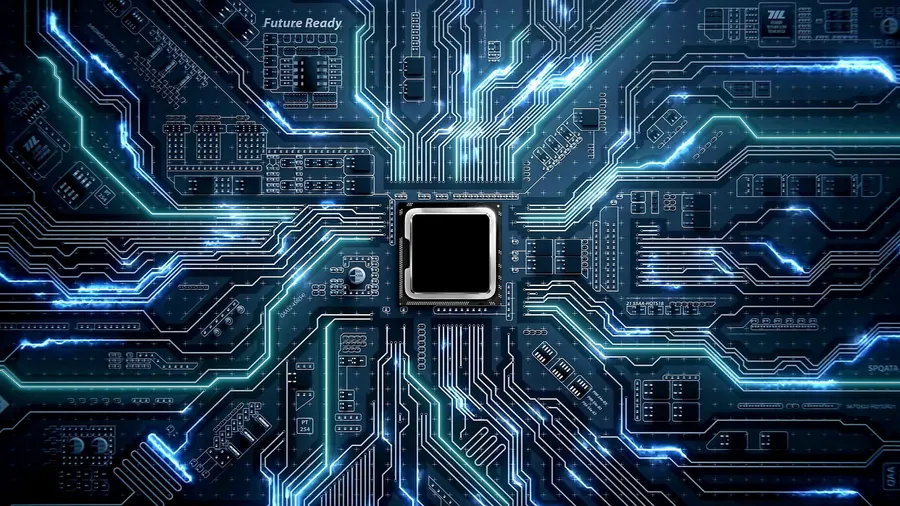
**UNITAT 6. PRÀCTICA 6.**

**CONNEXIÓ I RECURSOS**

**DE RED**

Alumne: David Peñalver Navarro

Professor: Manuel Enguídanos

Assignatura: Sistemes Informàtics

Índex

[Activitats resoltes 3](#_Toc165026248)

[1- Activitat resolta 1 3](#_Toc165026249)

[2- Activitat resolta 2 5](#_Toc165026250)

[3- Activitat resolta 3 10](#_Toc165026251)

[4- Activitat resolta 4 12](#_Toc165026252)

# Activitats resoltes

## 1- Activitat resolta 1

En primer lloc, obrim la nostra máquina virtual i comprovem amb sudo si tenim instal·lat el paquet ‘ufw’. Al tenir-lo instal:lat, comprovem si està activat o no amb ‘ufw status’.

A screenshot of a computer

Description automatically generated

Figura 1. Comprovant que el tenim instal·lat i l‘status.

Com podem vore, l’estat es inactiu, per la qual cosa deurem activar-ho amb ‘sudo ufw enable’:

A screenshot of a computer

Description automatically generated

Figura 2. Activant el tallafocs.

A continuació, llistem la llista d’aplicacions, permitim per exemple i comprovem l’estat de nou verbosament:

A screenshot of a computer

Description automatically generated

Figura 3. Configuració final del tallafocs de Linux.

## 2- Activitat resolta 2

Passem ara a utilitzar Windows. Obrim el Panel de Control i entrem en Firewall de Windows Defender.

A computer screen with a blue background

Description automatically generated

Figura 4. Obrint el Firewall de Windows Defender.

Com podem vore, està connectat per a les rets públiques o invitades i en les privades. No tenim que activar res per tant.

Ara anem a comprovar les regles que té habilitates. Per a això, anem a la configuració avançada, la qual es trova en el menú de l’esquerra. Ací podrem vore les regles d’entrada i d’eixida.

A screenshot of a computer

Description automatically generated

Figura 5. Entrant en les opcions avançades.

Si entrem en cada un dels següent apartats, podem vore les regles d’entrada (Figura 6), les regles d’eixida (7) i les regles de la connexió activa (Figura 8). En la columna de la dreta podem comprovar que estan permeses:

A screenshot of a computer

Description automatically generated

Figura 6. Regles d’entrada.

A screenshot of a computer

Description automatically generated

Figura 7. Regles d’eixida.

A screenshot of a computer

Description automatically generated

Figura 8. Regles de la connexió activa.

En este últim cas, no tenim regles de connexió específiques.

## 3- Activitat resolta 3

Per a Linux, anem a la ruta especificada i, al ver un “ls” enx eixirà el llistat de tots els certificats instal·lats en l’equip:

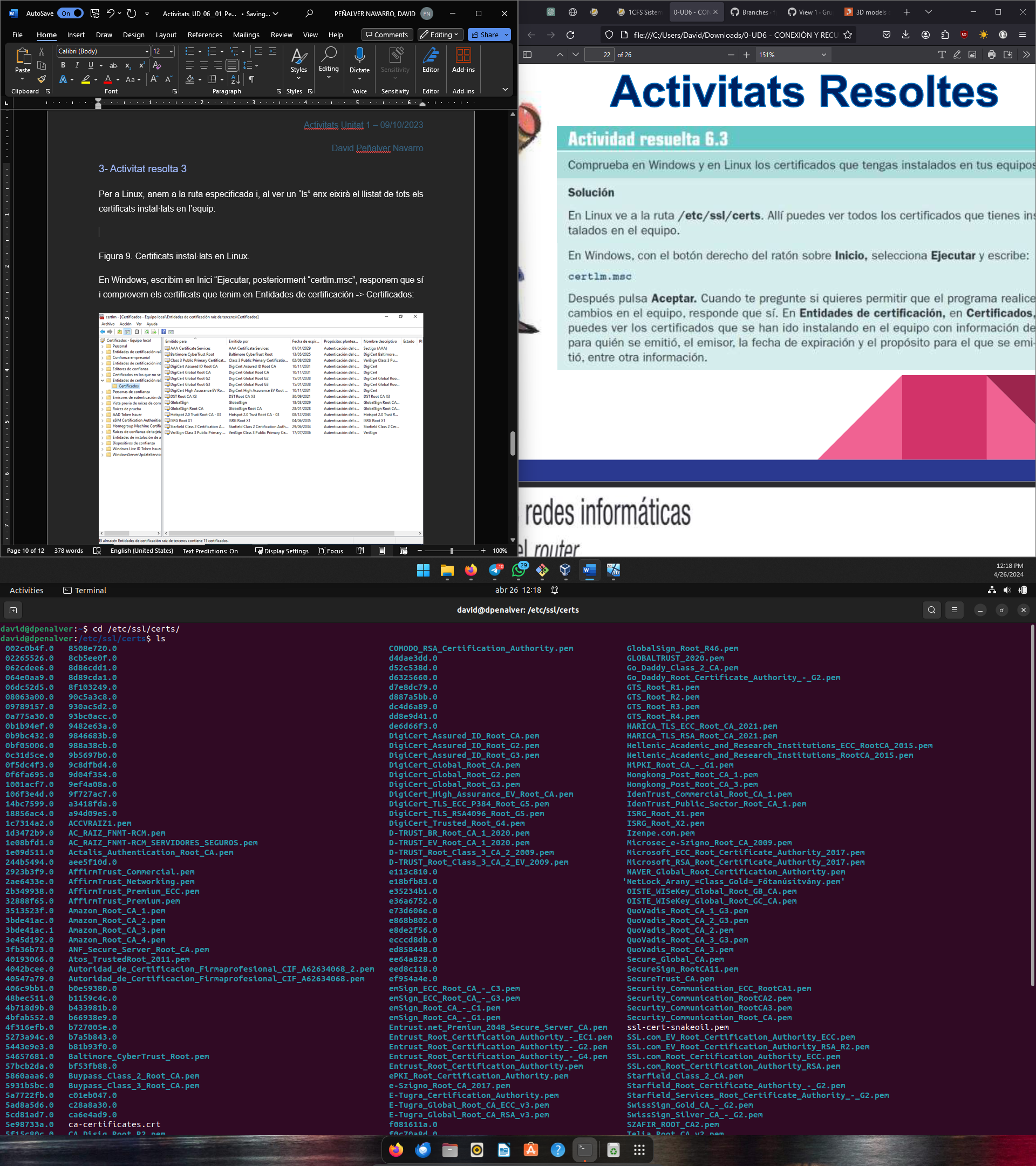


Figura 9. Certificats instal·lats en Linux.

En Windows, escribim en Inici “Ejecutar, posteriorment “certlm.msc”, responem que sí i comprovem els certificats que tenim en Entidades de certificación -> Certificados:

A screenshot of a computer

Description automatically generated

Figura 10. Certificats instal·lats en Windows.

## 4- Activitat resolta 4

En primer lloc, obrim la terminal de Windows per a utilitzar CMD i fiquem “ipconfig”. D’esta manera, podem vore la porta d’enllaç: 172.16.12.254.

A computer screen shot of a computer

Description automatically generated

Figura 11. Resultats de fer “ipconfig”.

A continuació, escrivim “tracert google.es” per a vore la primera línia, que mostra el paquete pel qual ix eixa direcció IP.

A screenshot of a computer

Description automatically generated

Figura 12. Resutlats de fer “tracert google.es”.

Ara passem a Linux. Obrim la terminal i fiquem “ip route” per a vore la porta d’enllaç.

A screenshot of a computer

Description automatically generated

Figura 13. Resultats de fer “ip route”.

Si mirem en la imatge prèvia, en la primera línia podem vore la porta d’enllaç (a on fica el “default via”).

Per a vore la ruta que seguixens els paquets cap a Google, insta·lem en primer lloc el paquet “traceroute” i així podem executar la comanda “traceroute google.es”.

A screenshot of a computer program

Description automatically generated

Figura 14. Resultats de fer “traceroute google.es”.

Finalment, instal·lem “netstat” i, a continuació, comprovem les connexions oberts i els ports d’escolta amb “netstat -an”.

A screenshot of a computer

Description automatically generated

Figura 15. Resultats de fer “netstat -an”.

Com és molt llarga, fiquem la tuberia i el “more” per a paginar tota la informació.

A screenshot of a computer

Description automatically generated

Figura 16. Resultats de fer “netstat -an | more”.