CAPITULO 3
Gestión de Riesgos
Crimen Informático - ataques contra las redes TCPIP

Jenny Torres, PhD.

Crimen Informático

Ataques a las Redes IP

- Hoy en día, las aplicaciones web tienen acceso a información valiosa:
  - Números de tarjetas de crédito
  - Información de cuentas bancarias
  - Información clasificada
  - Información personal
  - Historias médicas
  - Correo electrónico

Crimen Informático

Ataques a las Redes IP

- Y los ataques están dirigidos a:
  - Puertos
  - Servicios
  - Software de Terceros
  - Sistemas Operativos
  - Contraseñas
  - Ingeniería Social
  - Puertas Traseras (Back doors)
  - Caballos de Troya (Trojan horses)
  - Rookits
  - Canales Indirectos

Crimen Informático

Ataques a las Redes IP

- Los ataques más comunes son:
  - **Ingeniería Social,** es cuando se convence a la gente para que suministre información que no daría normalmente.
  - **Las backdoors**, o puertas traseras, son programas que permiten el acceso y control de un ordenador de forma remota. Suelen instalarse mediante troyanos.
  - **Los rootkits**, son conjuntos de programas que permiten al delincuente tomar el control del sistema con todos los privilegios.
  - **Canales Indirectos,** es un canal indirecto recopila la información de fuentes externas y de acontecimientos circundantes para deducir información principal importante

Crimen Informático

Vulnerabilidades de la capa de red

- Están estrechamente ligadas al medio sobre el que se realiza la conexión.
- Esta capa presenta problemas de control de acceso y de confidencialidad.
- Las vulnerabilidades a este nivel:
  - Desvío de los cables de conexión hacia otros sistemas
  - Interceptación intrusiva de las comunicaciones (pinchar la línea)
  - Escuchas no intrusivas en medios de transmisión sin cables, etc.

Crimen Informático

Vulnerabilidades de la capa de Internet

- En esta capa se puede realizar cualquier ataque que afecte un datagrama IP.
- Se incluyen como ataques contra esta capa las técnicas de:
  - Sniffing
  - La suplantación de mensajes
  - La modificación de datos
  - Los retrasos de mensajes y la denegación de mensajes

Crimen Informático

Vulnerabilidades de la capa de Transporte

- En esta capa podemos encontrar problemas de autenticación, de integridad y de confidencialidad.
- Algunos de los ataques más conocidos en esta capa son:
  - Las denegaciones de servicio debido a protocolos de transporte
  - Interceptación de sesiones TCP establecidas (secuestro de sesiones)

Crimen Informático

Vulnerabilidades de la capa de Aplicación

- Esta capa contiene varias deficiencias en seguridad.
- Esto se debe a la gran variedad de protocolos que actúan en ella.
- Algunas de las debilidades se presentan en los siguientes servicios:
  - Servicio de nombres de dominio
  - Telnet
  - File Transfer Protocol (FTP)
  - Hypertext Transfer Protocol (HTTP)

Crimen Informático

Actividades previas a la realización de un ataque

- Para obtener toda la información posible de la víctima, será necesario utilizar una serie de técnicas de obtención y recolección de información.
- Utilización de herramientas de administración:
  - *Nslookup*
  - *Ping*
  - *Traceroute*
  - *Whois*
  - *Finger*
  - *Rusers*
  - *Rpcinfo*
  - *telnet*
  - *Dig,* etc.

Crimen Informático

Exploración de puertos

- Técnica ampliamente utilizada para identificar los servicios que ofrecen los sistemas de destino.
- Suele ser la última actividad previa a la realización de un ataque.
  - TCP connect scan
  - TCP SYN scan
  - TCP FIN scan
  - TCP Xmas Tree scan
  - TCP Null scan

Crimen Informático

Herramientas para realizar la exploración de puertos

- La aplicación por excelencia para realizar exploración de puertos es *Nmap (Network Mapper).*

- Nmap junto con Nessus, son dos de las herramientas más frecuentes utilizadas tanto por administradores de redes como por posibles atacantes, puesto que ofrecen la mayor parte de los datos necesarios para estudiar el comportamiento de un sistema o red que se quiere atacar.

Crimen Informático

Herramientas para realizar ataques DoS

- **Hping3,** es una herramienta en línea de comandos que nos permite crear y analizar paquetes TCP/IP, y como tal tiene un muchas utilidades: hacer testing de firewalls, escaneo de puertos, redes y la capacidad de provocar un SYN Flood Attack DDoS.

- El objetivo de un ataque de este tipo es el envío de peticiones de conexión TCP más rápido de lo que una máquina puede procesar, al fin de saturar los recursos y evitar que la máquina pueda aceptar más conexiones.

Crimen Informático

Herramientas para realizar ataques DoS

- Un ataque clásico de DDoS sería el siguiente
  hping3 -p 80 -S --flood ip_victima

- donde :
  -p 80 es el puerto que elegimos atacar
  -S activa el flag Syn
  --flood le indica a hping que envíe los paquetes a la máxima velocidad posible
  ip_victima es la IP o dominio a atacar

- Si queremos que nuestra **ip no sea visible** podemos añadirle la opción -a y la IP que vamos a falsear
  hping3 -a ip_falsa -p 80 -S --flood ip_victima

Crimen Informático

Herramientas para realizar ataques de Fuerza Bruta

- Se denomina **ataque de fuerza bruta** a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.
- Los ataques por fuerza bruta, dado que utilizan el método de prueba y error, son muy costosos en tiempo computacional.
- Es la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

Crimen Informático

Herramientas para realizar ataques de Fuerza Bruta

- Ejemplos:
  - Medusa
  - Brutus
  - Jhon the Ripper
  - Hidra
  - Essential Net Tools

Longitud	Minúscula	Agrega Mayúscula	Números y y símbolos
6 caracteres	10 minutos	10 horas	18 días
7 caracteres	4 horas	23 días	4 años
8 caracteres	4 días	3 años	463 años
9 caracteres	4 meses	178 años	44.530 años

Crimen Informático

Herramientas para realizar ataques de Fuerza Bruta

- **John the Ripper** es un programa de Criptografía que aplica fuerza bruta para descifrar contraseñas. Es capaz de romper varios algoritmos de cifrado o hash, como DES, SHA-1 y otros.

- **John the Ripper** es capaz de auto-detectar el tipo de cifrado de entre muchos disponibles, y se puede personalizar su algoritmo de prueba de contraseñas. Eso ha hecho que sea uno de los más usados en este campo.

Referencias

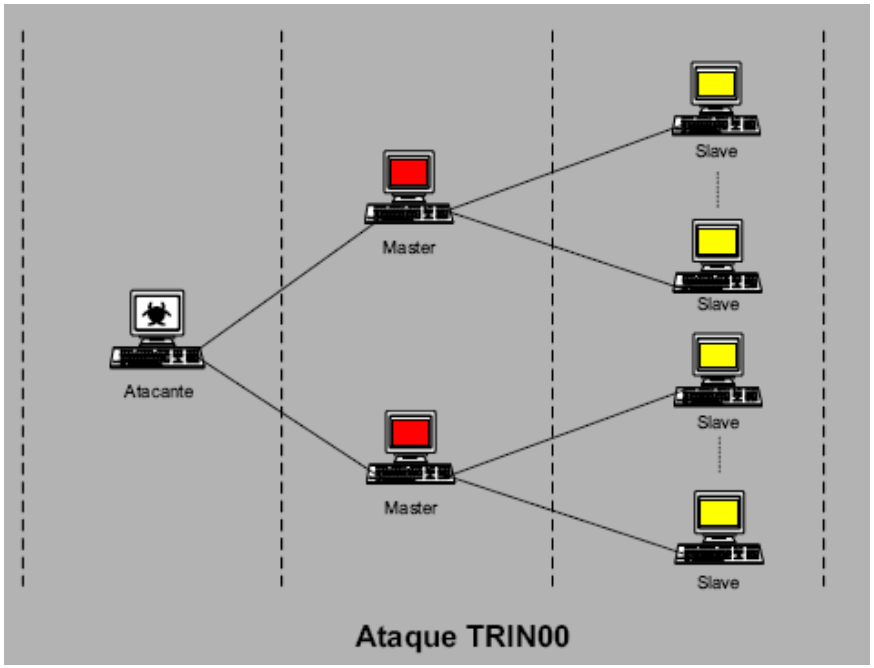
- Micki Krause, Harold F. Tipton. "**Information Security Management Handbook".** *Auerbach Publications. Fifth Edition.* ISBN: 08493-1997-8.
- Simson Garfinkel with Gene Spafford. "**Web Security, Privacy & Comerse"**. O'Really. Second Edition. ISBN 0-596000-456.
- Eric Maiwald, "**Network Security, Abegineer´s Guide**". McGraw-Hill. 2nd. Ed. ISBN 222957-8.
- Christopher Hadnagy, **Ingeniería Social: El Arte Del Hacking Personal**, Anaya Multimedia, 2011 ISBN 9788441529656.

Crimen Informático

Herramientas para realizar ataques distribuidos

- Es aquél en el que una multitud de sistemas (que previamente han sido comprometidos) cooperan entre ellos para atacar a un equipo objetivo, causándole una denegación de servicio.

- TRIN00 es un conjunto de herramientas master-slave utilizadas para sincronizar distintos equipos que cooperarán, de forma distribuida, en la realización de una denegación de servicio.



Ataque TRIN00