



Tema 3: Vulnerabilidades

Ataques

Índice 3

- Config. inadecuada del Sist
 - ↳ por defecto
 - ↳ Passwd, débiles
 - ↳ Vpn no corregidas
 - ↳ Vpn no conocidas (zero-day attacks)
- Errores en el SW (bugs)
 - ↳ Backdoor, buffer, combinaciones inesperadas de entrada, inyección código
- Debilidades de Algoritmos o Protocolos de seguridad
- Ingeniería Social
- Malware ejec. inadvertida de código malicioso

Cibercriminales

- Beneficio €€
- Extorsión, chantajes, sobornos,...
- Robo, identidad y/o credenciales
cambiar identidad, (fraude),...
- Espionaje industrial o comercial

Ataques Internos

- Los empleados y ex-empleados son peligrosos:
 - conocen nuestros sistemas
 - permisos de acceso
 - Pueden conocer como evadir la detección
 - Profesionales de Seguridad
- Sabotajes, hacking, robo, abuso recursos

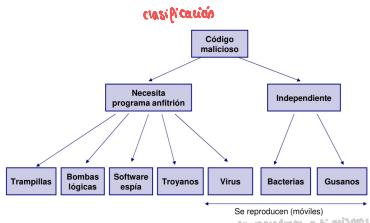
Código Malicioso (Malware)

Sus q. de manera **intencionada**, realiza acciones q. pueden dañar los datos o los sistemas.

- Introducción por vías: @, 2º archiver, P, web,...

Criterios de Clasificación

- Infeccioso → virus y gusanos
- Oculto → Trojanos, rootkits, parásitos tráseras
- Maliciosa → spyware, adware, troyanos
- Robo info → keyloggers y scatters
- De ataque → botnets y cibers



TRAMPILLAS → impudor
código q. duda los procedimientos de seg. → puntos de entrada & vulnerabilidades indiscut.

Bomba Lógica → Logic Bomb

código introducido en un Programa → se activa cuando se cumplen ciertas condiciones
verde licencia, dentro de...

Ataques de Falsa Confianza
código oculto q. se ejecuta por diversión, demostrar q. controlan su sistema → no destructivo

Salvo guardas: Revisión código

SW ESPIA → spyware
Recopila info P. fin su comportamiento

SW PUBLICITARIO → Adware
mostrar publ. en navegación

SECUESTRO NAVEGADOR → Browser hijackers
modifica la config. del navegador

Salvo guardas: uso anti-spyware, filtros publicidad, firewalls

Troyanos

trojan horse

- Programa aparentemente legítimo → realiza fun encubierta
- Normalmente se instala con un fij. priv.

Si se hace resaltar el programa legítimo → salteador puede dejar abierto huecos al sistema.
Rootkit → Backdoors

- Trojan/Rootkit → dificulta la func de detección
- Keyloggers, DDOS (comprob.), Netwars,...
- Vector de Infección: @, web,...

Salvo guardas: Antivirus, Firewall, IDS personal, estancos puertos, políticas seg.,
Intrusion Detection System

Ransomware

- cifrar archivos y exigir un rescate
- chantaje → amenazas q. pirateando las visto videos, fotografías, documentos, imágenes,...
- en muchos casos q. se fuerza a las víctimas a reaccionar con prisa

Salvo guardas: Antivirus, políticas seg., backups, bensates

VIRUS

- Generalmente introduciendo copias de él mismo
- Programa → infectado actua de vector de nuevas infecciones
- Puede自杀

BACTERIA → se replica q. se mismo consumiendo recursos del Sist.

GUSANO → worm → programa indep. q. puede reproducirse por su cuenta de él mismo por la red.

Salvo guardas: Antivirus, políticas seg., Parches, Firewall

Protección contra el malware

Medidas preventivas

A. Preventivas:

- Mantenerse informado sobre casos de fraudes, etc.
- Actualizar sistema operativo, programas y navegadores.
- No aceptar archivos de los que no sepa procedencia.
- Tener un antivirus instalado y actualizado. Dispositivo de Firewall.
- Tener copias de seguridad.
- Eliminación de los menores riesgos q. llegan por correo electrónico, no abrirlos, ni responderlos, ni responderlos.
- No hacer clic sobre ningún elemento (vídeo, dirección de correo, enlace, imagen, etc.) sin antes pasar el ratón sobre él para ver a qué página le dirige y si el lugar es legítimo.
- Comunicar con el personal de soporte y administradores.
- Consultar a un Centro de Respuesta a Incidentes de Seguridad EI: INCIBE. Línea de ayuda en obsequio.
- Denunciar el hecho ante las autoridades / FSE.
- Activar medidas administrativas (procedimientos, guías, etc.).

A. Reactivas

Ataques

El Triángulo de la intrusión (Proud Triangle)

para llevar a cabo un ataque es necesario:



Vectores de Ataques



Tema 3: Vulnerabilidades

(Ataques)

Fases de un Ataque

- ① Descubrimiento + Exploración Sist. Informáticos
 - Reconocimiento e **Footprinting** < **Activo e Passivo**
 - Recorridos e **fingerprinting**
 - OSINT → Open Source INtelligence
- ② Vulnerab. del Sistema
- ③ Explotación y Acceso
- ④ Escalada Privilegios
- ⑤ Corrupción o compromiso del sistema (Backdoors, nuevas cuentas,...) y ⑥ de nuevos objetivos (Pilfering)
- ⑦ Eliminación de pruebas (logs, bloques programas monitorización,...)

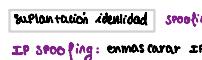
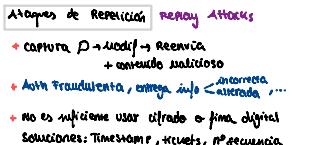
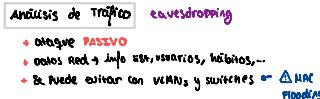
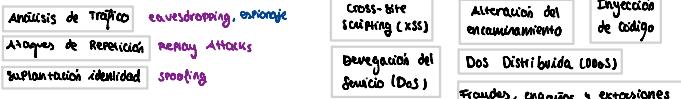
PTES → Penetration Testing Executive Standard



Herramientas (Hacking tools):

- Escáneres de puertos
- Sniffers
- Exploits
- Backdoor kits (para abrir y explotar puertas traseras)
- Rootkits (para ocultar puertas traseras sobre ejecutables o servicios)
- Auto-roots (herramientas de automatización del ataque)
- Password crackers
- Herramientas de spoofing
- Herramientas de encriptación
- ...

Tipos de Ataques



DNS spoofing: Respuetas DNS inválidas para devolver el tráfico de usuario a otros destinos de la red (o DoS)

SMIPT SPOOFING: 4^o con remitente falso

- Posibilidad de abrir un Relay
- Engaño a los destinatarios
- Envío de correo basura
- Dejar la repoblación de los supuestos originares

Nota: Registrars (DNS Root Authoritative Policy Framework), de DNS. Note: Registrar Authoritative Policy Framework (o RAP). Domain-based Message Authentication, Reporting and Conformance.

Identity spoofing: suplantación usuario usando las claves

- Registro de teclas pulsadas (Keyloggers sw o key)
- Perfiles de usuario (programas logueos o snoopers: logueos URLs que contienen identidades)
- Sniffers (fis): secuestro de browser
- Ingeniería social
- Fuerza bruta / ataques de diccionario

Deneg. tráfico normal para q pase por otros sist o redes intermedias

Alteración del encauamiento

- Encaminamiento fuente: Análisis de redes y encaminadores
- Encaminamiento fuente: Ruta de retorno para el IP spoofing
- Alteración de las tablas de encauamiento: ICMP Redirect, mensajes RIP, OSPF, EIGRP o BGP.

Cross-site Scripting (XSS)

Exploitación vía del Sist mediante un **zombie intermedio** (normalmente web)

- El atacante inserta código malicioso (VBS, JS,...) en el servidor (formularios, foros, etc) que lee el sistema atacado
- Se produce por falta de validación del código incrustado.

Inyección de código

→ **Medidas:** validar la entrada, filtrado info facilitada por el usuario

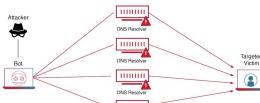
Denegación del servicio (DOS)

Sobrecarga red

- cantidad tráfico
- paquetes maliciosos formateados
- Actividades que degradan las prestaciones del sistema (envío de correos con contenidos innecesarios, envío de grandes volúmenes de datos,...)
- Alteración de DNS o encauamiento
- Bacteras que consumen los recursos del sistema
- Envío masivo de mensajes que colapsan los servidores de correo (**Mail bombing**)
- Incumplimiento de las reglas de un protocolo

Distribuidor DOS (DDoS)

- Un atacante crea una red (botnet) de hosts infectados llamados zombies, que son controlados por sistemas de manejo.
- Las computadoras buscan constantemente infectar más hosts, creando más y más zombies.
- Cuando está listo, el hacker proporciona instrucciones a los sistemas manipuladores para que los botnet de zombies lleven a cabo un ataque de DDoS.



Amenazas Persistentes Avanzadas (APT)

(largo plazo, múltiples fases, siguiendo, ...)

- Ataques sofisticados
- Avanzados: 2 obj. concretos + cambios ≠ ataques + seguimiento continuo e interacción
- Persistentes: enfoque **siguiente** + intentar romper iniciativas el mayor @ posible

Ejemplos: Titan Rain, Stuxnet,震网 (ciclo), Red October,...

Fraude, engaños y extorsiones

- Phising →
- Phising (variente): configura q el navegador se vaya a URL falsa cuando introduzcas el legítimo
- Ransomware: extrato usuarios + robarse
- Extorsiones: a menudo robarización de datos confidenciales, difamatorios,...

Hacking no técnico

Ingierencia social

- manipulación: A tendencia a confiar
- objetivo: engañar usuarios → combate con el ataque

Salvaguardas: concientización y normas

Otras técnicas

- shoulder surfing → mirar sobre el hombro, escuchando,...
- tailgating → entrar detrás de un usuario legítimo
- Acceder a estaciones de trabajo perdidas
- Passwd crac, Crac de admisión, dictionary, ...
- Dumpster diving escarbando entre la basura

Tema 3: Vulnerabilidades

(Gestión de Vulnerabilidades)

Auditoría de Vulnerabilidades

- Eval. sistemática de las debilidades de Θ nuestros Sist \hookrightarrow infra
- ↳ Detect. vulner.
- Permiten descubrir los puntos vuln q pueden ser explotados desde el interior o exterior usuarios ten cuenta en el Sist.
- Objetivo: mejorar Θ de nuestros Sist ✓ ventanas de vuln
- Punto de vista del atacante
- Gran parte del proceso puede estar automatizado
↳ herramientas de explotación NESSUS, Saint, Retina,...

Pasos a seguir

- ⇒ Realizar un inventario de sistemas a evaluar
↳ Mapa de la red, escaneo IP y de puertos
- ⇒ Instalar las herramientas de Θ automatizadas
↳ Basadas en la red / basadas en los hosts
- ⇒ Identif. debilidades \hookleftarrow visibles
↳ Test de Vuln conocidas
- ⇒ Tomar medidas correctoras + elaborar informes
↳ Política de actualizaciones y parches, eliminación genéricos innecesarios, uso contraseñas \clubsuit

Limitaciones de los escáneres automáticos

- ofrecen fotografía instantánea, no continuada sobre el estado de Θ
- Solo detectan vuln conocidas
- Necesitan intervención humana

Preparación

selección de pruebas y de Sist. Afectados

Interpretación resultados

Identif. problemas, falsos Θ , falsos Θ

- Pueden tener efectos sobre los servicios evaluados

Delitos Informáticos

- Convenio sobre la Ciberdelincuencia \hookrightarrow del Consejo de Europa Budapest 23/XI/2001

- ↳ 1º tratado internacional
- ↳ Establece bases para proteger a la sociedad \Rightarrow delitos
- ↳ Ratificado Θ 2010
- ↳ Necesidad adoptar legislación penal

- ↳ Ejes del tratado \hookrightarrow Tercerismo cooperación internacional
- contra CIO datos a Sist. informáticos (fabricación, fraude, ...)
- se identif. delitos relacionados con contenido pornográfico infantil, propiedad intelectual así como tentativa + complicidad

Código Penal. Artículo 197 (descubrimiento y revelación de secretos) 197 bis.

1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

197 ter.

- Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

- a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o
- b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.