M11 SEGURETAT I ALTA DISPONIBILITAT

Administració de Sistemes Informàtics en Xarxa

IES de l'Ebre

UF2 – Seguretat Activa i Accés Remot

Seguretat en la Xarxa Corporativa

Seguretat en la xarxa Corporativa

- La seguretat de la xarxa inclou totes les **eines i polítiques** adoptades per l'administrador del sistema per prevenir i controlar **l'accés no autoritzat, mal ús, modificació o inhabilitació** d'una xarxa informàtica i els seus recursos.
- El Monitoratge del trànsit de xarxes és un dels aspectes més importants a l'hora de tractar la seguretat en la xarxa. El podem classificar en:
  - **Monitoratge passiu:** es basa en l'escolta i anàlisi del trànsit real de la xarxa. Només es recull la informació i s'analitza.
  - **Monitoratge actiu:** l'aproximació activa consisteix a injectar paquets de prova a la xarxa, o enviar-ne als servidors i aplicacions, i a mesurar el temps de resposta obtingut.

Eines de monitoratge passiu

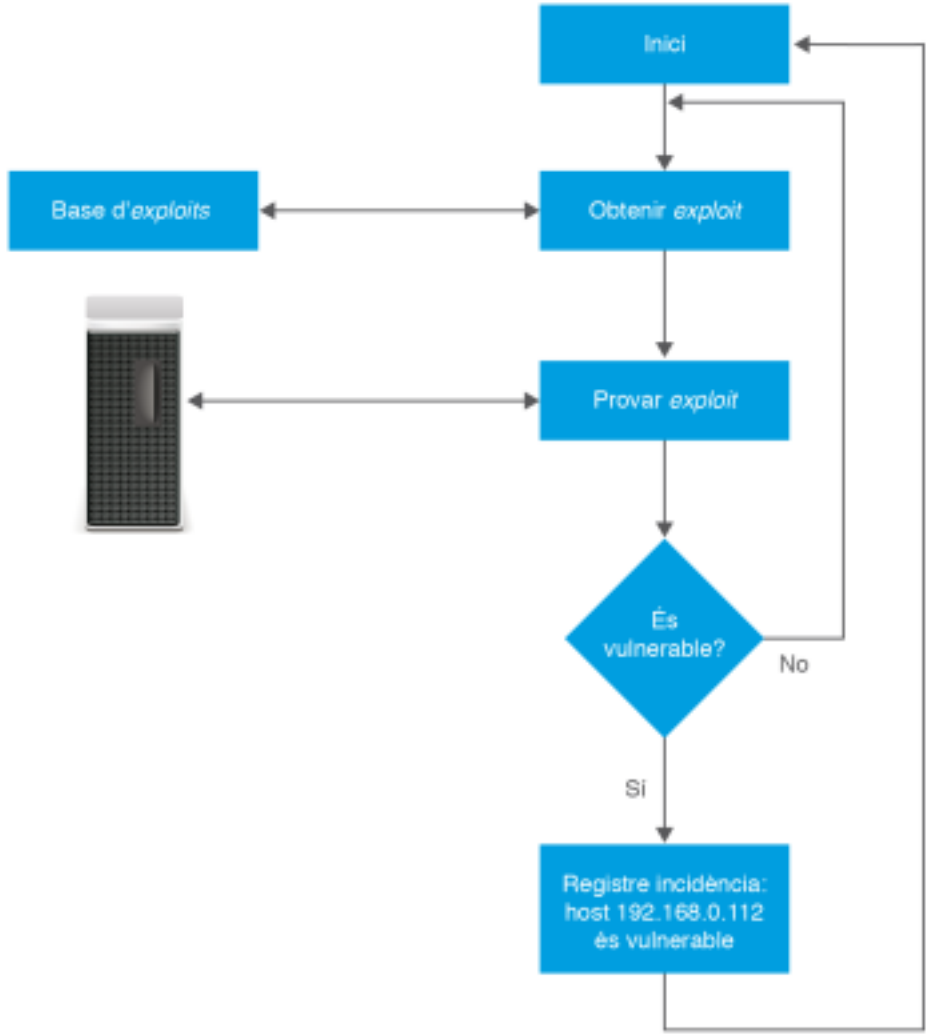
- S'anomenen **detectors (sniffers)** els programes que permeten la captura i l'enregistrament de la informació que circula per una xarxa.
  - Una manera d'esbrinar si hi ha detectors és cercar la presència de targetes en **mode promiscu**. Això es pot fer amb diverses eines: **ifconfig, ifstatus o Network Promiscous Ethernet Detector** (NEPED)...
- Es poden fer servir mesures de **protecció**:
  - Per exemple, si es **xifren els documents** que s'envien per la xarxa amb PGP.
  - Les eines criptogràfiques **protegeixen la informació** que circula, però no permeten establir connexions segures.
  - És de vital importància la instal·lació d'altres eines com un servidor de **Secure Shell** (SSH), que permet l'establiment d'inicis de sessió segurs i es pot fer servir com a substitut de l'ordre telnet.

Eines de monitoratge Actiu.

- Els **escàners** són eines de seguretat que serveixen per detectar les **vulnerabilitats** d'un sistema informàtic.
- **L'escaneig de ports** consisteix a esbrinar els ports TCP/UDP que estan oberts en una màquina remota pertanyent a una xarxa determinada.
- **Els ports oberts** constitueixen una informació molt interessant per als possibles intrusos, ja que **les vulnerabilitats** dels processos que estan en funcionament poden permetre l'accés no autoritzat al sistema.
- TCP és la sigla de **Transmission Control Protocol**, i UPD, la de **User Datagram Protocol**. Són els protocols que comparteixen tots els ordinadors connectats a Internet per poder-se connectar entre ells.

Esquema de funcionament d'un escàner

- Tots els **escàners** comparteixen, en trets generals, un esquema de funcionament similar



Ordres del sistema

- Per a una diagnosi ràpida de possibles errors en la comunicació, és recomanable utilitzar les ordres **ping i traceroute**.
- Amb **ping** es pot determinar si una màquina **està connectada o no** a la xarxa.
- Amb **traceroute** es pot obtenir una descripció del **camí que es va seguint** per arribar a una determinada màquina, de manera que en cas que una estació no respongui es pot determinar el lloc on es produeix el problema.
- Al mercat hi ha moltes **eines** que faciliten el **monitoratge de la xarxa**, com per exemple MRTG (Multi Router Traffic Grapher) o el conegut Nagios.

Seguretat en xarxes sense fil

- Les **comunicacions sense fil**, basades en ones de ràdio o infraroges, permeten connectar-se a la xarxa des de qualsevol lloc de l'organització i en qualsevol moment sense necessitat d'estendre cap cablejat.
- **Wi-Fi** significa *wireless fidelity* (fidelitat sense fil). Les xarxes locals sense fils s'anomenen **WLAN** (*Wireless Local Area Network*).
- Les xarxes locals sense fil poden operar en **mode** *ad hoc* o en **mode infraestructura**:
  - **Mode ad hoc** (client a client). Totes les màquines que es troben dins de la mateixa àrea es poden comunicar entre si directament. No és habitual, encara que és pràctic, per exemple, per enviar informació entre dos ordinadors.
  - **Mode infraestructura** (client a punt d'accés). Les estacions es comuniquen amb els anomenats **punts d'accés**, que actuen de repetidors i difonen la informació a la resta de la xarxa.

Seguretat en xarxes sense fil

- Cal tenir present que les xarxes locals sense fil requereixen, a causa de la seva natura intrínseca, unes **mesures de seguretat més grans** que les que s'adoptarien en una xarxa cablejada.
- **Recomanacions** per millorar la seguretat de les WLAN:
  - Canviar les **contrasenyes per defecte**.
  - Activar el **filtrat d'adreces MAC** de manera que només es puguin connectar els dispositius especificats
  - Activar el **xifratge** WEP/WPA/WPA2.
  - **Desactivar l'assignació d'IP per DHCP** si no és necessària.
  - **Eliminar la difusió (broadcast) del SSID**, és a dir, del nom lògic associat a la xarxa.

Riscos potencials dels serveis de xarxa

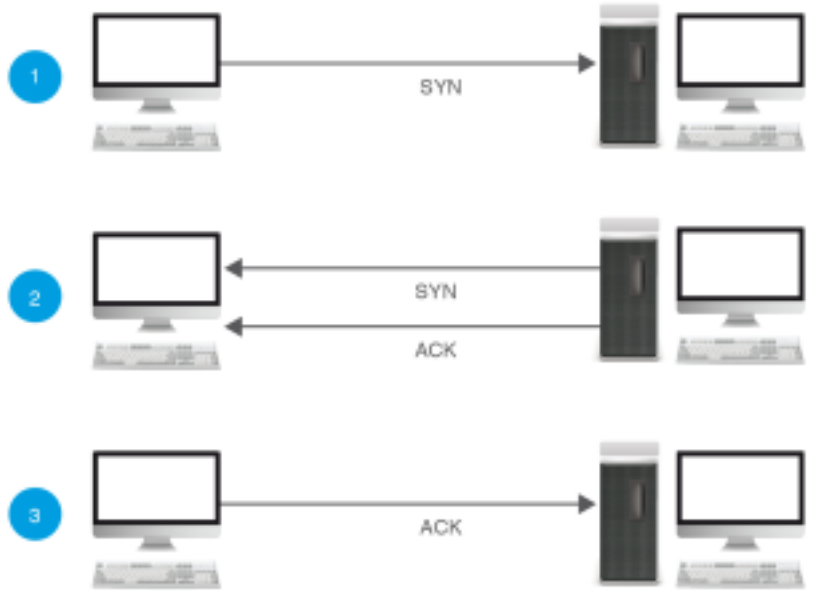
- Seguretat de les **topologies** i els tipus de xarxa
  - Per ***topologia* s'entén la forma o estructura de la xarxa** des del punt de vista lògic, que pot diferir del seu disseny físic.
  - Per exemple, una **topologia d'estrella** és especialment **resistent a la caiguda de les estacions de treball**, però en canvi té un punt crític, l'element central, que si és atacat o cau per qualsevol motiu pot provocar la caiguda de tota la xarxa.
- Seguretat del **maquinari de xarxa.** Pel que fa a la seguretat dels **commutadors, concentradors i encaminadors**, cal prendre les precaucions següents:
  - Activació del **xifratge** (en cas que els dispositius ho admetin).
  - En cas que no sigui necessari, cal **desactivar el control remot** d'administració.
  - **Canviar les contrasenyes** d'administració predeterminades d'aquests dispositius.
  - Usar **llistes d'accés** que permetin només els protocols, ports i adreces IP que la xarxa i els usuaris necessitin. Denegar la resta.

Control d'accés a la xarxa basat en autenticació

- Cal considerar els mètodes de **control d'accés dels dispositius** que es volen connectar a la xarxa. Aquest mètode requereix tres components i es basa en l'adreça MAC del dispositiu:
  - **Client**: dispositiu (per exemple un portàtil) que desitja connectar-se a la LAN mitjançant una xarxa de telecomunicacions.
  - **Autenticador**: és l'element que controla l'accés físic al medi, basant-se en l'estat d'autenticació del client. L'estat inicial dels ports de l'autenticador és "no controlat". Si el procés d'autenticació finalitza afirmativament, el port canvia el seu estat a "controlat" i el dispositiu és autoritzat a accedir al medi.
  - **Servidor d'autenticació**: és el dispositiu de "confiança" que s'encarrega d'efectuar la validació de la identitat del client. Notifica el resultat a l'autenticador.

Atacs als serveis de la xarxa

- **Atacs de denegació de servei**
  - S'anomena *atac de denegació de servei (denial of service)* tota acció iniciada per una persona o entitat que **inutilitza el maquinari o programari** de manera que els recursos del sistema no siguin accessibles des de la xarxa**.**
  - Aquest atac es basa en el *modus operandi* del **protocol d'establiment de sessió** entre client i servidor:
    - L'ordinador client envia una **sol·licitud de sincronització** (SYN) al servidor.
    - El servidor **respon amb un missatge ACK** (*acknowledgement*) i un missatge de **sincronització al client.**
    - En resposta a la sol·licitud de sincronització, **l'ordinador client envia una resposta ACK al servidor.**



https://www.youtube.com/watch?v=7xGdz5Li9Sw

Atacs de falsejament d'identitat

- En els atacs d'*spoofing* l'intrús fa servir tècniques de suplantació d'identitat.
- Les formes més conegudes d'aquests atacs són el **falsejament d'IP**, el **falsejament d'ARP** i el **falsejament de** DNS.
- Observem que amb tècniques de falsejament d'identitat es poden aconseguir atacs de denegació de servei.
- Les tècniques de **falsejament d'ARP** es poden fer servir per realitzar els anomenats *atacs man-in-the-middle*.
- Amb la tècnica del **falsejament de** DNS es pot realitzar un tipus d'atac anomenat *desencaminament (pharming)*, en el qual la màquina atacada, quan sol·licita una adreça IP determinada al seu servidor DNS (per exemple, www.el_meu_banc.es), rep una adreça falsa.

Sistemes de detecció d'intrusos

- Els sistemes de detecció d'intrusos (IDS) **monitoren els continguts** del flux d'informació de la xarxa a la **recerca i rebuig de possibles atacs.**
- Poden combinar **maquinari i programari**, i normalment s'instal·len en els dispositius més externs de la xarxa, com ara tallafocs. Admeten diferents tipus de classificacions:
- Segons la **font de la informació**
  - **Basats en xarxa** (*Network IDS*). Monitoren una xarxa a la recerca d'elements que puguin indicar un atac contra algun dels seus components. Són elements passius que no injecten trànsit a la xarxa (actuen en mode promiscu, escoltant tot el trànsit de xarxa).
  - **Basats en màquina** (*Host IDS*). Monitoren una màquina (o diverses, en el qual cas s'anomenen *multihost*) i recullen dades del sistema operatiu (per exemple, el registre d'esdeveniments). Consumeixen recursos de la màquina en la qual s'han instal·lat. Com que treballen amb el sistema operatiu i el sistema de fitxers de la màquina, poden detectar atacs que els IDS de xarxa no detecten.
  - **Basats en aplicacions**. Monitoren els fitxers de registre d'una aplicació específica per detectar activitats sospitoses (per exemple, els *logs* d'un servidor de l'FTP). Consumeixen molts recursos de la màquina.

Sistemes de detecció d'intrusos

- Segons el **tipus d'anàlisi** que realitzen
  - **Basats en firmes**. L'anàlisi s'efectua cercant firmes (patrons d'atac) que permetin identificar un atac ja conegut. Aquests tipus de IDS requereixen que les bases de dades de firmes siguin actualitzades constantment.
  - **Basats en anomalies**. En aquest cas, l'IDS cerca comportaments anòmals a la xarxa (un escaneig de ports, paquets mal formats…).
- Segons el **tipus de resposta de l'IDS**:
  - **Resposta passiva**. L'IDS enregistra l'alarma generada o avisa el responsable.
  - **Resposta activa**. Aquest IDS, a més de les accions de la resposta passiva, té capacitat de reacció i pot bloquejar les accions intrusives.

Les xarxes públiques. Seguretat en la connexió.

- Una xarxa pública pot ser usada per qualsevol a un preu molt reduït, està gestionada per una operadora de telecomunicacions i, per tant, la informació que hi viatja és susceptible de ser 'observada' durant el seu trànsit fins al destí. Cal prendre mesures per evitar-ho.
- L'ús de les xarxes públiques requereix l'establiment de relacions de confiança en un entorn gairebé anònim i intangible per definició. Aquesta és la principal motivació de la **signatura electrònica**.
- La **signatura electrònica**, basada en la criptografia de clau pública, permet que un emissor pugui enviar missatges a un receptor complint les tres propietats següents:
  - **Autenticitat**: la signatura d'un missatge per l'emissor permet que el receptor estigui segur de la identitat del remitent.
  - **Integritat**: certesa que el missatge no s'ha modificat durant la transmissió.
  - **No repudi**: l'emissor d'un missatge no pot repudiar o negar que l'ha enviat (per exemple, podria argumentar que l'ha enviat una tercera persona). La inclusió d'una signatura digital evita aquesta possibilitat.