Informe de Reconocimiento y Escaneo del Host 192.168.1.3

---

1. Verificación de conectividad con `ping`

Comando ejecutado:

ping -c 3 192.168.1.3

Explicación:
Se utiliza el comando `ping` para comprobar si el host objetivo responde a solicitudes ICMP. Esto permite verificar la conectividad y medir la latencia de la red entre el equipo atacante y el objetivo. El parámetro `-c 3` envía únicamente tres paquetes ICMP.

Resultado obtenido:
El host respondió a los tres paquetes enviados, mostrando una latencia promedio de **0.28 ms** con un **0% de pérdida de paquetes**, lo que confirma que el objetivo está en línea y accesible.

---

2. Consulta DNS inversa con `nslookup`

Comando ejecutado:

nslookup 192.168.1.3

Explicación:
El comando `nslookup` intenta resolver la dirección IP en un nombre de host mediante registros PTR en el servidor DNS configurado. Esto puede revelar información sobre el nombre del sistema o su rol en la red.

Resultado obtenido:
La consulta devolvió el error **NXDOMAIN**, indicando que no existe un registro PTR para la IP `192.168.1.3`. Esto es habitual en redes locales sin DNS configurado.

---

3. Consulta DNS inversa con `dig`

Comando ejecutado:

dig -x 192.168.1.3

Explicación:
`dig` es una herramienta avanzada de consultas DNS. La opción `-x` solicita específicamente la resolución inversa de la IP hacia un posible nombre de dominio.

Resultado obtenido:
La respuesta fue negativa, confirmando que no hay registros PTR asociados a la IP analizada. El servidor DNS (8.8.8.8) respondió con estado **NXDOMAIN**.

---

4. Escaneo de puertos y servicios con Nmap

Comando ejecutado:

nmap -sS -sV -O -Pn 192.168.1.3

Explicación:
Este comando realiza un escaneo TCP SYN (`-sS`) para identificar puertos abiertos sin establecer conexiones completas, lo que reduce la probabilidad de ser detectado por sistemas IDS. La opción `-sV` permite detectar versiones de los servicios en ejecución. Con `-O` se intenta identificar el sistema operativo y `-Pn` desactiva el ping previo, asumiendo que el host está activo.

Resultado obtenido:
Se detectaron los siguientes puertos abiertos y servicios:

- **22/tcp** – OpenSSH 9.6p1 (Ubuntu).
- **3000/tcp** – Servicio no reconocido (posiblemente web interno).
- **7070/tcp** – ssl/realserver.
- **8080/tcp** – Apache httpd 2.4.25 (Debian).
- **8081/tcp** – Apache httpd 2.4.7 (Ubuntu).

- **8082/tcp** – Apache httpd 2.4.7 (Ubuntu).
- **8083/tcp** – Apache Tomcat.
- **9000/tcp** – Gophish httpd.

Se identificó el sistema operativo como **Linux kernel 4.x - 5.x**, con una distancia de red de 1 salto.

---

5. Escaneo de vulnerabilidades con Nmap NSE

Comando ejecutado:

nmap --script=vuln -p 8081 192.168.1.3

Explicación:
Se utilizó el script `vuln` de Nmap para el puerto 8081, con el objetivo de detectar posibles vulnerabilidades en el servicio web que corre en ese puerto. Estos scripts analizan fallos conocidos basados en la respuesta del servicio.

Resultado obtenido:
El puerto **8081/tcp** está abierto y etiquetado como `blackice-icecap`. El script `broadcast-avahi-dos` reportó el CVE-2011-1002 como una referencia, pero indicó que los hosts analizados **no son vulnerables** a dicho DoS.

---

6. Escaneo con salida a archivo para documentación

Comando ejecutado:

nmap -sS -sV -O -oN mutillidae_scan.txt 192.168.1.3

Explicación:
Se repitió el escaneo SYN con detección de servicios y sistema operativo, pero esta vez se almacenó la salida en el archivo `mutillidae_scan.txt` para generar evidencias documentales.

Resultado obtenido:
Los resultados fueron consistentes con el escaneo anterior, confirmando los mismos puertos y servicios. El archivo `mutillidae_scan.txt` contiene el reporte detallado con banners de servicio y el fingerprint del sistema operativo.

Resumen General del Reconocimiento

El host `192.168.1.3` está activo, con múltiples servicios expuestos en puertos web (8080, 8081, 8082, 8083, 9000), además de SSH (22/tcp). Entre ellos destaca Apache httpd en diferentes versiones y un servicio Apache Tomcat. Este nivel de exposición sugiere que el host es un entorno de pruebas con varias aplicaciones vulnerables desplegadas.