

---

## **RA2. Implantació de mecanismes de seguretat activa**

---

# Índex

|                                                                       |          |
|-----------------------------------------------------------------------|----------|
| <b>1. Atacs i contramesures en sistemes personals</b>                 | <b>1</b> |
| 1.1. Classificació dels atacs . . . . .                               | 1        |
| 1.2. Anatomia dels atacs . . . . .                                    | 2        |
| 1.3. Eines preventives . . . . .                                      | 2        |
| 1.4. Eines pal·liatives . . . . .                                     | 3        |
| 1.5. Actualització de sistemes i aplicacions . . . . .                | 3        |
| 1.6. Seguretat en la connexió a xarxes públiques . . . . .            | 4        |
| 1.7. Pautes i pràctiques segures . . . . .                            | 4        |
| <b>2. Seguretat en la xarxa corporativa</b>                           | <b>5</b> |
| 2.1. Monitoratge del trànsit en xarxes . . . . .                      | 5        |
| 2.2. Seguretat en els protocols de comunicacions sense fils . . . . . | 5        |
| 2.3. Riscos potencials dels serveis en xarxa . . . . .                | 6        |
| 2.4. Intents de penetració . . . . .                                  | 6        |

**Cicle:** Administració de sistemes informàtics en xarxa (ASIX)

**Mòdul:** 0378. Seguretat i alta disponibilitat

## 1. Atacs i contramesures en sistemes personals

### 1.1. Classificació dels atacs

Les amenaces lògiques es poden agrupar segons el seu **objectiu**, el seu **mecanisme de propagació** i el **grau d'interacció humana** que requereixen.

**Segons el mecanisme de propagació (programari maliciós):**

| Tipus                   | Característica principal                                            | Necessita fitxer host? | Es propaga sol?                 |
|-------------------------|---------------------------------------------------------------------|------------------------|---------------------------------|
| Virus                   | S'insereix dins un altre fitxer executable                          | Sí                     | No (cal executar-lo)            |
| Cuc ( <i>worm</i> )     | Programa autònom que explota vulnerabilitats de xarxa               | No                     | Sí                              |
| Troià ( <i>trojan</i> ) | Es fa passar per programari legítim                                 | No                     | No                              |
| Ransomware              | Xifra dades i exigeix un rescat                                     | Variable               | Variable                        |
| Spyware                 | Recull informació sense consentiment                                | No                     | No                              |
| Adware                  | Mostra publicitat no desitjada                                      | No                     | No                              |
| Rootkit                 | Ocultia la seva presència modificant el nucli o binaris del sistema | No                     | No                              |
| Keylogger               | Registra les pulsacions de teclat                                   | No                     | No                              |
| Botnet (bot/zombi)      | Equip controlat remotament, formant part d'una xarxa de bots        | No                     | Sí (sol combinar-se amb un cuc) |

**Segons el vector d'atac:**

- **Enginyeria social:** phishing, *spear phishing*, *vishing*, *smishing*, pretextos.
- **Atacs a la xarxa:** *sniffing*, *spoofing* (ARP, IP, DNS), *man-in-the-middle* (MITM), *session hijacking*.
- **Atacs de denegació de servei:** DoS i DDoS (volumètrics, d'exhauriment de protocol, de capa d'aplicació).
- **Atacs a aplicacions web:** injecció SQL, *cross-site scripting* (XSS), *cross-site request forgery* (CSRF).
- **Atacs de força bruta i diccionari** contra credencials.
- **Exploits de dia zero (0-day):** aprofiten vulnerabilitats encara no publicades ni apedaçades.

## 1.2. Anatomia dels atacs

La majoria d'atacs dirigits segueixen un procés per fases, sovint descrit amb el model de la **Cadena de mort cibernètica** (*Cyber Kill Chain*, Lockheed Martin):

1. **Reconeixement**: recollida d'informació sobre l'objectiu (OSINT, escaneig de ports amb nmap, enumeració de serveis).
2. **Armamentització**: preparació del programari maliciós o l'exploit.
3. **Lliurament**: entrega de la càrrega (correu amb adjunt, USB, exploit web).
4. **Explotació**: aprofitament d'una vulnerabilitat per executar codi.
5. **Instal·lació**: implantació de persistència (tasca programada, servei, clau de registre).
6. **Comandament i control (C2)**: comunicació amb un servidor remot per rebre ordres.
7. **Accions sobre l'objectiu**: exfiltració de dades, xifratge (ransomware), moviment lateral.

### Anàlisi de programari maliciós en entorns controlats

- **Aïllament de xarxa**: màquines virtuals (VirtualBox/VMware) amb xarxa en mode *host-only* o sense connexió, mai en pont amb la xarxa de producció.
- **Instantànies (*snapshots*)**: permeten tornar a un estat net després de detonar la mostra.
- **Anàlisi estàtica**: inspecció del fitxer sense executar-lo (file, strings, hash amb sha256sum, comprovació a **VirusTotal**).
- **Anàlisi dinàmica**: execució controlada observant el comportament (**Cuckoo Sandbox**, **any.run**), monitoratge de processos (Process Monitor/Process Explorer de Sysinternals), captura de trànsit generat (Wireshark).
- **Honeypots**: sistemes senyal que simulen serveis vulnerables per capturar i estudiar atacs reals en curs (per exemple, **Cowrie** simulant un servei SSH/Telnet).

## 1.3. Eines preventives

### Verificació de l'origen i autenticitat de les aplicacions:

- Descarregar programari només de fonts oficials o repositoris signats.
- Comprovar sumes de verificació: sha256sum fitxer.iso i comparar-la amb la publicada pel fabricant.
- Validar signatures digitals de paquets:
  - Debian/Ubuntu: els paquets .deb es verifiquen automàticament amb les claus GPG del repositori (apt-key/gpg --verify).
  - Windows: comprovar el certificat de signatura de codi (*Authenticode*) fent clic dret → Propietats → Signatures digitals.

### Eines preventives instal·lables:

| Eina                                          | Funció                                      | Plataforma                                          |
|-----------------------------------------------|---------------------------------------------|-----------------------------------------------------|
| Tallafoc (firewall)                           | Filtra trànsit segons regles                | ufw/firewalld, Windows Defender Firewall            |
| Antivirus amb protecció en temps real         | Bloqueja execució de malware conegut        | Windows Defender, ClamAV (mode on-access amb clamd) |
| Control d'aplicacions ( <i>whitelisting</i> ) | Només permet executar programari autoritzat | AppLocker, <b>AppArmor</b>                          |
| Anti-exploit                                  | Bloqueja tècniques d'explotació de memòria  | Microsoft Defender Exploit Guard                    |

## 1.4. Eines pal·liatives

Un cop hi ha sospita o confirmació d'infecció, cal detecció i eliminació:

- **Windows:** Malwarebytes, Microsoft Safety Scanner, Windows Defender Offline (arrencada fora del SO infectat).
- **Linux:**
  - clamscan (ClamAV) per a escaneig sota demanda.
  - rkhunter i chkrootkit per a detecció de rootkits.
  - lynis per a auditoria general de seguretat del sistema.
- **Procediment recomanat davant una infecció:**
  1. Aïllar l'equip de la xarxa (desconnectar cable/Wi-Fi).
  2. Identificar l'abast (altres equips afectats, dades exfiltrades).
  3. Escanejar i eliminar amb eines actualitzades, preferiblement arrencant des d'un mitjà extern net.
  4. Restaurar des de còpia de seguretat si l'eliminació no és fiable (especialment en ransomware).
  5. Canviar credencials i aplicar pedaços abans de reconnectar.
  6. Documentar l'incident (causa arrel, vector d'entrada, lliçons apreses).

```
# Exemple d'escaneig complet amb ClamAV
sudo freshclam                # actualitza la base de signatures
sudo clamscan -r --bell -i /home # escaneig recursiu, només mostra
    ↳ infeccions

# Detecció de rootkits
sudo rkhunter --update
sudo rkhunter --check
```

## 1.5. Actualització de sistemes i aplicacions

La immensa majoria d'atacs exploten vulnerabilitats **ja conegudes i apedaçades**: mantenir el sistema actualitzat és la contramesura més rendible.

- **Linux (Debian/Ubuntu):** actualitzacions automàtiques amb unattended-upgrades.
- **Windows:** Windows Update, o **WSUS** (Windows Server Update Services) en entorn corporatiu per centralitzar i controlar el desplegament de pedaços.
- **Aplicacions de tercers:** gestors com apt, winget o Chocolatey faciliten mantenir actualitzat també el programari que no forma part del sistema base.
- Comprovar l'estat d'actualització:

```
# Debian/Ubuntu  
apt list --upgradable
```

```
# Windows PowerShell  
Get-WindowsUpdate
```

## 1.6. Seguretat en la connexió a xarxes públiques

- **VPN:** xifra tot el trànsit entre el client i un punt de sortida de confiança abans de sortir a una xarxa pública.
- **HTTPS/TLS:** certificat digital del servidor, emès per una **autoritat de certificació (CA)**, que permet xifrar la comunicació i autenticar el servidor.
- **Xifratge asimètric vs. simètric:** TLS combina xifratge asimètric (intercanvi de claus, RSA/ECDHE) amb xifratge simètric (AES) per a les dades de la sessió.
- **Signatura digital:** garanteix integritat i no repudi. Es genera xifrant el resum (*hash*) d'un document amb la clau privada de l'emissor; qui rep el document el verifica amb la clau pública.
- **Bones pràctiques en xarxes públiques (Wi-Fi obertes d'aeroports, cafeteries, etc.):**
  - Desactivar la connexió automàtica a xarxes conegudes.
  - Comprovar que el cadenet/HTTPS és present abans d'introduir credencials.
  - Utilitzar sempre una VPN de confiança.
  - Desactivar el compartiment de fitxers i el descobriment de xarxa mentre s'estigui en una xarxa no fiable.

```
# Comprovar el certificat d'un servidor remot  
openssl s_client -connect exemple.com:443 -showcerts  
  
# Generar un parell de claus i signar un fitxer  
openssl dgst -sha256 -sign clau_privada.pem -out fitxer.sig fitxer.txt  
openssl dgst -sha256 -verify clau_publica.pem -signature fitxer.sig  
↪ fitxer.txt
```

## 1.7. Pautes i pràctiques segures

- Aplicar el principi de **mínim privilegi** (no treballar habitualment com a administrador/root).
- Fer còpies de seguretat regulars i **provar-ne la restauració**.
- Utilitzar l'**autenticació multifactor (MFA)** sempre que sigui possible.
- Bloquejar la sessió en absentar-se de l'equip.
- Desconfiar d'adjunts i enllaços no sol·licitats (formació contra el phishing).
- Segmentar xarxes domèstiques/IoT de la xarxa principal.

## 2. Seguretat en la xarxa corporativa

### 2.1. Monitoratge del trànsit en xarxes

El monitoratge permet detectar comportaments anòmals abans que esdevinguin un incident greu:

- **Captura i anàlisi de paquets:** tcpdump (línia d'ordres) i **Wireshark** (interfície gràfica) per inspeccionar trànsit en temps real o capturat.
- **Flow monitoring:** NetFlow/sFlow per obtenir estadístiques de trànsit agregades sense capturar el contingut sencer.
- **Plataformes de monitoratge d'infraestructura:** **Zabbix** i **Wazuh** permeten centralitzar alertes de trànsit anòmal, ús de CPU/xarxa i esdeveniments de seguretat (SIEM).

```
# Captura bàsica filtrant per host i port
sudo tcpdump -i eth0 host 192.168.1.10 and port 443 -w captura.pcap

# Anàlisi posterior amb Wireshark
wireshark captura.pcap
```

### 2.2. Seguretat en els protocols de comunicacions sense fils

| Protocol | Xifratge                        | Estat de seguretat                                              |
|----------|---------------------------------|-----------------------------------------------------------------|
| WEP      | RC4, IV de 24 bits              | <b>Trencat</b> , no usar mai                                    |
| WPA      | TKIP                            | Obsolet, vulnerable                                             |
| WPA2     | AES-CCMP                        | Segur si la contrasenya és forta; vulnerable a KRACK (apedaçat) |
| WPA3     | AES-GCMP, SAE (substitueix PSK) | Recomanat actualment                                            |

#### Aspectes a avaluar en una auditoria de xarxa sense fils:

- Protocol de xifratge en ús i si està actualitzat.
- **WPS actiu:** vulnerable a atacs de força bruta al PIN; es recomana desactivar-lo.
- Ús de **802.1X/RADIUS** (WPA2/WPA3-Enterprise) en comptes d'una clau precompartida (PSK) en entorns corporatius, per tenir autenticació individual per usuari.
- Ocultació del SSID: no és una mesura de seguretat real (es pot descobrir fàcilment), només redueix la visibilitat casual.
- Filtratge per MAC: fàcilment evitable (suplantació de MAC), útil només com a capa addicional.
- Aïllament de clients (*client isolation*) a les xarxes convidat.

## 2.3. Riscos potencials dels serveis en xarxa

Cada servei escoltant en un port és una possible superfície d'atac. Cal mantenir un **inventari actualitzat** dels serveis actius i tancar tot l'in necessari.

```
# Inventariar ports en escolta al propi equip
sudo ss -tulnp

# Escaneig extern de serveis (amb autorització!)
nmap -sV -p- 192.168.1.0/24
```

- **Principi de superfície mínima:** desactivar/desinstal·lar serveis no utilitzats.
- Revisar periòdicament els serveis arrencats automàticament (`systemctl list-unit-files --state=enabled`).
- Documentar cada servei: propietari, port, versió, motiu pel qual és necessari.
- Relació amb l'inventari d'actius fet amb **GLPI + OCS Inventory**, que permet tenir una visió centralitzada del programari i maquinari desplegat a tota la xarxa.

## 2.4. Intents de penetració

**Tipus de sistemes de detecció/prevenió d'intrusions:**

| Tipus                                      | Descripció                                                       | Exemples                                                   |
|--------------------------------------------|------------------------------------------------------------------|------------------------------------------------------------|
| NIDS ( <i>Network IDS</i> )                | Analitza trànsit de xarxa cercant patrons d'atac                 | Snort, <b>Suricata</b> , Zeek                              |
| HIDS ( <i>Host IDS</i> )                   | Analitza registres i integritat de fitxers d'un equip            | <b>Wazuh</b> , OSSEC, Tripwire                             |
| IPS ( <i>Intrusion Prevention System</i> ) | Com un IDS, però actua bloquejant activament el trànsit maliciós | Suricata en mode <i>inline</i> , Snort amb <i>iptables</i> |

**Segons el mètode de detecció:**

- **Basat en signatures:** compara el trànsit/comportament amb una base de patrons coneguts. Ràpid i fiable contra amenaces conegudes, cec davant d'atacs nous (0-day).
- **Basat en anomalies:** estableix una línia base de comportament "normal" i alerta de desviacions. Pot detectar atacs desconeguts, però genera més falsos positius.

**Detecció d'intents de penetració a la pràctica:**

- **Honeypots:** que permeten observar i registrar les tècniques que fan servir els atacants en un entorn controlat, sense risc per als sistemes reals.
- Correlació d'esdeveniments en un **SIEM** (Wazuh) per detectar patrons com múltiples intents fallits d'inici de sessió (força bruta) o escanejos de ports.
- Revisió de registres (`/var/log/auth.log`, `journalctl`, Event Viewer de Windows) per identificar intents d'accés no autoritzat.

```
# Exemple: comptar intents fallits d'SSH per IP
sudo grep "Failed password" /var/log/auth.log | awk '{print $(NF-3)}'
↪ | sort | uniq -c | sort -nr | head
```

### Versions d'aquest document

- [HTML](#)
- [PDF](#)
- [ODT](#)
- [MD](#)

[Domini Públic \(CC0\)](#)