UD 2: Implantación de Mecanismos de Seguridade Activa e Pasiva

Ataques e Contramedidas

A seguridade informática é un proceso no que interveñen todos os activos do sistema informático: Hardware, Software, Instalación se Persoal.

Dependendo do xeito de tratar os activos podemos falar de :

- Seguridade Física / Seguridade Lóxica
- Seguridade Activa / Seguridade Pasiva

O establecemento de medidas para evitar o éxito dos ataques se denomina ***seguridade activa***, mentres que as medidas destinadas a minimizar o impacto do ataque se denominan ***seguridade pasiva.*** Todas as medidas tomadas para evitar o éxito de ataques concretos se denominan ***contramedidas.***

Un ataque informático é calquera acción que teña como finalidade desestabilizar o normal funcionamento do sistema.

Tipos de Ataque I

- Ataques de interrupción de servizo (DoS) – Afectan á dispoñibilidade.
  - Técnicas: SYN Flood, ICMP Flood
- Ataques de interceptación de información – Afectan á confidencialidade
  - Se utilizan habitualmente troianos ou ataques MiM
  - Técnicas: ARP Poisoning, DNS caché poisoning, DNS spoffing, rogue DHCP, IP spoofing...
- Ataques de modificación de información – Afectan á integridade
  - Técnicas: Ataques MiM, malware (virus/troianización dos sistemas)
- Ataques de intrusión nos sistemas – Afectan á autenticación
  - Técnicas: Ataques contra as passwords como forza bruta ou rainbow tables, ataques contra software vulnerable (Buffer Overflow, XSS scripting, SQL Injection...)

Fases dos Ataques

Tendo en conta o efecto producido nos sistemas podemos falar de:

- **Ataques Pasivos:** Se limitan a extracción de información sen alterar o sistema. Na maioría dos casos pasa desapercibido.
- **Ataque Activos**: Producen cambios no sistema, son a maior parte dos ataques e os cambios normalmente pasan pola instalación de backdoors ou troianos.

As fases dun ataque son moi similares as fases dun análise de vulnerabilidades:

- **Recoñecemento e identificación dos sistemas obxectivo**
- **Busca e explotación de vulnerabilidades**. Unha vez localizada unha vulnerabilidade nun sistema, se prodederá a utilizar un ***exploit***, ben de elaboración propia ou descargado dunha base de datos de exploits. O obxectivo final é habitualmente un dos seguintes: o roubo de información como poden ser as password, suplantación de identidade (***MiM***) ou a instalación de ***rootkits*** / ***troianos*** que permitan agregar o sistema comprometido a unha ***BotNet.*** Ataques comúns son:
  - Alteración do tráfico da rede (MiM attack)
  - XSS (Cross-Site Scripting) / SQL Injection
  - Ataques de diccionario
  - Ataques de Buffer Overflow
- **Eliminación de pegadas**. O obxectivo é eliminar calquera rastro dos logs do sistema que permita identificar que o sistema foi atacado e/ou aos autores do ataque.

Recoñecemento dos Sistemas

- **Footprinting**: Consiste na recopilación de información sobre o sistema obxectivo mediante información “pública”, como a simple busca en internet ou mediante enxeñería social sen ningún tipo de interacción cos sistemas. Existen ferramentas de footprinting moi efectivas como o Google Dorks (Google Hacking Database https://www.exploit-db.com/google-hacking-database), shodan, maltego, FOCA, Robtex (online), the harvester ...).

  Mediante footprinting habitualmente obtemos información sobre a estrutura da rede e dos seus usuarios, pautas de funcionamento.. etc.
- **Fingerprinting**: Consiste na recopilación de información de xeito activo realizando exploracións dos sistemas obxectivo. Nos permite recopilar información sobre os sistemas operativos e os servizos instalados e as súas versións, usuarios e grupos dos sistemas... etc. Ferramentas típicas son ***ping*** e ***nmap.*** En particular nmap é capaz de determinar os hosts existentes nunha rede, que servizos teñen dispoñibles, os sistemas operativos ea versión e numerosas características do hardware de rede. Nmap además soporta un sistema de scripting denominado NSE (Nmap Scripting Engine) que se pode utilizar para explotar as vulnerabilidades atopadas nas exploracións.

A exploración de sistemas sen permiso é unha actividade hostil considerada un ataque que pode ter consecuencias legais. O simple uso de nmap contra unha rede pode ser considerado un intento de intrusión e unha actividade hostil.

Contramedidas I

- Contramedidas contra a exploración dos sistemas
  - E difícil evitar a exploración dun sistema conectado a redes públicas. Entre outras medidas podemos citar:
    - Configurar transferencias de zonas DNS seguras (Ataque de transferencia de zona)
    - Ocultar os banners de aviso dos servizos de rede
    - Crear unha DMZ ben limitada
    - Expoñer unicamente os servizos imprescindibles
- Contramedidas contra o software defectuoso (Buffer Overflow, XSS Scripting, SQL Injection...). **(Ataques de intrusión / modificación / interceptación)**
  - A principal medida e non utilizar software defectuoso. Pero potencialmente calquera software pode ter erros proclives a súa explotación. Polo tanto, debemos:
    - Non expoñer máis que os servizos imprescindibles. Si coñecemos algunha vulnerabilidade nun software determinado e non dispoñemos de corrección debemos ou ben non utilizar ese software ou reducir ao máximo a súa exposición á rede.
    - Actualizar periodicamente todo o software

Contramedidas II

- **Contramedidas contra ataques DoS**. Difíciles de evitar. Podemos:
  - Recurrir a a redes de protección (CDN), a regras no firewall que limiten os intentos de conexión para paliar o ataque (**SynAttackProtect**, **TcpMaxPortsExhausted** ou **TcpMaxHalfOpen** en Windows, ***SYN cookie***, ***SYN cache*** e ***SYN proxy*** en Linux), ao uso de proxies inversos que repartan a carga das peticións e a separación dos servizos entre varios hosts.

```
/sbin/iptables -N syn-flood
/sbin/iptables -A syn-flood -m limit –limit 100/second –limit-burst 100 -j RETURN
/sbin/iptables -A syn-flood -j LOG –log-prefix "SYN-flood attempt: "
/sbin/iptables -A syn-flood -j DROP
```

  - No caso dos servizos web, se pode recurrir a ***Firewalls de Aplicacións Web (WAF)*** que controle e monitorice as conexións aos nosos sitios web evitando ataques DoS, SQL Injection, XSS.. . Existen WAF hardware e software. Existen proveedores de WAF moi utilizados como ***Akamai*** ou ***CloudFlare***
  - E tamén común o uso de ***captchas*** nas aplicacións que eviten peticións por parte de bots automáticos
- **Contramedidas contra ataques MiM / Phising. (Ataque de Interceptación de información)**
  - Os ataques MiM se dan maiormente nas redes internas, mediante técnicas moi difíciles de evitar. Ataques típicos son o ***ARP Poisoning***, ***IP Spoofing***, ***DNS Spoofing***, ***Web Spoofing*** ou ***IP hijacking***. Algunha das posibles medidas son:
    - Uso de entradas fixas na táboa ARP para os equipos importantes (gateways, servidores web...)
    - Limitar o acceso físico a rede local de equipamento non controlado
    - Instalar un sistema IDS (HIDS/NIDS) que nos permita detectar intentos de ataque (snort, / suricata)
    - Uso de servizos seguros (VPN IPSec / TLS, HTTPS, SSH)
    - Asegurarse dunha correcta configuración do servizo DNS evitando o DNS Spoofing, por exemplo mediante o uso de DHCP fraudulentos.
- **Existen numerosas ferramentas de creación de paquetes TCP/UDP como *hping3*, *ettercap* ou *scapy* que permiten a inxección de paquetes falsos facilitando ataques MiM / ARP poisoning ou roubo de información da rede.**

Contramedidas II

- Contramedidas contra o envío/recepción de SPAM
  - Uso de Filtros de spam(spamassasin),
  - Correcta configuración do servizo de correo evitando o SMTP Relay,
  - Identificación do servicio de correo mediante DMARC (SPF record)/DKIM
    - DKIM permite comprobar a autenticidade do remitente. O emisor do correo firma dixitalmente todo o correo saínte, que comproba o servidor receptor
- Contramedidas contra ataques de diccionario (ataque de intrusión)
  - Uso de contrasinais seguras
  - Limitar o número de intentos antes de bloquear o acceso por un tempo (fail2ban)
  - Uso de sistemas de autenticación multifactor
- Contramedidas contra a instalación de rootkits / troianización do sistema
  - Uso de ferramentas de integridade do sistema (rkhunter / tripwire / SFC)
  - Uso de antivirus e firewall que únicamente exponga os servizos imprescindibles.
  - Uso de sistemas de actualización automáticos que manteñan seguros os servizos e aplicacións

Ferramentas Preventivas

- Antivirus
- Firewalls
- Sistemas de actualización automáticos
- Cifrado / (Certificados PGP / X509, VPN, SSH, Https)
- Sistemas anti-spam (filtros como spam-assassin, DMARC SPF/DKIM a nivel DNS)
- Sistemas de detección de Intrusos (IDS / IDPS) --> snort, suricata
  - IDS / IPS
  - Host IDS vs Network IDS (HIDS vs NIDS)
  - Baseados en firmas / Baseados en anomalías
  - Monitorización da rede: Wireshark, Ethereal, Tcpdump

Boas Prácticas en Contornos de Risco

- Contrasinais seguras
  - Deben ter unha lonxitude mínima e unha mezcla apropiada de letras, números e caracteres especiais para dificultar os ataques de diccionario
  - Os nomes dos usuarios non deberían facilitar pistas sobre a súa función
- Uso de correo firmado e si é apropiado, cifrado
  - Os protocolos de e-mail son inseguros. Toda a transmisión é en texto plano
  - O correo firmado garantiza a autoría do correo e a súa integridade
  - O correo cifrado garantiza a privacidade da mensaxe
- Evitar o reenvío de correos e mensaxes
  - O reenvío de correos facilita información sobre os remitentes
  - O seguimento de cadeas de mensaxes pode producir situacións de saturación/denegación de servizo
  - As cadeas de reenvío son molestas
- Uso de HTTPS seguro e comunicacións cifradas (VPN, SSH)
  - O uso de sistemas cifrados garante a confidencialidade, integridade e o non repudio.
  - O uso de VPN permite o uso seguro (garante a confidencialidade, integridade e non repudio) dos recursos da rede corporativa dende localizacións remotas
- Uso de autenticación multifactor
  - O uso de autenticación multifactor é eficaz contra calquera intento de intrusión mediante ataques contra a autenticación.

Firma e Cifrado nas Comunicacións

- PGP vs X.509
- As cadeas de confianza
- As autoridades certificadoras e autoridades de segundo nivel
- PKI X.509
  - Globus-simple-ca
  - Easy-rsa
  - Let’s encrypt (python-certbot)
  - Creación dunha PKI

Seguridade WiFi

- SSID Oculto / SSID Público
- Redes Públicas
- Cifrado
  - WEP
  - WPA
  - WPA2-PSK
  - WPA2-Enterprise
  - WPS
- Filtrado MAC

Seguridade Pasiva: Ferramentas Paliativas

- Backups
  - Periódicos
  - Deslocalizados: Regra 3-2-1: Dous soportes distintos, un deles sempre fora da empresa (A nube, dropbox, google drive ... etc)
  - Automáticos
- Ferramentas
  - Rsync
  - Fsarchiver / Partimage
  - Tar
  - Rdiff-backup
  - Recuva
  - Uso de NAS (Synology: Hyper Backup/Hyper Backup Vault, Cloud Sync)

Manual de Seguridade e Plan de Continxencia

- Os obxectivos do manual de seguridade son:
  - o establecemento dos estándares de seguridade
  - Definir un conxunto de normas de actuación para evitar problemas
- O obxectivo do plan de continxencia é o establecemento das normas de actuación a seguir no caso de que se produza un desastre co obxectivo de recuperar o normal funcionamento dos sistemas
- O manual de seguridade debe ter en conta o xeito de traballo da organización e o grao de coñecemento e especialización dos profesionais da mesma. Para elo, se debe formar unha equipa composta por persoas de distintos departamentos de xeito que estean representados todos os aspectos da organización, elaborar o documento e publicalo de xeito oficial coa aprobación da dirección deixando constancia de que todo o mundo o recibe.
- O documento debe contemplar:
  - Os factores humáns e tecnolóxicos
  - A lexislación vixente, especialmente no relativo á protección de datos
  - Os criterios que delimitan e determinan a responsabilidade de cada usuario
  - Os criterios de actuación

O Plan de Continxencias

- O plan de continxencia se deseña para recuperar o normal funcionamento dos sistemas ante calquera incidencia que se poda producir. Debe contemplar como mínimo:
  - Un análise dos riscos do sistema
  - Un estudio das medidas de seguridade actuais
  - Un plan de recuperación que contemple as medidas que se deben tomar antes, durante e despois do incidente.
- O análise dos riscos ten como obxectivo dar unha resposta a preguntas como:
  - ¿ Que necesitamos protexer ?
  - ¿ Que pode fallar ou ir mal ?
  - ¿ Que consecuencias poden derivarse das posibles incidencias ?
- No estudo das medidas de seguridade actuais, deberemos indicar cales son e verificar o seu correcto funcionamento.
- O plan de recuperación debe contemplar de xeito claro tanto o orixe do fallo como o dano ocasionado. O procedemento de recuperación establecido debe ser cumprido tal e como se especifica. O responsable deberá verificar que o procedemento se leva a cabo segundo o plan. Este plan debe indicar as accións a tomar:
  - Antes da incidencia (Plan de respaldo)
  - Plan de emergencia (Accións a tomar durante a incidencia)
  - Plan de recuperación (Accións a tomar para a recuperación do funcionamento normal)

https://es.wikipedia.org/wiki/Plan_de_contingencias