Seguridad de la Información

Una introducción con enfoque práctico

Ing. Mariano Aliaga

Universidad Católica de Córdoba - Facultad de Ingeniería

2021

Panorama General

1. *ckers
   - Conceptos y tipificaciones
   - Historia y ejemplos
2. Malware
   - Definiciones y Clasificaciones
   - Virus y Gusanos
   - Troyanos y Backdoors
   - Ransomware
   - Herramientas de malware

Conceptos y tipificaciones

Hacker: una persona que disfruta de un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas, capaz de forzar sus capacidades al máximo. También se aplica a un programador experto o entusiasta de la seguridad.

Cracker: persona dedicada a romper las protecciones de un sistema. Generalmente ingresa por la fuerza y en forma oculta, obteniendo accesos del tipo administrativo.

Phreaker: de "phone freak". Quien rompe las protecciones de redes telefónicas, por ejemplo para hacer llamadas internacionales gratuitas.

Conceptos y tipificaciones

Hacker: una persona que disfruta de un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas, capaz de forzar sus capacidades al máximo. También se aplica a un programador experto o entusiasta de la seguridad.

Cracker: persona dedicada a romper las protecciones de un sistema. Generalmente ingresa por la fuerza y en forma oculta, obteniendo accesos del tipo administrativo.

Phreaker: de "phone freak". Quien rompe las protecciones de redes telefónicas, por ejemplo para hacer llamadas internacionales gratuitas.

Conceptos y tipificaciones

Hacker: una persona que disfruta de un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas, capaz de forzar sus capacidades al máximo. También se aplica a un programador experto o entusiasta de la seguridad.

Cracker: persona dedicada a romper las protecciones de un sistema. Generalmente ingresa por la fuerza y en forma oculta, obteniendo accesos del tipo administrativo.

Phreaker: de "phone freak". Quien rompe las protecciones de redes telefónicas, por ejemplo para hacer llamadas internacionales gratuitas.

Conceptos y tipificaciones

Algunas clasificaciones de "Hacker":

- **White Hat:** se refiere a un "ethical hacker" o "penetration tester" que se enfoca en asegurar y proteger sistemas de IT.
- **Gray Hat:** un hacker que actúa ilegalmente, algunas veces con buenas intenciones, y otras no.
- **Black Hat:** un "cracker", que ataca redes, equipos o sistemas con fines criminales. También son creadores de software maligno (virus, troyanos, etc.).
- **Blue Hat:** alguien externo a una firma de desarrollo de software que es contratado para detectar fallas de seguridad en sus productos.

Historia y ejemplos
Hackers

- El término “hacker” surge en los años ’60 en el MIT (Massachusetts Institute of Technology)
- Son los primeros creadores de los juegos y música en computadores.
- En los años ’70 hicieron posible el concepto de “una computadora en cada hogar”.
- La Internet de hoy fue posible por los desarrollos y filosofía de estos primeros hackers: TCP/IP, WWW, HTML, etc.

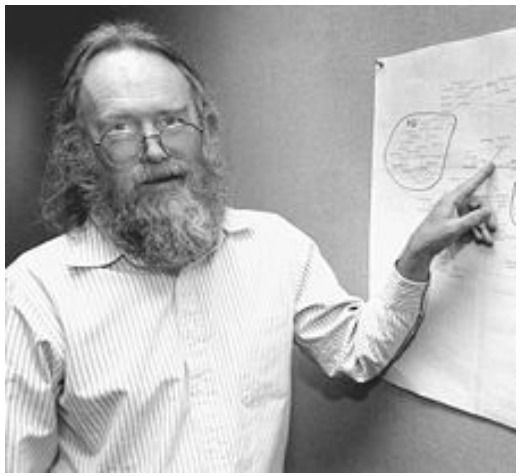
Historia y ejemplos
Hackers

Ética Hacker

1. El acceso a los ordenadores y a todo lo que te pueda enseñar alguna cosa sobre cómo funciona el mundo debe ser ilimitado y total.
2. Toda la información debería ser libre.
3. No creas a la autoridad. Promueve la descentralización.
4. Los hackers deberían ser juzgados por su hacking, sin importar sus títulos, edad, raza o posición.
5. Puedes crear arte y belleza con un ordenador.
6. Los ordenadores pueden cambiar tu vida para mejor.

Historia y ejemplos
Hackers

- **Jon Postel**
  - Uno de los padres de Internet. Formó parte del grupo que unió las dos primeras computadoras de Internet, en 1969.
  - Fue director durante casi 30 años de la Internet Assigned Numbers Authority (IANA), que asigna las direcciones IP y controla los servidores raíz del sistema de nombres de dominios (DNS).
  - Murió en 1998 a los 55 años.



Historia y ejemplos
Hackers

- **Ken Thompson**
  - Al comienzo de los '70 desarrolló junto a Dennis Ritchie el sistema operativo UNIX en los Laboratorios Bell.
  - Trabajó en el desarrollo de múltiples herramientas para UNIX en equipos PDP11.
  - Desarrolló en 1992 el formato de codificación de caracteres UTF-8.
  - Desde 2006 trabaja en Google y co-inventó el lenguaje de programación Go.

Ken Thompson y Dennis Ritchie,
creadores de Unix y del lenguaje C

Historia y ejemplos
Hackers

- **Steve Wozniak**
  - Es el gurú de los "hardware hackers".
  - Junto a John Draper desarrolló las primeras "blue boxes".
  - En 1977, junto a Steve Jobs, pusieron a la venta el primer Apple. Un año después, las ventas se habían multiplicado por diez.
  - Fundó la Electronic Frontier Foundation (EFF) para defender a los hackers.
  - Hoy es profesor de informática y filántropo.

Historia y ejemplos
Hackers

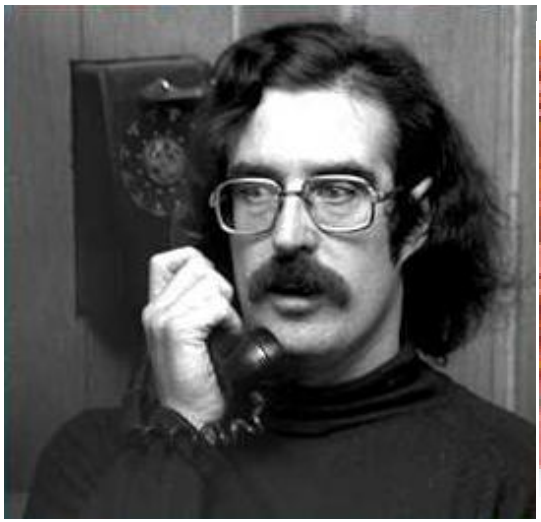
- **Margaret Hamilton**
  - Lideró el desarrollo del software de vuelo del módulo lunar en la misión Apollo 11
  - Acuñó el término "ingeniería de software" para diferenciarlo del hardware y otras ingenierías.
  - Reportó y documentó un bug en el "programa de prelanzamiento", que evitó un accidente en la misión Apollo 8.

Historia y ejemplos
Hackers

- **Vinton Cerf**
  - Uno de los padres de Internet. A principios de los 70 creó, junto a Roberth Kahn, el protocolo para la comunicación de paquetes Transfer Control Protocol/Internet Protocol (TCP/IP).
  - En 1992 co-fundó la Internet Society y fue su primer presidente.
  - Actualmente preside la Internet Corporation for Assigned Names and Numbers (ICANN) y es "Chief Internet Evangelist" de Google.

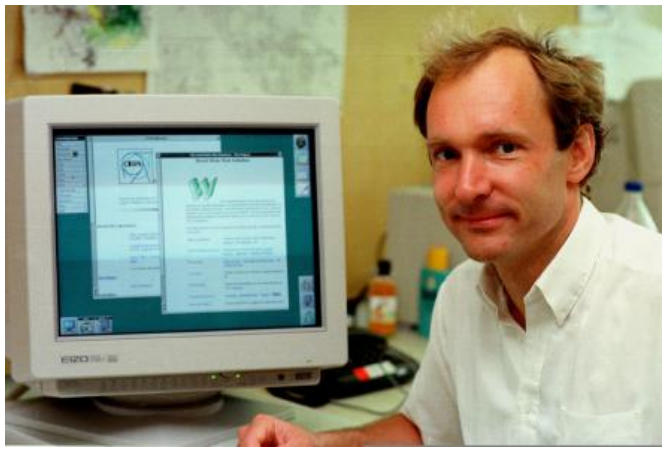
Historia y ejemplos
Hackers

- **John Drapper (Captain Crunch)**
  - Inventa la primera “blue box”
  - Admirado por sus acciones legendarias
  - Pesadilla para la compañía telefónica norteamericana, es detenido por fraude telefónico en varias ocasiones
  - Hoy trabaja como desarrollador de programas de seguridad



Historia y ejemplos
Hackers

- **Tim Berners-Lee**
  - Nacido en Londres en 1955.
  - Cuando estudiaba en la Universidad de Oxford, construyó un ordenador a partir de un televisor viejo.
  - En 1980 propuso un proyecto basado en el hipertexto. Era la World Wide Web, que presentó oficialmente en 1989, junto a un navegador, un editor y un servidor web.
  - Actualmente es director del World Wide Web Consortium.



Historia y ejemplos
Hackers

- **Richard Stallman**
  - Fundador del movimiento del "software" libre y la Free Software Foundation, en 1984.
  - Definió la idea del "software libre" y creó una licencia (GPL) que especificaba que cualquiera podía usar, estudiar, distribuir y mejorar los programas libremente.
  - Actualmente vive de las conferencias que da por todo el mundo.

Historia y ejemplos
Hackers

- **Linus Torvalds**
  - Nacido en 1969 en Helsinki. Creador del sistema operativo Linux en 1991.
  - Dirige el desarrollo del kernel.
  - Actualmente trabaja en la Linux Foundation.

Historia y ejemplos
Crackers

1971: "Phone phreaking". John Draper inventa la "blue box", logrando realizar llamadas de larga distancia sin cargo.
1988: Robert Morris Jr. crea un gusano auto-replicable que se distribuye rápidamente a través de ARPAnet e infecta más de 60000 equipos UNIX.
1989: Kevin Mitnick roba software de DEC y es la primera persona encarcelada por acceder a redes y equipos con fines criminales.
1999: Jonathan James, un adolescente de 16 años, accede a la NASA y descarga código propietario de la Estación Espacial Internacional.
1999: Un grupo de crackers noruegos rompe la clave para descifrar la protección anti-copia de los DVD.
2001: Se atacan los equipos que controlan el flujo de energía eléctrica del estado de California.
2008: Se detecta por primera vez el gusano Conficker. Se estimaban en 15 millones los equipos afectados.
2010: Anonymous lanza la operación "Avenge Assange": Amazon, PayPal, MasterCard, Visa, BankAmerica, etc.

Definiciones y Clasificaciones

Malware

Proviene del inglés **mal***icious soft***ware**, es un software que tiene como objetivo infiltrarse en el sistema y/o dañar la computadora sin el conocimiento de su dueño.

Adware: muestra o baja anuncios publicitarios que aparecen inesperadamente en el equipo.

Backdoor: un software que permite el acceso al sistema ignorando los procedimientos normales de autenticación, y eliminando toda evidencia de su existencia.

Botnet: son robots de software o bots, que se encargan de realizar funciones rutinarias y masivas.

Definiciones y Clasificaciones

Crackers: programas que descifran las contraseñas tanto del sistema operativo como de las aplicaciones y sistemas.

Dialers: programas que llaman a través del modem y sin el consentimiento del usuario, a un número telefónico de larga distancia o de tarifas especiales para redituar beneficios económicos al creador del malware.

Exploit: software que ataca una vulnerabilidad particular de una aplicación, servicio o sistema operativo.

Keylogger: programa espía que registra todas las pulsaciones del teclado para robar claves e información sensible del usuario.

Definiciones y Clasificaciones

Pharming: suplanta el servicio de DNS mediante el archivo *hosts* local, dirigiendo así al usuario a un sitio distinto del que cree estar abriendo.

Phishing: consiste en obtener información confidencial engañando al usuario con páginas o correos que se hacen pasar por entidades a las que normalmente accede o utiliza.

Definiciones y Clasificaciones

MasterCard S.A <avisos@serviciosrecuperacion.com>
Tue 18/03/06, 20:45
You;

Fecha: 06/03/2018

Estimado Cliente:

Recientemente, hemos determinado que una persona puede usar su tarjeta sin su autorizacion. Ahora tenemos que confirmar la informacion de tu tarjeta de credito. Para proteger la tarjeta contra el uso fraudulento, y habilitar el sistema de actualizacion de seguridad MasterConsultas, por favor, siga este enlace:

click aqui

Nota: Si usted no completa este procedimiento antes del 12 de Marzo de 2018, nos veremos obligados a suspender su tarjeta de forma permanente, ya que puede ser utilizada de manera fraudulenta.
Gracias por considerar esta informacion y ayudarnos a mantener la confidencialidad y seguridad de su tarjeta de credito.

Cordialmente, © Copyright 2018 MasterCard S.A. Todos los derechos reservados.

Master Card, Perú 143, Ciudad De Buenos Aires, Buenos Aires, 1067, Argentina

UNSUBSCRIBE

Definiciones y Clasificaciones

Ransomware: cifra los archivos del usuario con una determinada clave, que sólo el creador del ransomware conoce y proveerá al usuario que la reclame a cambio de un pago.

Rootkit: programas que se agregan a un equipo luego de haber ganado el control del mismo. Generalmente borran los rastros del ataque y ocultan los procesos del atacante.

Spam: correo electrónico masivo no deseado con fines publicitarios.

Spyware: aplicaciones que recopilan información del sistema en el que se encuentran instaladas para luego enviarla a través de Internet.

Troyano: un programa o conjunto de programas relacionados que bajo una apariencia inofensiva se ejecuta de manera oculta en el sistema y permite el acceso remoto de un usuario no autorizado al sistema.

Virus: software malicioso que se adosa a un ejecutable, macro, correo, etc. Tiene la capacidad de auto-replicarse infectando otros archivos, y generalmente se utiliza como un vector para transferir troyanos o backdoors.

Worm (gusano): es un tipo de virus, pero que se replica de un sistema a otro en forma automática a través de la red.

Virus y Gusanos
Qué infectan?

- Archivos
- Macros
- Librerías
- Sectores del disco
- Archivos de scripts (.BAT)
- Código fuente

Virus y Gusanos
Cómo infectan?

- **Virus polimórficos:** cifran o cambian su código de distintas maneras con cada infección para evadir su detección.
- **Virus furtivos:** ocultan las características normales de un virus para evitar ser detectados.
- **Virus multiparte:** se dividen en varias partes para no ser detectados.
- **Virus de "cavidad":** aprovechan los espacios vacíos en algunos archivos.
- **Virus de túnel:** se envían a través de protocolos alternativos o canales encubiertos.

Troyanos y Backdoors

Objetivos de un Troyano

- Robo o eliminación de información.
- Caídas o demoras en los sistemas.
- Realizar ataques distribuídos de denegación de servicio DDoS.
- Anunciar la infección de un equipo para que pueda ser utilizado.

Métodos de comunicación

- Overt channels (canales descubiertos): el modo "normal" como los programas se comunican con computadoras o redes.
- Covert channels (canales encubiertos): usa medios de comunicación de formas para las que no fueron pensados.
- Conexión reversa: permiten el acceso externo a una red interna generando conexiones de adentro hacia afuera.

Troyanos y Backdoors

Tipos de troyanos

- **Troyanos de acceso remoto (RATs):** usados para obtener acceso al sistema.
- **Troyanos que envían datos:** buscan datos en un sistema y los envían al atacante.
- **Troyanos destructivos:** se utilizan para eliminar o corromper archivos en un sistema.
- **Troyanos de denegación de servicio**: se usan para lanzar ataques de DoS.
- **Troyanos proxy:** permiten lanzar ataques desde otro sistema.
- **Troyanos que deshabilitan software de seguridad:** generalmente detienen el antivirus.

Ransomware
Historia

- **AIDS (1989):** un biólogo repartió 20.000 diskettes a los asistentes de la conferencia sobre el SIDA de la OMS. Los diskettes con el nombre de "Información sobre el SIDA – Diskettes de introducción", tenían advertencias como "tu ordenador dejará de funcionar de manera normal". Se cifraban todos los archivos y se pedían $189 como rescate

Ransomware
Historia

- **Archievus (2005):** primer ransomware en usar criptografía asimétrica. Cifraba la carpeta "Mis Documentos" y obligaba a hacer compras en una farmacia online para recuperar la información.
- **Cryptolocker (2013):** ingresa a través de archivos adjuntos de correos electrónicos, o del puerto remoto 3389 (RDP). Modifica las claves de registro y se copia a varias carpetas. Cifra sólo ciertos archivos: Office, fotos, AutoCAD, etc. Utiliza la red Tor y Bitcoin para el rescate. Habría recaudado entre U$ 3 y 27 millones.
- **Ransom32 (2016):** el primero escrito en Javascript y uno de los primeros "ransomware as a service". Es decir, cualquiera puede meter su dirección de Bitcoin e intentar infectar a la gente para ganar dinero.
- **Petya y Mischa (2016):** se instala en el sector de arranque del disco y cifra "todo el disco". Funciona uno u otro dependiendo de si se tiene permiso de administrador.

Ransomware
Historia

- **WannaCry (2017):** consiguió paralizar al servicio nacional de salud de Reino Unido, y a compañías como Telefónica, FedEx o Deutsche Bahn. Es decir, consiguió un efecto brutal en el mundo empresarial. Un investigador británico consiguió detener su expansión encontrando un dominio web en el código y registrándolo.

Herramientas de malware
Troyanos

- **Tini:** pequeño backdoor que escucha en un puerto (7777/TCP) y brinda al atacante un prompt de comandos remoto.
- **SubSeven:** troyano de acceso remoto (RAT) que notifica al atacante cuando el sistema infectado se conecta a Internet, enviándole información sobre el sistema.
- **BackOrifice 2000:** herramienta de administración remota que un atacante puede utilizar para controlar un sistema a través de una conexión TCP/IP usando una interfaz GUI.
- **BoSniffer:** intenta conectarse a un canal de IRC y anuncia su direción IP para que pueda ser utilizado para futuros ataques.

Herramientas de malware
Troyanos

- **Beast:** corre en la memoria asignada al servicio Winlogon.exe y se inserta en el ejecutable de Windows Explorer o Internet Explorer. Posee la funcionalidad de cliente, servidor y editor en la misma aplicación.
- **Firekiller:** desabilita los programas de antivirus y firewall.
- **Hard drive killer Pro:** destruye toda la información de un disco de manera irrecuperable.

Herramientas de malware
Detección de troyanos

- **Fport:** reporta todos los puertos TCP y UDP que estén abiertos y cuál es el proceso correspondiente.
- **TCPView:** muestra información detallada de todas las conexiones TCP y UDP en el sistema.
- **PrcView:** un visor de procesos que muestra información detallada de los procesos corriendo bajo Windows.
- **Inzider:** muestra los procesos con los puertos que cada uno utiliza.

Herramientas de malware
Wrappers

Wrappers: programas que se utilizan para "envolver" un troyano en un software legítimo. Ambos, el troyano y el programa se combinan en un único ejecutable.

- **Graffiti:** es un juego animado que puede envolverse con un troyano.
- **Silk Rope 2000:** un wrapper que combina el BackOrifice con cualquier otra aplicación que se especifique.
- **ELiTeWrap:** un avanzado wrapper de .exe's para Windows usado para instalar y correr programas.

Más información

- **Wikipedia**. *Hacker (computer security)*. http://en.wikipedia.org/wiki/Hacker_(computer_security)
- **Molist, Mercè**. *¿Qué tenemos que agradecer a los Hackers?*. http://ww2.grn.es/merce/2006/graciashackers.html
- **Focus Editors**. *The History of Hacking*. http://www.focus.com/fyi/it-security/history-hacking/
- **Wikipedia**. *Malware*. http://es.wikipedia.org/wiki/Malware
- **Wikipedia**. *Back Orifice 2000*. http://en.wikipedia.org/wiki/Back_Orifice_2000
- **GRAVES, Kimberly**. *Official Certified Ethical Hacker.* Capítulo 5.
- **Historia del ransomware**. https://omicrono.elespanol.com/2017/11/historia-del-ransomware/time
- **The Zoo malware repository**. https://github.com/ytisf/theZoo
- **Malware museum**. https://archive.org/details/malwaremuseum/