



ICA1-C038-RA1-PR2

Objectius

- Detectar evidències digitals bàsiques d'un atac en un sistema, utilitzant eines senzilles de Windows o Linux.

Procediment

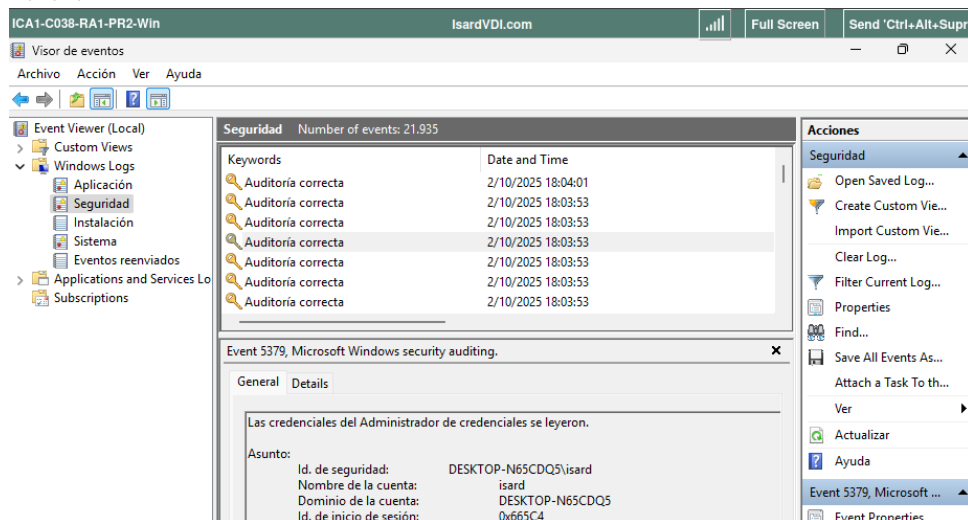
Un usuari sospita que el seu equip ha estat atacat. La vostra missió és actuar com a analistes de ciberseguretat i buscar evidències que confirmin o descartin l'atac.

1. Revisió dels logs del sistema

- 1.1. Buscar esdeveniments d'inicis de sessió fallits repetits i anotar com a evidència: nombre d'intents fallits, data i hora

1.1.1. Windows

1.1.2.



Windows: obrir Visor d'esdeveniments → Registres de Windows → Seguretat.

1.1.3. Linux:

obrir terminal i executar: `sudo tail -n 50 /var/log/auth.log`



```
isard@ubuntu-24:~/Escriptori$ sudo tail -n 50 /var/log/auth.log
2025-10-02T18:54:16.611579+02:00 ubuntu-24 gdm-autologin]: pam_env(gdm-autologin:session): Expandable variables must be wrapped in {} <@valencia:es_ES:es_MX> - ignoring
2025-10-02T18:54:16.612145+02:00 ubuntu-24 gdm-autologin]: pam_unix(gdm-autologin:session): session opened for user isard(uid=1000) by isard(uid=0)
2025-10-02T18:54:16.675387+02:00 ubuntu-24 systemd-logind[733]: New session 1 of user isard.
2025-10-02T18:54:16.721189+02:00 ubuntu-24 (systemd): pam_unix(systemd-user:session): session opened for user isard(uid=1000) by isard(uid=0)
2025-10-02T18:54:17.492669+02:00 ubuntu-24 gdm-autologin]: gkr-pam: couldn't unlock the login keyring.
2025-10-02T18:54:18.559204+02:00 ubuntu-24 gnome-keyring-daemon[1154]: The PKCS#11 component was already initialized
2025-10-02T18:54:18.560355+02:00 ubuntu-24 gnome-keyring-daemon[1338]: discover_other_daemon: 1
2025-10-02T18:54:18.565907+02:00 ubuntu-24 gnome-keyring-daemon[1154]: The Secret Service was already initialized
2025-10-02T18:54:18.566661+02:00 ubuntu-24 gnome-keyring-daemon[1342]: discover_other_daemon: 1
2025-10-02T18:54:18.580401+02:00 ubuntu-24 gnome-keyring-daemon[1344]: discover_other_daemon: 1
2025-10-02T18:54:24.869812+02:00 ubuntu-24 polkitd[651]: Registered Authentication Agent for unix-session:1 (system bus name :1.36 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ca_ES.UTF-8)
2025-10-02T18:55:02.113563+02:00 ubuntu-24 CRON[2168]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-10-02T18:55:02.121974+02:00 ubuntu-24 CRON[2168]: pam_unix(cron:session): session closed for user root
2025-10-02T18:57:21.185849+02:00 ubuntu-24 sudo: pam_unix(sudo:auth): authentication failure; logname=isard uid=1000 euid=0 tty=/dev/pts/0 ruser=isard rhost= user=isard
2025-10-02T18:57:29.657102+02:00 ubuntu-24 sudo: pam_unix(sudo:auth): conversation failed
2025-10-02T18:57:29.657509+02:00 ubuntu-24 sudo: pam_unix(sudo:auth): auth could not identify password for [isard]
2025-10-02T18:57:29.657825+02:00 ubuntu-24 sudo: isard : 1 incorrect password attempt ; TTY=pts/0 ; PWD=/home/isard/Escriptori ; USER=root ; COMMAND=/usr/bin/vim /etc/passwd
```

2. Anàlisi dels processos en execució

2.1. Revisar si algun procés és sospitos (per exemple: un binari desconegut en segon pla).

2.2. Anotar com a evidència: nom del procés, consum de CPU/memòria.

2.2.1. Windows:

Obrir Administrador de tasques.





Nom	Estat	100% CPU	32% Memòria	15% Disc	0% Xarxa
Windows PowerShell (10)		91,3%	243,5 MB	0,1 MB/s	0 Mbps
Windows PowerShell		23,1%	30,5 MB	0,1 MB/s	0 Mbps
Windows PowerShell		23,1%	30,2 MB	0,1 MB/s	0 Mbps
Windows PowerShell		22,5%	54,1 MB	0,1 MB/s	0 Mbps
Windows PowerShell		22,2%	53,9 MB	0,1 MB/s	0 Mbps
Windows PowerShell		0,3%	40,9 MB	0,1 MB/s	0 Mbps
Windows PowerShell		0%	30,8 MB	0 MB/s	0 Mbps
Host de ventana de cons...		0%	0,8 MB	0 MB/s	0 Mbps
Host de ventana de cons...		0%	0,8 MB	0 MB/s	0 Mbps
Host de ventana de cons...		0%	0,8 MB	0 MB/s	0 Mbps
Host de ventana de cons...		0%	0,8 MB	0 MB/s	0 Mbps
WidgetBoard		3,0%	37,4 MB	1,3 MB/s	0 Mbps
Administrador de tasques		1,7%	42,8 MB	0 MB/s	0 Mbps
Antimalware Service Executable		1,0%	210,4 MB	0,1 MB/s	0 Mbps
System		0,7%	0,1 MB	1,5 MB/s	0 Mbps

2.2.2. Linux:
`ps -aux --sort=-%cpu | head -10`

```
isard@ubuntu-24:~/Escriptori$ ps -aux --sort=-%cpu | head 10
head: no s'ha pogut obrir '10' per a llegir: El fitxer o directori no existeix
isard@ubuntu-24:~/Escriptori$ ps -aux --sort=-%cpu | head -10
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
isard        40877 50.0   0.1  12524   5408 pts/0    R+   19:05   0:00 ps -aux --sor
t=-%cpu
isard        3345 15.2   0.0   7360   3480 ?        S    19:04   0:04 bash -c while
(( $(date +%s) < 1759424737 )); do ;; done
isard        3344 15.1   0.0   7360   3576 ?        S    19:04   0:04 bash -c while
(( $(date +%s) < 1759424737 )); do ;; done
isard        1353  4.1   7.8 3922288 313072 ?        Ssl  18:54   0:27 /usr/bin/gnom
e-shell
isard        3301  0.6   1.3 695632 55468 ?        Ssl  19:02   0:01 /usr/libexec/
gnome-terminal-server
isard        1720  0.4   0.7 419676 30236 ?        Sl   18:54   0:03 /usr/libexec/
ibus-extension-gtk3
root          1  0.4   0.3  23152  14208 ?        Ss   18:54   0:03 /sbin/init sp
lash
isard        1543  0.2   0.3 386580 12484 ?        Ssl  18:54   0:01 /usr/bin/ibus
-daemon --panel disable
isard        2086  0.2   1.7 2880280 69880 ?        Sl   18:54   0:01 gjs /usr/shar
e/gnome-shell/extensions/ding@rastersoft.com/app/ding.js -E -P /usr/share/gnome-
shell/extensions/ding@rastersoft.com/app
isard@ubuntu-24:~/Escriptori$
```

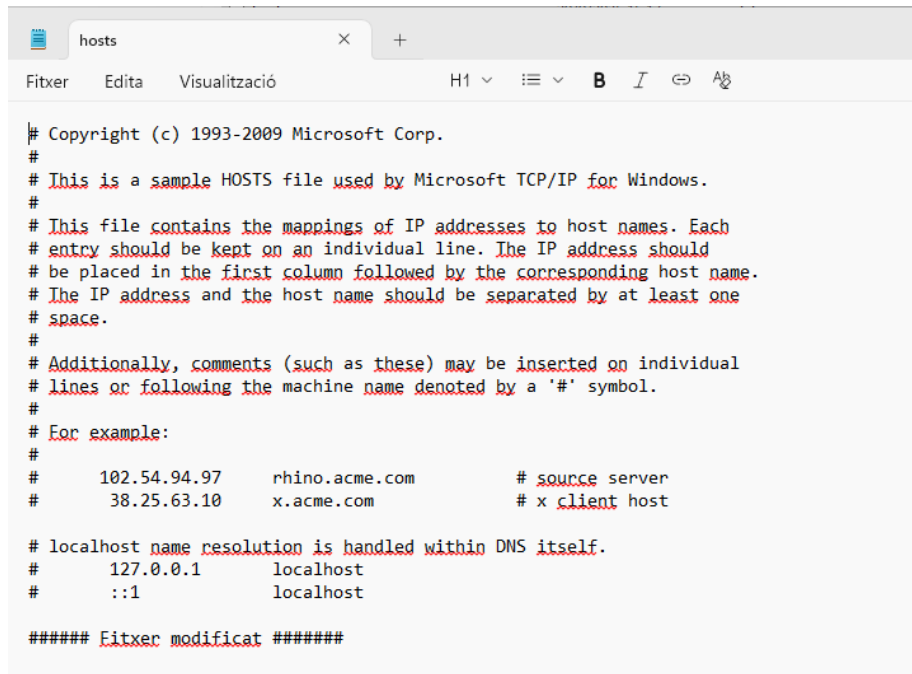
3. Revisió dels fitxers modificats



3.1. Detectar fitxers nous o modificats sense que l'usuari ho recordi.

3.1.1. Windows:

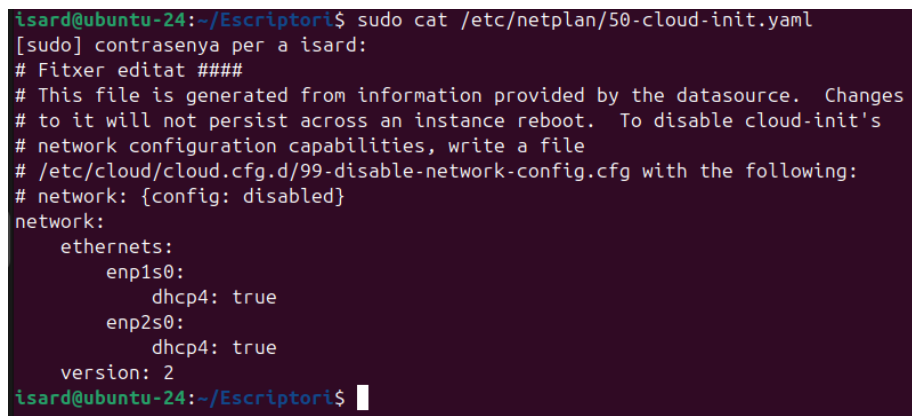
pista: dins de localhost



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com   # source server
#       38.25.63.10      x.acme.com        # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
##### Fitxer modificat #####
```

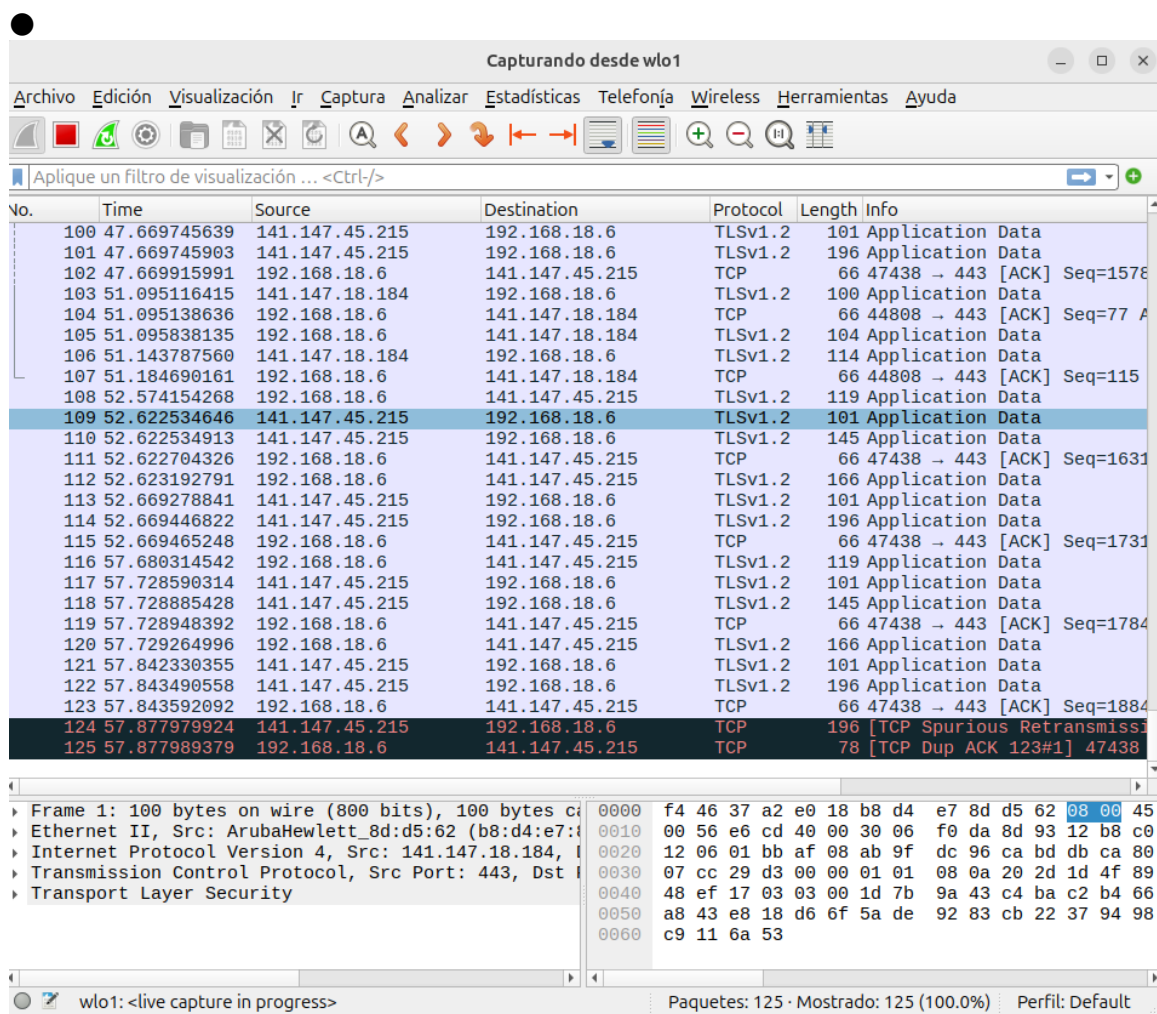
3.1.2. Linux:

pista: netplan



```
isard@ubuntu-24:~/Escriptori$ sudo cat /etc/netplan/50-cloud-init.yaml
[sudo] contrasenya per a isard:
# Fitxer editat #####
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    enp1s0:
      dhcp4: true
    enp2s0:
      dhcp4: true
  version: 2
isard@ubuntu-24:~/Escriptori$
```

4. Anàlisi del tràfic de xarxa



Executar Wireshark i capturar 2-3 minuts de tràfic.

Entrega

Documentació de les evidències

Omple una taula com la següent:

DATA/HORA	TIPUS D'EVIDÈNCIA	RESULTAT TROBAT	POSSIBLE ATAC
02/10/2025	Ataque de fuerza bruta	Denegacioon de cautenticacion	Ataque de fuerza bruta



Badia
del Vallès

Àrea Departament: DEPARTAMENT INFORMÀTICA

Elaborat: Departament d'informàtica

Pàg. 5 de 6

El document vàlid està dipositat en el programa informàtic de gestió documental. Aquest document pot esdevenir obsolet.



02/10/2025	CPU al límit de uso	Un script ejecutado en segundo plano	DDOS
------------	---------------------	--------------------------------------	------

En aquesta pràctica hauràs de confeccionar una memòria amb tots els exercicis proposats a continuació. Per a cada exercici, documenta tots els passos que hagi realitzat amb captures de pantalla, i explicacions, en les que pugui veure's el teu nom i la data. Indica també totes les instruccions que hagi fet servir, amb paràmetres i fitxers.