

Ficha y Control de Resultados de las Prácticas

Datos de Identificación

Apellido, Nombre	Cédula de Identidad	Nro. de Práctica	Fecha
Diego Bastardo	27948046	14	21/10/2022
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:

Para el desarrollo de esta práctica utilizamos la interfaz gráfica de Zenmap, esta es una herramienta gratuita que podemos utilizar para escanear los puertos de un computador o servicio web. Zenmap fue diseñado para facilitar el uso de los comandos y banderas de Nmap, debido a que los comandos están previamente escritos para nuestro consumo. Recordemos que Nmap es un programa de código abierto que permite escanear en detalle todos los puertos de los dispositivos conectados a una red. De igual forma podemos ver qué puertos hay abiertos en cualquier dispositivo con Zenmap, en esta práctica explicaremos el desarrollo para este proceso, para ello debemos agregar en el apartado de objetivo la dirección IP que corresponde a un equipo, asignamos el Url scanme.nmap.org, introducimos un tipo de escaneo, el cual lo agregamos en el apartado de perfil y por último el tipo de comando con su flag, cabe destacar que podemos tener múltiples perfiles con diferentes tipos de escaneo listo para ejecutarlos.

En la análisis de esta práctica se debe tener en cuenta algunas definiciones antes de abordar los resultados obtenidos, se hicieron algunos escaneos que realizan peticiones http a un url, estas peticiones http son un conjunto de métodos de petición para indicar una acción que se desea realizar para obtener o realizar en un recurso determinado. Método Get, este es utilizado para

siempre recibir o recuperar información de un recurso dado. El método HEAD pide una respuesta idéntica a la de una petición GET, pero sin el cuerpo de la respuesta, es decir, devuelve la información de solo el encabezado.

Al crear un perfil nuevo en Zenmap, estamos indicando el Flag y el tipo de script que va a utilizar el escaneo, esto es muy importante, porque se puede observar diferentes resultados después de ejecutar un escaneo.

```

Zenmap
Escaneo Herramientas Perfil Ayuda (H)
Objetivo: scanme.nmap.org Perfil: Grupo 14 Escaneo
Comando: nmap -T4 -A -v --script vulners scanme.nmap.org

Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos
OS Servidor
scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-13 10:25 Hora estándar de Venezuela
NSE: Loaded 46 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:25
Completed NSE at 10:25, 0.00s elapsed
Initiating NSE at 10:25
Completed NSE at 10:25, 0.00s elapsed
Initiating Ping Scan at 10:25
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 10:25, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:25
Completed Parallel DNS resolution of 1 host. at 10:25, 0.00s elapsed
Initiating SYN Stealth Scan at 10:25
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Completed SYN Stealth Scan at 10:25, 9.96s elapsed (1000 total ports)
Initiating Service scan at 10:25
Scanning 1 service on scanme.nmap.org (45.33.32.156)
Completed Service scan at 10:25, 0.64s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)
Initiating Traceroute at 10:25
Completed Traceroute at 10:25, 0.01s elapsed
NSE: Script scanning 45.33.32.156.
Initiating NSE at 10:25
Completed NSE at 10:25, 1.30s elapsed
Initiating NSE at 10:25
Completed NSE at 10:25, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.033s latency).
Not shown: 928 filtered tcp ports (no-response), 71 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 20.04.2 LTS (Ubuntu Linux; protocol 2.0)
vulners:
| cpe:/a:openbsd:openssh:6.6.1p1:
| CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
| CVE-2015-6564 6.9 https://vulners.com/cve/CVE-2015-6564
| CVE-2018-15919 5.0 https://vulners.com/cve/CVE-2018-15919
| CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617
| CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145
| CVE-2015-5352 4.3 https://vulners.com/cve/CVE-2015-5352
| CVE-2015-6563 1.9 https://vulners.com/cve/CVE-2015-6563
Aggressive OS guesses: Linux 2.6.32 (94%), Linux 2.6.32 or 3.10 (94%), Linux 4.4 (94%), Linux 2.6.32 - 2.6.35 (92%), Linux 2.6.32 - 2.6.39 (92%), Linux 4.0 (91%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 1.00 ms scanme.nmap.org (45.33.32.156)

NSE: Script Post-scanning.
Initiating NSE at 10:25
Completed NSE at 10:25, 0.00s elapsed
Initiating NSE at 10:25
Completed NSE at 10:25, 0.00s elapsed
  
```

```

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
vulners:
| cpe:/a:openssh:openssh:6.6.1p1:
| CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
| CVE-2015-6564 6.9 https://vulners.com/cve/CVE-2015-6564
| CVE-2018-15919 5.0 https://vulners.com/cve/CVE-2018-15919
| CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617
| CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145
| CVE-2015-5352 4.3 https://vulners.com/cve/CVE-2015-5352
| CVE-2015-6563 1.9 https://vulners.com/cve/CVE-2015-6563
Aggressive OS guesses: Linux 2.6.32 (94%), Linux 2.6.32 or 3.10 (94%), Linux 4.4 (94%), Linux 2.6.32 - 2.6.35 (92%), Linux 2.6.32 - 2.6.39 (92%), Linux 4.0 (91%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 1.00 ms scanme.nmap.org (45.33.32.156)

NSE: Script Post-scanning.
Initiating NSE at 10:25
Completed NSE at 10:25, 0.00s elapsed
Initiating NSE at 10:25
Completed NSE at 10:25, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 17.09 seconds
Raw packets sent: 2941 (132.936KB) | Rcvd: 127 (5.988KB)

```

En la imagen mostrada anteriormente, es la ejecución de script vulners en un perfil creado por nosotros de Grupo 14, al crear este perfil estaríamos indicando que flags utilizaremos en la ejecución de este escaneo, el script vulners imprime las vulnerabilidades registradas y las puntuaciones CVSS correspondientes. Estas puntuaciones por sus siglas son sistema de puntuación de vulnerabilidad común, este permite definir numéricamente el nivel de gravedad de un fallo en la seguridad, puede ayudar en indicar a un analista de riesgo qué tan dañino puede resultar explotar una vulnerabilidad.

Objetivo:
scanme.nmap.org
Perfil:
Quick scan

Comando:
nmap -T4 -F scanme.nmap.org

Servidores
Servicios

OS
Servidor

scanme.nmap.org

Salida Nmap
Puertos / Servidores
Topología
Detalles del servidor
Escaneos

nmap -T4 -F scanme.nmap.org

Starting Nmap 7.92 (https://nmap.org) at 2022-10-13 11:04 Hora estándar de Venezuela
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Not shown: 85 filtered tcp ports (no-response)

PORT	STATE	SERVICE
22/tcp	open	ssh
53/tcp	closed	domain
80/tcp	open	http
88/tcp	closed	kerberos-sec
135/tcp	closed	msrpc
389/tcp	closed	ldap
443/tcp	closed	https
445/tcp	closed	microsoft-ds
3389/tcp	closed	ms-wbt-server
49152/tcp	closed	unknown
49153/tcp	closed	unknown
49154/tcp	closed	unknown
49155/tcp	closed	unknown
49156/tcp	closed	unknown
49157/tcp	closed	unknown

Nmap done: 1 IP address (1 host up) scanned in 2.73 seconds

En la imagen anterior, se muestra un escaneo rápido con la herramienta, se cambió el perfil a Quick Scan, es un escaneo rápido ya que limita solo los 100 puertos TCP más comunes, nos indica el estado del puerto en ese momento, podemos observar que dos de los puertos estaban en el estado abierto, el resto de los puertos estaban en el estado cerrado.

The screenshot shows the Nmap Quick Scan Plus interface. The target is 'scanme.nmap.org' and the command is 'nmap -sV -T4 -O -F --version-light scanme.nmap.org'. The scan results show the host is up with a latency of 0.12s. The scan detected 86 filtered TCP ports (no-response) and 71 closed TCP ports (reset). The open ports are 22/tcp (ssh), 53/tcp (domain), 80/tcp (http), 135/tcp (msrpc), 389/tcp (ldap), 443/tcp (https), 445/tcp (microsoft-ds), 3389/tcp (ms-wbt-server), 49152/tcp (unknown), 49153/tcp (unknown), 49154/tcp (unknown), 49155/tcp (unknown), 49156/tcp (unknown), and 49157/tcp (unknown). The OS is detected as Linux 2.6.32 (94%).

```

nmap -sV -T4 -O -F --version-light scanme.nmap.org

Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-13 11:05 Hora estándar de Venezuela
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.12s latency).
Not shown: 86 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 6.6.1p1 Ubuntu Zubuntu2.13 (Ubuntu Linux; protocol 2.0)
53/tcp    closed domain
80/tcp    closed http
135/tcp   closed msrpc
389/tcp   closed ldap
443/tcp   closed https
445/tcp   closed microsoft-ds
3389/tcp  closed ms-wbt-server
49152/tcp closed unknown
49153/tcp closed unknown
49154/tcp closed unknown
49155/tcp closed unknown
49156/tcp closed unknown
49157/tcp closed unknown
Aggressive OS guesses: Linux 2.6.32 (94%), Linux 2.6.32 or 3.10 (94%), Linux 4.4 (94%), Linux 2.6.32 - 2.6.35 (92%), Linux 2.6.32 - 2.6.39 (92%), Linux 2.6.32 - 3.0 (90%), Linux 4.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 0.91 seconds
  
```

En la imagen mostrada anteriormente, se muestra el escaneo rápido plus, es muy parecido a Quick Scan, en cambio este escaneo detalla el sistema operativo y su versión que está operando en el puerto. Si un software o servicio está desactualizado en su sistema operativo esto supone una vulnerabilidad para el sistema. Podemos observar que en el puerto 22/tcp, está usando el sistema operativo de linux ubuntu en su versión 2.13 y Apache ubuntu v2.4.7 y openSSH 6.6.1.

The screenshot shows the Nmap Regular Scan interface. The target is 'scanme.nmap.org' and the command is 'nmap scanme.nmap.org'. The scan results show the host is up with a latency of 0.12s. The scan detected 927 filtered TCP ports (no-response) and 71 closed TCP ports (reset). The open ports are 22/tcp (ssh) and 80/tcp (http). The OS is detected as Linux 2.6.32 (94%).

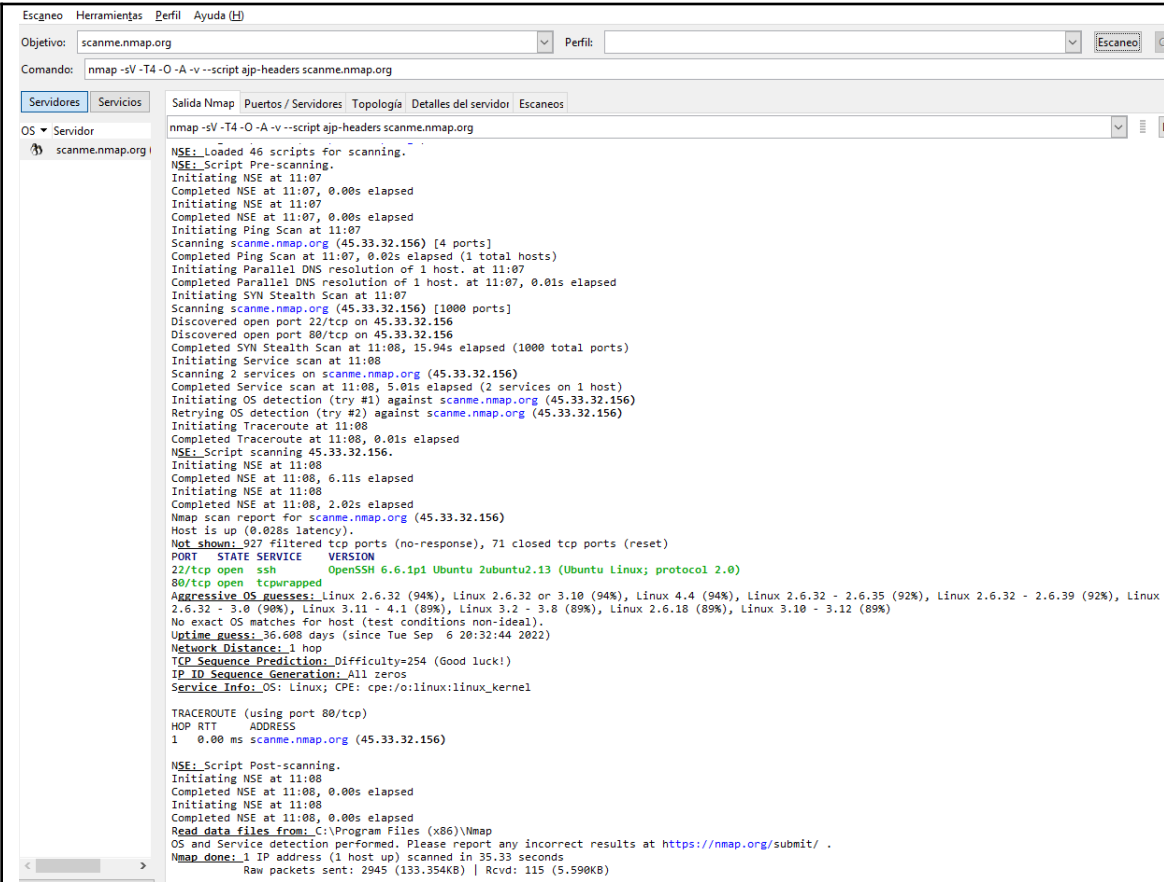
```

nmap scanme.nmap.org

Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-13 10:59 Hora estándar de Venezuela
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.12s latency).
Not shown: 927 filtered tcp ports (no-response), 71 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 22.04 seconds
  
```

El Regular Scan emite un escaneo TCP SYN para los 1000 puertos TCP más comunes, utilizando solicitudes ping para la detección de host.



```
Escaneo Herramientas Perfil Ayuda [H]
Objetivo: scanme.nmap.org Perfil:
Comando: nmap -sV -T4 -O -A -v --script ajp-headers scanme.nmap.org

Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos
OS Servidor scanme.nmap.org
nmap -sV -T4 -O -A -v --script ajp-headers scanme.nmap.org
NSE: Loaded 46 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:07
Completed NSE at 11:07, 0.00s elapsed
Initiating NSE at 11:07
Completed NSE at 11:07, 0.00s elapsed
Initiating Ping Scan at 11:07
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 11:07, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:07
Completed Parallel DNS resolution of 1 host. at 11:07, 0.01s elapsed
Initiating SYN Stealth Scan at 11:07
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Completed SYN Stealth Scan at 11:08, 15.94s elapsed (1000 total ports)
Initiating Service scan at 11:08
Scanning 2 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 11:08, 5.01s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)
Initiating Traceroute at 11:08
Completed Traceroute at 11:08, 0.01s elapsed
NSE: Script scanning 45.33.32.156.
Initiating NSE at 11:08
Completed NSE at 11:08, 6.11s elapsed
Initiating NSE at 11:08
Completed NSE at 11:08, 2.02s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.028s latency).
Not shown: 927 filtered tcp ports (no-response), 71 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  httpd          Apache/2.4.18 (Ubuntu)
Aggressive OS guesses: Linux 2.6.32 (94%), Linux 2.6.32 or 3.10 (94%), Linux 4.4 (94%), Linux 2.6.32 - 2.6.35 (92%), Linux 2.6.32 - 2.6.39 (92%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%), Linux 3.10 - 3.12 (89%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 36.608 days (since Tue Sep 6 20:32:44 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=254 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.00 ms scanme.nmap.org (45.33.32.156)

NSE: Script Post-scanning.
Initiating NSE at 11:08
Completed NSE at 11:08, 0.00s elapsed
Initiating NSE at 11:08
Completed NSE at 11:08, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 35.33 seconds
Raw packets sent: 2945 (133.354KB) | Rcvd: 115 (5.590KB)
```

En la imagen anterior, se muestra un scan combinando varios flags asignados en el perfil, -A, -O y -sV, escaneo agresivo combinando una detección de servicios con una detección del sistema operativo del servidor, nos permite determinar el sistema operativo del objetivo, se usa para la detección de las versiones de los servicios, utilizando de script ajp-headers. En combinación de estas banderas tenemos como resultado, escaneo de los puertos TCP que están abiertos de forma agresiva para detectar la versión y el tipo de sistema operativo que está utilizando ese puerto. Esta información es guardada en la carpeta de Nmap del computador.



Escaneo Herramientas Perfil Ayuda (H)

Objetivo: scanme.nmap.org Perfil: Grupo14-S

Comando: nmap -sV -T4 -v --script fingerprint-strings scanme.nmap.org

Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos

OS ▾ Servidor

scanme.nmap.org

```
nmap -sV -T4 -v --script fingerprint-strings scanme.nmap.org

Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-13 10:56 Hora estándar de Venezuela
NSE: Loaded 45 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Initiating Ping Scan at 10:56
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 10:56, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:56
Completed Parallel DNS resolution of 1 host. at 10:56, 0.00s elapsed
Initiating SYN Stealth Scan at 10:56
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Completed SYN Stealth Scan at 10:56, 11.06s elapsed (1000 total ports)
Initiating Service scan at 10:56
Scanning 1 service on scanme.nmap.org (45.33.32.156)
Completed Service scan at 10:56, 0.23s elapsed (1 service on 1 host)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Not shown: 928 filtered tcp ports (no-response), 71 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.67 seconds
Raw packets sent: 2865 (126.028KB) | Rcvd: 81 (3.232KB)
```

En la figura anterior se muestra, el scan con el flag de -sV y el script fingerprint-strings, este script se usa para la detección de versiones de aplicaciones y servicios de Nmap envía sondeos con nombre a los servicios de destino e intenta identificarlos en función de la respuesta. Cuando no hay ninguna coincidencia, Nmap produce una huella digital de servicio para su envío. A veces, la inspección de esta huella dactilar puede dar pistas sobre la identidad del servicio.

Objetivo:
Perfil:

Comando:

Servidores
Servicios
Salida Nmap
Puertos / Servidores
Topología
Detalles del servidor
Escaneos

OS
Servidor

scanme.nmap.org

```

nmap -sV -T4 -v --script http-headers scanme.nmap.org

Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-13 10:53 Hora estándar de Venezuela
NSE: Loaded 46 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:53
Completed NSE at 10:53, 0.00s elapsed
Initiating NSE at 10:53
Completed NSE at 10:53, 0.00s elapsed
Initiating Ping Scan at 10:53
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 10:53, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:53
Completed Parallel DNS resolution of 1 host. at 10:53, 0.00s elapsed
Initiating SYN Stealth Scan at 10:53
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Completed SYN Stealth Scan at 10:53, 16.26s elapsed (1000 total ports)
Initiating Service scan at 10:53
Scanning 2 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 10:53, 24.04s elapsed (2 services on 1 host)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 10:53
Completed NSE at 10:54, 14.28s elapsed
Initiating NSE at 10:54
Completed NSE at 10:54, 2.03s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Not shown: 927 filtered tcp ports (no-response), 71 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 10:54
Completed NSE at 10:54, 0.00s elapsed
Initiating NSE at 10:54
Completed NSE at 10:54, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.03 seconds
Raw packets sent: 3794 (166.888KB) | Rcvd: 90 (3.620KB)

```

En la figura anterior se muestra, que se utiliza el flag -sV y el script http, recordemos que -sV se usa para la detección de las versiones de los servicios que están corriendo. Con la opción del Script http header, este realiza una solicitud HEAD para la carpeta raíz de un servidor web y muestra los encabezados HTTP devueltos.

Abril 2022

Formato Elaborado por Francis Ferrer



Escaneo Herramientas Perfil Ayuda [H]

Objetivo: scanme.nmap.org Perfil: Escaneo

Comando: nmap -sV -T4 -O -A -v --script ajp-headers scanme.nmap.org

Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos

OS Servidor scanme.nmap.org

```

nmap -sV -T4 -O -A -v --script ajp-headers scanme.nmap.org
NSE: Loaded 46 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:07
Completed NSE at 11:07, 0.00s elapsed
Initiating NSE at 11:07
Completed NSE at 11:07, 0.00s elapsed
Initiating Ping Scan at 11:07
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 11:07, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:07
Completed Parallel DNS resolution of 1 host. at 11:07, 0.01s elapsed
Initiating SYN Stealth Scan at 11:07
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Completed SYN Stealth Scan at 11:08, 15.94s elapsed (1000 total ports)
Initiating Service scan at 11:08
Scanning 2 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 11:08, 5.01s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)
Initiating Traceroute at 11:08
Completed Traceroute at 11:08, 0.01s elapsed
NSE: Script scanning 45.33.32.156.
Initiating NSE at 11:08
Completed NSE at 11:08, 6.11s elapsed
Initiating NSE at 11:08
Completed NSE at 11:08, 2.02s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.028s latency).
Not shown: 927 filtered tcp ports (no-response), 71 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (94%), Linux 2.6.32 or 3.10 (94%), Linux 4.4 (94%), Linux 2.6.32 - 2.6.35 (92%), Linux 2.6.32 - 2.6.39 (92%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%), Linux 3.10 - 3.12 (89%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 36.608 days (since Tue Sep  6 20:32:44 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=254 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP  RTT      ADDRESS
1    0.00 ms scanme.nmap.org (45.33.32.156)

NSE: Script Post-scanning.
Initiating NSE at 11:08
Completed NSE at 11:08, 0.00s elapsed
Initiating NSE at 11:08
Completed NSE at 11:08, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 35.33 seconds
Raw packets sent: 2945 (133.354KB) | Rcvd: 115 (5.590KB)

```

En la figura anterior muestra, Realiza un scan con el flag -sV y el script ajp-headers, el cual hace una solicitud HEAD o GET contra el directorio raíz o cualquier directorio opcional de un servidor de protocolo Apache JServ y devuelve los encabezados de respuesta del servidor. Este puede devolver información para hacer observar alguna petición en ese servidor. La información extraída por este escaneo se guarda en la carpeta de Nmap del computador.

Referencias Bibliográficas

<https://nmap.org/nsedoc/scripts/vulners.html>

<https://www.first.org/cvss/>

<https://es.acervolima.com/metodo-head-solicitudes-de-python/>

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

Ejecutar los comandos directamente en la terminal utilizando Nmap es un método muy querido por una gran cantidad de informáticos, pero por otro lado, las interfaces gráficas cambiaron la forma en la que se veía la informática. A raíz de esta práctica aprendimos a utilizar una herramienta un poco más intuitiva para realizar escaneos. El Zenmap a diferencia del nmap nos mostró una interfaz gráfica en la cual podemos especificar fácilmente los criterios de escaneo que queremos ejecutar. Una ventaja primordial del Zenmap es su capacidad de gestionar diferentes perfiles con distintos tipos de comandos, flags y scripts con la finalidad de hacer diferentes escaneos más rápido. Logramos obtener las diferentes vulnerabilidades de los activos que jugaron el papel de víctimas en nuestra práctica y hacer una recolección de información profunda.

Contribución de esta actividad en su Proyecto:

La interfaz de Zenmap 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, las diferentes vulnerabilidades entre otras características.