Pràctica 1 - Interfícies de xarxa.
Sessió 4 - Anàlisi de la xarxa.

Alumnes:
Mariona Farré Tapias,
Francesco Oncins Spedo

- Respon a cadascuna de les següents preguntes tot seguint aquesta estructura:
  - Breu raonament de la resposta.
  - Comanda / menú / opció a utilitzar.
    Nota: evitar comandes obsoletes.
  - Fitxers de configuració involucrats, si s'escau.
  - Evidència d'ús.
  - Bibliografia.

apt install tcpdump
apt install nmap
apt install whois

1 - Monitorització (tcpdump).

Per fer les següents preguntes ens hem hagut d'instal·lar el paquet de tcpdump en la màquina virtual, executant:

root@seax1:~# apt install tcpdump

MAN permisos tcpdump -> -Z root (problema de permisos)

- 1.1 Com es pot saber quines interfícies es poden monitoritzar amb tcpdump?

Per poder saber les interfícies que es poden monitoritzar utilitzant el tcpdump, s'ha de fer utilitzant el paràmetre -D que ens retorna una llista de interfícies de xarxa del sistema que podem capturar amb el tcpdump.

Executar: root@seax1:~# tcpdump -D

Fitxers d'evidència:

- 1_1_interficies_monitoritzar.txt

Es poden veure els resultats de l'execució de les comandes anteriors

Font informació: man tcpdump (en comandes a la terminal de Debian)

- 1.2 Com es captura i desa tràfic en fitxers consecutius compatibles amb whireshark i comprimits cada 60 segons?

Per fer una captura de fitxers compatibles amb wireshark els .pcap i cada 60 segons, ho hem de especificar com a paràmetres en l'execució de tcpdump,a qualsevol interfície amb any, també ho podem guardar sota un nom, com ara captura60s.pcap

Executar: root@seax1:~# tcpdump -i any -G 60 -w captura60s.pcap

Si després ho volem comprimir ho podem fer executant:

root@seax1:~# tar -cvzf captures60s.tar captures60s.pcap

Fitxers d'evidència:

- 1_2_captures60s.txt

Es poden veure els resultats de l'execució de les comandes anteriors

Es pot veure fent un ls -la que els fitxers s'han creat correctament, les captures en .pcap: captura60s.pcap i les comprimides: captura60s.tar i es poden veure les mides son de: 4862 bytes la captura i 849 bytes en el tar.

També ho podem mirar utilitzant la comanda: root@seax1:~# tcpdump -r captures60s.pcap i podem veure els continguts de la captura.

Font informació: man tcpdump (en comandes a la terminal de Debian)

- 1.3 Com es captura i desa tràfic en un fitxer compatible amb whireshark d'una mida de 10MB?

Per fer una captura de fitxers compatibles amb wireshark els .pcap i d'una mida de 10MB, ho hem de especificar com a paràmetres en l'execució de tcpdump, a qualsevol interfície amb any, especificant amb -C la capacitat màxima de captura sigui de 10 (mb), també ho podem guardar sota un nom, com ara captura10M.pcap

Executar: root@seax1:~# tcpdump -i any -C 10 -w 'captura10M.pcap'

Fitxers d'evidència:

- 1_3_captures10Mb.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Es pot veure fent un ls -la | grep captura on podem, que els fitxers s'han creat correctament, la captura en .pcap: captura10M.pcap amb una mida de 8724 bytes.
També ho podem mirar utilitzant la comanda: root@seax1:~# tcpdump -r captura10M.pcap i podem veure els continguts de la captura.

Font informació: man tcpdump (en comandes a la terminal de Debian)

- 1.4 Com es captura un cert nombre de paquets?

Per fer una captura de fitxers compatibles amb wireshark els .pcap especificant un cert nombre de paquets, ho hem de especificar com a paràmetres en l'execució de tcpdump, a qualsevol interfície amb any, especificant amb -c la limitació de paquets que pot capturar, en el nostre cas li posem com limit 255 paquets, també ho podem guardar sota un nom, com ara captura255paquets.pcap
Executar: root@seax1:~# tcpdump -i any -c 225 -w 'captura255paquets.pcap'
tcpdump -r captura.pcap

Fitxers d'evidència:

- 1_4_captures255paquets.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Es pot veure fent un ls -la | grep captura on podem, que els fitxers s'han creat correctament, la captura en .pcap: captura255paquets.pcap amb una mida de 4870 bytes.
També ho podem mirar utilitzant la comanda: root@seax1:~# tcpdump -r 'captura255paquets.pcap i podem veure els continguts de la captura.

Font informació: man tcpdump (en comandes a la terminal de Debian)

- 1.5 Com es capturen tots els bytes de dades dels paquets?

Per capturar tots els bytes dels paquets, s'ha d'especificar en l'execució de tcpdump, a qualsevol interfície amb any, especificant amb -s 0 per capturar tots els bytes dels paquets, també ho podem guardar sota un nom, com ara capturatotsb.pcap
Executar: root@seax1:~# tcpdump -i any -s 0 -w capturatotsb.pcap

Fitxers d'evidència:

- 1_5_capturestotsb.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Es pot veure fent un ls -la on podem, que els fitxers s'han creat correctament, la captura en .pcap: capturatotsb.pcap amb una mida de 5344 bytes.
També ho podem mirar utilitzant la comanda: root@seax1:~# tcpdump -r capturatotsb.pcap i podem veure els continguts de la captura.

Font informació: man tcpdump (en comandes a la terminal de Debian)

- 1.6 Com es captura tràfic d'una interfície?

Per capturar el tràfic d'una sola interfície s'ha d'especificar en l'execució de tcpdump, al costat del -i donant el nom a la interfície a captura, també ho podem guardar sota un nom, com ara capturaenp0s8.pcap
Per saber les interfícies es poden capturar podem utilitzar la comanda:
root@seax1:~# tcpdump -D
Que ens retornarà la llista de les interfícies que pot capturar, en el nostre cas triarem la interfície: enp0s8:
Executarem: root@seax1:~# tcpdump -i enp0s8 -w capturaenp0s8.pcap

Fitxers d'evidència:

- 1_6_capturaenp0s8.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Es pot veure fent un ls -la on podem, que els fitxers s'han creat correctament, la captura en .pcap: capturaenp0s8.pcap amb una mida de 1577190 bytes.
També ho podem mirar utilitzant la comanda: root@seax1:~# tcpdump -r capturaenp0s8.pcap i podem veure els continguts de la captura.

Font informació: man tcpdump (en comandes a la terminal de Debian)

- 1.7 Com es captura tràfic d'una adreça MAC concreta?

Per capturar el tràfic d'una sola interfície s'ha d'especificar en l'execució de tcpdump, al costat del -i donant el nom a la interfície a captura, també ho podem guardar sota un nom, com ara capturaenp0s8.pcap
Per saber les adreces mac que podem arribar podem utilitzar la comanda:
root@seax1:~# ip addr
I podem veure totes les interfícies de la màquina amb les seves ips i macs, nosaltres triarem la mac de la interfície enp0s3 que es: 08:00:27:55:d8:44
Per saber les interfícies es poden capturar podem utilitzar la comanda:
Executarem: root@seax1:~# tcpdump ether host 08:00:27:55:d8:4d -w capturamac.pcap

Fitxers d'evidència:

- 1_7_capturamac.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Es pot veure fent un ls -la on podem, que els fitxers s'han creat correctament, la captura en .pcap: capturamac.pcap amb una mida de 24 bytes.
També ho podem mirar utilitzant la comanda: root@seax1:~# tcpdump -r capturamac.pcap i podem veure els continguts de la captura.

Font informació: man tcpdump (en comandes a la terminal de Debian)

- 1.8 Com es captura tràfic d'una adreça IP concreta?

Per capturar tràfic d'una adreça IP concreta ho farem de la següent manera:
root@seax1:~# tcpdump -i any -n host 192.168.1.160 -w 1_8_captura_trafic_IP.pcap
L'opció -i especifica la interfície de xarxa que tcpdump hauria d'escoltar. En aquest cas, any fa referència a totes les interfícies de xarxa disponibles. tcpdump escoltarà en totes les interfícies per capturar els paquets.

L'opció -n impedeix que tcpdump tradueixi les adreces de xarxa a noms (evita la resolució de noms DNS).
L'opció -w (write) s'utilitza per indicar a tcpdump que escrigui els paquets capturats a un arxiu en lloc de mostrar-los a la pantalla.

Per llegir la captura hem executat la següent comanda:
root@seax1:~# tcpdump -r 1_8_captura_trafic_IP.pcap

Fitxers d'evidència:

- 1_8_captura_trafic_IP.txt

Font informació: man tcpdump (en comandes a la terminal de Debian)

- 1.9 Com es captura tràfic entre una adreça IP1 i les adreces IP2 o IP3?

Per capturar tràfic entre una adreça IP1 i les adreces IP2 o IP3 amb tcpdump hem utilitzat la següent comanda:
root@seax1:~# tcpdump -i any -n 'host 10.0.2.2 and 192.168.1.160 or 192.168.1.162' -w 1_9_captura_trafic_IP2.pcap
L'opció -i especifica la interfície de xarxa que tcpdump hauria d'escoltar. En aquest cas, any fa referència a totes les interfícies de xarxa disponibles. tcpdump escoltarà en totes les interfícies per capturar els paquets.
L'opció -n impedeix que tcpdump tradueixi les adreces de xarxa a noms (evita la resolució de noms DNS).
L'opció -w (write) s'utilitza per indicar a tcpdump que escrigui els paquets capturats a un arxiu en lloc de mostrar-los a la pantalla.

Per llegir la captura hem executat la següent comanda:
root@seax1:~# tcpdump -r 1_9_captura_trafic_IP2.pcap

Fitxers d'evidència:

- 1_9_captura_trafic_IP2.txt

Font informació: man tcpdump (en comandes a la terminal de Debian)

- 1.10 Com es captura tràfic IP entre una adreça IP1 i qualsevol altre menys IP2?

Per capturar tràfic IP entre una adreça IP1 i qualsevol altra adreça IP que no sigui IP2 utilitzarem la següent comanda:
root@seax1:~# tcpdump -i any -n 'host 192.168.1.162 and not 10.0.2.2' -w 1_10_captura_trafic_no_IP2.pcap

Per llegir la captura hem executat la següent comanda:
root@seax1:~# tcpdump -r 1_10_captura_trafic_no_IP2.pcap

Fitxers d'evidència:

- 1_10_captura_trafic_no_IP2.txt

Font informació: man tcpdump (en comandes a la terminal de Debian)

- 1.11 Com es captura tràfic IP que provingui o s'adreci d'una certa xarxa?

Per capturar tràfic IP que provingui o s'adreci a una certa xarxa amb tcpdump ho farem amb la següent comanda:
root@seax1:~# tcpdump -i any -n net 192.168.1.0/24 -w 1_11_captura_trafic_xarxa.pcap

Per llegir la captura hem executat la següent comanda:
root@seax1:~# tcpdump -r 1_11_captura_trafic_xarxa.pcap

Fitxers d'evidència:

- 1_11_captura_trafic_xarxa.txt

Font informació: man tcpdump (en comandes a la terminal de Debian)

- 1.12 Com es captura tràfic IP que no provingui o s'adreci d'una certa xarxa?

Per capturar tràfic IP que no provingui o s'adreci a una certa xarxa amb tcpdump:
root@seax1:~# tcpdump -i any -n not net 192.168.1.0/24 -w
1_12_captura_trafic_no_xarxa.pcap

Per llegir la captura hem executat la següent comanda:
root@seax1:~# tcpdump -r 1_12_captura_trafic_no_xarxa.pcap

Fitxers d'evidència:

- 1_12_captura_trafic_no_xarxa.txt

Font informació: man tcpdump (en comandes a la terminal de Debian)

- 1.13 Com es captura tràfic d'un cert port TCP?

Per capturar tràfic d'un cert port TCP:
root@seax1:~# tcpdump port 80 -w 1_13_captura_trafic_port_TCP.pcap

Per llegir la captura hem executat la següent comanda:
root@seax1:~# tcpdump -r 1_13_captura_trafic_port_TCP.pcap

Fitxers d'evidència:

- 1_13_captura_trafic_port_TCP.txt

Font informació: man tcpdump (en comandes a la terminal de Debian)

- 1.14 Com es capturen només les peticions DNS d'una IP a Google (8.8.8.8)?

Per capturar només les peticions DNS d'una IP a Google (8.8.8.8) utilitzem la següent comanda:
root@seax1:~# tcpdump dst port 53 and dst host 8.8.8.8
Aquesta comanda filtra el tràfic per port de destí 53 (port DNS) i per adreça IP de destí 8.8.8.8 (servidor DNS de Google).

Per llegir la captura hem executat la següent comanda:
root@seax1:~# tcpdump -r 1_14_captura_trafic_IP_google.pcap

Fitxers d'evidència:

- 1_14_captura_trafic_IP_google.txt

Font informació: man tcpdump (en comandes a la terminal de Debian)

2 - Identificació d'equips i serveis (nmap).

Per fer les següents preguntes ens hem hagut d'instal·lar el paquet de tcpdump en la màquina virtual, executant:
root@seax1:~# apt install nmap

- 2.1 Com s'escaneja un conjunt d'adreces ip?

Per escanejar un conjunt d'adreces ip utilitzant la eina nmap, s'ha de fer especificant-ho en els paràmetres, es pot fer de vàries maneres, posant una llista d'adreces ip dividides entre espais o especificant amb guionets un rang o a partir d'un fitxer, però aquesta ja té una resposta pròpia a la pregunta 2.2.

Executarem: root@seax1:~#nmap 192.168.1.1-20
Ens retorna la informació de totes les adreces ip disponibles a escanejar dins d'aquest rang

root@seax1:~# nmap 192.168.1.1 192.168.1.7 192.168.1.20
Ens retorna la informació de totes les adreces ip disponibles a escanejar donades aquestes ips.

Fitxers d'evidència:

- 2_1_conjunt_ips.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Al executar root@seax1:~#nmap 192.168.1.1-20, només ens retorna la informació de les següents adreces ips: 192.168.1.1,192.168.1.10, 192.168.1.11,192.168.1.13,192.168.1.14, 192.168.1.20 i 192.168.1.15, això es degut a poden estar apagades o no connectades, tenen un firewall activat, problemes de xarxa o simplement que no s'ha pogut arribar per qualsevol raó externa.

Al executar root@seax1:~# nmap 192.168.1.1 192.168.1.7 192.168.1.20 ,només ens retorna la informació de les següents adreces ips: 192.168.1.1 i 192.168.1.20 això es degut a poden estar apagades o no connectades, tenen un firewall activat, problemes de xarxa o simplement que no s'ha pogut arribar per qualsevol raó externa.

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.2 Com s'escaneja un llistat d'adreces ip d'un fitxer?

Per escanejar un conjunt d'adreces ip utilitzant la eina nmap a partir d'un fitxer, s'ha de fer especificant-ho en els paràmetres posant la opció -iL seguit pel nom del fitxer on estan guardades les ips a escanejar, en el nostre cas es diu: llistat_ips.txt

Executarem: root@seax1:~#nmap -iL llistat_ips.txt
Ens retorna la informació de totes les adreces ip que ha sigut possible escanejar dins del llistat donat.

Fitxers involucrats:

- llistat_ips.txt

On a dins tenim el següent llistat de ips:

192.168.1.1
192.168.1.10
192.168.1.11
192.168.1.13
192.168.1.17
192.168.1.19
192.168.1.20

Fitxers d'evidència:

- 2_2_fitxer_llistat_ips.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Al executar root@seax1:~#nmap -iL llistat_ips.txt, només ens retorna la informació de les següents adreces ips: 192.168.1.1, 192.168.1.10, 192.168.1.11 i 192.168.1.20, això es degut a poden estar apagades o no connectades, tenen un firewall activat, problemes de xarxa o simplement que no s'ha pogut arribar per qualsevol raó externa.

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.3 Com s'escaneja els equips actius d'una xarxa?

Per escanejar els equips actius d'una xarxa utilitzant la eina nmap, s'ha de fer especificant-ho en els paràmetres, posant un -sn i la ip amb la seva màscara seguidament.

Executarem: root@seax1:~#nmap -sn 192.168.1.0/24
Ens retorna la informació de totes les adreces ip disponibles a escanejar dins d'aquesta xarxa.

Fitxers d'evidència:

- 2_3_equips_actius_xarxa.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Al executar root@seax1:~#nmap -sn 192.168.1.0/24 , només ens retorna la informació de les següents adreces ips: 192.168.1.1,192.168.1.10, 192.168.1.11, 192.168.1.13, 192.168.1.14, 192.168.1.20 i 192.168.1.15, això és degut a poden estar apagades o no connectades, tenen un firewall activat, problemes de xarxa o simplement que no s'ha pogut arribar per qualsevol raó externa.

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.4 Com s'escaneja els serveis actius d'una xarxa?

Per escanejar els serveis actius d'una xarxa utilitzant la eina nmap, s'ha de fer especificant-ho en els paràmetres, posant un -sn i la ip amb la seva màscara seguidament.
Executarem: root@seax1:~#nmap -sV 192.168.1.0/24
Ens retorna la informació de totes les adreces ip disponibles a escanejar dins d'aquesta xarxa.

Fitxers d'evidència:

- 2_3_equips_actius_xarxa.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Al executar root@seax1:~#nmap -sn 192.168.1.0/24 , només ens retorna la informació de les següents adreces ips: 192.168.1.1,192.168.1.10, 192.168.1.11, 192.168.1.13, 192.168.1.14, 192.168.1.20 i 192.168.1.15, això és degut a poden estar apagades o no connectades, tenen un firewall activat, problemes de xarxa o simplement que no s'ha pogut arribar per qualsevol raó externa.

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.5 Com s'escaneja normalment els ports TCP i UDP d'un equip?

Per escanejar un de ports tcp i udp utilitzant la eina nmap, s'ha de fer especificant-ho en els paràmetres, posant un -sS i un -sU al principi seguit per -p per especificar els diferents ports, que s'hauran de dividir en U pels ports udp i en T els ports tcp, finalment s'ha de posar la ip de que vols comprovar.
Executarem: root@seax1:~# nmap -sS -sU -p U:53,111,137,T:21-25,80,443,8080 192.168.1.1
Ens retorna la informació de totes les adreces ip disponibles a escanejar dins d'aquesta xarxa.

Fitxers d'evidència:

- 2_5_ports_tcp_udp_equip.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Podem veure els ports donats en els paràmetres, el seu estat i per quin servei s'utilitzen.

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.6 Com s'escaneja la totalitat de ports TCP d'un equip?

Per escanejar tots els ports tcp utilitzant la eina nmap, s'ha de fer especificant-ho en els paràmetres, posant un -p- per especificar tots els ports, no cal posar el protocol tcp ja que es el que esta predefinit, finalment s'ha de posar la ip de que vols comprovar.
Executarem: root@seax1:~# nmap -p- 192.168.1.1
Ens retorna la informació de tots els ports de tcp d'un equip.

Fitxers d'evidència:

- 2_6_totsports_tcp_equip.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Podem veure els ports tcp del equip el seu estat i per quin servei s'utilitzen.

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.7 Com es pot gestionar el nivell de detall de la sortida?

Amb la eina nmap, ofereix diverses opcions per controlar el nivell de detall de la sortida:
-v: Augmenta els detalls de la sortida.
-vv: Encara més detalls.
-oN: Guarda la sortida en un fitxer en format normal.
-oX: Guarda la sortida en un fitxer en format XML.

Executarem: root@seax1:~# nmap -v -oN resultats.txt 192.168.1.1
On tindrem els resultats al fitxer resultats.txt
Executarem: root@seax1:~# nmap -vv -oN resultats2.txt 192.168.1.1
On tindrem els resultats amb més detall al fitxer resultats2.txt

Fitxers involucrats:
- resultats.txt
- resultats2.txt

On estan guardats els resultats amb els diferents detalls en la sortida.

Fitxers d'evidència:
- 2_7_detalls_sortida.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Podem veure els ports tcp del equip el seu estat i per quin servei s'utilitzen.

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.8 Com es pot gestionar la velocitat d'escaneig?

Per gestionar la velocitat d'escaneig de la eina nmap, s'ha de fer especificant-ho en els paràmetres, el min rate especificant la velocitat mínima i amb el max rate la velocitat màxima, finalment s'ha de posar la ip de que vols comprovar.
Executarem: root@seax1:~# nmap --min-rate 100 --max-rate 1000 192.168.1.1

Fitxers d'evidència:
- 2_8_velocitat_escaneig.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Podem veure els ports tcp del equip el seu estat i per quin servei s'utilitzen.

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.9 Com es pot incorporar la traça de la ruta en un escaneig?

Per incorporar la traça de la ruta amb la eina nmap, s'ha de fer especificant-ho en els paràmetres posant --traceroute i la ip de que vols comprovar.
Executarem: root@seax1:~# nmap --traceroute 192.168.1.1

Fitxers d'evidència:
- 2_9_traca_ruta.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Es pot veure que fins la ip 192.168.1.1 només hi ha un salt, però si ho provem amb altres ips com la 192.170.1.1 es poden provocar més salts.

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.10 Com es desa el resultat d'un escaneig en un fitxer?

Per desar el resultat d'un escaneig en un fitxer, hem utilitzat l'opció -oN seguit del nom del fitxer on volem guardar els resultats.

Comanda:
root@seax1:~# nmap 192.168.1.160 -oN 2_11_escaneig_DNS.txt

Fitxers d'evidència:

- 2_11_escaneig_DNS.txt

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.11 Com s'escaneja amb i sense resolució de noms?

Per defecte, nmap realitza la resolució de noms dels hosts que escaneja, per tant si fem un escaneig només amb l'adreça de xarxa, ja escanejarem amb resolució de noms. Per evitar aquest la resolució de noms hem utilitzat l'opció -n.

Comandes utilitzades.
Per escanejar amb resolució de noms:
root@seax1:~# nmap 10.0.2.0/24

Per escanejar sense resolució de noms:
root@seax1:~# nmap -n 10.0.2.0/24

Fitxers d'evidència:

- 2_11_escaneig_DNS.txt

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.12 Com s'escaneja un equip per una determinada interfície?

Per indicar a nmap que utilitzi una interfície de xarxa específica, pots utilitzar l'opció -e. Aquesta comanda farà un escaneig de la IP 10.0.2.2 utilitzant específicament la interfície enp0s3.

Comanda: root@seax1:~# nmap -e enp0s3 10.0.2.2

Fitxers d'evidència:

- 2_12_escaneig_interficie.txt1

Hem utilitzat la ruta per defecte, que en aquest cas, és de la interfície enp0s3.

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.13 Com s'escaneja un equip per un determinat port d'origen?

Per especificar un port d'origen en un escaneig amb nmap, pots utilitzar l'opció --source-port o -g.
Aquesta comanda escanejarà l'adreça 10.0.2.15 utilitzant el port d'origen 22.

Comanda utilitzada: root@seax1:~# nmap –source-port 22 10.0.2.15

Fitxers d'evidència:

- 2_13_escaneig_port_origen.txt

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.14 Com s'escaneja el sistema opeatiu d'un equip?

Nmap pot intentar identificar el sistema operatiu d'un equip amb l'opció -O.
Aquesta comanda intentarà identificar el sistema operatiu de l'equip amb adreça IP 10.0.2.15.

Comanda utilitzada: root@seax1:~# nmap -O 10.0.2.15

Fitxers d'evidència:

- 2_14_escaneig_SO.txt

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.15 Com s'escaneja enviant paquets a nivell IP o Ethernet?

Per escanejar enviant paquets a nivell IP o Ethernet utilitzarem 2 comandes diferents.

Comanda escaneig IP:
root@seax1:~# nmap -Pn 10.0.2.0/24
Si afegim l'opció -Pn diem a nmap que ometi la fase de discovery i escanegi només els ports especificats.

Comanda escaneig ETHERNET:
root@seax1:~# nmap -PR 10.0.2.0/24 –send-eth
Amb l'opció --send-eth forçem l'enviament a nivell Ethernet. I -PR indica a nmap que realitzi un escaneig ARP, només efectiva en xarxes locals.

Fitxers d'evidència:

- 2_15_escaneig_IP_ethernet.txt

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.16 Com s'identifiquen els scripts que es poden utilitzar amb nmap?

Per identificar els diferents scripts que venen amb la comanda nmap, hem d'accedir a la carpeta /usr/share/nmap/scripts/
Si fem un ls de la carpeta, obtindrem el contingut del fitxer d'evidència.

Fitxers d'evidència:

- 2_16_identificacio_scripts.txt

Si volem obtenir més informació d'un script en concret, utilitzarem la següent comanda:
root@seax1:~# nmap –script-help tso-brute.nse

Font informació: man nmap (en comandes a la terminal de Debian)

- 2.17 Com s'executa un script per detectar si una adreça IP té la interfície en mode promiscu?

Si volem detectar si una adreça IP té la interfície en mode promiscu, haurem de trobar, quina és la xarxa de la adreça IP, per exemple fent ip route, veurem les diferents adreces de xarxa de cada interfície, i executar la següent comanda:
root@seax1:~# nmap --script sniffer-detect 10.0.2.0/24

Fitxers d'evidència:

- 2_17_script_interficie_promiscu.txt

Font informació: man nmap (en comandes a la terminal de Debian)

3 - Rendiment de la xarxa (iperf3).

- Pots utilitzar l'opció -t per especificar la duració de la prova (per defecte són 10 segons).
- Pots utilitzar l'opció -p per especificar un port diferent si el port per defecte (5201) no és adequat o està en ús.
- Pots afegir l'opció -u per realitzar proves amb UDP en lloc de TCP, el que pot ser útil per mesurar la pèrdua de paquets i el jitter.

- 3.1 Com es pot avaluar que es pot assolir una certa velocitat de transmissió d'un servidor a un client?

Per avaluar la velocitat de transmissió del servidor al client:

Haurem d'iniciar iperf3 en mode servidor (a la màquina que faci de servidor). Executant la següent comanda:
root@seax1:~# iperf3 -s

El client es connectarà al servidor utilitzant iperf3 amb l'adreça IP del servidor. Comanda:
root@seax2:~# iperf3 -c 192.168.1.160
Aquesta comanda mesurarà la velocitat de transmissió del servidor al client.

Fitxers d'evidència:

- 3_1_velocitat_servidor_client.txt

Font informació: man iperf3 (en comandes a la terminal de Debian)

- 3.2 Com es pot avaluar que es pot assolir una certa velocitat de transmissió d'un client a un servidor?

Per avaluar la velocitat de transmissió del client al servidor, haurem d'iniciar el serivdor de la mateixa manera que a l'apartat anterior:
root@seax1:~# iperf3 -s

I el client tornarà a iniciar una prova de transmissió cap al servidor, però aquesta vegada utilitzant l'opció -R, que indica a iperf3 de realitzar la prova en la direcció inversa.
Comanda a utilitzar:

root@seax2:~# iperf3 -c 192.168.1.160 -R
Això mesurarà la velocitat de transmissió del client al servidor.

Fitxers d'evidència:
- 3_2_velocitat_client_servidor.txt

Font informació: man iperf3 (en comandes a la terminal de Debian)

- 3.3 Com es pot esbrinar la velocitat màxima de transmissió d'un servidor a un client?

Per esbrinar la velocitat màxima de transmissió del servidor al client, hem de seguir el mateix procés que a l'exercici 3.1. Ja que iperf3 per defecte intenta assolir la màxima velocitat de transmissió possible. Amb la opció -t podem dir que l'iperf s'executi durant més temps, nosaltres li hem dit 25 segons, i així la velocitat màxima serà més exacte.

Comanda a executar com a servidor:
root@seax1:~# iperf3 -s

Comanda a executar com a client:
root@seax2:~# iperf3 -c 192.168.1.160 -t 25

Fitxers d'evidència:
- 3_3_velocitatmax_servidor_client.txt

Font informació: man iperf3 (en comandes a la terminal de Debian)

- 3.4 Com es pot esbrinar la velocitat màxima de transmissió d'un client a un servidor?

Per trobar la velocitat max client-servidor, seguirem el mateix procés que a l'apartat 3.2. L'opció -R invertirà la direcció de la prova per mesurar la velocitat màxima de transmissió del client al servidor. Amb la opció -t podem dir que l'iperf s'executi durant més temps, nosaltres li hem dit 25 segons, i així la velocitat màxima serà més exacte.

Comanda a executar com a servidor:
root@seax1:~# iperf3 -s

Comanda a executar com a client:
root@seax2:~# iperf3 -c 192.168.1.160 -R -t 25

Fitxers d'evidència:
- 3_4_velocitatmax_client_servidor.txt

Font informació: man iperf3 (en comandes a la terminal de Debian)

4 - Informació de l'entitat propietària (whois).

Per fer les següents preguntes ens hem hagut d'instal·lar el paquet de whois en la màquina virtual, executant:
root@seax1:~# apt install whois

- 4.1 Com s'obté informació whois d'una adreça IP des de la línia de comandes?

Per obtenir la informació d'una adreça ip utilitzant la eina whois, és molt fàcil, només cal posar-ho després com a paràmetre de la eina.
En el nostre cas utilitzem la ip 8.8.8.8
Executarem: root@seax1:~# whois 8.8.8.8

Fitxers d'evidència:

- 4_1_whois_adreca_ip.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Ens retorna que la ip 8.8.8.8 és de Google.com

Font informació: man whois(en comandes a la terminal de Debian)

- 4.2 Com s'obté informació whois d'un domini des de la línia de comandes?

Per obtenir la informació d'una domini utilitzant la eina whois, és molt fàcil, només cal posar-ho després com a paràmetre de la eina.
En el nostre cas utilitzarem el domini de google.com
Executarem: root@seax1:~# whois google.com

Fitxers d'evidència:

- 4_2_whois_domini.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Ens retorna de qui es el domini de google.com

Font informació: man whois(en comandes a la terminal de Debian)

- 4.3 Com s'obté l'adreça de xarxa a que pertany una certa adreça IP?

Per obtenir la informació d'una domini utilitzant la eina whois, és molt fàcil, només cal posar-ho després com a paràmetre de la eina.
En el nostre cas utilitzarem el domini de google.com
Executarem: root@seax1:~# whois google.com

Fitxers d'evidència:

- 4_2_whois_domini.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Ens retorna de qui es el domini de google.com

Font informació: man whois(en comandes a la terminal de Debian)

- 4.4 Com s'obté el nom de l'organització a la que pertany una certa adreça IP?

Per obtenir la informació de la organització amb una ip utilitzant la eina whois,

En el nostre cas utilitzarem el domini de google.com
Executarem: root@seax1:~# whois 8.8.8.8 | grep Organization

Fitxers d'evidència:

- 4_4_whois_organitzacio.txt

Es poden veure els resultats de l'execució de les comandes anteriors
Ens retorna el nom de la organització de la ip 8.8.8.8

Font informació: man whois(en comandes a la terminal de Debian)

- Programa un script "info_connect.sh" que proporcioni informació sobre la connectivitat a un equip destí.
  - cal identificar l'equip destí amb 3 paràmetres: adreça IP, port i protocol de transport. Per exmple: ~#./info_connect.sh 147.83.2.135 80/tcp
  - Cal utilitzar el llenguatge bash.
  - Cal que generi un fitxer de sortida anomenat "log_connect.log".
  - Cal que proporcioni la mateixa informació de l'equip on s'executi, com a l'exemple aportat.
  - Cal que contempli la possibilitat d'existència de múltiples interfícies Ethernet o Wi-Fi.
  - Cal que diferenciï un valor nul de no obtenir el valor.
  - Cal utilitzar les comandes de les preguntes anteriors.
  - Cal que maqueti la informació com a l'exemple aportat.

- Aspectes a tenir en compte.
  - Robustesa
    - Verificar programari necessari (paquets, rutes, etc).
    - Verificar condicions de contorn (usuari, sistema operatiu, etc).
    - Verificar paràmetres d'entrada (interfície, protocol, número de port, etc).
  - Usabilitat
    - Interacció de l'usuari amb el programari.
    - Informació cap a l'usuari.
    - Seguiment de l'evolució de les accions.
    - Maquetació dels resultats.
  - Fiabilitat
    - Interacció amb el sistema operatiu.
    - Coherència dels resultats.
    - Implementació en bash (shellcheck).

- Lliura els resultats mitjançant Atenea (2 fitxers).
  - Fitxer 1: Informe de la pràctica p1_s4_cognom1_nom.txt.
  - Fitxer 2: Script i sortides de les proves necessàries per justificar els resultats, tot encapsulat en el fitxer p1_s4_cognom1_nom.zip.

- Recomanació de comandes més utilitzades.
  - awk case cat column curl dhclient dig echo for grep hostname if ifdown ifup ip ls lspci lsusb mktemp nano paste ping printf reboot sed service sort udevadm uniq
---