Clase HE 24/25
Informe de resultados de la evaluación de la seguridad
Metasploitable 2

Fecha: 18 de diciembre de 2024
Proyecto: 100-01
Version 1.0

Índice general

Información de contacto

Nombre	Título	Contacto
José María Alcaraz	Docente / Principal	Email: josemaria.alcaraz2@murciaeduca.es

Antecedentes

El pasado 11 de diciembre de 2024, durante una sesión de clase de Hacking Ético, asigné a mis alumnos la tarea de realizar su primera auditoría de seguridad en un lapso aproximado de 3 horas. Tras recibir sus reportes a través de la plataforma Moodle, ahora procederé, como docente, a presentar mi propia auditoría realizada bajo las mismas condiciones de tiempo.

Para hacer más realista dicha auditoría, vamos a suponer que es para un cliente. El cliente solicita ayuda a los participantes de la clase de Hacking Ético en el instituto Ingeniero de la Cierva 2024/2025 debido a un fallo de seguridad detectado en una de sus máquinas. Según indica, se trata de una máquina virtual antigua que pertenecía al anterior informático de la empresa. Desde que esta persona dejó su puesto, nadie la ha actualizado ni sabe cómo acceder a ella, ya que actualmente no tienen personal informático en plantilla.

El único dato que poseen es la dirección IP de la máquina. Al parecer, el cliente tiene indicios de que alguien podría haber accedido a dicha máquina sin autorización, pero desconoce cómo se ha producido dicho acceso. Por ello, solicita a los participantes de la clase que realicen una auditoría de seguridad de la máquina virtual e intenten identificar las posibles vías de acceso utilizadas por los atacantes.

Fases de la auditoria

Las fases de las actividades de pruebas de penetración incluyen las siguientes:

- **Planificación** – Se recopilan los objetivos del cliente y se obtienen las reglas de compromiso.
- **Descubrimiento** – Se realizan análisis y enumeración para identificar posibles vulnerabilidades, áreas débiles y exploits.
- **Ataque** – Se confirman las vulnerabilidades potenciales a través de la explotación y se realiza un descubrimiento adicional tras obtener nuevos accesos.
- **Reporte** – Se documentan todas las vulnerabilidades y exploits encontrados, los intentos fallidos y las fortalezas y debilidades de la empresa.

Calificación de la gravedad

La siguiente tabla define los niveles de gravedad y el rango de puntuación CVSS correspondiente que se utilizan a lo largo del documento para evaluar las vulnerabilidades y el impacto del riesgo.

Gravedad	Rango de puntuación CVSS V3	Definición
Crítica	9.0 – 10.0	La explotación es directa y, por lo general, resulta en un compromiso a nivel de sistema. Se recomienda crear un plan de acción y aplicar parches de inmediato.
Alta	7.0 – 8.9	La explotación es más difícil pero podría ocasionar privilegios elevados y, potencialmente, la pérdida de datos o interrupciones en el servicio. Se recomienda crear un plan de acción y aplicar parches lo antes posible.
Moderada	4.0 – 6.9	Existen vulnerabilidades, pero no son explotables directamente o requieren pasos adicionales, como ingeniería social. Se recomienda crear un plan de acción y aplicar parches después de resolver los problemas de alta prioridad.
Baja	0.1 – 3.9	Las vulnerabilidades no son explotables, pero aumentan la superficie de ataque de la organización. Se recomienda crear un plan de acción y aplicar parches durante la próxima ventana de mantenimiento.
Informativa	N/A	No existe vulnerabilidad conocida. Se proporciona información adicional sobre elementos observados durante la prueba, controles robustos y documentación adicional.

Alcance

Exclusiones del alcance

El cliente especificó que no se debían crear, modificar ni eliminar ningún archivo o carpeta del servidor.

Permisos otorgados

No se proporcionaron permisos especiales para ayudar en la realización de la auditoría.

Información adicional proporcionada

El cliente nos proporciona la siguiente dirección IP: 192.168.56.101

Planificación

La fase de planificación es esencial para garantizar que la auditoría de seguridad se realice de manera controlada y cumpliendo con los objetivos definidos por el cliente. En este caso, como parte del escenario simulado en el contexto de la clase de Hacking Ético, se establecieron los siguientes objetivos y reglas de compromiso:

- **Objetivos del cliente:** El cliente ficticio, representado por una empresa que opera sin personal técnico en plantilla, planteó un problema relacionado con una máquina virtual antigua que había quedado desatendida desde la salida de su último informático. El principal objetivo de la auditoría es identificar posibles vulnerabilidades que permitan o hayan permitido accesos no autorizados, comprender cómo se pudo haber comprometido dicha máquina y proporcionar recomendaciones claras para mitigar los riesgos identificados.
- **Contexto del cliente:** La máquina virtual en cuestión no ha sido actualizada ni gestionada durante un periodo prolongado. El único dato proporcionado por el cliente es la dirección IP de la máquina, ya que no cuentan con credenciales ni documentación adicional. Esto refleja un escenario realista donde los auditores deben trabajar con información limitada y depender de técnicas de descubrimiento y enumeración.
- **Reglas de compromiso:** El cliente especificó explícitamente las siguientes restricciones:
  - No crear, modificar ni eliminar ningún archivo o carpeta en la máquina virtual.
  - No realizar ataques destructivos, como pruebas de Denegación de Servicio (DoS).
  - Limitar el tiempo de la auditoría a un máximo de 3 horas.

  Estas reglas aseguran que la auditoría se realice de forma controlada y que no se comprometa la integridad de los sistemas evaluados.
- **Preparativos:** Antes de iniciar la auditoría, se definió un plan de acción detallado que incluye las herramientas y técnicas a utilizar. Entre ellas:
  - Herramientas para escaneo de red y enumeración de servicios, como `nmap`.
  - Herramientas de análisis de vulnerabilidades para evaluar los servicios detectados.
  - Herramientas de explotación de vulnerabilidades, como `metasploit`

  Además, se estableció un flujo de trabajo claro para registrar todas las actividades realizadas, documentar cualquier vulnerabilidad identificada y garantizar que el análisis fuera replicable.
- **Alcance temporal:** Se asignó un tiempo máximo de 3 horas para completar la auditoría, incluyendo las fases de descubrimiento, análisis y documentación inicial.

En esta etapa, se dejó claro que el propósito principal de la auditoría no era únicamente identificar vulnerabilidades, sino también proporcionar a los participantes un enfoque práctico y controlado de cómo realizar un análisis de seguridad estructurado en un entorno profesional.

Descubrimiento

Debido a la limitación de tiempo, es posible que la fase de descubrimiento esté incompleta.

Puertos abiertos

Listing 1: Comando Nmap usado

```
nmap -sS -sV -O -T3 --top-ports 1000 --reason --open 192.168.56.101
```

Puerto	Estado	Servicio	Detalles
21/tcp	Abierto	FTP	vsftpd 2.3.4
22/tcp	Abierto	SSH	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	Abierto	Telnet	Linux telnetd
25/tcp	Abierto	SMTP	Postfix smtpd
53/tcp	Abierto	DNS	ISC BIND 9.4.2
80/tcp	Abierto	HTTP	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	Abierto	RPCbind	Versión 2 (RPC #100000)
139/tcp	Abierto	NetBIOS-SSN	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	Abierto	NetBIOS-SSN	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	Abierto	Exec	netkit-rsh rexecd
513/tcp	Abierto	Login	OpenBSD o Solaris rlogind
514/tcp	Abierto	Shell	Netkit rshd
1099/tcp	Abierto	Java-RMI	GNU Classpath grmiregistry
1524/tcp	Abierto	Bind Shell	Metasploitable root shell
2049/tcp	Abierto	NFS	Versiones 2-4 (RPC #100003)
2121/tcp	Abierto	FTP	ProFTPD 1.3.1
3306/tcp	Abierto	MySQL	MySQL 5.0.51a-3ubuntu5
5432/tcp	Abierto	PostgreSQL	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	Abierto	VNC	VNC (protocolo 3.3)
6000/tcp	Abierto	X11	Acceso denegado
6667/tcp	Abierto	IRC	UnrealIRCd
8009/tcp	Abierto	AJP13	No identificado claramente (ajp13?)
8180/tcp	Abierto	HTTP	Apache Tomcat/Coyote JSP engine 1.1

Información Adicional:

- **Sistema Operativo Estimado:** Linux 2.6.X (detalles: Linux 2.6.9 - 2.6.33).
- **CPE OS:** cpe:/o:linux:linux_kernel:2.6.
- **Distancia de Red:** 1 salto.
- **Información del Host:**
  - **MAC Address:** 08:00:27:25:81:9F (Oracle VirtualBox virtual NIC).
  - **Nombres de Host:** metasploitable.localdomain, irc.Metasploitable.LAN.
- **Servicio OS y detección:** Realizado correctamente.

Vulnerabilidades

Objetivo: Identificar puertos abiertos, servicios activos y vulnerabilidades en el sistema objetivo utilizando el reporte de Nessus.

Resultados obtenidos: Se identificaron varias vulnerabilidades significativas durante la fase de descubrimiento. A continuación, se destacan las más relevantes. Debido al límite de tiempo disponible para la auditoría, muchas vulnerabilidades no serán tratadas en este informe.

Puerto	Gravedad	Descripción
`5900 (tcp/vnc)`	**Crítica**	El servidor VNC permite autenticación con una contraseña débil (`"password"`), lo que podría permitir a un atacante tomar control del sistema.
`1524 (tcp/wild_shell)`	**Crítica**	Se detectó un backdoor activo que permite acceso remoto no autenticado, comprometiendo el sistema.
`80 (tcp/www)`	**Crítica**	phpMyAdmin en versiones anteriores a 4.8.6 es vulnerable a inyecciones SQL, exponiendo o modificando datos arbitrarios.
`80 (tcp/www)`	**Crítica**	Vulnerabilidad en PHP-CGI que permite a un atacante ejecutar comandos en el sistema afectado.
`8180 (tcp/www)`	**Crítica**	La versión de Apache Tomcat instalada (<= 5.5.x) ha alcanzado su fin de vida útil, exponiendo múltiples vulnerabilidades no resueltas.
`8009 (tcp/ajp13)`	**Crítica**	Vulnerabilidad 'Ghostcat' en el conector AJP de Apache Tomcat permite lectura de archivos y ejecución remota de código.
`22 (tcp/ssh)`	**Crítica**	Debilidad en Debian OpenSSH/OpenSSL permite generar claves SSH vulnerables, facilitando ataques de fuerza bruta y MITM.
`22 (tcp/ssh)`	**Crítica**	La cuenta `service` utiliza una contraseña por defecto `"service"`, lo que permite acceso administrativo remoto.
`23 (tcp/telnet)`	**Crítica**	La cuenta `user` utiliza una contraseña por defecto `üser"`, permitiendo escalada de privilegios en el sistema.
`21 (tcp/ftp)`	**Crítica**	Versión vulnerada de vsFTPd permite apertura de un shell de escucha en el puerto 6200 mediante un backdoor integrado.
`513 (tcp/rlogin)`	**Alta**	El servicio rlogin transmite datos en texto claro, exponiendo credenciales a posibles ataques de interceptación.

(Continuación de la tabla anterior)

Puerto	Gravedad	Descripción
445 (tcp/cifs)	**Alta**	Vulnerabilidad conocida como 'Badlock' en Samba permite ataques man-in-the-middle comprometiendo la autenticación.
2049 (tcp/rpc-nfs)	**Alta**	El servidor NFS permite acceso sin restricciones a recursos compartidos, exponiendo información sensible.
80 (tcp/www)	**Alta**	La versión de TWiki instalada permite ejecutar comandos arbitrarios mediante manipulación del parámetro 'rev'.
53 (udp/dns)	**Alta**	La versión de ISC BIND es vulnerable a ataques Reflected DoS y degradación de rendimiento debido a configuraciones inseguras.
23 (tcp/telnet)	**Media**	El servidor Telnet está sin cifrado, exponiendo credenciales y comandos en texto claro.
8180 (tcp/www)	**Media**	Archivos por defecto en Apache Tomcat revelan información sobre la configuración del servidor.
6000 (tcp/x11)	**Baja**	El servidor X11 expone tráfico no cifrado, permitiendo a un atacante eavesdropping sobre conexiones gráficas remotas.
111 (tcp/rpcbind)	**Informativa**	Enumeración de servicios RPC mediante solicitud DUMP a portmapper. Esto permite identificar servicios y puertos asociados que podrían ser explotados.

Enumeración de usuarios

Durante la enumeración del sistema, se identificaron los siguientes usuarios. Estos se han clasificado en dos categorías: **usuarios nativos del sistema Linux** y **usuarios asociados a software de terceros**.

Usuarios nativos del sistema Linux:

Usuario	RID
root	0x3e8
daemon	0x3ea
bin	0x3ec
sys	0x3ee
sync	0x3f0
games	0x3f2
man	0x3f4
lp	0x3f6
mail	0x3f8
news	0x3fa
uucp	0x3fc
nobody	0x1f5
proxy	0x402
backup	0x42c
syslog	0x4b4
sshd	0x4b8
dhcp	0x4b2
klog	0x4b6
list	0x434

Usuarios asociados a software de terceros:

Usuario	RID	Software Asociado
www-data	0x42a	Servidor Web Apache
postgres	0x4c0	PostgreSQL
mysql	0x4c2	MySQL Server
proftpd	0x4ca	ProFTPD
tomcat55	0x4c4	Apache Tomcat
distccd	0x4c6	distcc Daemon
irc	0x436	Servidor IRC
telnetd	0x4c8	Servicio Telnet
ftp	0x4be	Servicio FTP
bind	0x4ba	Servidor DNS (BIND)
libuuid	0x4b0	Librería UUID
msfadmin	0xbb8	Usuario de prueba (Metasploitable)
user	0xbba	Usuario de prueba (Metasploitable)
service	0xbbc	Usuario de servicio

Ataque y reporte

Contraseña por defecto en cuenta `service` (Crítica)

Gravedad	CVSS	Descripción
Crítica	9.0	La cuenta `service` utiliza una contraseña por defecto (`"service"`), permitiendo acceso administrativo remoto al sistema vulnerable.

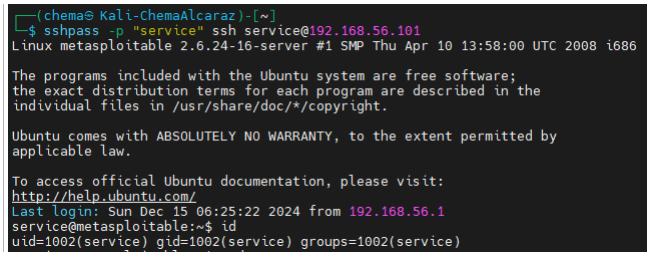
Descripción: La cuenta `service` utiliza una contraseña por defecto preconfigurada (`"service"`). Esta mala práctica permite a un atacante autenticarse y obtener privilegios administrativos en el sistema remoto a través del puerto SSH.

Impacto: El acceso no autorizado a la cuenta con privilegios administrativos permite a un atacante realizar cambios en el sistema, robar información o comprometer completamente la seguridad.

Evidencia: Salida del comando:

```
ssh service@192.168.56.101
```

Autenticación exitosa utilizando la contraseña por defecto `service`.



Recomendación:

- Cambiar la contraseña de la cuenta `service` por una contraseña robusta.
- Deshabilitar la cuenta si no es necesaria.
- Configurar políticas de contraseñas seguras.

Contraseña por defecto en cuenta `user` (Crítica)

Gravedad	CVSS	Descripción
Crítica	9.0	La cuenta `user` utiliza una contraseña por defecto (`üser"`), lo que permite a un atacante obtener acceso remoto y escalar privilegios en el sistema.

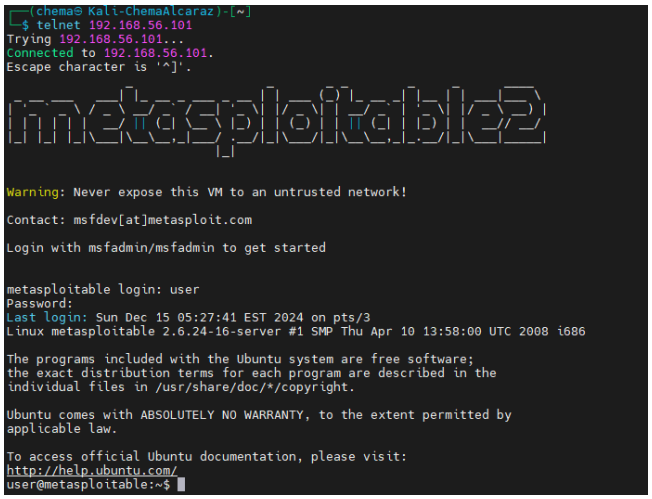
Descripción: La cuenta `user` utiliza una contraseña por defecto preconfigurada (`üser"`). Esta vulnerabilidad facilita que un atacante obtenga acceso al sistema a través del servicio Telnet (puerto 23).

Impacto: El acceso no autorizado a la cuenta permite al atacante ejecutar comandos en el sistema, acceder a datos sensibles y realizar escalada de privilegios.

Evidencia: Salida del comando:

```
telnet 192.168.56.101
```

Autenticación exitosa utilizando la contraseña por defecto `user`.



Recomendación:

- Cambiar la contraseña de la cuenta `user` por una contraseña robusta.
- Deshabilitar la cuenta si no es necesaria.
- Configurar políticas de contraseñas seguras.

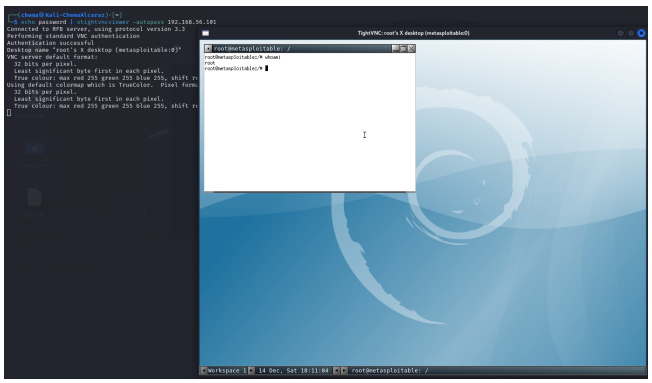
Servidor VNC con contraseña débil ("password") (Crítica)

Gravedad	CVSS	Descripción
Crítica	10.0	El servidor VNC permite autenticación con una contraseña débil ("password"). Esto podría permitir a un atacante tomar control completo del sistema afectado.

Descripción: Se detectó que el servidor VNC en el puerto **5900/tcp** utiliza una contraseña predeterminada débil ("password"), que no cumple con los estándares básicos de seguridad. Esta vulnerabilidad permite a un atacante remoto autenticarse sin dificultad y tomar control del sistema. El servidor VNC vulnerable fue identificado en el host **192.168.56.101**.

Impacto: La explotación de esta vulnerabilidad puede resultar en el control remoto completo del sistema afectado, comprometiendo la confidencialidad, integridad y disponibilidad de los datos. Un atacante podría usar este acceso para instalar malware, exfiltrar información sensible o realizar actividades maliciosas en la red.

Evidencia: Se obtuvo acceso al servidor VNC utilizando la contraseña predeterminada ("password") con herramientas como `Nmap` y `vncviewer`.



Recomendación:

- Cambiar inmediatamente la contraseña del servidor VNC por una contraseña segura, que cumpla con los estándares de complejidad (mínimo 12 caracteres, con mezcla de letras, números y símbolos).
- Deshabilitar las cuentas con contraseñas predeterminadas o débiles.
- Configurar controles de acceso adicionales, como la autenticación basada en certificados o listas de control de acceso (ACL).
- Implementar mecanismos de monitoreo para detectar accesos no autorizados al servidor VNC.

Backdoor activo en Bind Shell (Crítica)

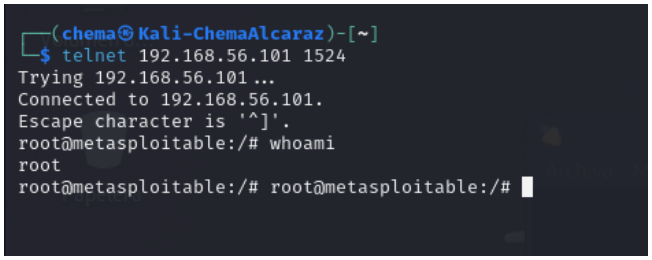
Gravedad	CVSS	Descripción
Crítica	10.0	Se detectó un backdoor activo en el puerto **1524/tcp**, permitiendo a un atacante acceder remotamente con privilegios de root sin autenticación.

Descripción: Un atacante puede explotar esta vulnerabilidad para obtener acceso remoto al sistema mediante un shell activo (bind shell) en el puerto **1524/tcp**. Este tipo de backdoor fue instalado probablemente como resultado de un compromiso previo y brinda acceso administrativo al sistema comprometido.

Impacto: La presencia de este backdoor pone en grave riesgo la seguridad del sistema y de toda la red asociada. Un atacante puede:

- Ejecutar comandos con privilegios de root.
- Instalar malware o herramientas maliciosas adicionales.
- Acceder, modificar o eliminar información crítica.
- Usar el sistema como un punto de entrada para comprometer otros dispositivos en la red.

Evidencia: Durante el escaneo, se detectó la presencia de un servicio activo en el puerto **1524/tcp**, identificado como un shell remoto accesible sin autenticación.



Recomendación:

- Cerrar inmediatamente el puerto **1524/tcp** en el firewall para evitar accesos no autorizados.
- Analizar el sistema para detectar otros backdoors o herramientas maliciosas.
- Reinstalar el sistema operativo afectado desde una fuente confiable para garantizar la eliminación completa del backdoor.
- Implementar medidas de detección de intrusiones (IDS) y monitoreo de tráfico para identificar actividades sospechosas.
- Revisar y fortalecer las políticas de acceso remoto y autenticación.

Backdoor en vsftpd 2.3.4 (Crítica)

Gravedad	CVSS	Descripción
Crítica	9.8	La versión de `vsftpd 2.3.4` contiene una puerta trasera que permite abrir una shell de escucha en el puerto 6200 enviando un nombre de usuario específico.

Descripción: La versión `vsftpd 2.3.4` del servidor FTP contiene una puerta trasera introducida por un atacante desconocido en el código fuente original. Si se envía un nombre de usuario que termine en el carácter '`:)`', el servicio abrirá una shell de escucha en el puerto 6200 permitiendo la ejecución remota de comandos como el usuario **root**.

Impacto: Un atacante no autenticado puede obtener acceso completo al sistema como usuario **root**, comprometiendo la confidencialidad, integridad y disponibilidad del sistema.

Evidencia:

```
# telnet 192.168.56.101 21
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
user chema:)
331 Please specify the password.
pass invalid
^]
telnet> quit
Connection closed.

# telnet 192.168.56.101 6200
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
id;
uid=0(root) gid=0(root)
```

Recomendación:

- **Actualizar** la versión de `vsftpd` a la última versión estable disponible que no contenga esta vulnerabilidad.
- **Verificar** la integridad del código fuente o de los binarios descargados para evitar versiones comprometidas.
- **Monitorear y restringir** el acceso al puerto 21 y 6200 mediante un firewall o políticas de red.
- **Deshabilitar temporalmente** el servicio FTP si no es absolutamente necesario.

phpMyAdmin vulnerable a inyecciones SQL (Crítica)

Gravedad	CVSS	Descripción
Crítica	9.8	phpMyAdmin en versiones anteriores a **4.8.6** es vulnerable a inyecciones SQL, exponiendo datos sensibles o permitiendo modificaciones arbitrarias en la base de datos.

Descripción: El servicio phpMyAdmin en el puerto **80/tcp** se encontró en una versión obsoleta (**3.1.1**), conocida por ser vulnerable a inyecciones SQL (SQLi). Esta vulnerabilidad permite a un atacante enviar consultas SQL maliciosas al servidor, comprometiendo la confidencialidad e integridad de la base de datos.

Impacto: Un atacante puede explotar esta vulnerabilidad para:

- Acceder a información sensible almacenada en la base de datos (e.g., contraseñas, datos de usuarios, etc.).
- Modificar o eliminar registros críticos.
- Obtener acceso administrativo al servidor de la base de datos.
- Escalar privilegios para comprometer otros servicios conectados.

Evidencia: El escaneo identificó phpMyAdmin ejecutándose en la versión **3.1.1**, que es anterior a la versión segura **4.8.6**.

Sin evidencia grafica. Link a CVE: CVE-2019-11768

Recomendación:

- Actualizar phpMyAdmin a la última versión disponible (4.8.6 o superior).
- Restringir el acceso al servicio phpMyAdmin mediante listas de control de acceso (ACL).
- Configurar parámetros seguros en el servidor de la base de datos, como limitar usuarios con permisos administrativos.
- Monitorear y registrar las actividades en el servicio phpMyAdmin para detectar posibles intentos de explotación.

PHP-CGI permite ejecución remota de comandos (Crítica)

Gravedad	CVSS	Descripción
Crítica	9.8	Una configuración insegura en PHP-CGI permite a un atacante pasar argumentos arbitrarios y ejecutar comandos en el sistema afectado.

Descripción: El servidor web que opera en el puerto **80/tcp** contiene una instalación vulnerable de **PHP-CGI** que permite a un atacante remoto ejecutar comandos arbitrarios en el sistema. Esta vulnerabilidad se produce debido a que el parámetro de consulta puede manipularse para enviar argumentos de línea de comandos directamente a PHP.

Impacto: Un atacante puede explotar esta vulnerabilidad para:

- Ejecutar comandos con los mismos privilegios que el usuario del servidor web.
- Comprometer la seguridad del sistema completo.
- Exfiltrar datos sensibles almacenados en el servidor.
- Instalar malware o persistencias maliciosas en el servidor afectado.

Evidencia: Se detectó una versión vulnerable de PHP-CGI configurada en el servidor web.

Recomendación:

- Actualizar PHP-CGI a una versión más reciente que no esté afectada por esta vulnerabilidad (recomendado: 5.3.13 o superior).
- Revisar la configuración del servidor web para asegurarse de que no se permiten parámetros arbitrarios en el intérprete PHP.
- Implementar restricciones en el acceso al servidor web para evitar intentos de explotación.
- Monitorear y registrar las actividades del servidor para detectar intentos de explotación.

Servicio rlogin transmite datos en texto claro (Crítica)

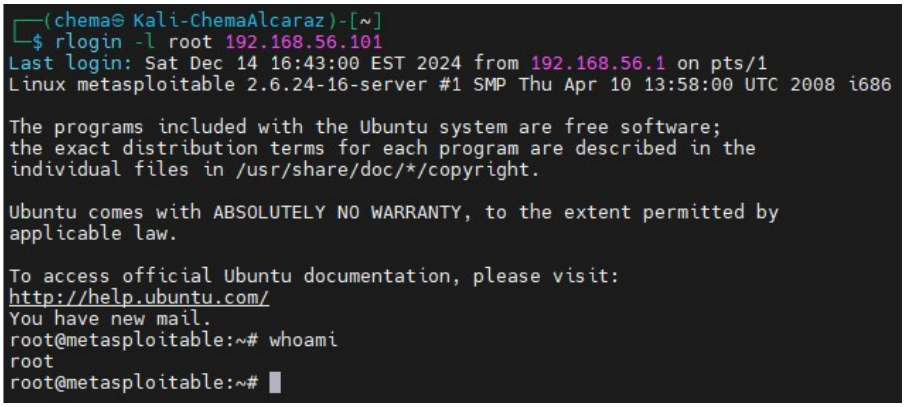
Gravedad	CVSS	Descripción
Crítica	9.8	El servicio rlogin en el puerto **513/tcp** transmite datos, incluidas credenciales, en texto claro, exponiéndolos a posibles ataques de interceptación.

Descripción: El servicio rlogin detectado en el puerto **513/tcp** permite a los usuarios autenticarse y acceder remotamente al sistema. Sin embargo, este protocolo transmite los datos en texto claro, lo que lo hace vulnerable a ataques de tipo "man-in-the-middlez permite que un atacante intercepte credenciales o comandos.

Impacto: Un atacante que intercepte el tráfico rlogin podría:

- Obtener credenciales de usuarios en texto claro.
- Suplantar la identidad de usuarios legítimos y acceder al sistema afectado.
- Ejecutar comandos maliciosos en el sistema con los privilegios del usuario autenticado.
- Comprometer la confidencialidad de la comunicación entre el cliente y el servidor.

Evidencia: Durante el escaneo, se identificó el servicio rlogin en el puerto **513/tcp**.



Recomendación:

- Deshabilitar inmediatamente el servicio rlogin en el sistema afectado.
- Configurar **SSH** como alternativa segura para accesos remotos.
- Actualizar las políticas de acceso remoto para prohibir el uso de protocolos no cifrados.
- Implementar reglas en el firewall para bloquear conexiones al puerto **513/tcp**.
- Monitorear la red en busca de intentos de conexión al servicio rlogin.

Badlock en Samba permite ataques man-in-the-middle (Alta)

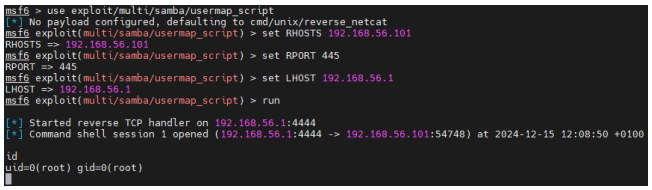
Gravedad	CVSS	Descripción
Alta	7.8	La vulnerabilidad Badlock en Samba permite a un atacante realizar ataques man-in-the-middle para interceptar y modificar el tráfico entre clientes y servidores.

Descripción: El servicio Samba identificado en los puertos **139/tcp** y **445/tcp** contiene una vulnerabilidad conocida como **Badlock**, que afecta la autenticación de SMB. Este fallo permite a un atacante interceptar el tráfico de la red y, en algunos casos, reducir el nivel de seguridad del protocolo para manipular llamadas SMB.

Impacto: Un atacante puede explotar esta vulnerabilidad para:

- Interceptar credenciales de usuarios en tránsito.
- Modificar el contenido del tráfico SMB para comprometer datos.
- Realizar ataques de tipo replay"para suplantar usuarios legítimos.
- Escalar privilegios dentro del sistema comprometido.

Evidencia: Durante el escaneo, se identificó el servicio Samba con soporte SMB en los puertos **139/tcp** y **445/tcp**.



Recomendación:

- Actualizar Samba a las versiones seguras (4.2.11, 4.3.8 o 4.4.2 o superiores).
- Configurar SMB para requerir autenticación fuerte y cifrada.
- Deshabilitar versiones antiguas del protocolo SMB (e.g., SMBv1).
- Implementar medidas de monitoreo para detectar actividades sospechosas relacionadas con SMB.
- Establecer reglas de firewall que limiten el acceso a los puertos **139/tcp** y **445/tcp** solo a hosts confiables.

Acceso no restringido a recursos compartidos NFS (Alta)

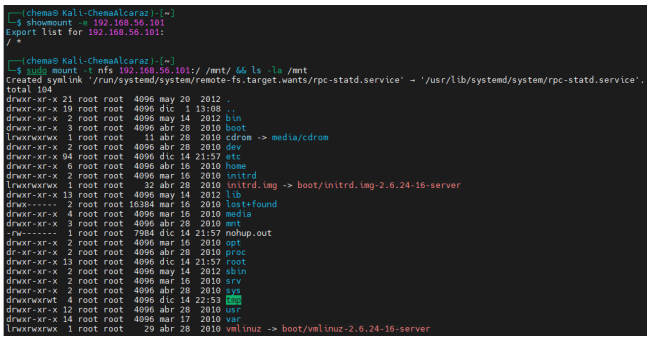
Gravedad	CVSS	Descripción
Alta	7.5	El servidor NFS en el puerto **2049/tcp** permite acceso no restringido a recursos compartidos, exponiendo información sensible y aumentando el riesgo de manipulación no autorizada.

Descripción: El servicio NFS (Network File System) en el puerto **2049/tcp** permite que usuarios no autenticados accedan a recursos compartidos sin restricciones de acceso adecuadas. Esto representa un grave riesgo para la confidencialidad y la integridad de los datos almacenados en el sistema.

Impacto: Un atacante podría explotar esta vulnerabilidad para:

- Acceder y leer datos sensibles almacenados en los recursos compartidos NFS.
- Modificar o eliminar archivos en los recursos compartidos sin autorización.
- Realizar movimientos laterales dentro de la red utilizando los datos comprometidos.
- Utilizar los recursos compartidos como punto de apoyo para ataques más amplios en la infraestructura.

Evidencia: Durante el escaneo, se identificó que el servidor NFS en el puerto **2049/tcp** estaba exportando recursos compartidos sin aplicar restricciones de acceso (e.g., por dirección IP o rango de red).



Recomendación:

- Configurar las restricciones de acceso en el servidor NFS utilizando listas de control de acceso basadas en IP (hosts.allow/hosts.deny).
- Limitar los permisos de escritura en los recursos compartidos a usuarios específicos.
- Habilitar el cifrado en las conexiones NFS para proteger los datos en tránsito.
- Monitorizar el acceso a los recursos compartidos NFS para detectar actividades sospechosas.

TWiki permite ejecución remota de comandos (Alta)

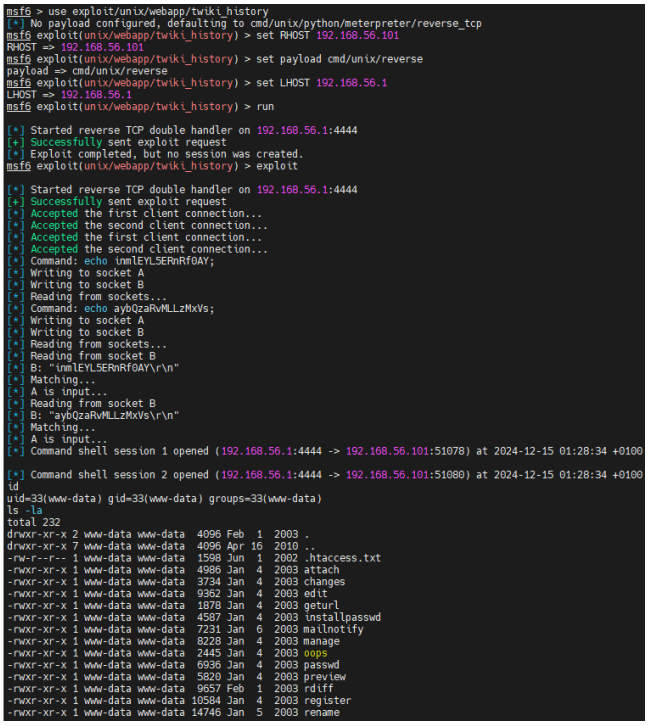
Gravedad	CVSS	Descripción
Alta	8.8	TWiki permite a un atacante manipular el parámetro 'rev' para ejecutar comandos arbitrarios en el servidor afectado.

Descripción: El servicio web que opera en el puerto **80/tcp** incluye una versión vulnerable de TWiki, un software de gestión de contenido. Esta vulnerabilidad permite a un atacante ejecutar comandos del sistema a través de la manipulación del parámetro 'rev' en las solicitudes HTTP, comprometiendo el servidor.

Impacto: Un atacante podría explotar esta vulnerabilidad para:

- Ejecutar comandos arbitrarios en el servidor con los privilegios del usuario del servidor web.
- Exfiltrar datos sensibles almacenados en el servidor.
- Escalar privilegios para comprometer el sistema completo.
- Instalar malware o persistencias en el servidor afectado.

Evidencia: Durante el análisis, se detectó una vulnerabilidad en el parámetro 'rev' de TWiki, permitiendo la ejecución remota de comandos.



Recomendación:

- Actualizar TWiki a la versión más reciente que no esté afectada por esta vulnerabilidad.
- Restringir el acceso al servicio TWiki mediante controles de acceso basados en IP.
- Monitorear el tráfico HTTP hacia el servidor para detectar patrones maliciosos.
- Aplicar políticas de validación de entradas en el servidor para evitar inyecciones y manipulaciones de parámetros.

Apache Tomcat versión obsoleta con múltiples vulnerabilidades (Crítica)

Gravedad	CVSS	Descripción
Crítica	9.8	La versión de Apache Tomcat instalada (<= 5.5.x) ha alcanzado su fin de vida útil, dejando múltiples vulnerabilidades sin parchear.

Descripción: El servicio Apache Tomcat identificado en el puerto **8180/tcp** está ejecutándose en una versión obsoleta que ya no recibe soporte ni actualizaciones de seguridad. Esto lo hace susceptible a vulnerabilidades conocidas y desconocidas.

Impacto: Un atacante puede aprovechar las vulnerabilidades de esta versión para:

- Obtener acceso remoto al servidor.
- Comprometer aplicaciones web desplegadas en Tomcat.
- Escalar privilegios en el sistema afectado.
- Realizar ataques de denegación de servicio (DoS).

Evidencia: Se identificó que Apache Tomcat ejecuta una versión anterior a 5.5.x, que es vulnerable a múltiples fallos críticos.

Recomendación:

- Actualizar Apache Tomcat a una versión soportada, como 9.x o superior.
- Revisar todas las aplicaciones web desplegadas en el servidor para verificar su integridad.
- Configurar reglas de firewall para restringir el acceso al puerto **8180/tcp** solo a hosts confiables.
- Monitorear continuamente el servidor en busca de intentos de explotación.

Conector AJP vulnerable a Ghostcat (Crítica)

Gravedad	CVSS	Descripción
Crítica	9.8	Vulnerabilidad "Ghostcat.[en] el conector AJP de Apache Tomcat que permite lectura de archivos y ejecución remota de código.

Descripción: El conector AJP identificado en el puerto **8009/tcp** es vulnerable a la explotación conocida como **Ghostcat**. Esto permite a un atacante remoto acceder a archivos confidenciales del servidor y, en ciertos casos, ejecutar código arbitrario.

Impacto: Un atacante podría:

- Leer archivos confidenciales desde el servidor, incluyendo configuraciones críticas.
- Subir archivos maliciosos para obtener ejecución remota de código.
- Comprometer aplicaciones web alojadas en el servidor Apache Tomcat.
- Escalar privilegios dentro del sistema comprometido.

Evidencia: Se identificó la presencia del conector AJP en el puerto **8009/tcp**, junto con configuraciones vulnerables explotables por Ghostcat.

Recomendación:

- Actualizar Apache Tomcat a una versión segura (7.0.100, 8.5.51, 9.0.31 o superior).
- Deshabilitar el conector AJP si no es estrictamente necesario.
- Configurar autenticación para proteger el acceso al conector AJP.
- Monitorear los logs de acceso de Tomcat para identificar actividades sospechosas.