Laboratorio 1 de Seguridad de Sistemas Computacionales

Descubrimiento de hosts

Pregunta D1

Únicamente con los datos de descubrimiento obtenidos previamente, ¿cuál host consideraría usted como el más valioso para investigar más a fondo primero? En 2–3 oraciones, justifique su respuesta citando 1 línea exacta de la salida obtenida (incluya la IP). Si no puede seleccionar un host, indique 2–3 datos específicos que le hacen falta y que le ayudarían con la priorización. Límite: 60–80 palabras.

Respuesta D1

No puedo seleccionar un host como el más valioso para investigar más a fondo de primero, dado que muestran cada uno la dirección IP, latencia y dirección MAC.

Para priorizar el host tendría que:

1. Saber la cantidad de puertos abiertos.
2. Saber cuáles son los puertos abiertos, por ejemplo, el puerto 22 de SSH asociados a la IP del host.
3. El sistema operativo, por ejemplo, Unix, Linux, Microsoft Windows, entre otros.

Pregunta D2

Basándose en los datos obtenidos anteriormente, mencione dos hechos y dos aspectos desconocidos sobre hosts específicos. Para cada hecho, refiérase a una línea exacta de la salida que lo respalde (incluya la IP). Para cada desconocido, escriba una oración que explique por qué esa información no se puede inferir todavía a partir del descubrimiento. Límite: 60-80 palabras. ¿Cuál es su nivel de confianza sobre su respuesta y por qué? En 1–2 oraciones, indique su nivel de confianza y respalde su respuesta basado en los resultados obtenidos.

Respuesta D2

Hechos:

1. Nmap escanea las direcciones IP: Nmap scan report for 172.16.10.12
2. Tiene una dirección MAC asociada: MAC Address: C6:0F:AA:37:3C:25

Aspectos desconocidos:

1. Sistema operativo y no se puede inferir esa información dado que no hay ningún indicativo como OS: Unix o similar.
2. Los estados de los puertos que cada dirección IP tiene por ejemplo, abiertos, dado que no indica por ejemplo port 22/tcp open.

Nivel de confianza de la respuesta

Mi nivel de confianza sobre la respuesta es alto, dado que por el tipo de salida se muestran los datos que mencioné y no hay información sobre los puertos ni sistemas operativos, tal como se muestra en la salida.

Comando:

```
nmap -sn 172.16.10.0/24 --exclude 172.16.10.1 --reason
```

Salida que respalda mi respuesta con la IP 172.16.10.12:

```
Nmap scan report for 172.16.10.12
Host is up, received arp-response (0.000029s latency).
MAC Address: C6:0F:AA:37:3C:25 (Unknown)
```

Escaneo de puertos

Práctica E1

Se selecciona un host distinto al anterior.

Anterior = 172.16.10.11

Actual = 172.16.10.12

Comando:

```
nc -zv 172.16.10.12 1-1024
```

Práctica evidenciada basada en el log salida:

```
172.16.10.12: inverse host lookup failed: Unknown host
(UNKNOWN) [172.16.10.12] 80 (http) open
```

Pregunta E1

¿Qué permite concluir (o no) la evidencia obtenida en la Práctica E1 sobre el host escaneado? Refiérase a los resultados obtenidos. Límite: 50 palabras.

Respuesta E1

Lo que afirma la salida es que se ejecuta un escaneo de puertos al host 172.16.10.12 usando netcat e indica que el puerto 80 está abierto y el servicio asociado al mismo, que puede utilizarse para atacar al puerto abierto.

Evidencia:

```
(UNKNOWN) [172.16.10.12] 80 (http) open
```

Práctica E2

Se selecciona un host distinto al anterior.

Anterior = 172.16.10.11

Actual = 172.16.10.12

Comando:

```
nmap -sV -F 172.16.10.12
```

Práctica evidenciada basada en el log de la salida:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-05 18:58 EDT
Nmap scan report for 172.16.10.12
Host is up (0.0000060s latency).
Not shown: 99 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
MAC Address: C6:0F:AA:37:3C:25 (Unknown)
```

Pregunta E2

¿Qué información “accionable” añade nmap -sV -F respecto a la Práctica 1? Mencione 2–3 aspectos respaldados por la salida obtenida en la Práctica 2. Límite: 50 palabras

Respuesta E2

Añade los siguientes aspectos accionables:

1. La versión del servidor web asociado a ese puerto en este caso Apache.
2. Los estados closed de los puertos tcp.
3. Se puede utilizar la versión de Apache para encontrar vulnerabilidades que no han sido resueltas por los parches de seguridad.

Evidencia de la IP 172.16.10.12:

```
Not shown: 99 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
```

Pregunta E3

Con la nueva información de puertos/servicios, ¿qué host investigaría primero ahora? Justifique su respuesta incluyendo dos líneas de la salida obtenida (por ejemplo, presencia de un servicio relevante o combinación de

puertos). ¿Cuál es su nivel de confianza sobre su respuesta y por qué? En 1–2 oraciones, indique su nivel de confianza y respalde su respuesta basado en los resultados obtenidos. Límite: 80 palabras.

Respuesta E3

El host que investigaría primero sería: **172.16.10.13**, porque tiene el puerto 22 ssh abierto, y ssh permite acceso al servidor, siendo vulnerable a un ataque de fuerza bruta, además sé la versión que utiliza, el sistema operativo y el CPE se puede utilizar NMAP para tener más detalles.

Nivel de confianza

Es alto dado que con esa información uno tiene mayor acceso a buscar recursos, por ejemplo, al investigar más sobre el puerto 22, la versión y el CPE.

Evidencia:

```
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.13 (Ubuntu Linux; protocol
2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Captura de banners (banner grabbing)

Práctica B1

Elija un host/puerto diferente al ejemplo anterior y que haya visto abierto. Ejecute: nc -v

Anterior: nc -v 172.16.10.11 21

Actual:

```
nc -v 172.16.10.13 22
```

Evidencia de la salida basada en el log:

```
172.16.10.13: inverse host lookup failed: Unknown host
(UNKNOWN) [172.16.10.13] 22 (ssh) open
SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.13

Invalid SSH identification string.
```

Práctica B2

En un host con servicio web diferente al ejemplo anterior, ejecute una captura de banner: curl --head http://:

Anterior: curl --head http://172.16.10.10:8081

Actual: curl --head http://172.16.10.11:80

Extracto de salida basada en el log:

```
HTTP/1.1 200 OK

□[1mDate□[0m: Fri, 05 Sep 2025 23:27:49 GMT

□[1mServer□[0m: Apache/2.4.58 (Ubuntu)

□[1mLast-Modified□[0m: Mon, 11 Aug 2025 03:56:00 GMT
```

Práctica B3

Utilizando el siguiente comando, intente buscar scripts NSE relacionados con servidores web: Anterior: ls -l /usr/share/nmap/scripts | grep banner

Actual:

```
ls -l /usr/share/nmap/scripts | grep http
```

Extracto de salida basada en el log:

```
-rw-r--r-- 1 root root  2153 May 15 11:37 □[01;31m□[Khttp□[m□[K-adobe-
coldfusion-apsa1301.nse
-rw-r--r-- 1 root root  5149 May 15 11:37 □[01;31m□[Khttp□[m□[K-affiliate-id.nse
-rw-r--r-- 1 root root  1950 May 15 11:37 □[01;31m□[Khttp□[m□[K-apache-
negotiation.nse
```

Pregunta B1

Con la nueva información de puertos/servicios y banners/encabezados, ¿qué host investigaría primero ahora? Justifique su respuesta incluyendo dos líneas exactas de su salida (por ejemplo, un banner revelador o un servicio identificado por nmap). ¿Cuál es su nivel de confianza sobre su respuesta y por qué? En 1–2 oraciones, indique su nivel de confianza y respalde su respuesta basado en los resultados obtenidos. Límite: 80 palabras

Respuesta B1

Evidencia obtenida de la salida basada en el log:

Comando: nc -v 172.16.10.11

```
(UNKNOWN) [172.16.10.11] 80 (http) open
```

Comando:

```
ls -l /usr/share/nmap/scripts | grep http
```

Extracto de salida que analizaría más detalladamente:

```
-rw-r--r-- 1 root root 17388 May 15 11:37 □[01;31m□[Khttp□[m□[K-default-
accounts.nse
-rw-r--r-- 1 root root 13893 May 15 11:37 □[01;31m□[Khttp□[m□[K-domino-enum-
passwords.nse
```

Justificación y razonamiento de la elección

Investigaría primero el host 172.16.10.11 porque tiene abierto el puerto 80, y por el comando de grep se obtuvieron una cantidad considerable de resultados, es por ello que analizaría los scripts instalados localmente como los usuarios y contraseñas y revisaría si el servidor está mal configurado para explotar vulnerabilidades.

Nivel de confianza

Medio-alto, dado de que uno tiene las salidas obtenidas puede investigar más y probar si el servidor está desactualizado.

Enumeración de directorios

Práctica EN1

Elija uno de los directorios encontrados en anteriormente e intente acceder con el navegador. Si encuentra un error (p. ej., 403/401/404) o una redirección, tome nota.

Comando:

```
dirsearch -u http://172.16.10.10:8081/
```

Elección de directorio Con http://172.16.10.10:8081/upload

Se obtiene un redireccionamiento hacia una página que permite subir una imagen con los formatos jpg, jpeg, gif and png.

Pregunta EN1

Con base en lo que vio en el navegador y en la línea correspondiente de dirsearch, explique en 1–2 oraciones si el hallazgo es útil para continuar la investigación y por qué. Límite: 50 palabras.

Respuesta EN1

En mi opinión el hallazgo presenta utilidad, dado que uno puede descubrir si la página tiene más páginas accesibles desde la raíz y saber cuáles tiene éxito como el 200 o un error como 500, es decir los código de

estado de HTTP.

Evidencia basada en el log:

```
□[32m[19:34:26] 200 -  380B  - /upload□[0m
```

Referencia a lo visto en el navegador para esa ruta:

```
ACME Hyper Branding

Uplod any image!

This form supports file formats such as: jpg, jpeg, gif and png.

Browse... No file selected       Upload
```

Es decir, se muestra una página que permite subir cualquier archivo que cumpla con el formato.

Anotación: Se escribe la imagen dado que markdown al pasarlo a pdf no soporta imagenes, la información fue extraida de la imagen guardada durante el laboratorio.

Práctica EN2

Anterior: dirsearch -u http://172.16.10.10:8081/

Actual:

```
dirsearch -u http://172.16.10.11:80/
```

Pregunta EN2

De su ejecución, seleccione dos resultados con códigos diferentes (por ejemplo, 200 y 403/302) y refiérase a esas líneas en su explicación. En 2–3 oraciones, describa qué infiere de cada código en este contexto (p. ej., “existe y es accesible”, “existe pero requiere autorización”, “redirecciona”). Límite: 80 palabras.

Respuesta EN2

Evidencia basada en el log:

```
□[34m[19:46:21] 403 -  277B  - /.htaccess.bak1□[0m
□[32m[19:46:31] 200 -  481B  - /backup/□[0m
```

Explicación del significado de cada código en este contexto:

1. En el primer caso existe pero requiere autorización, dado que el codigo 403 de HTTP significa que el servidor rechaza enviar la respuesta porque no se tienen los permisos necesarios.
2. En el segundo caso existe y es accesible, dado que muestra el índice del backup dividido en tres columnas:

Name	Last modified	Size Description
Parent Directory		
acme-hyper-branding/	2025-08-11 03:57	