**PARTE 1**: Utiliza los comandos nslookup y whois para resolver la siguiente tabla

|  |  |
| --- | --- |
| **Dominio** | **IP** |
| marca.com | Hay dos (depende de si pones www o no)  151.101.133.50  34.147.120.111 |
| elmundo.es | 131.0.136.66 |
| manerasdevivir.com | 31.47.78.72 |

|  |  |
| --- | --- |
| **IP/Dominio** | **Dueño de dominio(En caso de no poder saberlo, indicarlo también)** |
| 195.53.165.153 | Jesus Feliz Fernandez (Instituto Nacional de Ciberseguridad de España) |
| 151.101.2.137 | No lo indica (Fastly Inc.) |
| 147.96.1.15 | Manuel Hernandez Urrea (UCM) |
| 91.146.100.130 | Javier Narvaez Segura (Loading S ystm) |

**PARTE 2**: Descubrimiento de hosts

1. Realiza un escaneo de la subred en la que te encuentres con diferentes parámetros y rellena la tabla que se encuentra a continuación:

[Descubrimiento de Host](https://nmap.org/man/es/man-host-discovery.html)

|  |  |  |
| --- | --- | --- |
| **Opción/Parámetro de nmap** | **Comando utilizado (pega el que utilices tal cual)** | **Número de host encontrados** |
| Sin parámetros:  Ejemplo: nmap 192.168.1.0/24 (/24 es para escanear toda la red) | nmap 192.168.21.0/24 | 6 hosts |
| -sP (escaneo ping)  Ejemplo: nmap -sP 192.168.1.0/24nmap 192.168.21.0/24 | Nmap -sP 192.168.21.0/24 | 7 host |
| -PS (tcp -syn/ack, discovery a los puertos) | nmap -PS 192.168.21.0/24 | 7 host |
| -PU (Udp discovery a los puertos) | nmap 192.168.21.0/24 | 19 hosts |
| -PR (Ping ARP) | nmap 192.168.21.0/24 | 21 hosts |

1. ¿Con cuál has logrado descubrir más host de la subred? ¿Por qué crees que ha sido?

Con el último nmap encuentro mas hosts. Creo que es porque con el protocolo ARP son menos usados para realizar ataques por tanto la seguridad en la red no intenta pararlo tanto como a otros.

1. Elige uno de los host levantados y trata de detectar su sistema operativo. A continuación escribe el comando que has utilizado, qué sistema operativo crees que corre en ese host, y adjunta una captura de pantalla

|  |  |
| --- | --- |
| **Comando utilizado** | **Sistema operativo más probable(solo sistema operativo, sin versión)** |
| Nmap -O 192.168.21.23  como me ha bloqueado el pin he puesto al final:  Nmap -O 192.168.21.23 -Pn | Microsoft Windows |

|  |
| --- |
| **Captura de Pantalla del resultado obtenido** |
|  |

1. Para uno de los host, realiza los siguientes sondeos de puertos e indica qué puertos has encontrado abiertos.

[Scan Methods](https://nmap.org/book/scan-methods.html)

[Técnicas de sondeo](https://nmap.org/man/es/man-port-scanning-techniques.html)

[Puertos TCP/UDP](https://direccionip.net/puertos-ip/)

|  |  |  |  |
| --- | --- | --- | --- |
| **Tipo de sondeo** | **Puertos sondeados** | **Comando utilizado copiado** | **Puertos abiertos**  **(ej: 22-SSH, 80-HTTP, etc..)** |
| Tiple apretón de manos completo(con conexión) | 65.535 puertos | Nmap -sT -p- 192.168.21.23 (son todos los puertos disponibles) |  |
| Triple apretón de manos semicompleto(TCP/SYN) | 22,23,25,43,443 | Nmap -sS -p 22,23,25,43,443 192.168.21.23 |  |
| Sondeo UDP | 5 puertos udp que consideres | Nmap -sU -p 161,162,174,177,53 192.168.21.23 |  |
| Triple apretón de manos semicompleto(TCP/SYN) | por defecto (1000 puertos más populares) | Sudo nmap -sS 192.168.21.23 (el nmap simple escanea los mas populares) |  |

**PARTE 3**: En este apartado se trabajará simultáneamente con **wireshark** y **nmap**, para lo cual se elegirá uno de los host de la red

1a) Se quiere hacer un escaneo con **nmap** sobre la máquina objetivo que haga lo siguiente:

Sondeo de triple apretón sobre los 3500 primeros puertos con escaneo de versiones, y detección de sistema operativo (puedes añadir el parámetro verbose, -v, para ampliar información). En la siguiente caja escribe el comando utilizado.

|  |
| --- |
| Sudo nmap -sV -O v ~~-p~~ 03500 |

1b) Filtra en **wireshark** por tu propia máquina, la objetivo y el puerto 22 para analizar el tráfico que se produce al lanzar el comando del punto anterior. Escribe en la siguiente caja el filtro o filtros que has utilizado.

|  |
| --- |
| ip.src==192.168.21.206&&ip.dst==192.168.22.23&&Tcp.port==22 |

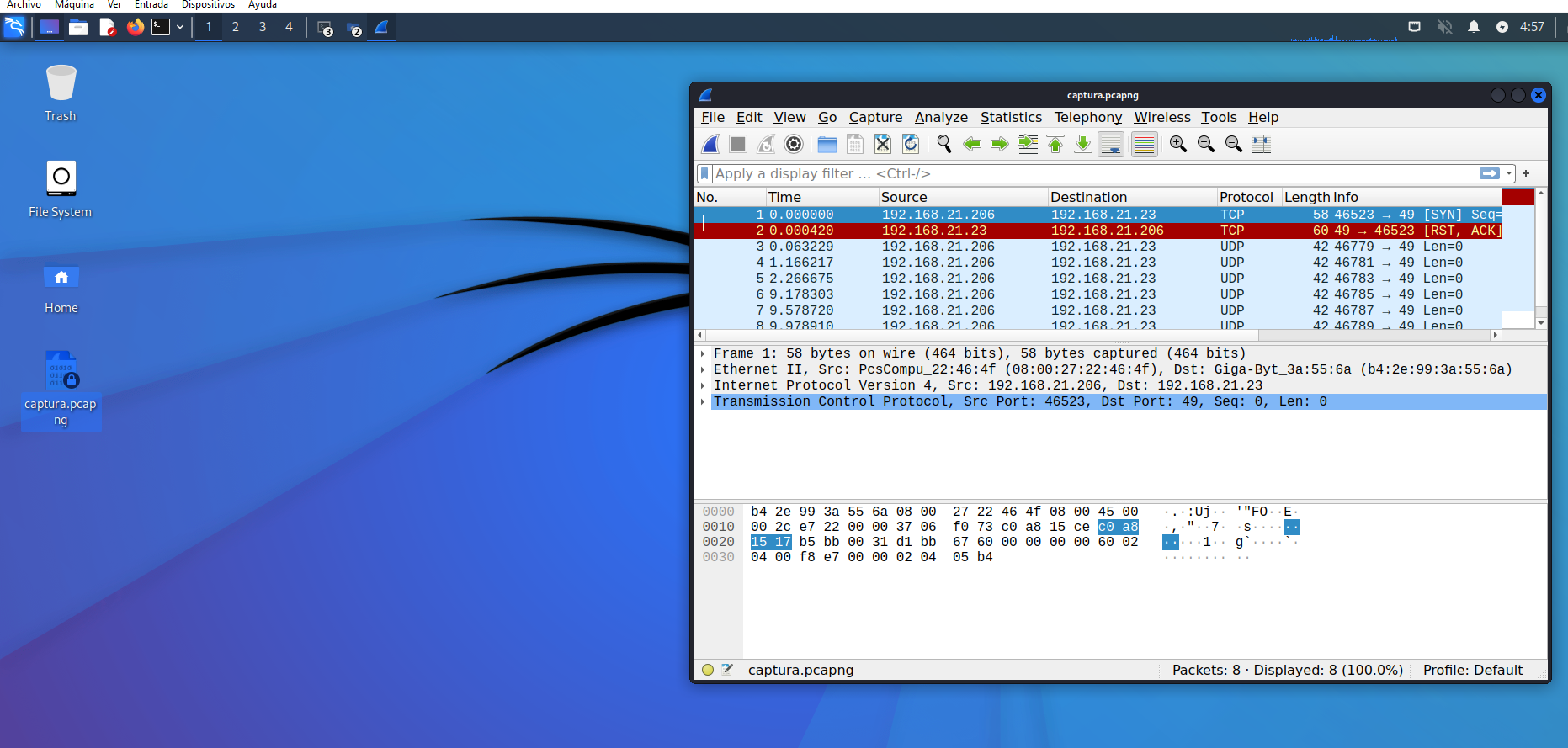
2a) Se quiere hacer un escaneo con **nmap** sobre la máquina objetivo que haga lo siguiente:

Simultáneamente ejecutar un sondeo ARP, sondeo de apretón semicompleto(TCP/SYN) y sondeo UDP sobre los puertos 49 a 80 los puertos con escaneo de versiones, y detección de sistema operativo (puedes añadir el parámetro verbose, -v, para ampliar información. Este comando puede tardar un rato en ejecutarse). En la siguiente caja escribe el comando utilizado.

|  |
| --- |
| Sudo nmap -pR -sS -sU -p 49-80 -O -v 192.168.21.23 |

2b) Captura el tráfico con **tcpdump** filtrándolo exclusivamente por el puerto 49 para analizar el tráfico que se produce al lanzar el comando del punto anterior y guarda el resultado en un fichero llamado captura2b(con su extensión). Después ábrelo. Copia los **comandos** utilizados(el de captura filtrando con escritura en fichero; y el de lectura) en la siguiente caja.

|  |
| --- |
| Sudo tcpdump -v -i eth0 port 49 -w /*home*/kali/Desktop/captura.pcapng |



**PARTE 4**: ¿Qué conclusiones puedes extraer del análisis que has realizado sobre esa máquina?

Es una maquina con sistema Operativo Microsoft Windows 10. La maquina tiene algunos puertos abiertos conocidos como pueden ser el mysql (3306) o el 135.He encontrado varias versiones interesantes como pueden ser la de mysql (8.0.30) o el servicio de Vmware (Daemon 1.0)., por tanto podemos asumir que es un afintrión.