



UNIVERSIDAD DE GRANADA

Transmisión de Datos y Redes de Computadores
Seminario 2
Amador Carmona Méndez



Tarea 1: Probar nmap en vuestra casa. Contestar a las siguientes preguntas. Para cada una de ellas, muestre un ejemplo si es posible.

- ¿Cómo podemos emplear nmap para sondear los hosts activos en una red?
- ¿Cómo podemos emplear nmap para sondear los puertos abiertos en un host?
- ¿Cómo podemos conocer el sistema operativo del host? ¿Es totalmente fiable?
- ¿Cuántos puertos pueden ser comprobados?
- ¿Cómo podemos emplear nmap para detectar un cortafuegos entre el host y nuestro equipo?

Sondear hosts activos en una red:

El comando `nmap -sn [dirección de red/máscara de subred]`. Esto enviará paquetes ICMP echo request a todos los hosts en la red especificada y mostrará los que respondan.

Ejemplo: `nmap -sn 192.168.1.0/24`

```
[~ » sudo nmap -sn 192.168.1.0/24      amadorcarmonamendez@MacBook-Pro-de-Amador ]  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-10 22:59 CEST  
Nmap scan report for 192.168.1.1  
Host is up (0.0031s latency).  
MAC Address: 34:57:60:DC:A6:A7 (MitraStar Technology)  
Nmap scan report for 192.168.1.39  
Host is up (0.0065s latency).  
MAC Address: 7E:8D:2E:EF:A5:F0 (Unknown)  
Nmap scan report for 192.168.1.45  
Host is up (0.0078s latency).  
MAC Address: 04:D9:F5:7B:2F:DE (ASUSTek Computer)  
Nmap scan report for 192.168.1.56  
Host is up (0.059s latency).  
MAC Address: A4:50:46:38:31:8B (Xiaomi Communications)  
Nmap scan report for 192.168.1.60  
Host is up (0.0054s latency).  
MAC Address: A4:4B:D5:27:E3:14 (Xiaomi Communications)  
Nmap scan report for 192.168.1.66  
Host is up (0.012s latency).  
MAC Address: FC:AA:14:CB:13:83 (Giga-byte Technology)  
Nmap scan report for 192.168.1.34  
Host is up.  
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.13 seconds  
[~ » ] amadorcarmonamendez@MacBook-Pro-de-Amador
```



Sondear puertos abiertos en un host:

El comando `nmap -p [rango de puertos] [dirección IP del host]`. Esto realizará un escaneo de todos los puertos en el host especificado y mostrará cuáles están abiertos.

Ejemplo: `nmap -p 1-1000 192.168.1.1`

```
~ » sudo nmap -p 1-1000 192.168.1.1      amadorcarmonamendez@MacBook-Pro-de-Amador
[Password:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-10 23:08 CEST
Nmap scan report for 192.168.1.1
Host is up (0.10s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE     SERVICE
21/tcp    filtered  ftp
22/tcp    open      ssh
23/tcp    filtered  telnet
80/tcp    open      http
443/tcp   open      https
MAC Address: 34:57:60:DC:A6:A7 (MitraStar Technology)

Nmap done: 1 IP address (1 host up) scanned in 3.27 seconds
```

Conocer el sistema operativo del host:

El comando `nmap -O [dirección IP del host]`. Esto intentará determinar el sistema operativo del host objetivo basándose en diferentes características y patrones. No es siempre fiable.

Ejemplo: `nmap -O 192.168.1.1`

```
[~ » sudo nmap -O 192.168.1.1      1 ↵ amadorcarmonamendez@MacBook-Pro-de-Amador      ]
[Password:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-10 22:57 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0057s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE     SERVICE
21/tcp    filtered  ftp
22/tcp    open      ssh
23/tcp    filtered  telnet
80/tcp    open      http
443/tcp   open      https
MAC Address: 34:57:60:DC:A6:A7 (MitraStar Technology)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.05 seconds
```



Número de puertos comprobados:

Por defecto, `nmap` comprueba los 1000 puertos más comunes. Sin embargo, puedes especificar un rango específico de puertos para comprobar utilizando el argumento `-p`. El máximo número de puertos que `nmap` puede comprobar es 65535.

Detectar un cortafuegos entre el host y nuestro equipo:

Si `nmap` encuentra un cortafuegos entre tu equipo y el host objetivo, es posible que algunos puertos aparezcan filtrados o cerrados. Puedes intentar determinar si hay un cortafuegos mediante el uso del comando `nmap -sA [dirección IP del host]`, que envía paquetes TCP ACK y espera una respuesta. Si no hay respuesta, puede indicar la presencia de un cortafuegos.

Ejemplo: `nmap -sA 192.168.1.1`

```
[~] » sudo nmap -sA 192.168.1.1                               1 ↳ amadorcarmonamendez@MacBook-Pro-de-Amador
[Password:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-10 23:19 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0082s latency).
Not shown: 998 unfiltered tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    filtered  ftp
23/tcp    filtered  telnet
MAC Address: 34:57:60:DC:A6:A7 (MitraStar Technology)

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
-----[~] » sudo nmap -A 192.168.1.1                           amadorcarmonamendez@MacBook-Pro-de-Amador
```

Tarea 2: Probar traceroute en casa para algún dominio (e.g. www.ugr.es). Contestar a las siguientes preguntas:

```
~ » traceroute www.ugr.es amadorcarmonamendez@MacBook-Pro-de-Amador
[traceroute to www.ugr.es (150.214.27.71), 64 hops max, 52 byte packets
 1 192.168.1.1 (192.168.1.1) 4.609 ms 2.811 ms 2.761 ms
 2 41.red-81-46-37.customer.static.ccgg.telefonica.net (81.46.37.41) 4.189 ms 3.484 ms 8.338 ms
 3 113.red-81-46-31.customer.static.ccgg.telefonica.net (81.46.31.113) 27.252 ms 16.165 ms 17.156 ms
 4 157.red-81-46-31.customer.static.ccgg.telefonica.net (81.46.31.157) 16.548 ms 15.921 ms 16.531 ms
 5 129.red-80-58-73.staticip.rima.tde.net (80.58.73.129) 16.542 ms * *
 6 rediris.alta.espanix.net (185.79.175.154) 21.131 ms 16.985 ms 55.964 ms
 7 rediris.baja.espanix.net (193.149.1.26) 21.355 ms 19.762 ms
 ciemat-rt2.ethtrunk3.cica.rt2.and.red.rediris.es (130.206.245.38) 26.574 ms
 8 ciemat-rt2.ethtrunk3.cica.rt2.and.red.rediris.es (130.206.245.38) 26.264 ms
 rica-ppal-router.red.rediris.es (130.206.194.2) 26.590 ms 26.266 ms
 9 rica-ppal-router.red.rediris.es (130.206.194.2) 26.557 ms
 et-5-0-5.granada01.red.cica.es (150.214.231.22) 41.566 ms 29.740 ms
10 et-5-0-5.granada01.red.cica.es (150.214.231.22) 29.625 ms
 ugr-router.red.cica.es (150.214.231.138) 30.128 ms 30.187 ms
11 ugr-router.red.cica.es (150.214.231.138) 30.275 ms * 31.429 ms
12 * * *
13 * * *
14 bofiweb.ugr.es (150.214.27.71) 32.680 ms * 32.656 ms
-----]
~ » amadorcarmonamendez@MacBook-Pro-de-Amador
```

➤ ¿Qué nos indica la salida del comando traceroute?

Nos indica información sobre la ruta que los paquetes recorren desde el dispositivo que lanza el comando hasta llegar a la ip indicada en el comando. nos indica el número de salto, el nombre dns y la ip y el RTT.

➤ ¿Se pueden ocultar los nombres DNS? En tal caso, muéstralos con una captura de pantalla.

Si, en la captura de pantalla se ve que los saltos 12 y 13 ponen *** eso significa que sabemos que hay un salto pero no sabemos más información es decir el nombre DNS no lo sabemos.

➤ ¿Es la ruta obtenida siempre la misma? Si no lo es, muéstralos con una captura de pantalla.

No comparando la siguiente captura con la anterior, hay diferencias por ejemplo el salto 5:

```
~ » traceroute www.ugr.es amadorcarmonamendez@MacBook-Pro-de-Amador
[traceroute to www.ugr.es (150.214.27.71), 64 hops max, 52 byte packets
 1 192.168.1.1 (192.168.1.1) 6.302 ms 3.207 ms 3.626 ms
 2 41.red-81-46-37.customer.static.ccgg.telefonica.net (81.46.37.41) 4.175 ms 4.436 ms 3.664 ms
 3 113.red-81-46-31.customer.static.ccgg.telefonica.net (81.46.31.113) 15.941 ms 16.522 ms 16.051 ms
 4 157.red-81-46-31.customer.static.ccgg.telefonica.net (81.46.31.157) 16.129 ms 15.986 ms 17.904 ms
 5 * *
 6 142.red-81-46-9.customer.static.ccgg.telefonica.net (81.46.9.142) 40.322 ms
 rediris.alta.espanix.net (185.79.175.154) 16.110 ms 15.876 ms
 7 ciemat-rt2.ethtrunk3.cica.rt2.and.red.rediris.es (130.206.245.38) 27.137 ms
 rediris.baja.espanix.net (193.149.1.26) 16.857 ms
 ciemat-rt2.ethtrunk3.cica.rt2.and.red.rediris.es (130.206.245.38) 26.067 ms
 8 rica-ppal-router.red.rediris.es (130.206.194.2) 26.613 ms 26.750 ms
 ciemat-rt2.ethtrunk3.cica.rt2.and.red.rediris.es (130.206.245.38) 28.344 ms
 9 rica-ppal-router.red.rediris.es (130.206.194.2) 26.736 ms
 et-5-0-5.granada01.red.cica.es (150.214.231.22) 29.612 ms 29.186 ms
10 et-5-0-5.granada01.red.cica.es (150.214.231.22) 29.799 ms
 ugr-router.red.cica.es (150.214.231.138) 30.383 ms 30.666 ms
11 * ugr-router.red.cica.es (150.214.231.138) 31.068 ms *
12 * * *
13 * * *
14 * * *
15 bofiweb.ugr.es (150.214.27.71) 29.822 ms 30.324 ms 30.566 ms
-----]
~ » amadorcarmonamendez@MacBook-Pro-de-Amador
```

Tarea 3: Probar Wireshark.

- Abrir una de las trazas de ejemplo que se proporcionan aquí:
<https://wiki.wireshark.org/SampleCaptures>
- Analizar el protocolo tal y como se ha hecho en el ejemplo de la pág. 14. Nota: No vale analizar el mismo protocolo que se ha mostrado en clase.

ARP

ARP es un protocolo parecido a SHCP solo que trabaja a nivel de capa de enlace a nivel de MAC y se utiliza para descubrir la MAC de otro dispositivo. El funcionamiento del protocolo ARP se puede describir en los siguientes pasos:

Solicitud ARP (ARP Request):

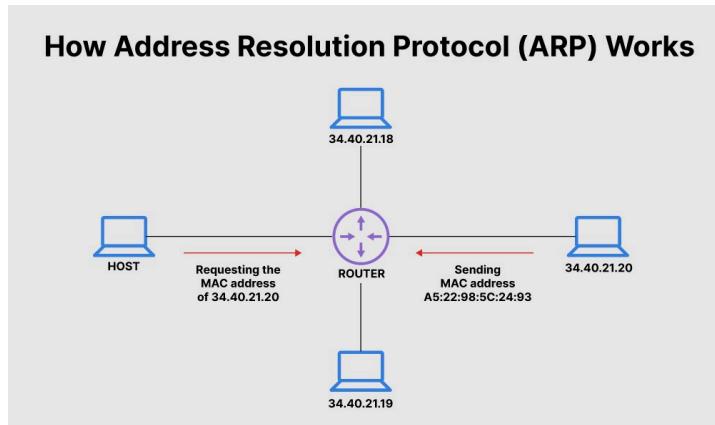
Cuando un dispositivo necesita comunicarse con otro dispositivo en la misma red local, pero solo conoce la dirección IP del destino y no su dirección MAC, envía una solicitud ARP de difusión a la dirección MAC de difusión FF:FF:FF:FF:FF y solicita la dirección MAC asociada a la dirección IP del destino. Esta solicitud contiene la dirección IP del dispositivo emisor y la dirección IP del dispositivo destino que se está buscando.

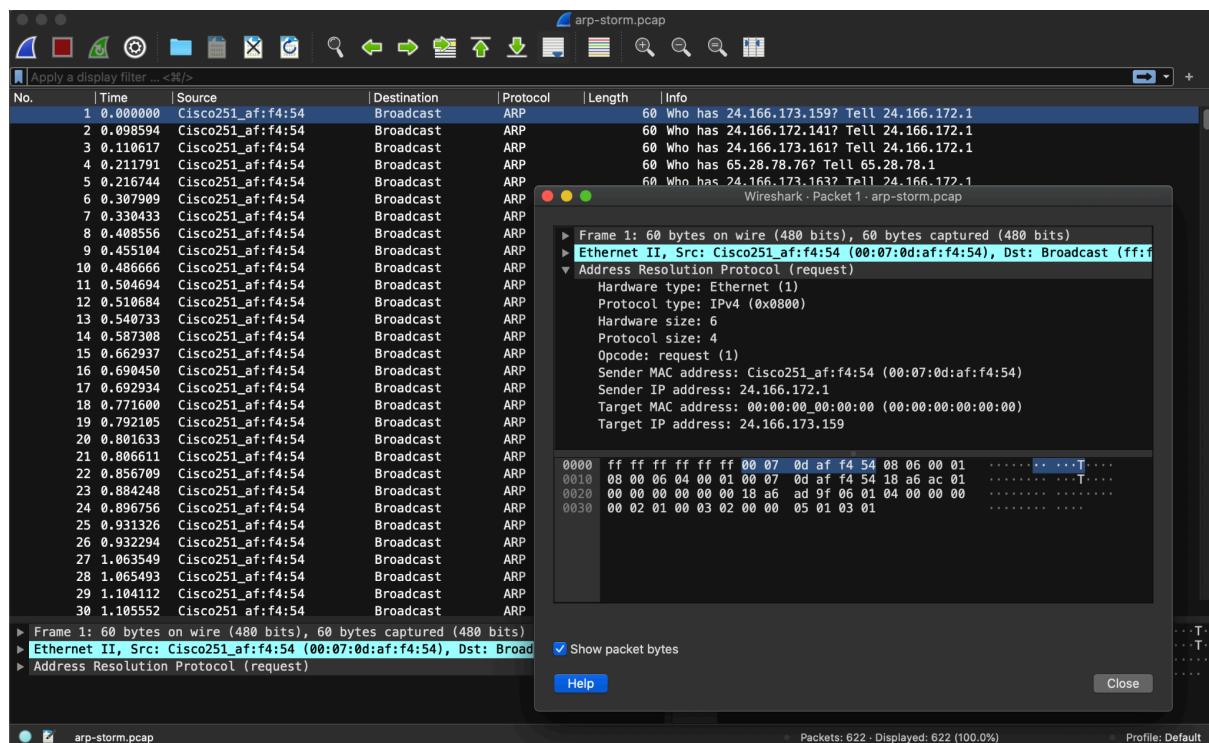
Respuesta ARP (ARP Reply):

Cuando el dispositivo destino recibe la solicitud ARP, verifica si la dirección IP de destino coincide con la suya. Si es así, responde a la solicitud ARP enviando un paquete de respuesta ARP que contiene su dirección MAC. Esta respuesta se envía directamente al dispositivo emisor de la solicitud ARP.

Almacenamiento en caché (ARP Caching):

Después de recibir la respuesta ARP, el dispositivo emisor almacena la dirección IP y la dirección MAC del dispositivo destino en su tabla ARP local, que es una tabla de asociaciones de direcciones IP y MAC conocidas. Esta tabla se utiliza para futuras comunicaciones con ese dispositivo, evitando así la necesidad de realizar solicitudes ARP repetitivas para la misma dirección IP.





Tarea 4: Probar Cisco Packet. Se creará un escenario con un host y un router Cisco 2911. Se mostrarán capturas de todos los pasos.

➤ **Configurar el hostname como: PrimerApellidoNombre. Ejemplo: GaleoteJuanElias**

➤ **Configurar las direcciones IP de cada interfaz. Nota: Recordad que cada interfaz pertenece a una subred diferente.**

Como solo tenemos un host solo hay una subred.

➤ **Mostrar las estadísticas y métricas de cada interfaz**

