Ficha y Control de Resultados de las Prácticas

Datos de Identificación

Apellido, Nombre	Cédula de Identidad	Nro. de Práctica	Fecha
Diego Bastardo	27948046	14	13/10/2022
Gabriel Manrique	26921248		
Nombre de la Práctica	**Preparando el entorno de trabajo**		
Grupo (últimos 2 dígitos del NRC)	1489	**Mesa**	

Direccionamiento IP/Máscara:

Equipo origen/fuente:	172.30.114.4	**Equipo Objetivo/Destino:**	172.30.114.5
Otros Equipos involucrados:			

Ejecución de la práctica:

Por cada actividad desarrollada durante la ejecución de la práctica debe narrar la(s) actividad(es) llevadas a cabo y colocar las evidencias resultantes, a saber: evidencia de comandos, aplicaciones, programas ejecutados, así como los resultados obtenidos de la ejecución de los mismos:

Dando un enfoque más práctico en los laboratorios de seguridad de la información llevamos a cabo la actividad práctica 1. Esta constó de la ejecución, análisis y estudio del comando Nmap el cual es un programa que utilizamos para la recopilación de información (Information gathering).

Creamos una máquina virtual con virtualbox llamada Analista que ejecutaba el sistema operativo kali linux 2022.1. Junto con la PC creamos una redNat asignando la dirección de red 172.30.114.0/24.

El sistema operativo kali linux viene fuertemente equipado con un conjunto de herramientas para seguridad y una de ellas es el programa Nmap, la dinámica de la práctica se desenvolvió en ejecutar el comando nmap en la terminal de linux utilizando el conjunto de flags que nos proporciona el comando nmap. Cada comando tiene una funcionalidad específica.

Antes de explicar la funcionalidad del comando, debemos tener presente algunos conceptos, como por ejemplos los puertos, este es un conector de un elemento informático que se utiliza para la comunicación de elementos de hardware o software que permite el envío de datos entre

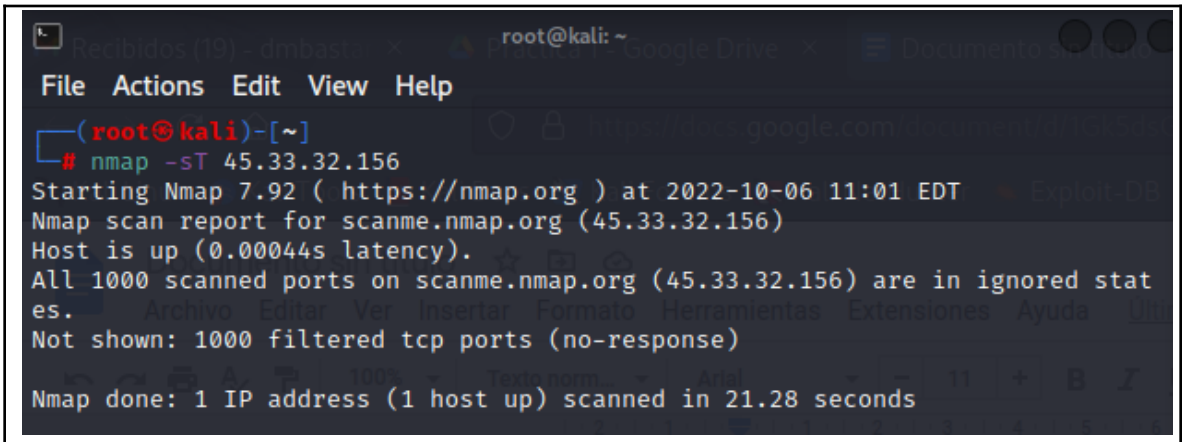
ellos, estos puertos pueden tener algún tipo de estado, cerrado, filtrado o abierto. El estado cerrado es para los puertos que no aceptan alguna transmisión hacia el o que no están recibiendo envío de datos para su comunicación con el software. Estado filtrado es para algunos puertos que tienen un software para filtrar paquetes de datos y no permitir de alguna manera la comunicación con ese puerto, este estado en el puerto puede frustrar a los atacantes de algún servidor o computador. Estado abierto, este sería el puerto en estado ideal para los atacantes, ya que está configurado para la comunicación de paquetes con elementos externos con el software, los estados explicados son los más comunes que se observan al ejecutar el comando Nmap. El sondeo es una operación de consulta constante hacia un dispositivo de hardware, para crear una actividad sincrónica de comunicación sin interrupciones.

Primero ejecutamos el comando con el conjunto de banderas sT, sA, sU,sS. Estas banderas nos permitieron hacer un análisis exhaustivo acerca de las propiedades del servidor que estábamos examinando en el ejemplo fue scanme.nmap.org y scanme2.nmap.org. El comando sS nos retornó al cabo de unos cuantos minutos los puertos del servidor que se encontraban abiertos, su número y su servicio como también la cantidad de puertos TCP que se encontraban filtrados por motivos de seguridad.

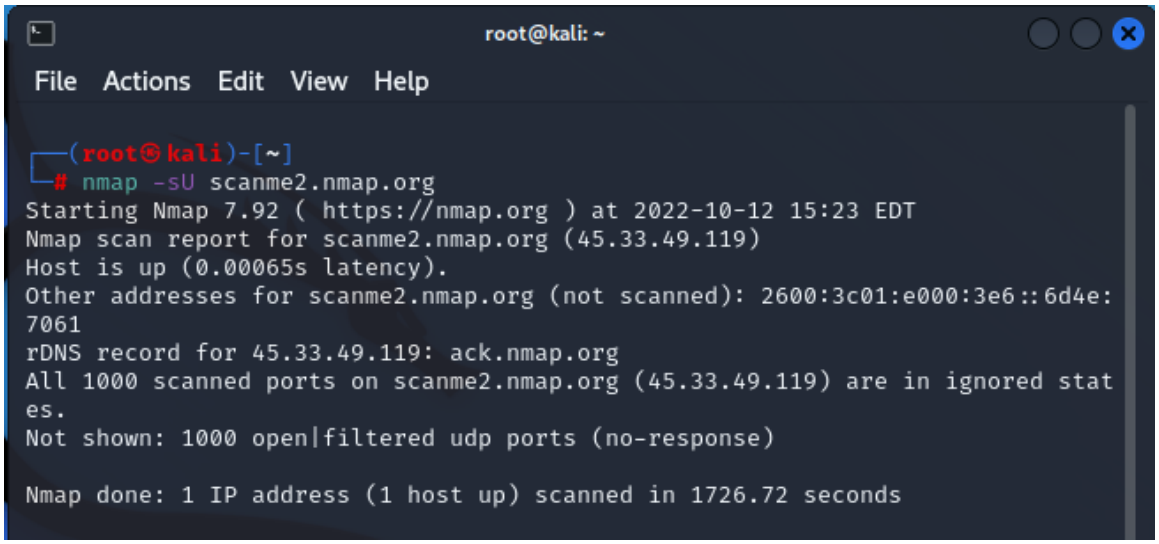
El flag sS nos sirve para realizar un scan de los puertos TCP.

```
┌──(root㉿kali)-[~]
└─# nmap -sS 45.33.32.156
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 10:55 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00029s latency).
Not shown: 961 filtered tcp ports (no-response), 37 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 717.72 seconds
```

El flag sT se utiliza para realizar un escaneo de las máquinas y su ventaja con respecto al comando anterior es que permite escanear máquinas que utilicen el protocolo IPv6. En la práctica el resultado arrojado por el comando fue que el host está activo y que tenía 1000 puertos tcp filtrados.



El flag sU no terminó de correr por consiguiente no arrojó un resultado concreto, sin embargo, este es utilizado para el escaneo de puertos UDP los cuales son importantes a la hora de encontrar vulnerabilidades siendo estos puertos inseguros.



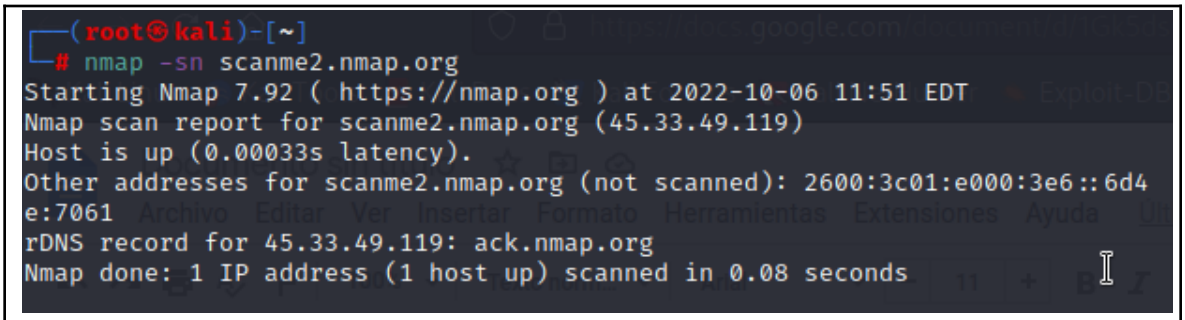
El flag sA es utilizado para realizar un mapeo sobre las reglas del firewall, es llamado escaneo ACK ya que lo hace mediante los mensajes que envía el destino al origen con el objetivo de confirmar la comunicación. En la práctica este flag nos mostró que en el servidor víctima se encuentran 1000 puertos tcp que no están filtrados.

```
┌──(root㉿kali)-[~]
└─# nmap -sA 45.33.32.156
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 11:03 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00017s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored stat
es.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

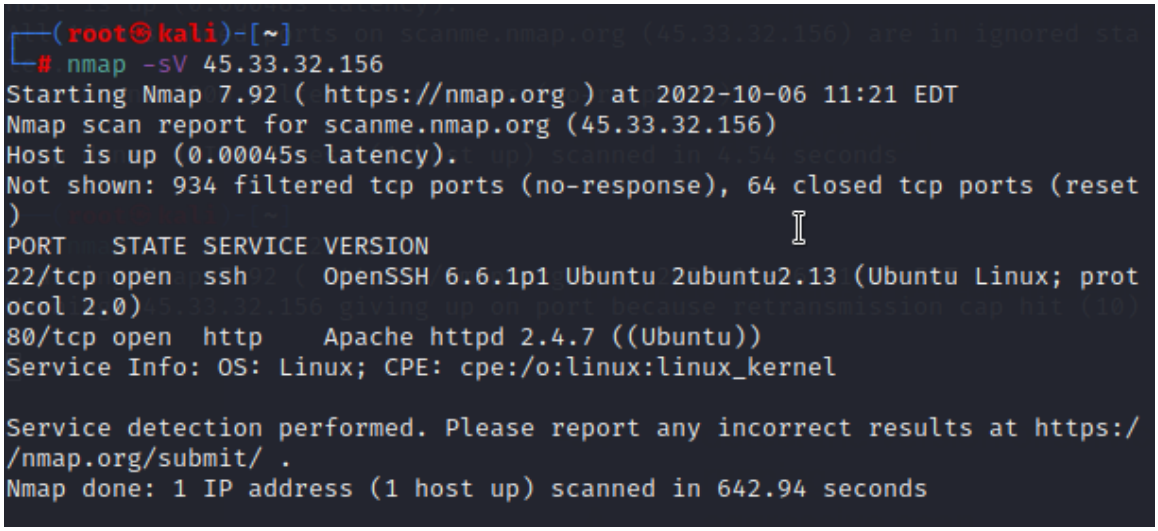
El flag -Pn (disable ping) este comando es veloz debido a que se salta un ping y escanea cada host que se provee. En la práctica obtuvimos el estado del host el cual estaba activo, la latencia, la dirección IPv6 del host, su dirección IPv4, puertos tcp filtrados y los puertos ;con estado servicios abiertos.

```
┌──(root㉿kali)-[~]
└─# nmap -Pn scanme2.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 11:50 EDT
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 15.70% done; ETC: 11:52 (0:01:31 remaining)
Nmap scan report for scanme2.nmap.org (45.33.49.119)
Host is up (0.12s latency).
Other addresses for scanme2.nmap.org (not scanned): 2600:3c01:e000:3e6::6d
e:7061
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 98.80 seconds

┌──(root㉿kali)-[~]
└─#
```

El flag -sn tambien llamado disable port scan, nos permite cancelar el escaneo de los puertos una vez se descubran un host. Con esto podemos divisar todos los host que están disponibles para escanear, en el caso de la práctica, sólo existe un host disponible.



El flag -sV se usa para la detección de las versiones de los servicios, si un software o servicio está desactualizado este supone una vulnerabilidad para el sistema. En la práctica determinamos que el servidor tenía un sistema operativo linux ubuntu en su versión 2.13 y Apache ubuntu v2.4.7 y openSSH 6.6.1



El flag -O nos permite determinar el sistema operativo del objetivo, en la práctica utilizamos esta flag y los resultados obtenidos fueron bastante particulares ya que pudimos concluir un sistema operativo exacto.

```
┌──(root㉿kali)-[~]
└─# nmap -O 45.33.32.156
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 11:16 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.079s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at leas
t 1 open and 1 closed port
Aggressive OS guesses: 2N Helios IP VoIP doorbell (98%), Grandstream GXP110
5 VoIP phone (98%), Garmin Virb Elite action camera (95%), Advanced Illumin
ation DCS-100E lighting controller (90%), Enlogic PDU (FreeRTOS/lwIP) (90%)
, FireBrick FB2700 firewall (89%), Ocean Signal E101V emergency beacon (Fre
eRTOS/lwIP) (89%), AzBox Bravissimo Twin satellite TV decoder (89%), Cognex
 DataMan 200 ID reader (lwIP TCP/IP stack) (89%), DTE Energy Bridge (lwIP s
tack) (89%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.17 seconds
```

El flag -A nos sirve para realizar un escaneo un poco más agresivo combinando una detección de servicios con una detección del sistema operativo del servidor. En la práctica realizada con este comando obtuvimos que el servidor http-server es apache /2.4.6 con CentOS una distribución de linux basada en red hat, también nos arrojó un conjunto de subdominios entre otra información relevante.

```
┌──(root㉿kali)-[~]
└─# nmap -A scanme2.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 12:03 EDT
Nmap scan report for scanme2.nmap.org (45.33.49.119)
Host is up (0.0066s latency).
Other addresses for scanme2.nmap.org (not scanned): 2600:3c01:e000:3e6::6d
e:7061
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
22/tcp  open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp  open  tcpwrapped
|_http-server-header: Apache/2.4.6 (CentOS)
443/tcp open  tcpwrapped
| ssl-cert: Subject: commonName=insecure.com
| Subject Alternative Name: DNS:insecure.com, DNS:insecure.org, DNS:issues
nmap.org, DNS:issues.npcap.org, DNS:nmap.com, DNS:nmap.net, DNS:nmap.org,
NS:npcap.com, DNS:npcap.org, DNS:seclists.com, DNS:seclists.net, DNS:secli
ts.org, DNS:sectools.com, DNS:sectools.net, DNS:sectools.org, DNS:secwiki.
om, DNS:secwiki.net, DNS:secwiki.org, DNS:svn.nmap.org, DNS:www.nmap.org
| Not valid before: 2022-08-15T09:03:55
|_Not valid after:  2022-11-13T09:03:54
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.6 (CentOS)
|_http-title: Did not follow redirect to https://nmap.org/
Warning: OSScan results may be unreliable because we could not find at lea
t 1 open and 1 closed port
Device type: storage-misc
Running (JUST GUESSING): British Gas embedded (92%)
Aggressive OS guesses: British Gas GS-Z3 data logger (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.20 ms ack.nmap.org (45.33.49.119)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.22 seconds
```

El flag -PR este puede sondear los puertos de una red local de un Url, podremos saber qué direcciones IP están siendo utilizadas y cuáles no. El sondeo de este flag es ARP, este envía mensajes de solicitud con la dirección del emisor establecido en 0.0.0.0 y la dirección de destino establecido en la dirección AutoIP.

```
┌──(root㉿kali)-[~]
└─# nmap -PR scanme2.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 11:52 EDT
Nmap scan report for scanme2.nmap.org (45.33.49.119)
Host is up (0.017s latency).
Other addresses for scanme2.nmap.org (not scanned): 2600:3c01:e000:3e6::6d4
e:7061
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds
```

El flag -n se utiliza para indicar las direcciones IP activas que no se deben hacer la resolución de la Url.

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nmap -n scanme2.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 11:54 EDT
Nmap scan report for scanme2.nmap.org (45.33.49.119)
Host is up (0.015s latency).
Other addresses for scanme2.nmap.org (not scanned): 2600:3c01:e000:3e6::6d
e:7061
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 11.60 seconds
```

El flag -p es utilizado para especificar los puertos que se desean averiguar, con este flag se puede asignar un rango de los puertos a indagar deseados, además de saber qué protocolos utilizan los puertos especificados. Se pudiera saber que puertos están abiertos para poder hacer algún ataque por allí y también que puertos están filtrados o cerrados.

```
┌──(root㉿kali)-[~]
└─# nmap -p 1-30 scanme2.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 11:56 EDT
Nmap scan report for scanme2.nmap.org (45.33.49.119)
Host is up (0.012s latency).
Other addresses for scanme2.nmap.org (not scanned): 2600:3c01:e000:3e6::6d
e:7061
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 29 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
```

El flag -p- escanea todos los puertos del rango de un Url, especificando como se explicó anteriormente el flag de -p, este muestra los puertos filtrados, los puertos cerrados y los puertos abiertos, con los protocolos que estos utilizan.

```
┌──(root㉿kali)-[~]
└─# nmap -p- scanme2.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 11:57 EDT
Nmap scan report for scanme2.nmap.org (45.33.49.119)
Host is up (0.00037s latency).
Other addresses for scanme2.nmap.org (not scanned): 2600:3c01:e000:3e6::6d
e:7061
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 105.44 seconds
```

El flag -F se utiliza para averiguar todos los puertos de forma rápida, cuantos se escanearon y en qué estados están estos puertos, puede dar menos detalle que la bandera -P-, no especificar el número del puerto específico y el protocolo que utiliza.

```
┌──(root㉿kali)-[~]
└─# nmap -F scanme2.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 12:00 EDT
Nmap scan report for scanme2.nmap.org (45.33.49.119)
Host is up (0.00028s latency).
Other addresses for scanme2.nmap.org (not scanned): 2600:3c01:e000:3e6::6d
e:7061
rDNS record for 45.33.49.119: ack.nmap.org
All 100 scanned ports on scanme2.nmap.org (45.33.49.119) are in ignored st
tes.
Not shown: 100 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 1.90 seconds
```

El flag -T0 no pudimos obtener respuesta en el tiempo estimado para realizar la práctica, este comando quedó cargando el porcentaje de ping, este es utilizado para el sondeo de puertos uno a la vez, además envía un sondeo por cada puerto después de 5 minutos de carga, el cual sería un motivo para tener un tiempo de espera alto para terminar de ejecutar el comando.

```
┌──(root㉿kali)-[~]
└─# nmap -T0 scanme2.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 12:05 EDT
Stats: 0:05:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 0.00% done
```

El flag -T3 es utilizado de igual modo que la ejecución de -T0, la diferencia es que envía el sondeo en todos los protocolos de forma paralela, el tiempo de ejecución es menor.

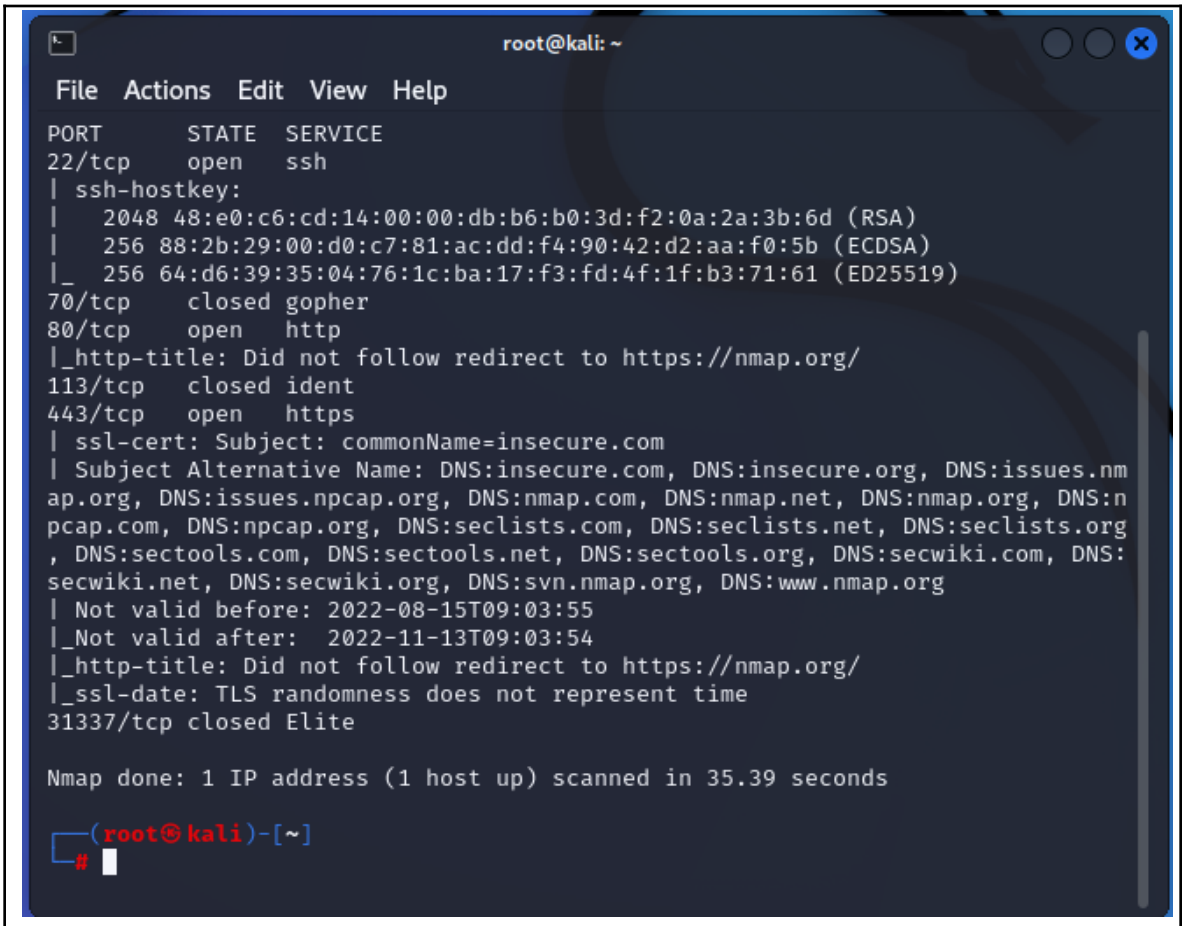
```
┌──(root㉿kali)-[~]
└─# nmap -T3 scanme2.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 12:01 EDT
Nmap scan report for scanme2.nmap.org (45.33.49.119)
Host is up (0.016s latency).
Other addresses for scanme2.nmap.org (not scanned): 2600:3c01:e000:3e6::6d
e:7061
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
```

El flag -T5 es utilizado para analizar los puertos con sondeo con un tiempo establecido de envío de sondeo, esto puede permitir que el análisis sea mucho más rápido.

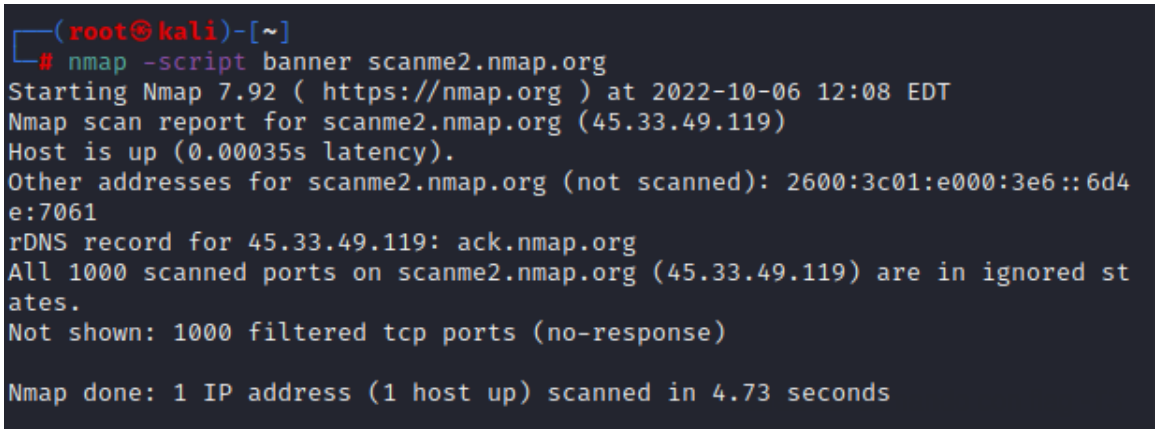
```
┌──(root㉿kali)-[~]
└─# nmap -T5 scanme2.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 12:06 EDT
Nmap scan report for scanme2.nmap.org (45.33.49.119)
Host is up (0.017s latency).
Other addresses for scanme2.nmap.org (not scanned): 2600:3c01:e000:3e6::6d4
e:7061
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.26 seconds
```

El flag -sC es un sondeo de puertos por el protocolo UDP, el cual los puertos que utilizan este tipo de protocolo puede ocurrir que la auditoría de seguridad pasa por alto e ignora el puerto.

```
root@kali: ~
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~]
└─# nmap -sC scanme2.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-12 15:25 EDT
Nmap scan report for scanme2.nmap.org (45.33.49.119)
Host is up (0.019s latency).
Other addresses for scanme2.nmap.org (not scanned): 2600:3c01:e000:3e6::6d4e:
7061
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
| ssh-hostkey:
|   2048 48:e0:c6:cd:14:00:00:db:b6:b0:3d:f2:0a:2a:3b:6d (RSA)
|   256 88:2b:29:00:d0:c7:81:ac:dd:f4:90:42:d2:aa:f0:5b (ECDSA)
|_  256 64:d6:39:35:04:76:1c:ba:17:f3:fd:4f:1f:b3:71:61 (ED25519)
70/tcp    closed gopher
80/tcp    open   http
|_http-title: Did not follow redirect to https://nmap.org/
113/tcp   closed ident
443/tcp   open   https
| ssl-cert: Subject: commonName=insecure.com
| Subject Alternative Name: DNS:insecure.com, DNS:insecure.org, DNS:issues.nm
ap.org, DNS:issues.npcap.org, DNS:nmap.com, DNS:nmap.net, DNS:nmap.org, DNS:n
pcap.com, DNS:npcap.org, DNS:seclists.com, DNS:seclists.net, DNS:seclists.org
, DNS:sectools.com, DNS:sectools.net, DNS:sectools.org, DNS:secwiki.com, DNS:
secwiki.net, DNS:secwiki.org, DNS:svn.nmap.org, DNS:www.nmap.org
```



El flag -script banner es utilizado para incluir scripts en la ejecución de tareas específicas como captura de banners, fuerza bruta. También permite escribir scripts para automatizar las tareas de escaneo.



Referencia bibliográficas

https://nmap.org/book/port-scanning-options.html

https://respuestasrapidas.com.mx/que-significa-que-un-puerto-esta-filtrado/
https://www.ordenadores-y-portatiles.com/puerto-servidor/
https://nmap.org/book/man-version-detection.html

Hallazgos y/o conclusiones de la actividad desarrollada (Explique su experiencia y el análisis de los resultados):

Pudimos aprender que el comando nmap puede recibir tanto una dirección ip como un dominio para identificar la dirección de un servidor, en la práctica utilizamos el comando nslookup en la url scanme.nmap.org y scanme.nmap.org2 para obtener sus direcciones ip y probamos el comando nmap con ambas la dirección ip y la url siendo los resultados satisfactoriamente coincidentes.

Comprobamos la solidez y poder que tiene el comando Nmap al momento de realizar escaneos con la finalidad de recopilar información la cual será utilizada posteriormente a la hora de identificar vulnerabilidades y posibles amenazas. Debido a que existen diversos tipos de flags el conocimiento de cada una de ellas es casi imposible, por lo cual una buena documentación de dichos comandos,que podemos encontrar en la página nmap.org, nos ayudaron a comprender, estudiar y complementar lo realizado en la práctica de laboratorio.

Comparamos los diferentes banderas simples que pertenecen a un tipo o funciones específicas para el comando Nmap, como fueron las técnicas de scanning para escanear los puertos en la dirección url, descubriendo host para el escaneo de redes locales, especificación de puertos para identificar los tipos de protocolos que pueden usar en la red, detección de sistemas operativos conocer los diferentes de sistemas operativos que pueden estar usan los dispositivos de la red, tiempo y rendimiento para el escaneo de la velocidad que puede tener una comunicación de la red, NSE Scripts escribir scripts simples para automatizar la variedad de tareas de red.

Contribución de esta actividad en su Proyecto:

El comando Nmap nos permitirá saber varias características y recolectar información de la red que pudiéramos analizar en el proyecto, cómo los sistemas operativos que usan los equipos, los puertos que estarían abiertos, los protocolos de red que están utilizando, entre otras características.