M11 SEGURETAT I ALTA DISPONIBILITAT

Administració de Sistemes Informàtics en Xarxa

IES de l'Ebre

UF2 – Seguretat Activa i Accés Remot

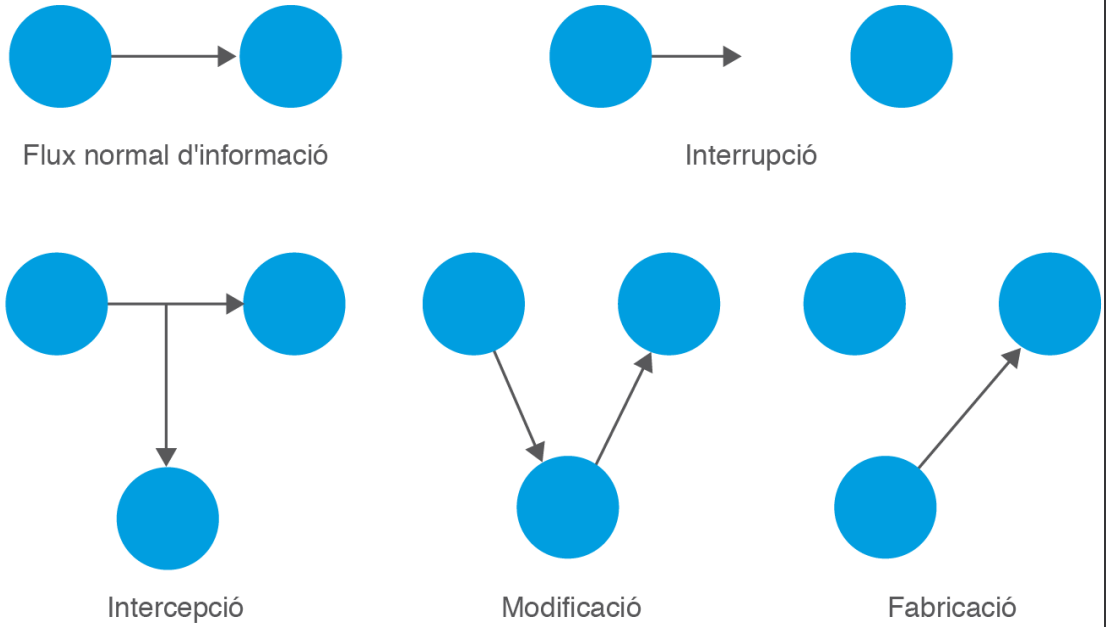
Mecanismes de Seguretat Activa

Introducció

- La protecció de la informació és la conseqüència de **l'aplicació d'un conjunt de mecanismes o estratègies** de seguretat.
- A grans trets, aquestes estratègies han de considerar els **principis** següents:
  - La seguretat ha de ser un **objectiu global**.
  - La seguretat s'ha de dissenyar com quelcom que **és part de l'organització**, tenint en compte tots aquells aspectes que la puguin conformar.
  - El **marc legal** s'ha de considerar, des de l'inici, com una part més del disseny de les polítiques de seguretat.
- Entenem per **seguretat activa** tots aquells mecanismes i mesures (físics i lògics) que permeten prevenir i detectar possibles intents de comprometre els components d'un sistema informàtic.

Sistemes personals. Atacs i contramesures.

- Atacs segons l'objectiu:
  - **Interrupció**: atac contra la disponibilitat en el qual es destrueix, o queda no disponible, un recurs del sistema.
  - **Intercepció**: atac contra la confidencialitat en el qual un element no autoritzat aconsegueix l'accés a un recurs. Aquest tipus d'atac no es limita a possibles usuaris que actuïn com a espies en la comunicació entre emissor i receptor.
  - **Modificació**: atac contra la integritat en el qual, a més d'aconseguir l'accés no autoritzat a un recurs, també s'aconsegueix modificar-lo, esborrar-lo o alterar-lo de qualsevol manera.
  - **Fabricació**: atac contra la integritat en el qual un element aconsegueix crear o inserir objectes falsificats en el sistema (per exemple, afegir de manera no autoritzada un nou usuari i la contrasenya corresponent al fitxer d'usuaris).



Sistemes personals. Atacs i contramesures.

- Atacs segons la seva forma:
  - **Atacs passius:** l'atacant no modifica ni destrueix cap recurs del sistema informàtic, simplement l'observa, normalment amb la finalitat d'obtenir alguna informació confidencial.
  - **Atacs actius:** l'atacant altera o destrueix algun recurs del sistema. Un intrús podria causar problemes molt seriosos, com els que exposem a continuació:
    - **Suplantació d'identitat.**
    - **Re-actuació**: un o diversos missatges legítims són interceptats i reenviats diverses vegades per produir un efecte no desitjat.
    - **Degradació fraudulenta del servei**: l'espia evita el funcionament normal dels recursos del sistema informàtic.
    - **Modificació de missatges**: es modifica una part del missatge interceptat i es reenvia a la persona a qui anava adreçat originalment.

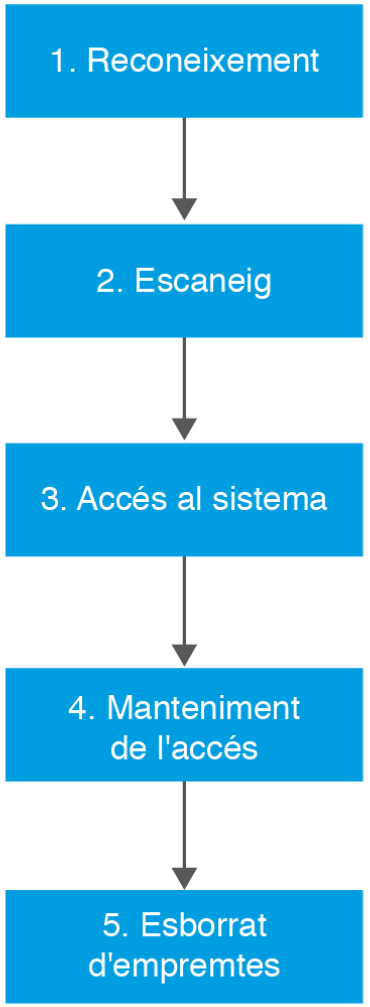
Sistemes personals. Atacs i contramesures.

- Atacs segons el tipus d'atacant:
  - Cal tenir present que un atac pot provenir tant de l'interior de la xarxa (***insiders***) com de l'exterior (***outsiders***).
  - Acostumem a pensar que la gran majoria dels atacs provenen de l'exterior de l'organització i que són escassos, però les estadístiques demostren tot el contrari. La realitat és que:
    - Els atacs **externs són més nombrosos** que els interns.
    - El percentatge d'**èxit** en els atacs **interns és més elevat**.
    - El **dany** causat per atacs **interns és molt més gran** que el provocat per atacs externs.
  - Els principals **possibles atacants** d'un sistema informàtic són:
    - **Personal de la mateixa organització**. No cal que aquests atacs siguin intencionats (tot i que, quan ho són, són els més devastadors que es poden produir); poden ser accidents provocats pel desconeixement del personal
    - **Antics treballadors.**
    - **Intrusos informàtics** (***hackers***). Els intrusos informàtics normalment duen a terme atacs passius destinats a obtenir informació confidencial (per exemple, un examen d'un curs) o amb la finalitat de posar-se a prova per obtenir el control del sistema atacat. No oblidem, però, que aquesta activitat és un **delicte** de danys recollit en el Codi Penal.
    - **Intrusos remunerats**. En aquest cas, els intrusos estan perfectament organitzats (poden estar en diferents localitzacions geogràfiques fins i tot) i ataquen de manera coordinada una entitat determinada.

Anatomia dels atacs.

- Els atacs informàtics solen constar d'un cicle de cinc fases:
  1. Reconeixement
  2. Escaneig
  3. Accés al sistema
  4. Manteniment accés
  5. Esborrat empremtes

- El coneixement del funcionament intern d'un atac informàtic ens ajuda a avançar-nos als esdeveniments i preveure activitats que podrien comprometre el nostre sistema informàtic.



Anatomia dels atacs. Reconeixement.

- Aquesta primera fase té caràcter **preparatori** i consisteix en la **recopilació**, per part de l'atacant, de tota la **informació** possible del sistema que pretén comprometre.
- L'atacant pot utilitzar diverses tècniques a l'hora de reconèixer un sistema. Per exemple, pot emprar **enginyeria social o *trashing***, amb la finalitat d'aconseguir informació valuosa per accedir al sistema.
- Altres tècniques pròpies d'aquesta fase són:
  - Fer **recerques** a Internet.
  - **Capturar** el trànsit de xarxa (***sniffing***).
  - Utilitzar l'ordre **whois** per esbrinar dades relatives al sistema que volem investigar.
    - https://www.whois.com/whois/
    - https://whois.icann.org/es

Anatomia dels atacs. Exploració.

- L'atacant utilitzarà tota la informació obtinguda en l'apartat anterior per **sondejar el sistema** que pretén atacar i detectar una **vulnerabilitat** (o vulnerabilitats) específica, **que pugui aprofitar** per accedir al sistema.
- Es pretén obtenir informació dels **comptes d'usuari**, de les versions del **sistema operatiu** i de les aplicacions, així com els ports oberts. Moltes eines d'administració de sistemes es poden emprar en aquesta fase amb finalitats il·lícites, com per exemple els escàners de xarxa o de ports (***nmap).***
- Hi ha moltes més eines que es poden emprar en aquesta fase. D'entre elles, podríem destacar, per exemple, les ordres ***tracert*** en entorns Windows o ***traceroute*** en entorns Linux/Unix, per esbrinar els canvis de xarxa que realitzen els paquets per la xarxa fins arribar a la seva destinació.

Anatomia dels atacs. Accés.

- Aquesta és la fase en la qual es du a terme **l'atac de manera efectiva**, **aprofitant les vulnerabilitats** localitzades a la fase anterior.
- Sol iniciar-se amb les tècniques de **crackeig de contrasenyes**, les quals es poden realitzar:
  - **Online**, és a dir amb tests en viu amb eines especials (Hydra) que fan servir la tècnica de diccionari.
  - **Offline**, obtenint els arxius on s'emmagatzemen les contrasenyes encriptades i recorrent a tècniques de diccionari, força bruta o criptoanàlisi, amb eines específiques (Cain i Abel).
- És tracta d'una fase **complicada**, ja que s'ha de evadir els **Firewalls**, realitzar evasió **d'IDS**(Intrusion Detection System)**, IPS**(Intrusion Prevention System) i **Honeypots** per realitzar la penetració. Es fan servir eines com ara **007 Shell, ICMP Shell o AckCmd**, per tenir èxit.

Anatomia dels atacs. Manteniment de l'Accés.

- Una vegada l'intrús ha obtingut l'accés al sistema, intentarà **preservar la possibilitat** d'efectuar nous accessos en el futur.
- En aquesta tasca l'ajudaran diversos programes de **codi maliciós**, com els **cavalls de Troia i els *rootkits***.
- No és només la possibilitat de causar danys evidents al sistema el que ens ha d'inquietar; **l'atac també pot servir** per:
  - Instal·lar ***malware*** que monitori les accions que estem fent (*keylogger*).
  - **Capturar** tot el trànsit de la xarxa (*sniffing*).
  - Instal·lar un FTP de **contingut il·lícit**.
  - Utilitzar el sistema atacat com a **plataforma per atacar** altres sistemes informàtics.

Anatomia dels atacs. Manteniment de l'Accés.

- Els concepte de **rootkit** inclou **root** (de màxims privilegis) i **kit** (conjunt d'eines o programes) i fa referència a eines informàtiques emprades normalment amb finalitats malicioses que permeten **l'accés il·lícit al sistema** per part d'un atacant remot.
- Fan servir tècniques per **ocultar la seva presència** i la d'altres processos que puguin estar realitzant accions malicioses sobre el sistema.
- Els *rootkits* són molt perillosos, perquè **cedeixen el control del sistema a l'atacant** remot.
- Poden treballar a tres nivells:
  - **Kernel**: afegeixen codi al nucli del sistema, per a ocultar portes del darrera, mitjançant controladors de dispositius. Son difícils de detectar.
  - **Llibreries**: permeten realitzar crides al sistema, ja que modifiquen llibreries del sistema operatiu. S'utilitzen per a amagar informació de l'intrús i no ser identificat.
  - **Aplicacions**: permeten substituir els binaris de les aplicacions amb falsificacions de troians, que poden modificar el comportament de les aplicacions existent.

Anatomia dels atacs. Esborrat d'empremtes.

- És vital per a l'intrús **esborrar les empremtes** del que ha fet en el sistema.
- Moltes de les accions que ha dut a terme segurament hauran quedat, amb independència del sistema operatiu emprat, **enregistrades en fitxers de registre** (*log*).
- Per evitar ser culpat i que ningú desxifri les tècniques utilitzades per a perpetuar l'atac al sistema els **passos a realitzar** són els següents:

1. **Deshabilitar l'Auditoria** del sistema en cas que estigui activa.
2. **Realitzar l'esborrat de tots els logs** possibles en el sistema i aplicacions compromeses.
3. **Esborrar l'evidència o pistes de les eines utilitzades**, o possibles programes instal·lats, segons l'atac realitzat perquè no puguin rastrejar ni deixar cap pista, es pot usar l'esteganografia per ocultar els arxius usats.