1 ASIX

**MÒDUL 16: CIBERSEGURETAT I HACKING ÈTIC**

ACTIVITAT 1 : Scanning and Enumeration (I)

línea horizontal

# 

**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Sergi Andrés

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

ÍNDEX

[**Exercici 1 – Eines bàsiques per descobrir informació de la xarxa**](#_bogt2rmp6d81) **4**

[a. Per a què serveix la eina NSlookup? Prova el seu funcionament i raona la resposta.](#_hia1ev9tqrw6) 4

[b. Per a què serveix la eina Route? Prova el seu funcionament i raona la resposta.](#_bsfojmkpnwdv) 4

[c. Amb els resultats obtinguts...](#_glqswoxyxezm) 5

[- Quin és el teu servidor DNS?](#_mhv51erheaqa) 5

[- Quina és la teva porta d’enllaç?](#_lyey6sv5lr1a) 5

[**Exercici 2 – Netdiscover**](#_3h1aal886gqp) **6**

[a. Per a què serveix la eina Netdiscover?](#_r4om4emg7xtj) 6

[b. Obre una màquina Kali Linux i 2 màquines client (Windows i Linux) i comprova el funcionament de Netdiscover en mode Actiu, executant-lo des de la màquina Kali.](#_8i5g6p2lmu73) 6

[→Recorda que el mode actiu de Netdiscover fa un flooding de paquets ARP a tota la xarxa, i tots els equips que els reben, contestaran.](#_2b94qhux1xdt) 6

[c. Comprova el funcionament en mode Passiu.](#_ofu61pdcvcdn) 8

[→Recorda que el mode passiu de Netdiscover no envia paquets directament, sinó que escolta el què passa a la xarxa i a partir de les dades que veu, reconstrueix poc a poc els elements de la xarxa.](#_s39z09et1hld) 8

[**Exercici 3 – ARP-Scan**](#_ynt3v5loax5b) **10**

[a. Per a què serveix la eina ARP-Scan?](#_jsj2gyf072bx) 10

[b. En el mateix escenari que en l’exercici anterior (2 clients + Kali Linux) executa ARP-scan i utilitzant Wireshark captura el flooding de paquets ARP que generen a la xarxa.](#_pnimus5n20pe) 10

[c. Raona el resultat obtingut.](#_fxi2do5pxbj0) 10

[**Exercici 4 – Protocol ICMP (ping)**](#_tkpnrqjd5m8s) **11**

[a. Per a què serveix la eina Ping?](#_t5ip42jc8e47) 11

[b. Obre un client Windows i desactiva el Firewall, per assegurar que pugui rebre els paquets ICMP dels Pings (també anomenats paquets à Echo entrants)](#_yynwln5aizb1) 11

[c. Des d’un Kali Linux i utilitzant Wireshark captura els paquets ICMP i ARP que es generen quan Kali Linux envia pings a la màquina Windows. Raona la resposta dels paquets que has capturat.](#_9v1j3nma4gq4) 12

[d. Torna a activar el Firewall de Windows (assegura’t que els pings queden bloquejats) i torna a capturar amb Wireshark els pings que fa Kali Linux cap a la màquina Windows. Comprova que els paquets ICMP enviats per Kali Linux no tenen resposta. Raona la resposta.](#_4h8n1lb5e0n1) 13

[**Exercici 5 – FPING**](#_7w5a74bmxbmg) **15**

[a. Utilitzant la eina fping, busca tots els hosts que hi ha a la xarxa.](#_g5uj40nlu31v) 15

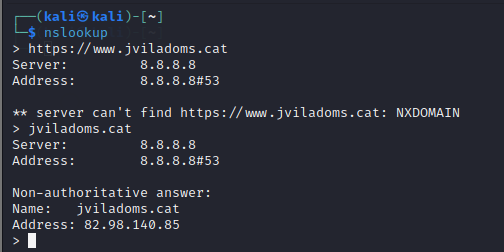
[b. Comprova les diferències quan hi ha el Firewall de la màquina Windows activat i desactivat](#_k892chyd5ntn) 16

# Exercici 1 – Eines bàsiques per descobrir informació de la xarxa

## a. Per a què serveix la eina NSlookup? Prova el seu funcionament i raona la resposta.

L’eina NSlookup serveix per a trobar la direcció IP d’un equip determinat, o també serveix per realitzar una búsqueda DNS inversa, és a dir, trobar el nom d’un domini a través d’una direcció IP.

Obrirem la terminal de kali linux i executarem nslookup, seguidament posarem el nom de la web:

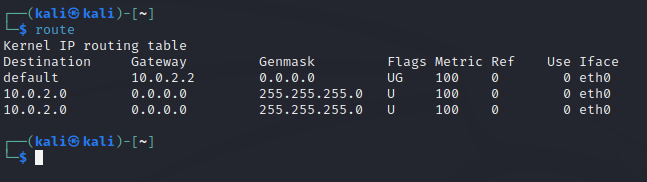


Podem veure que a partir del nom, ha tret la IP de la web.

## b. Per a què serveix la eina Route? Prova el seu funcionament i raona la resposta.

Aquesta eina ens permet manipular les taules dels routers del nostre sistema.

Per tal de comprovar el seu funcionament, haurem d’anar a la terminal (en el meu cas dde Kali Linux) i executar la comanda route:



Ens dirà la porta d’enllaç, la mascara de xarxa, etc.

## c. Amb els resultats obtinguts...

### - Quin és el teu servidor DNS?

El meu servidor DNS es 10.0.2.0

### - Quina és la teva porta d’enllaç?

La meva porta d’enllaç es 10.0.2.2

# Exercici 2 – Netdiscover

## a. Per a què serveix la eina Netdiscover?

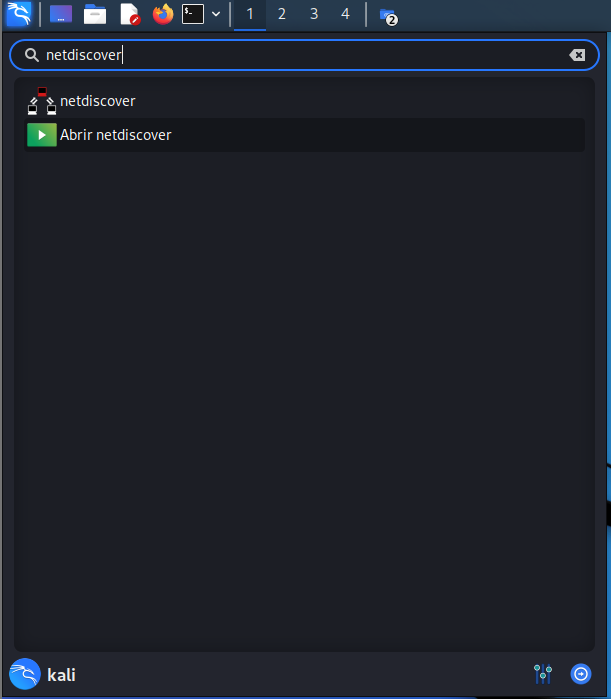
L’eina Netdiscover serveix per reconèixer direccions, està desenvolupada per xarxes inalàmbriques sense un servidor DHCP determinat, quan està fent al wardriving.

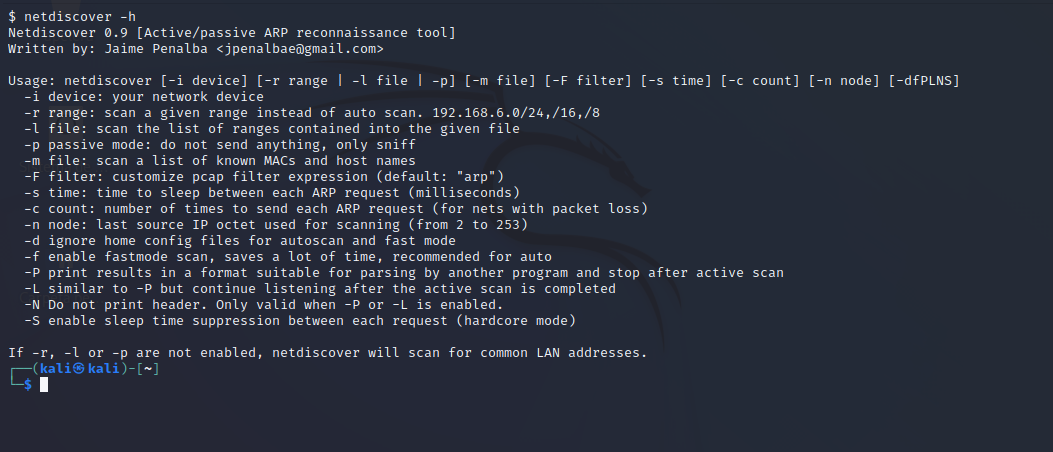
Pot detectar de manera pasiva hosts que estan funcionant, una búsqueda d’aquests enviant solicituts ARP, aquesta eina pot ser emprada per inspeccionar el tràfic en la xarxa ARP, o trobar direccions de xarxa utilitzant el mode de escaneig automàtic, que li permet escanejar per les xarxes locals.

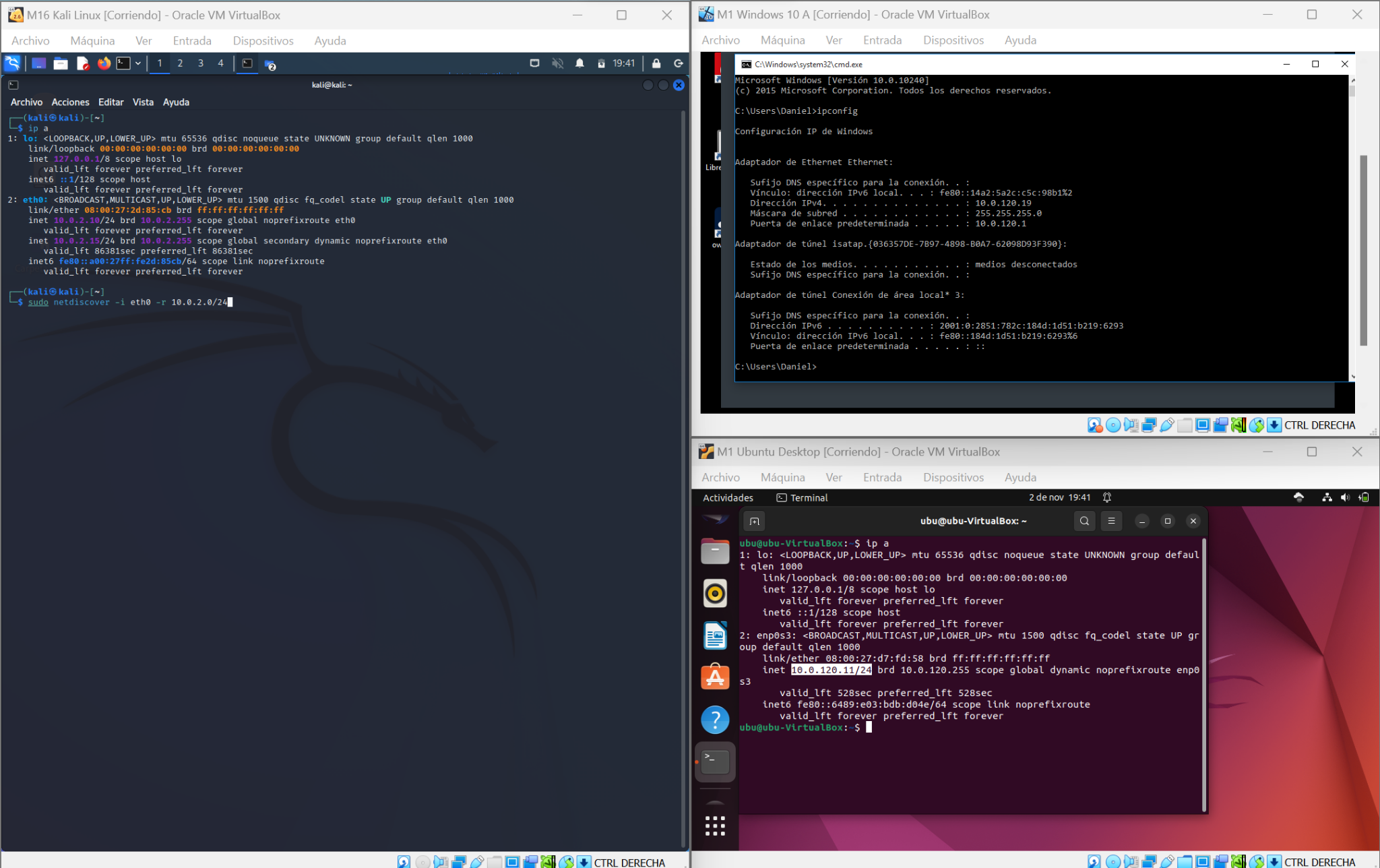
## b. Obre una màquina Kali Linux i 2 màquines client (Windows i Linux) i comprova el funcionament de Netdiscover en mode Actiu, executant-lo des de la màquina Kali.

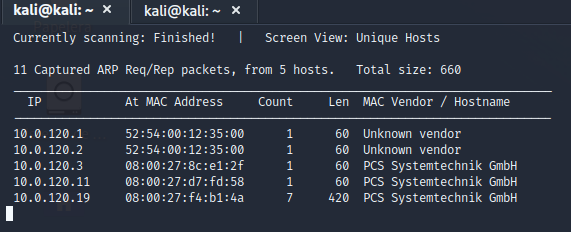
### →Recorda que el mode actiu de Netdiscover fa un flooding de paquets ARP a tota la xarxa, i tots els equips que els reben, contestaran.

Obrirem netdiscover.





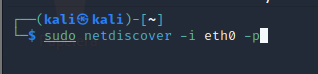




Amb el mode actiu, l’eina Netdiscover ens mostra tot el que esta en la xarxa en aquest precís moment. Cal dir que dos o tres direccions de màquines son per defecte de virtualbox, en aquest cas les que el vendor es unknown

## c. Comprova el funcionament en mode Passiu.

### →Recorda que el mode passiu de Netdiscover no envia paquets directament, sinó que escolta el què passa a la xarxa i a partir de les dades que veu, reconstrueix poc a poc els elements de la xarxa.



### 

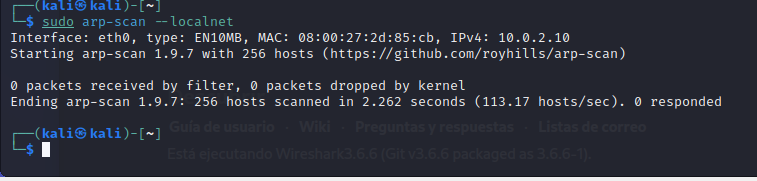
Amb el mode passiu el que fa és que quan es fa un ping o una interacció de dues màquines, l’eina NetDiscover ho detecta i ens mostra la IP, direcció MAC, etc.

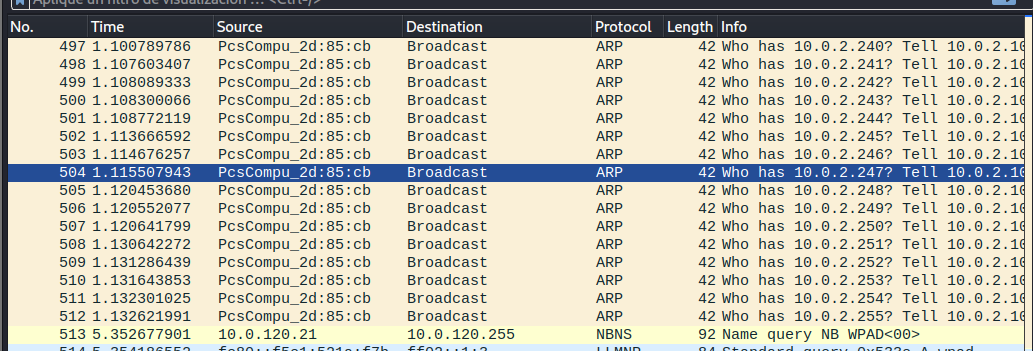
# Exercici 3 – ARP-Scan

## a. Per a què serveix la eina ARP-Scan?

És una eina que s’utilitza en linia de comandes per al descobriment i reconeixement de sistemes. Aquesta eina construeix i envia peticions ARP cap a diverses direccions IP concretes, i mostra les respostes rebudes d’aquestes IP

## b. En el mateix escenari que en l’exercici anterior (2 clients + Kali Linux) executa ARP-scan i utilitzant Wireshark captura el flooding de paquets ARP que generen a la xarxa.





Amb wireshark capturem els paquets arp que s’han fet a la nostra xarxa local

## c. Raona el resultat obtingut.

Podem observar que l’eina wireshark ha capturat diversos paquets del tipus ARP, en un periode curt de temps, que ens diuen la font del paquet, el destí del paquet i informació sobre aquest paquet enviat.

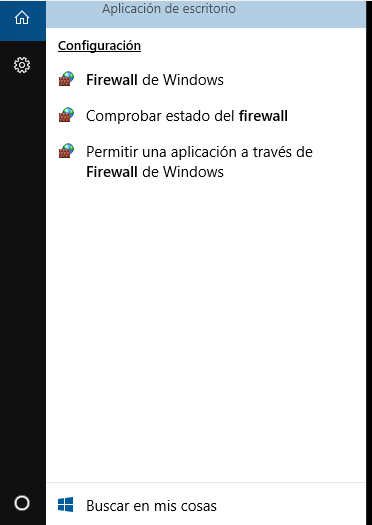
# Exercici 4 – Protocol ICMP (ping)

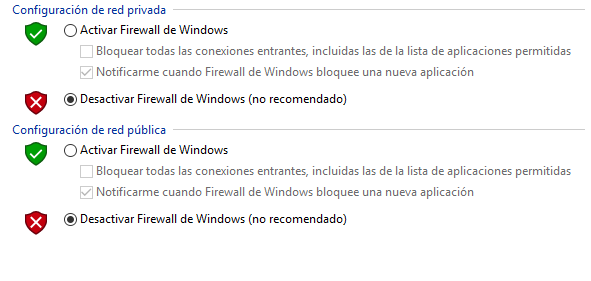
## a. Per a què serveix la eina Ping?

L’eina ping serveix per determinar l’estat d’un host a distància. Al executar-ho, el protocol ICMP envia al host un datagrama per solicitar resposta. El protocol ICMP s’ocupa dels errors en les xarxes TCP/IP.

## b. Obre un client Windows i desactiva el Firewall, per assegurar que pugui rebre els paquets ICMP dels Pings (també anomenats paquets à Echo entrants)

Entrarem a Inicio i escriurem Firewall, i el desactivarem



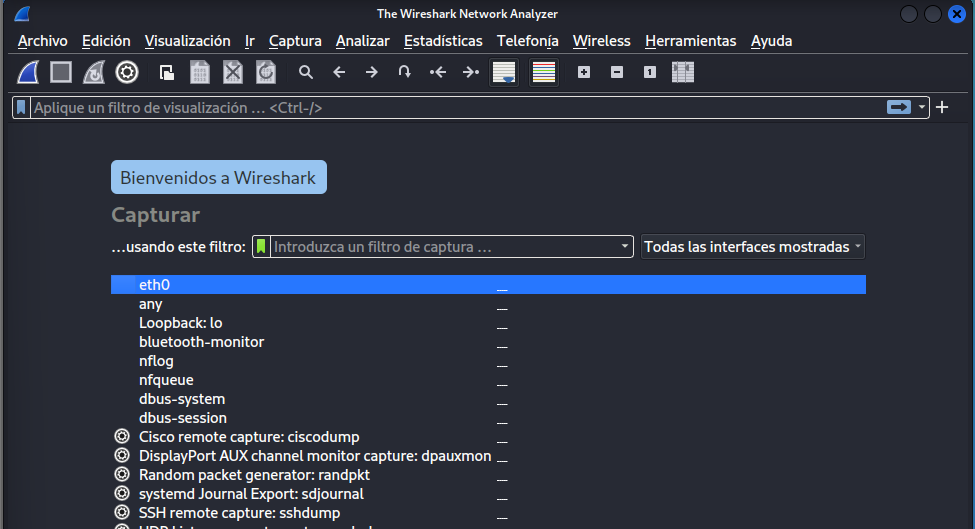


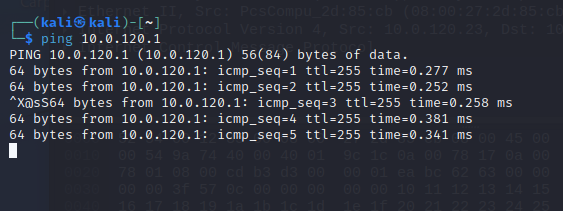
Un cop desactivar, guardarem els canvis.

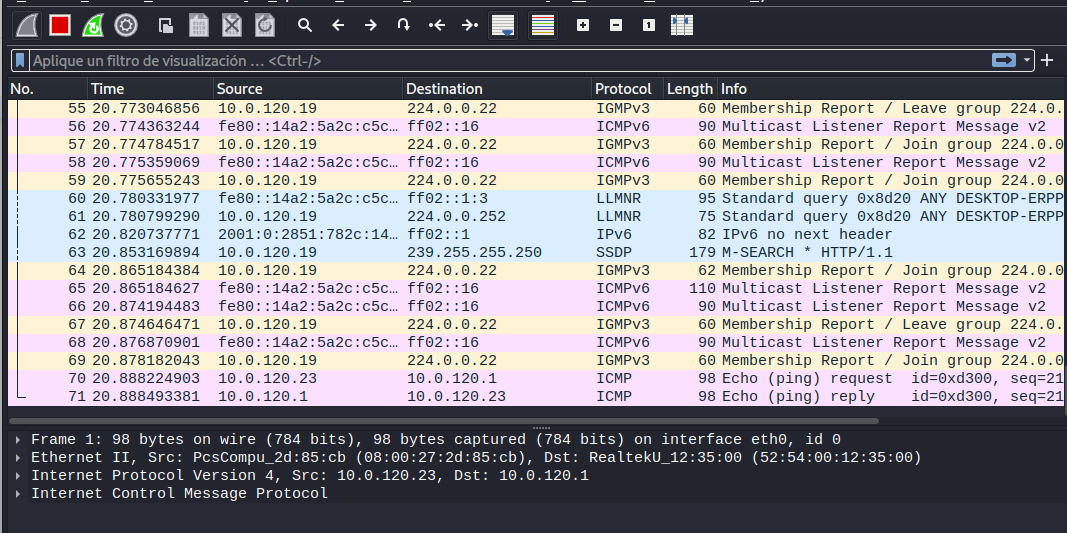
Ara comprovarem que podem fer pings sense cap inconvenient:

## c. Des d’un Kali Linux i utilitzant Wireshark captura els paquets ICMP i ARP que es generen quan Kali Linux envia pings a la màquina Windows. Raona la resposta dels paquets que has capturat.

Obrirem wireshark a kali:

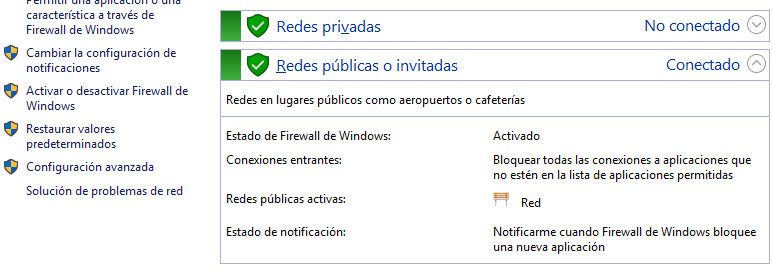
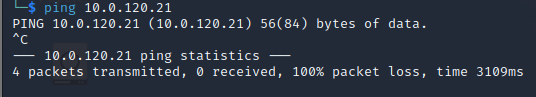


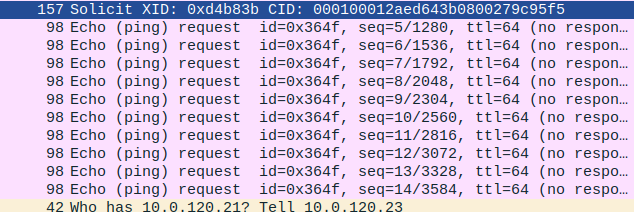




Podem veure en aquesta caputra que ha captat diversos paquets del tipus ICMO, ICMPv3, ICMPv6, etc.

## d. Torna a activar el Firewall de Windows (assegura’t que els pings queden bloquejats) i torna a capturar amb Wireshark els pings que fa Kali Linux cap a la màquina Windows. Comprova que els paquets ICMP enviats per Kali Linux no tenen resposta. Raona la resposta.

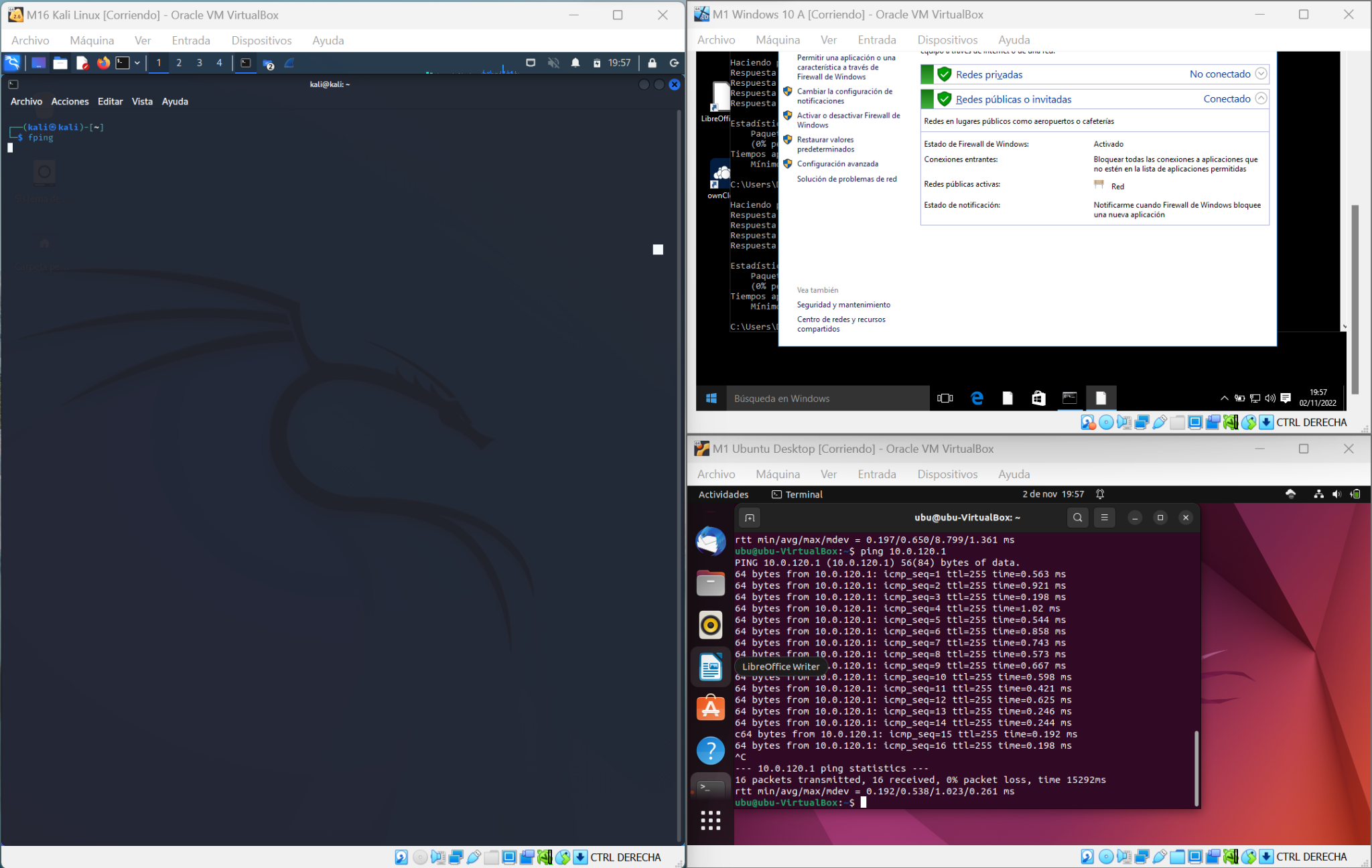


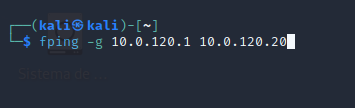
Al fer el ping amb el firewall actiu, podem veure que aquests paquets enviats a la màquina de windows no tenen cap resposta, això es perquè el firewall ha denegat els paquets enviats per la màquina Kali.

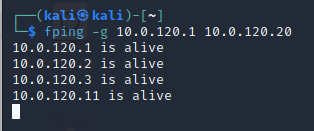
# Exercici 5 – FPING

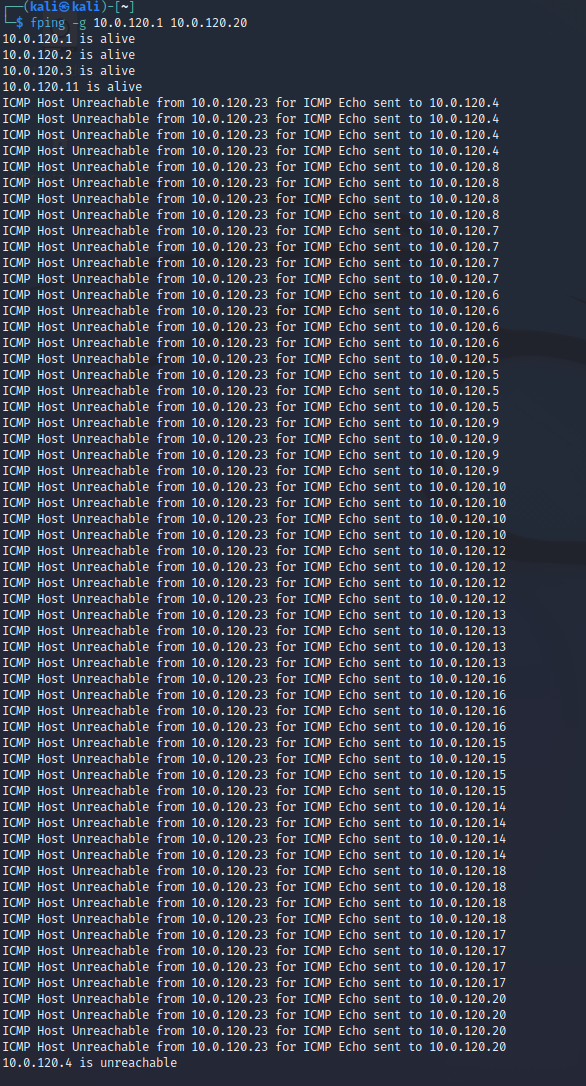
A partir de la màquina Kali Linux i 2 màquines client (Windows i Linux)

## a. Utilitzant la eina fping, busca tots els hosts que hi ha a la xarxa.

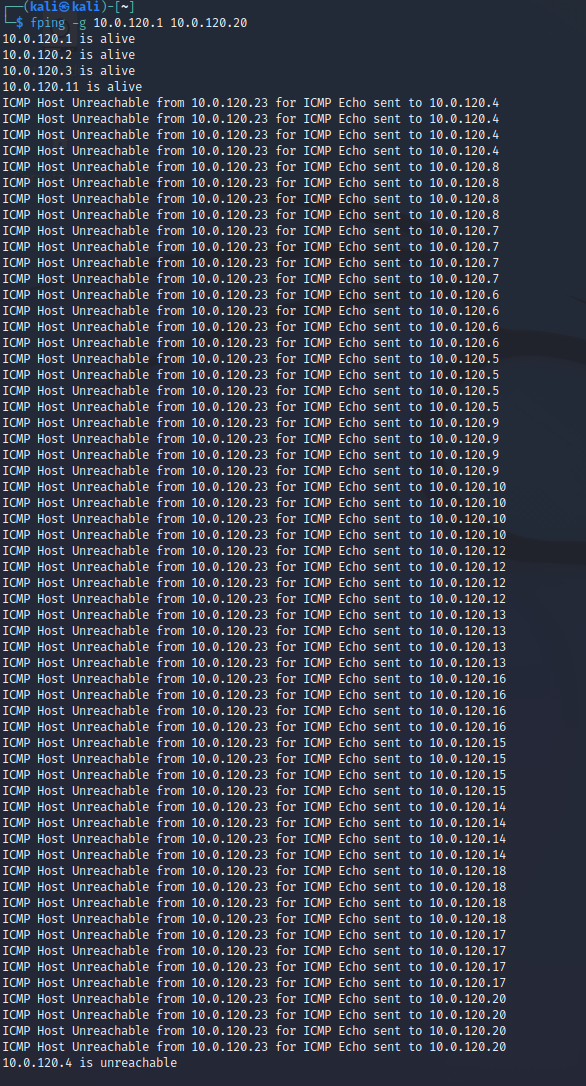




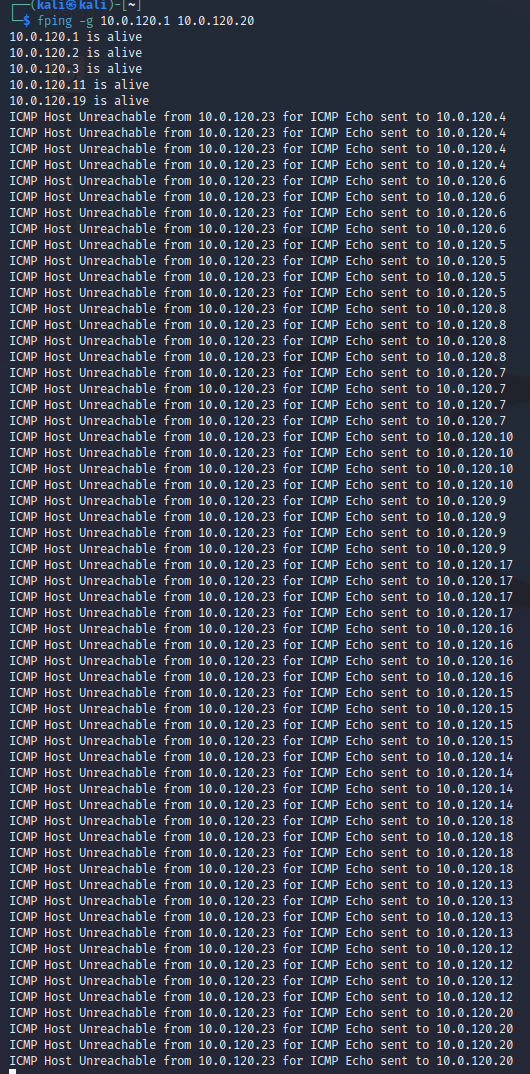




## b. Comprova les diferències quan hi ha el Firewall de la màquina Windows activat i desactivat



En aquesta imatge està activat, i en la següent desactivat



Quan el firewall es desactivat, ens mostra una direcció IP que no era viva abans de desactivar el firewall de windows