconocimiento Activo: Realiza la evaluación de la red para descubrir hosts únicos, direcciones IP, y servicios en la red. Este proceso Implica un mayor riesgo de detección que el reconocimiento pasivo. Proporciona indicios de los mecanismos de seguridad, pero este proceso también incrementa las posibilidades de ser detectado.

Ambos tipos de reconocimiento permiten descubrir información útil a ser utilizado en el ataque.



Fases involucradas en el Hacking Ético (Cont.)

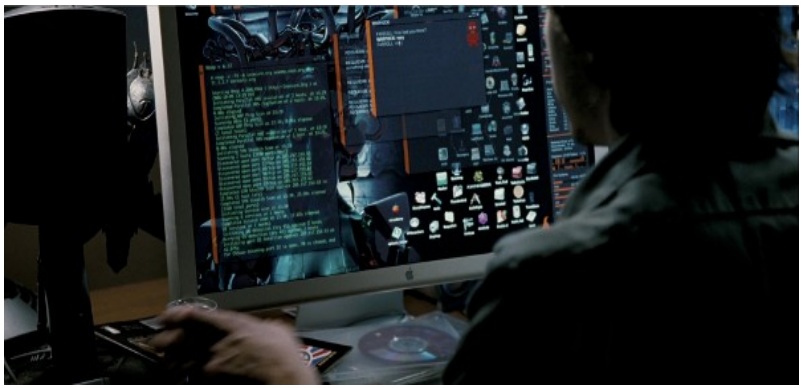
NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Escaneo

Esta fase involucra tomar la información descubierta durante la fase de Reconocimiento y utilizarla para proceder a examinar la red. Entre las herramientas que el Hacker Ético utiliza durante la fase de Escaneo se incluyen:

1. Dialers (Marcadores)
2. Port Scanners (Escaners de Puertos)
3. Network Mappers (Mapeadores de red)
4. Sweepers (Barredores)
5. Vulnerability Scanners (Escaners de Vulnerabilidades)

Los Hackers buscan cualquier información que ayude a realizar el ataque; como por ejemplo el nombre de las computadoras, las direcciones IP, cuentas de usuario, etc.



Fases involucradas en el Hacking Ético (Cont.)

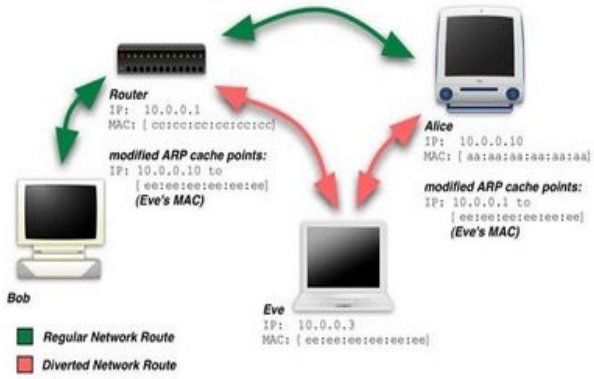
NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

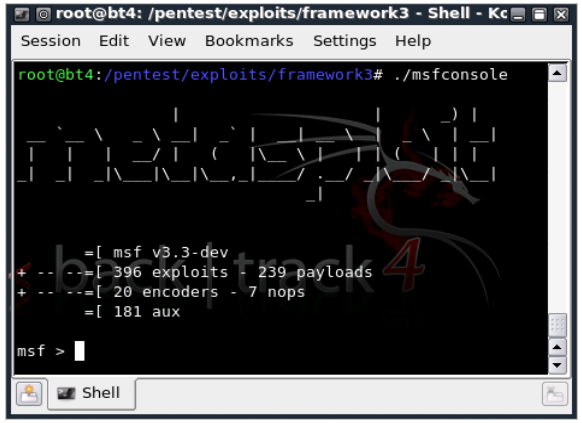
Ganar Acceso

Aquí es donde se manifiesta el Hacking “Real”. Todas las vulnerabilidades que han sido descubiertas durante la fase de Reconocimiento y la fase de Escaneo ahora se explotan para ganar y obtener acceso.

El método de conexión que el Hacker utiliza para realizar la explotación puede ser sobre una Red de Área Local (LAN, ya sea cableada o inalámbrica), tener acceso local al objetivo, internet, o fuera de línea (off-line).

Algunas de las técnicas utilizadas incluyen, desbordamiento de buffer basados en pila, secuestro e interceptación de sesiones, etc.





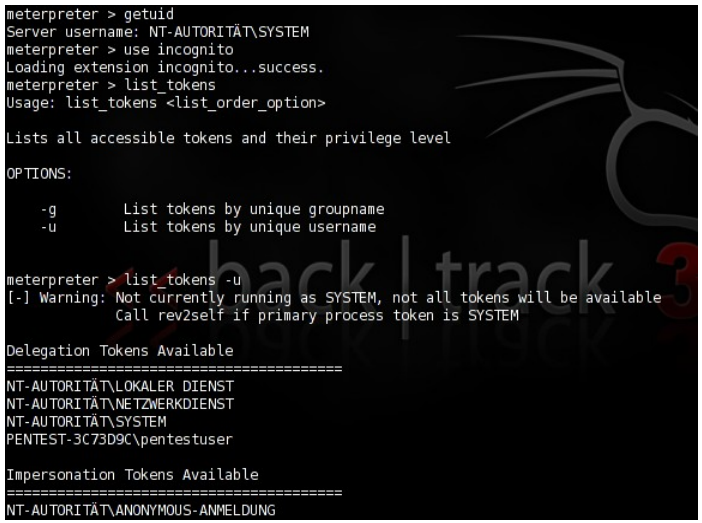
Fases involucradas en el Hacking Ético (Cont.)

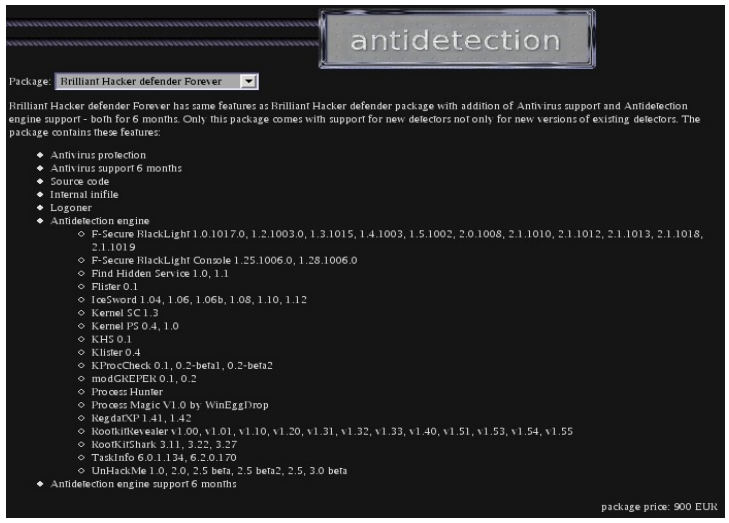
NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Mantener Acceso

Cuando se gana el acceso, se desea mantener el acceso para realizar otros ataques y futuras explotaciones. El Hacker procede a “fortalecer” el sistema de otros Hackers o del personal de seguridad, asegurando su acceso exclusivo mediante puertas traseras (backdoors), rootkits, troyanos u otros mecanismos adecuados.

Si el Hacker se apropia del sistema, puede utilizarlo como estación base para lanzar otros tipos de ataques a su entorno. A un sistema en esta situación se le denomina un sistema zombi.





Fases involucradas en el Hacking Ético (Cont.)

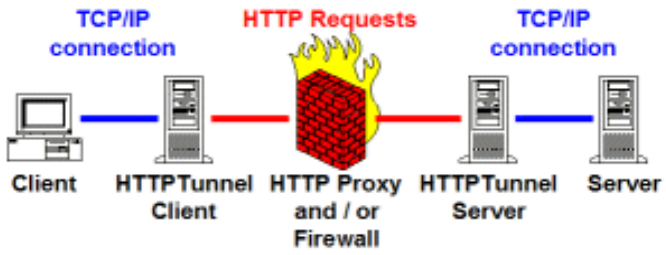
NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

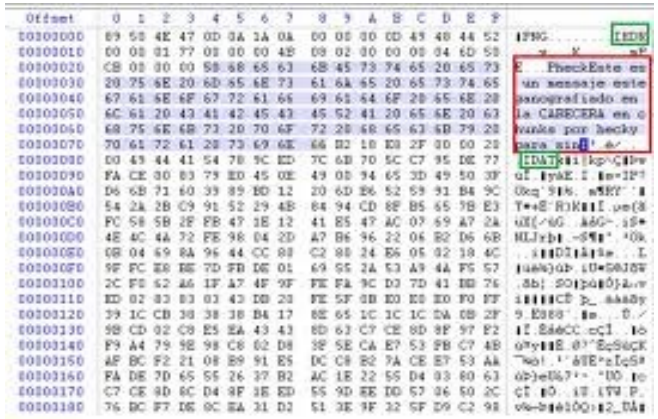
Cubrir Huellas

Cuando el Hacker ha ganado y mantiene acceso a las redes de computadoras y sistemas, desea cubrir sus huellas para evitar ser detectado por el personal de seguridad, seguir utilizando el sistema comprometido, remover evidencia del “ataque”, o evitar acciones legales.

En esta fase se intenta eliminar los rastros del ataque, tales como los dejados en los archivos de registro (logs), o alarmas de los IDS o IPS.

Algunas de las actividades realizadas incluyen el uso de esteganografía, utilizar protocolos mediante “túneles”, y alterar los archivos de registros.

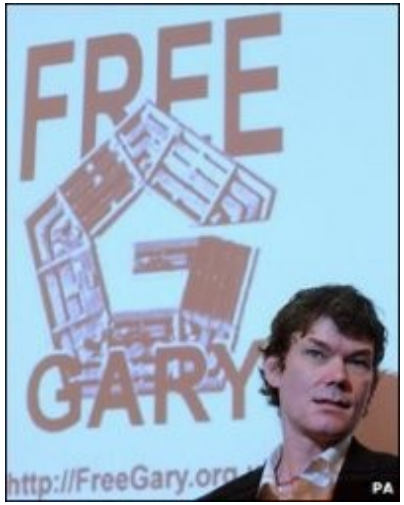




¿Qué es el Hacktivismo?

El Hacktivismo consiste en realizar una acción de “Hacking” por alguna causa. Aquí se tiene generalmente una agenda política o social. Sus intenciones son enviar un mensaje mediante una acción de “Hacking” mientras se gana visibilidad para diferentes causas y motivaciones.

Muchos de estos Hackers participan en actividades tales como, desfigurar sitios web, creación de malware, DoS, u otros ataques que generan mucha notoriedad mediática. Estos “ataques” tienen como objetivo agencias del gobierno, grupos políticos, y cualquier otra entidad que estos grupos o individuos perciban como “malos” o “equivocados”.



Diferentes Tipos de Hackers

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

1. Sombrero Blanco: Son los Hackers Éticos que utilizan sus conocimientos para propósitos defensivos. Son profesionales en seguridad que utilizan sus conocimientos para ubicar debilidades e implementar medidas correctivas que mejoren la postura de seguridad de as organizaciones.

2. Sombrero Negro: Son los Hackers “maliciosos” o Crackers quienes utilizan sus conocimientos para propósitos ilegales o dañinos. Estos rompen, irrumpen o violan la integridad de los sistemas remotos que atacan con intenciones totalmente dañinas e ilgales.

3. Sombrero Gris: Son los Hackers que trabajan de manera ofensiva o defensiva, dependiendo de la situación. Esta es la línea que divide a un Hacker y un Cracker. Muchos individuos caen en ambas categorías.

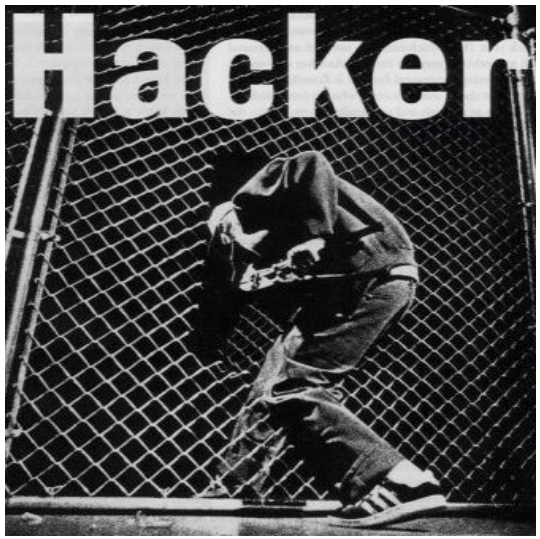


Diferentes Tipos de Hackers (Cont.)

Los “auto” proclamados Hackers Éticos desean resaltar los problemas de seguridad en un sistema o educar a las víctimas para que puedan asegurar sus sistemas. Supuestamente hacen un “favor” a sus víctimas.

Muchos considera un acto de “Hacking” por si mismo como NO ético. Pero el Hacking “Ético”, excluye la destrucción e implica un comportamiento moderado y legal.

La gran mayoría de empresas no ven con mucho agrado que alguien toque su puerta o se presente con datos confidenciales de su organización ofreciendo solucionar sus fallas de seguridad por un monto económico determinado. La respuesta puede ir desde un sencillo “Gracias, por esta información”, hasta llamar a la policía y arrestar al auto proclamado Hacker Ético.



Diferentes Tipos de Hackers (Cont.)

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

¿Quienes son los Crackers y Hackers Éticos?

Los Hackers son profesionales en seguridad o que realizan Pruebas de Penetración utilizando su experiencia y conocimientos en Hacking y herramientas con propósitos defensivos y de protección.

El término Cracker describe a un Hacker que utiliza sus conocimientos de Hacking y herramientas con propósitos ofensivos o destructivos tales como esparcir malware, o realizar un DoS, para comprometer o hacer caer un sistema.

Los Crackers pueden dañar la reputación de una organización, robar y revelar información de tarjetas de crédito, mientras aletargan los procesos de las empresa y comprometen la integridad de la organización.

Diferentes Tipos de Hackers (Cont.)

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

¿Qué hacen los Hackers Éticos?

Su propósito es el mismo que los Crackers o Hackers “Maliciosos”: Tratan de determinar lo que un atacante puede ver en la red o sistema objetivo, y lo que un Hacker haría con esta información. Este proceso de evaluar la seguridad de un sistema o red se conoce como Prueba de Penetración.

Los Hackers Éticos entran en los sistemas de computo. Esto no implica un conocimiento misterioso ni mágico, pero si la persistencia y la repetición de trucos conocidos, poco difundidos o complejos que explotan debilidades de seguridad en los sistemas que evalúan.

El Hacker Ético consulta a la organización Que es lo que desea proteger, de Quienes, y Cuales son los recursos que la empresa está dispuesta a adquirir para ganar protección.

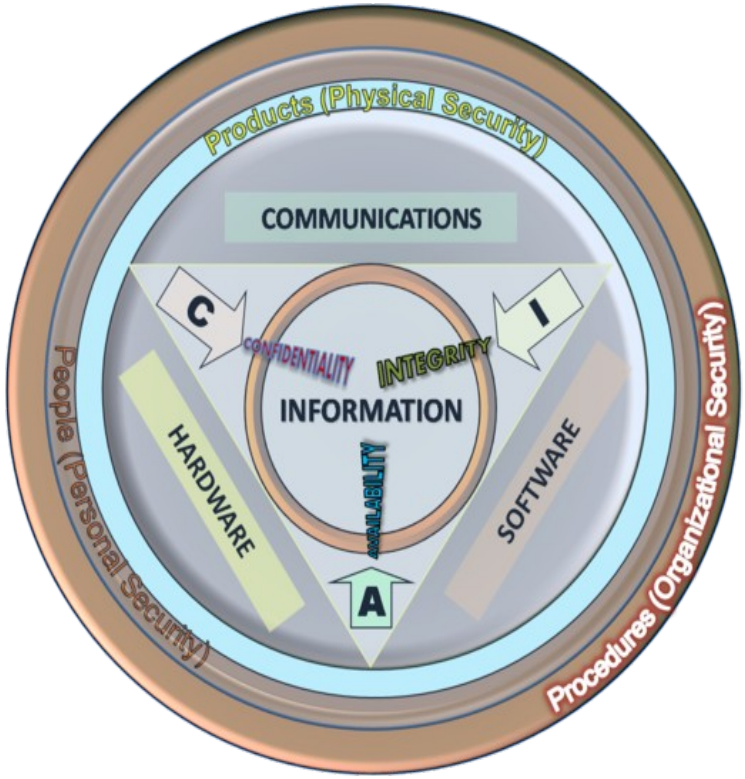
Diferentes Tipos de Hackers (Cont.)

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Objetivos de los Atacantes

La Seguridad consiste de cuatro elementos básicos:

1. Confidencialidad Robo de Información.
2. Autenticidad Spoofing.
3. Integridad Manipulación de Datos.
4. Disponibilidad Negación de Servicio (DoS).

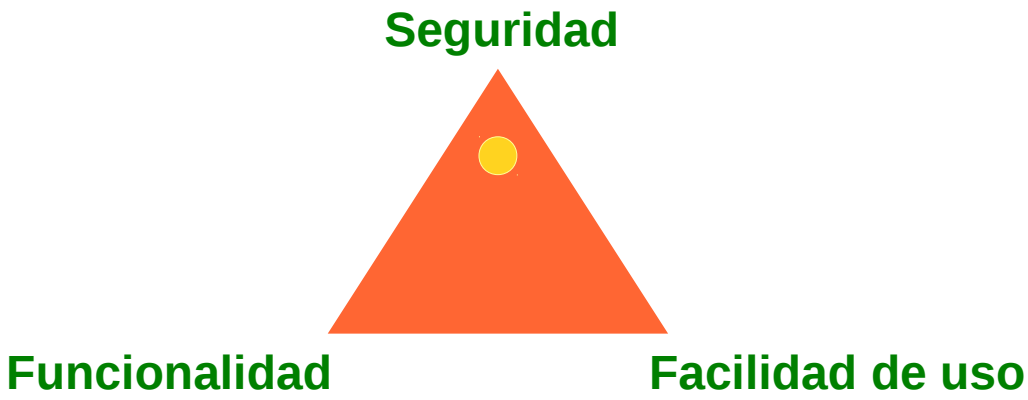


El objetivo del Hacker es explotar vulnerabilidades es un sistema o red para encontrar debilidades en uno o más de los cuatro elementos de la seguridad.

Diferentes Tipos de Hackers (Cont.)

Facilidad de uso, Funcionalidad y Seguridad

Este triángulo representa el balance entre la Seguridad, la Funcionalidad y Facilidad de uso para los usuarios. *Cuando la seguridad se incrementa, la facilidad de uso y funcionalidad del sistema disminuye.*



Los profesionales en seguridad desean tener el nivel más alto de seguridad en todos los sistemas; sin embargo esto no siempre es posible. Muchas barreras de seguridad dificultan al usuario utilizar el sistema e impiden la funcionalidad del sistema.

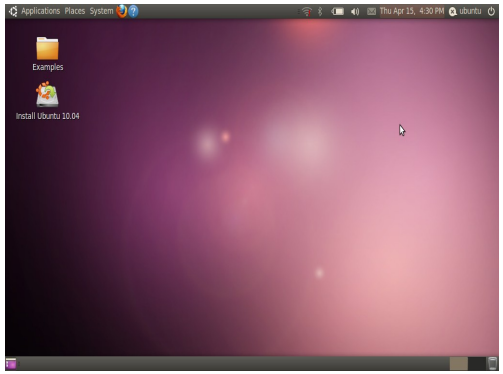
Conocimientos para ser un Hacker

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Los Hackers Éticos deben estar siempre un paso adelante de los Hackers maliciosos, deben tener elevada experiencia en computadoras, con conocimientos de programación, redes, sistemas operativos y las plataformas (Windows, GNU/Linux, Mac).

Los Hackers Éticos requieren, paciencia, persistencia, y una inmensa perseverancia, los cuales son importantes cualidades que muchos Hackers poseen debido al tiempo y el nivel de concentración requerida.

Algunos Hackers Éticos tienen conocimientos de las áreas de seguridad y temas relacionados, pero no tienen necesariamente un solido conocimiento de las medidas correctivas para prevenir ciertos tipos de ataques.



¿Qué es la Investigación de Vulnerabilidades?

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Es el proceso de descubrir vulnerabilidades en el diseño que deriven en un ataque a un sistema. Existen en internet muchas páginas web y herramientas que ayudan a mantener una lista actualizada de vulnerabilidades y posibles exploits para las redes o sistemas.

Es fundamental que el administrador de los sistemas se mantenga actualizado de los últimos virus, troyanos, rootkits, backdoors, exploits, y otros tipos de amenazas para proteger adecuadamente sus redes y sistemas.

También debe estar familiarizado con las nuevas amenazas. Un administrador debe poder detectar, prevenir y recuperarse de un ataque.

Procedimiento para realizar un Hacking Ético

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Un Hacking Ético se realiza de una manera organizada y estructurada, como parte de una Prueba de Penetración o Auditoría de Seguridad. La intensidad y alcance de los sistemas y aplicaciones a ser evaluados son determinadas por las necesidades del cliente.

1. Hablar con el cliente, discutir las necesidades de las pruebas.

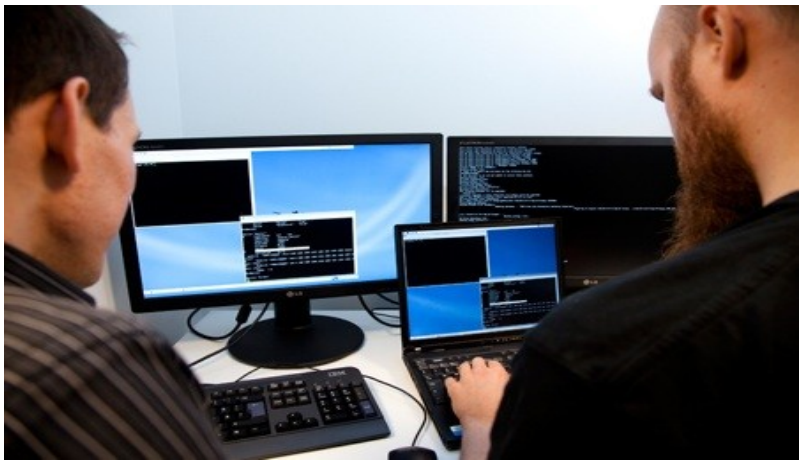
2. Preparar y firmar un documento de acuerdo de NO divulgación (Acuerdo de Confidencialidad) con el cliente.

3. Organizar al equipo de Hackers Éticos, y preparar los horarios de las pruebas.

4. Realizar las pruebas.

5. Analizar los resultados de las pruebas, y preparar un reporte.

6. Presentar el reporte al cliente.



Procedimiento para realizar un Hacking Ético (Cont.)

Creando un Plan de Evaluación de Seguridad

Muchos Hackers Éticos actúan en un rol de profesionales de seguridad, utilizando sus conocimientos para realizar evaluaciones de seguridad o Pruebas de Penetración. Estas Pruebas involucran tres fases debidamente ordenadas como siguen:

La fase de preparación involucra un acuerdo formal entre las partes.

Este acuerdo debe incluir el alcance de las pruebas, los tipos de ataques, y tipos de pruebas.

Procedimiento para realizar un Hacking Ético (Cont.)

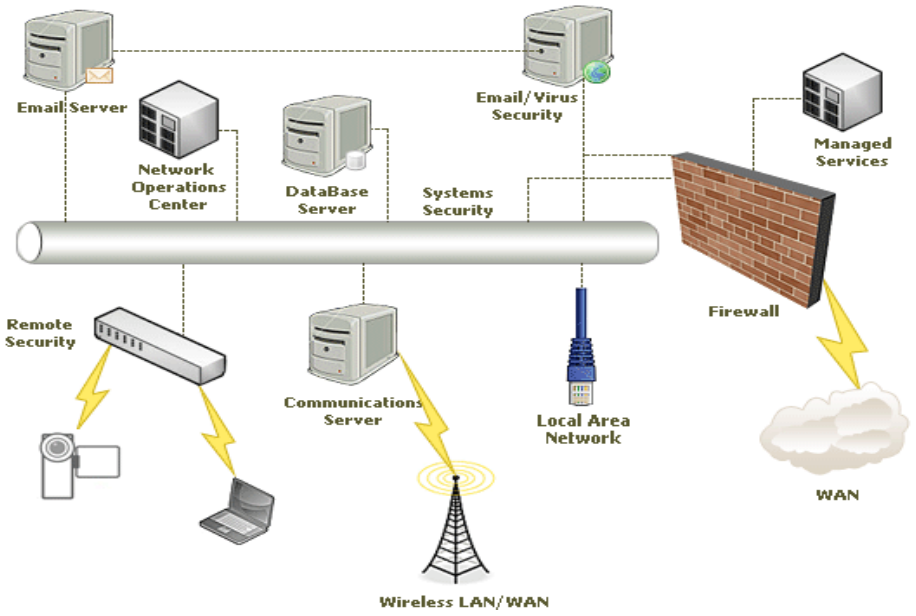
NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Tipos de Hacking Ético

1. Red Remota: Simula el intento de Hacking a través de internet. Rompe o encuentra vulnerabilidades desde fuera de las defensas de la red, como vulnerabilidades en los firewalls, proxys o routers.

2. Red Remota Dial-up: Simula el intento de Hacking lanzando ataques contra el pool de modems del cliente. (War Dialing).

3. Red Local: Simula el Hacking de alguien que ganó acceso físico y acceso no autorizado a la red local. El Hacker Ético debe ganar acceso directo a la red local para poder lanzar este tipo de ataque.



Procedimiento para realizar un Hacking Ético (Cont.)

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Tipos de Hacking Ético (Cont.)

4. Robo de Equipo: Simula un Hacking de robo de recursos con información crítica como una laptop de un empleado. Se pueden obtener; nombres de usuario, contraseñas, configuraciones de seguridad, tipos de cifrado. etc.

5. Ingeniería Social: Simula un ataque que verifica la integridad de los empleados de una organización utilizando comunicaciones telefónicas o personales, para obtener información que se utilizará en un ataque. De esta manera se pueden obtener; nombres de usuario, contraseñas y otras medidas de seguridad de la empresa.

6. Ingreso Físico: Ataca y compromete físicamente a la empresa. Si se obtiene acceso físico se puede plantar malware en un sistema de la red objetivo.

Procedimiento para realizar un Hacking Ético (Cont.)

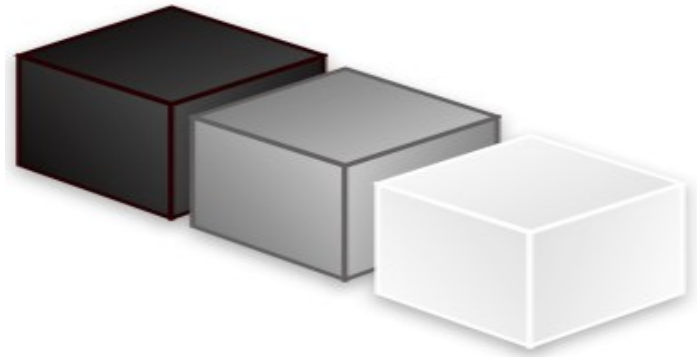
NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Tipos de Pruebas

1. Caja Negra: Realizar pruebas de seguridad con un conocimiento previo de la infraestructura de red o sistemas a ser evaluados. Este tipo de pruebas simula el ataque de un Hacker malicioso externo al perímetro de seguridad de la organización.

2. Caja Blanca: Realiza las evaluaciones de seguridad con un conocimiento pleno de la infraestructura de la red, tal como lo tendría el administrador de la red.

3. Caja Gris: Involucra realizar una evaluación en seguridad de manera interna. Este tipo de pruebas examina el alcance del acceso de un insider (interno) desde el Interior de la red.



Procedimiento para realizar un Hacking Ético (Cont.)

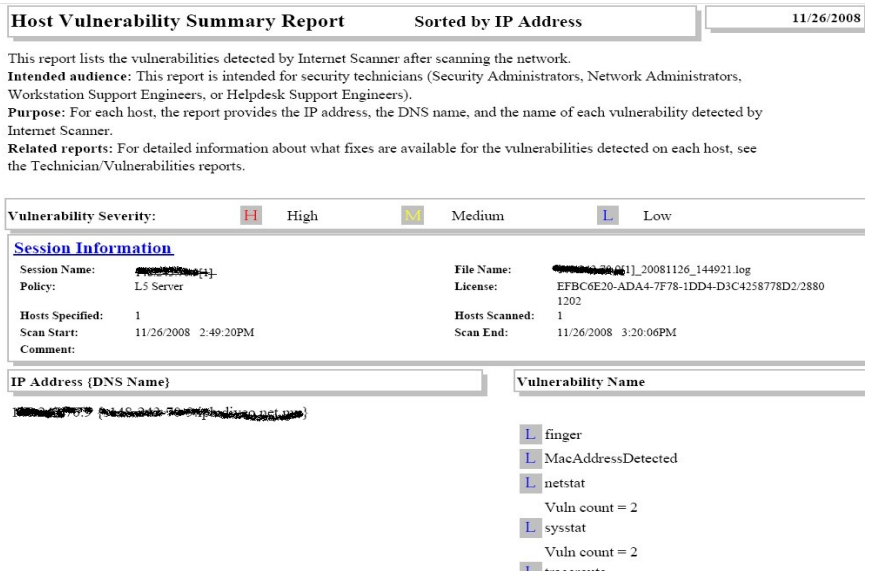
NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

El Reporte del Hacking Ético

El resultado de una Prueba de Penetración de redes o auditoría de seguridad es un reporte. Este reporte detalla los resultados de la actividad del Hacking Ético, los tipos de pruebas realizadas, y los métodos de Hacking utilizados.

En el reporte se debe detallar cualquier vulnerabilidad identificada, y además se sugieren las medidas correctivas. Se entrega generalmente a la organización, en un formato adecuado, por razones de seguridad.

El reporte es confidencial.
Si cae en manos equivocadas,
el resultado puede ser
desastroso para la organización.



Host Vulnerability Summary Report **Sorted by IP Address** **11/26/2008**

This report lists the vulnerabilities detected by Internet Scanner after scanning the network.
Intended audience: This report is intended for security technicians (Security Administrators, Network Administrators, Workstation Support Engineers, or Helpdesk Support Engineers).
Purpose: For each host, the report provides the IP address, the DNS name, and the name of each vulnerability detected by Internet Scanner.
Related reports: For detailed information about what fixes are available for the vulnerabilities detected on each host, see the Technician/Vulnerabilities reports.

Vulnerability Severity: H High M Medium L Low

Session Information

Session Name: [redacted] **File Name:** [redacted]_20081126_144921.log
Policy: L5 Server **License:** EFBC6E20-ADA4-7F78-1DD4-D3C4258778D2/2880 1202
Hosts Specified: 1 **Hosts Scanned:** 1
Scan Start: 11/26/2008 2:49:20PM **Scan End:** 11/26/2008 3:20:06PM
Comment:

IP Address {DNS Name}	Vulnerability Name
[redacted]	L finger
	L MacAddressDetected
	L netstat
	Vuln count = 2
	L sysstat
	Vuln count = 2

¿Preguntas?

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

Comentarios, dudas, sugerencias, anotaciones, correcciones, aclaraciones, invitaciones, etc.

Cursos del Año 2012

NPROS Perú los invita cordialmente a participar en los últimos cursos del presente año:

Curso de Hacking Ético (Lima)
(CNHE) Certificado NPROS Perú en Hacking Ético
Sábado 25 & Domingo 26 de Agosto del 2012 (9:00am a 8:00pm)

Curso de Cómputo Forense (Lima)
(CNCF) Certificado NPROS Perú en Cómputo Forense
Sábado 18 & Domingo 19 de Agosto del 2012 (9:00am a 8:00pm)

Curso de Hacking Ético (Trujillo)
(CNHE) Certificado NPROS Perú en Hacking Ético
Sábado 1 & Domingo 2 de Setiembre del 2012 (9:00am a 7:00pm)

Más información:
Sitio Web: http://www.npros.com.pe
Celular: 948351218 - RPM: #948891476 - RPC: 980715946
Correo Electrónico: cursos@npros.com.pe

NPROS
NETWORK PROFESSIONAL SECURITY PERU S.A.C.

¡Muchas Gracias!

Alonso Eduardo Caballero Quezada
Consultor de NPROS Perú S.A.C.
Sitio Web: http://www.npros.com.pe
Correo electrónico: cursos@npros.com.pe
Correo personal: reydes@gmail.com