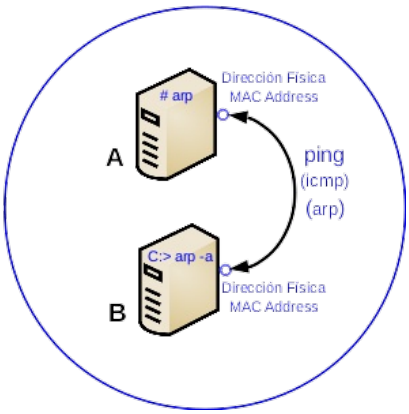
Wireshark: ICMP/ARP

ESCENARIO

Máquinas virtuais:
Rede: 10.0.0.0

Máquina virtual A:	**Máquina virtual B:**
RAM ≥ 2048MB	RAM ≥ 1024MB
CPU ≥ 2	CPU ≥ 1
PAE/NX habilitado	
Rede Interna	Rede Interna
ISO: Kali Live i386	Disco virtual: Microsoft Windows 10
IP/MS: 10.10.10.10/8	IP/MS: 10.10.10.11/8



NOTAS:

(1) SMR_ALUXY -onde XY pode tomar os valores 01, 02, ..., 30 e corresponde ao número de PC que tes asignado.

(2) Debes facer entrega desta exercicio mediante **un arquivo en formato PDF**, noutro formato non será corrixido. O arquivo debe conter respostas/imaxes coa solución dos apartados. O arquivo a entregar na aula virtual terá o nome: **Solucion-RL-Exercicio3_ALUXY.pdf**

Exercicio 3 - Wireshark: ICMP/ARP

Máquina virtual A: Kali i386

1. Configuración da rede:
   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
   root@kali:~# /etc/init.d/network-manager stop #Parar o demo network-manager(xestor de rede) para poder configurar de forma manual a configuración de rede e non ter conflicto con este xestor.
   root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo), NAT(enps03) e interna(enps08).
   root@kali:~# ip addr add 10.10.10.10/8 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 10.10.10.10 e máscara de subrede: 255.0.0.0.
   root@kali:~# ifconfig eth0 10.10.10.10/8 #Comando equivalente ao anteriro, é dicir, configurar a tarxeta de rede interna eth0, coa IP: 10.10.10.10 e máscara de subrede: 255.0.0.0.
   root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de rede: loopback(lo) e interna(eth0).

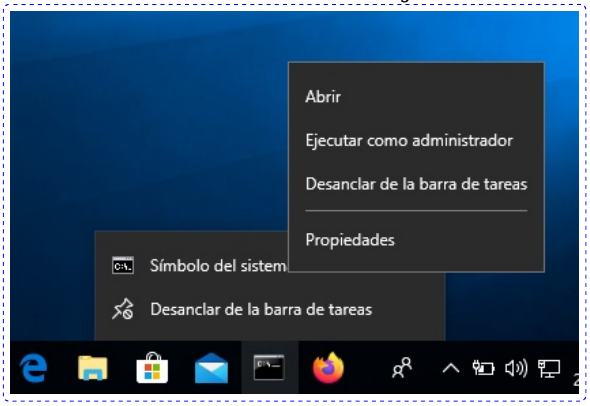
2. Táboa arp:
   root@kali:~# arp #Revisar a táboa arp, é dicir, visualizar a caché arp do sistema: asignación IP coa súa correspondente dirección física (MAC Address).
   root@kali:~# exit #Saír da consola do usuario root, para voltar á consola do usuario kali sen permisos de root
   kali@kali:~$

3. Arrancar Wireshark:
   kali@kali:~$ sudo wireshark & #Lanzar o programa wireshark (sniffer) para poder visualizar o que acontece na rede (protocolos, paquetes). O comando sudo permite executar o programa wireshark con permisos de root(administrador) e o caracter & serve para executar en segundo plano o programa e así devolver o prompt da consola para poder seguir traballando nela.

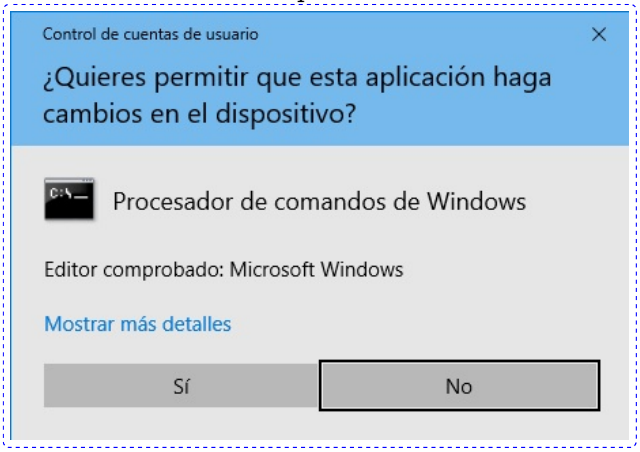
4. Agora minimizamos a máquina virtual A (Kali i386) xa que imos traballar coa máquina virtual B (Microsoft Windows 10).

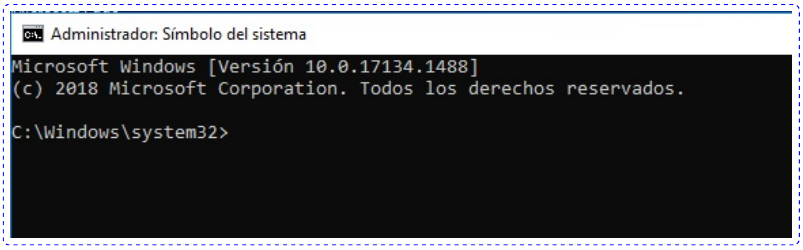
Máquina virtual B: Microsoft Windows 10

5. Configuración da rede:
   a. Arrancar a consola de comandos con permisos de administrador(clic botón dereito icono cmd → clic botón dereito Símbolo del sistema → Ejecutar como administrador):

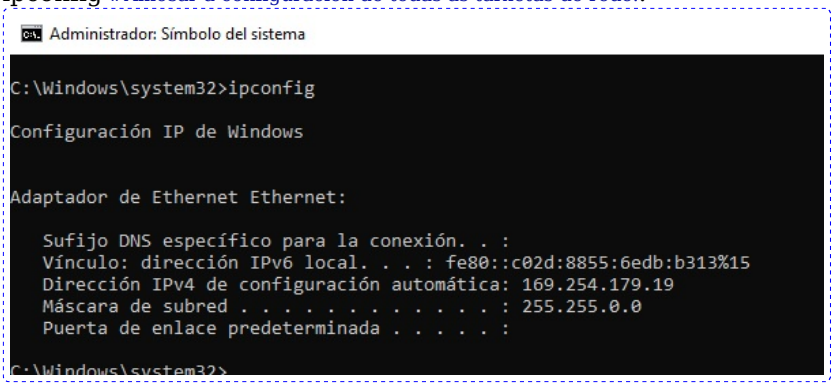


   b. Permitir cambios no dispositivo: Sí



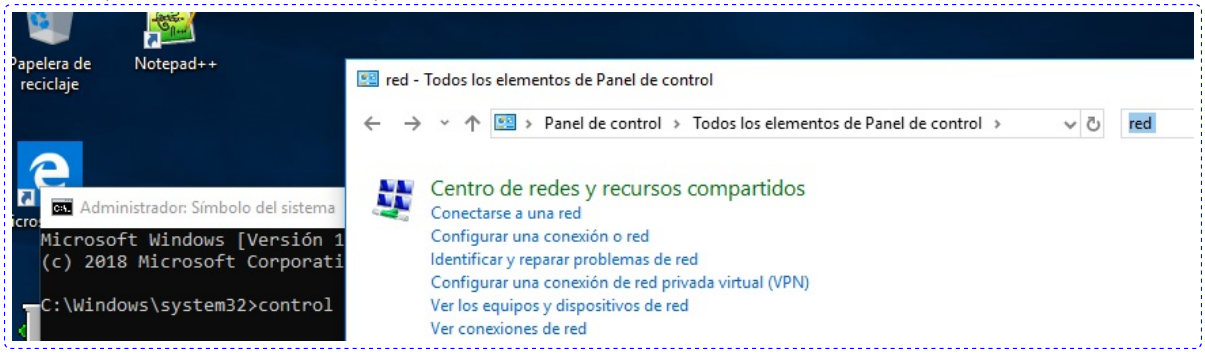


   c. ipconfig #Amosar a configuración de todas as tarxetas de rede..

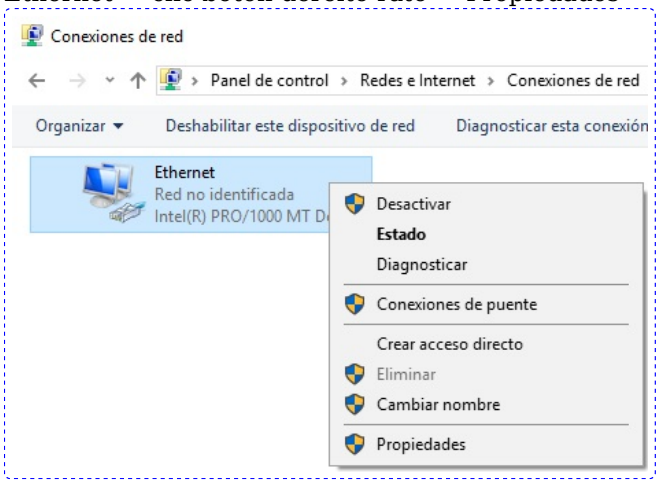


d. Configurar a tarxeta de rede interna coa IP: 10.10.10.11 e máscara de subrede: 255.0.0.0

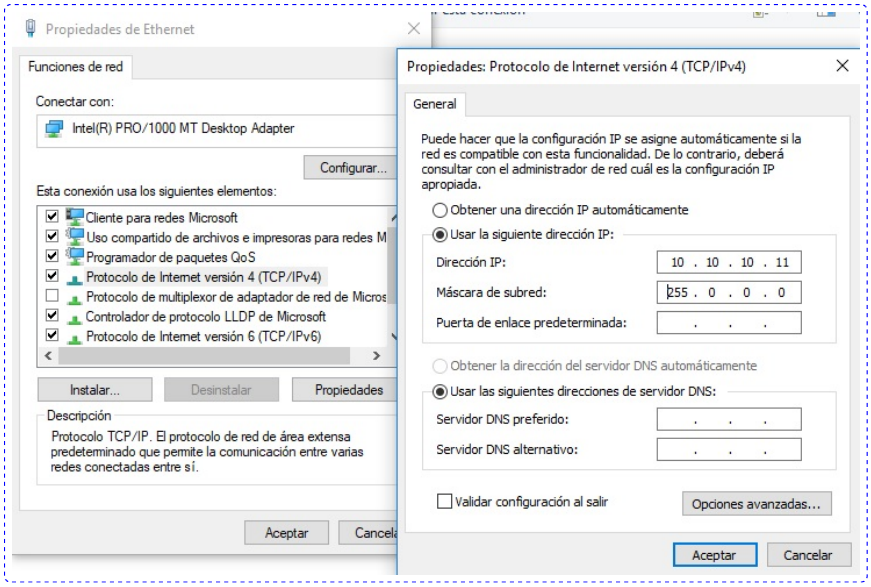
i. No cmd(consola de comandos): control → red → Ver conexiones de red



ii. Ethernet → clic botón dereito rato → Propiedades

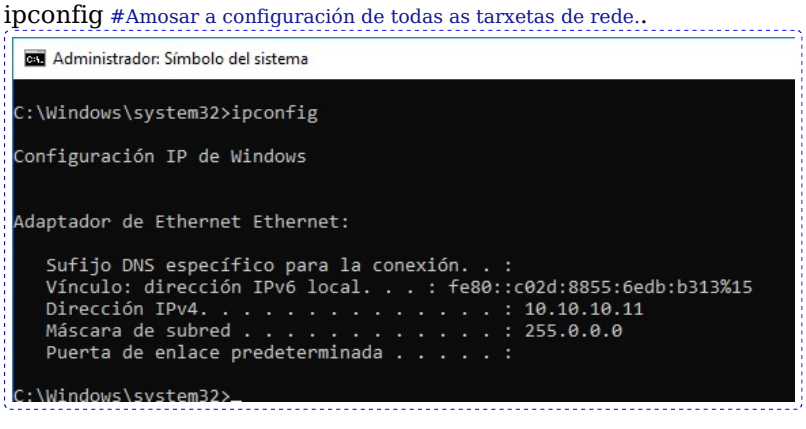


iii. Protocolo de internet versión 4 (TCP/IPv4) → dobre clic botón esquerdo rato → Usar la siguiente dirección IP:
Dirección IP: 10.10.10.11
Máscara de subred: 255.0.0.0



Aceptar → Aceptar

iv. ipconfig #Amosar a configuración de todas as tarxetas de rede..



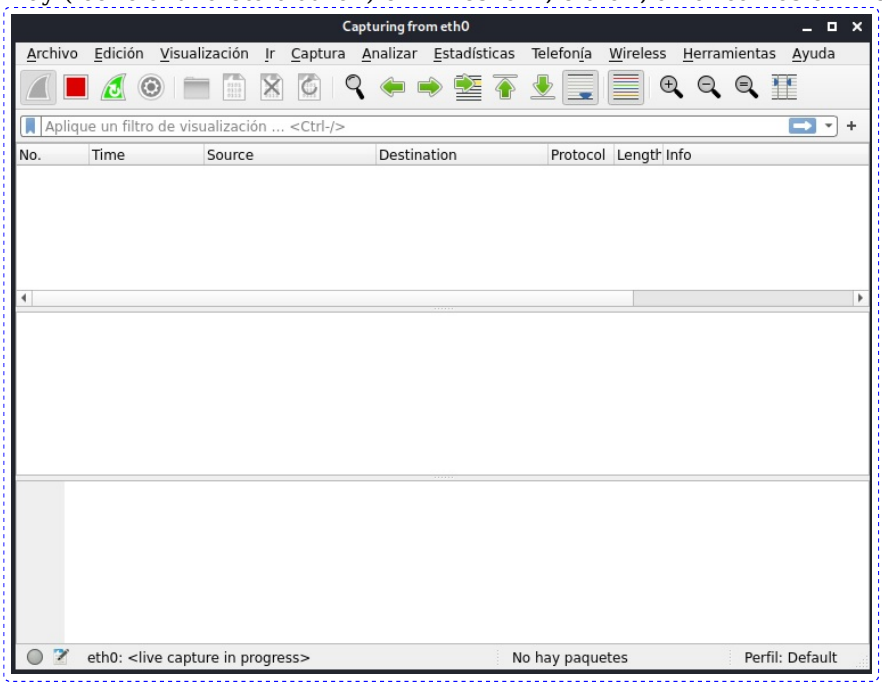
6. Táboa arp:
   a. arp -a #Revisar a táboa arp, é dicir, visualizar a caché arp do sistema: asignación IP coa súa correspondente dirección física (MAC Address).

7. Agora minimizamos a máquina virtual B (Microsoft Windows 10) xa que imos traballar coa máquina virtual A (Kali i386).

Máquina virtual A: Kali i386

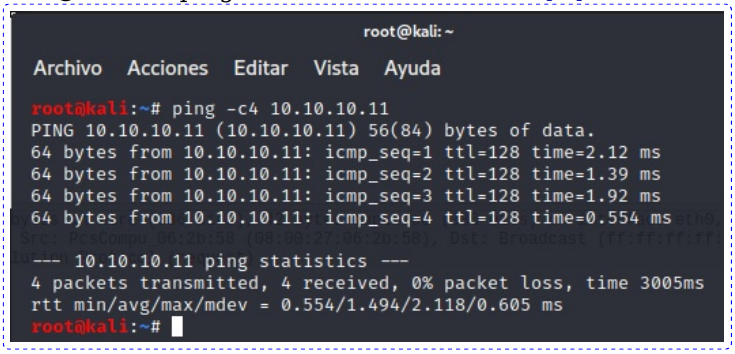
8. Agora maximizamos a máquina virtual A (Kali i386).

9. Play (icono azul aleta tiburón) en wireshark, é dicir, arrancamos o wireshark.

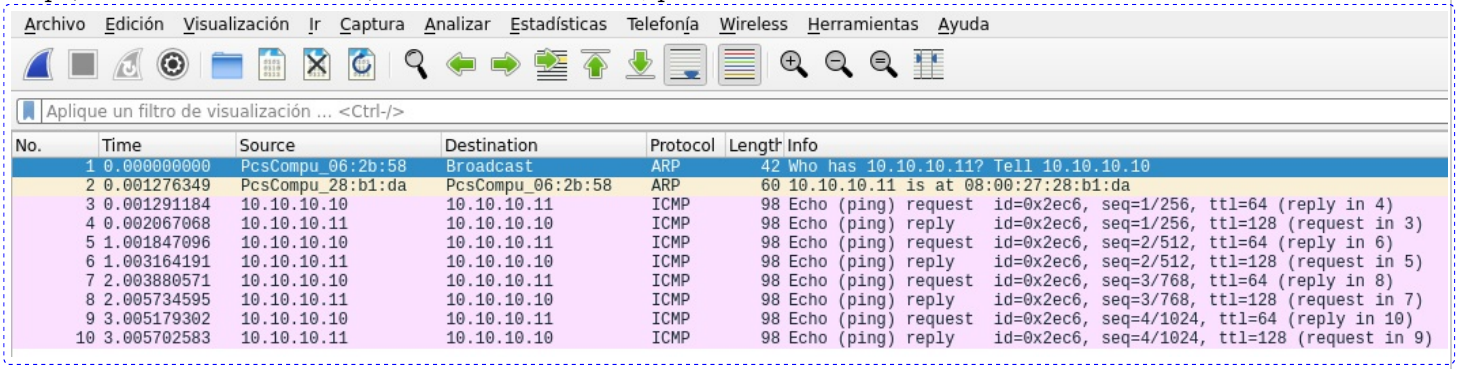


10. Facer ping á máquina virtual B(Microsoft Windows 10):

    root@kali:~# ping -c4 10.10.10.11 #Envíar 4 paquetes ICMP dende a máquina Kali a Máquina Windows 10



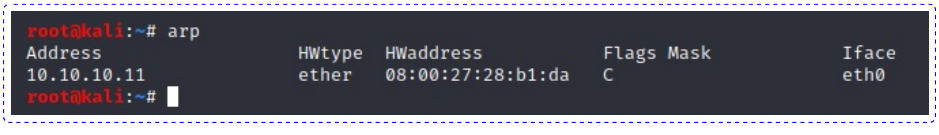
11. Stop (icono vermello cadrado) en wireshark, é dicir, paramos o wireshark.



    Podemos observar que como na táboa arp de Kali non estaba recoñecida a dirección física (MAC Address) de Windows 10, averiguase mediante o protocolo ARP. Así, envíase dende Kali unha mensaxe de broadcast(difusión) a todos os nodos da rede preguntando que host ten a dirección física correspondente á IP 10.10.10.11; e o host que posee esa IP, o de Windows 10, resposta indicando mediante un paquete ARP a súa dirección física. Deste xeito, agora xa se poden transmitir os paquetes ICMP, porque Kali sabe a que dirección física dirixilos para que poidan ser recibidos. Como podemos observar na imaxe, por cada paquete ICMP de Kali envíase unha pregunta (echo request), o cal ten a súa resposta correspondente da máquina Windows 10 con outro paquete ICMP (echo reply).

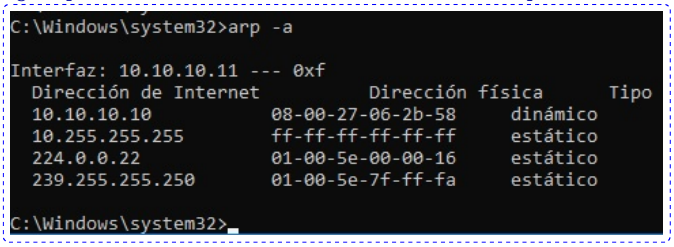
12. Comprobar a táboa arp:

    root@kali:~# arp #Revisar a táboa arp, é dicir, visualizar a caché arp do sistema: asignación IP coa súa correspondente dirección física (MAC Address). Agora podemos observar como si existe unha entrada para o Windows 10, onde se asigna a IP 10.10.10.11 a súa dirección física (MAC Address ou HWaddress).



Máquina virtual B: Microsoft Windows 10

13. Comprobar a táboa arp:
    a. arp -a #Revisar a táboa arp, é dicir, visualizar a caché arp do sistema: asignación IP coa súa correspondente dirección física (MAC Address). Agora podemos observar como si existe unha entrada para Kali, onde se asigna a IP 10.10.10.10 a súa dirección física.



Contesta e razoa brevemente:

1. Que acontece se voltas a realizar de novo a práctica unha vez existen as entradas arp correspondentes, é dicir, se en Kali xa existe a entrada arp de Windows 10 e viceversa?
2. Captura imaxes demostrando o que respostaches na cuestión 1.
3. Executa na máquina Kali o comando: **arp -d 10.10.10.11**
   Executa na máquina Windows o comando: **arp -d ***
   Captura imaxes coa execución e saída dos comandos anteriores. Que acontece se voltas a realizar de novo a práctica?
4. Captura imaxes demostrando o que respostaches na cuestión 3.

Ricardo Feijoo Costa