

S5-L5

metasploit

[Back to My Scans](#)

Configure

Audit Trail

Launch ▾

Report

Export ▾

Hosts 1

Vulnerabilities 65

Remediations 2

Notes 2

History 1

Filter ▾

Search Vulnerabilities



65 Vulnerabilities

<input type="checkbox"/>	Sev ▾	CVSS ▾	VPR ▾	Name ▲	Family ▲	Count ▾		
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1		
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1		
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1		
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2		
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1		
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1		
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3		
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1		
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1		
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	General	28		
<input type="checkbox"/>	MIXED	ISC Bind (Multiple Issues)	DNS	5		
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2		

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:27 AM
End: Today at 11:55 AM
Elapsed: 28 minutes

Vulnerabilities



```
From 192.168.1.102 icmp_seq=3 Destination Host Unreachable
From 192.168.1.102 icmp_seq=4 Destination Host Unreachable
From 192.168.1.102 icmp_seq=5 Destination Host Unreachable
From 192.168.1.102 icmp_seq=6 Destination Host Unreachable

From 192.168.1.102 icmp_seq=7 Destination Host Unreachable
From 192.168.1.102 icmp_seq=8 Destination Host Unreachable
From 192.168.1.102 icmp_seq=9 Destination Host Unreachable

--- 192.168.1.100 ping statistics ---
11 packets transmitted, 0 received, +9 errors, 100% packet loss, time 10096ms
, pipe 4
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin#
```

i seguenti comandi sono
serviti per eliminare una
vulnerabilit  trovata con
lo scan da nessus
“vncpasswd” per
cambiare la password
dato che risultava troppo
insicura

scansione utilizzando
nmap delle porte che
vedremo più avanti
per 2 vulnerabilità

```
kali@kali: ~  
File Actions Edit View Help  
Stats: 0:00:08 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan  
Parallel DNS resolution of 1 host. Timing: About 0.00% done  
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 21.74% done; ETC: 15:15 (0:00:22 remaining)  
Stats: 0:00:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 86.96% done; ETC: 15:15 (0:00:03 remaining)  
Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 91.30% done; ETC: 15:15 (0:00:03 remaining)  
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 95.65% done; ETC: 15:15 (0:00:02 remaining)  
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 95.65% done; ETC: 15:16 (0:00:03 remaining)  
Stats: 0:01:41 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 95.65% done; ETC: 15:16 (0:00:04 remaining)  
Stats: 0:02:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 95.65% done; ETC: 15:17 (0:00:05 remaining)  
Stats: 0:02:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 99.90% done; ETC: 15:17 (0:00:00 remaining)  
Nmap scan report for 192.168.1.102  
Host is up (0.00020s 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  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  ccproxy-ftp?   
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  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 185.57 seconds  
  
(kali@kali)~[-] ssh -p 22 root@192.168.1.102
```

```
root@metasploitable:/etc# ufw deny
```

```
Usage: ufw COMMAND
```

```
Commands:
```

enable	Enables the firewall
disable	Disables the firewall
default ARG	set default policy to ALLOW or DENY
logging ARG	set logging to ON or OFF
allow deny RULE	allow or deny RULE
delete allow deny RULE	delete the allow/deny RULE
status	show firewall status
version	display version information

```
root@metasploitable:/etc# ufw deny 1524
```

```
Rule added
```

```
root@metasploitable:/etc# ufw status
```

```
Firewall loaded
```

To	Action	From
--	-----	----
1524:tcp	DENY	Anywhere
1524:udp	DENY	Anywhere

```
root@metasploitable:/etc# _
```

abbiamo modificato
le regole del firewall
per riuscire ad
eliminare le
vulnerabilità qui
vediamo l'utilizzo
delle porte trovate in
precedenza su nmap

```
root@metasploitable:/etc# ufw status
Firewall loaded
```

To	Action	From
--	-----	----
1524:tcp	DENY	Anywhere
1524:udp	DENY	Anywhere

```
root@metasploitable:/etc# ufw deny 139
Rule added
```

```
root@metasploitable:/etc# ufw deny 445
Rule added
```

```
root@metasploitable:/etc# ufw status
Firewall loaded
```

To	Action	From
--	-----	----
1524:tcp	DENY	Anywhere
1524:udp	DENY	Anywhere
139:tcp	DENY	Anywhere
139:udp	DENY	Anywhere
445:tcp	DENY	Anywhere
445:udp	DENY	Anywhere

```
root@metasploitable:/etc# _
```

la porta 139 e 445 sono servite per eliminare le vulnerabilità data da samba

```
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
/mnt/newdisk      192.168.1.102(rw,sync,no_root_squash,no_subtree_check)
```

[Wrote 12 lines]

root@metasploitable:/etc#

Hosts1

Vulnerabilities54

Remediations1

Notes2

History4

Filter

Search Vulnerabilities

54 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
MIXED	SSL (Multiple Issues)	General	24	
MIXED	ISC Bind (Multiple Issues)	DNS	5	
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	
MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1	
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	
MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1	
MIXED	SSH (Multiple Issues)	Misc.	6	

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 3:38 PM

End:

Today at 4:06 PM

Elapsed:

28 minutes

Vulnerabilities

CRITICAL

HIGH

MEDIUM

LOW

INFO

Scan Details

Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 3:38 PM
 End: Today at 4:06 PM
 Elapsed: 28 minutes

Vulnerabilities



vediamo che non sono più presenti le vulnerabilità che volevamo eliminare