S5-L5

metasploit

‹ Back to My Scans

Configure | Audit Trail | Launch | Report | Export

Hosts 1 | **Vulnerabilities 65** | Remediations 2 | Notes 2 | History 1

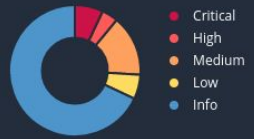
Filter | Search Vulnerabilities | **65** Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	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	9.8		Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	...	...	15 SSL (Multiple Issues)	General	28
MIXED	...	...	5 ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2

Scan Details

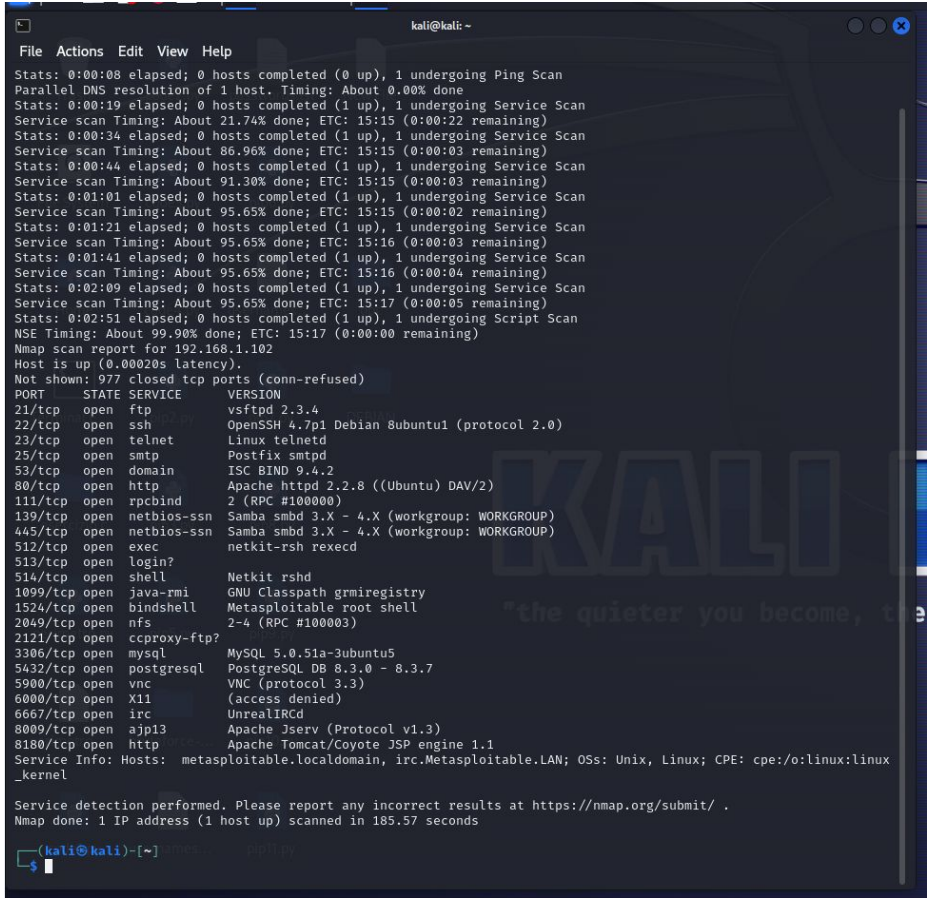
Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 11:27 AM
End:	Today at 11:55 AM
Elapsed:	28 minutes

Vulnerabilities

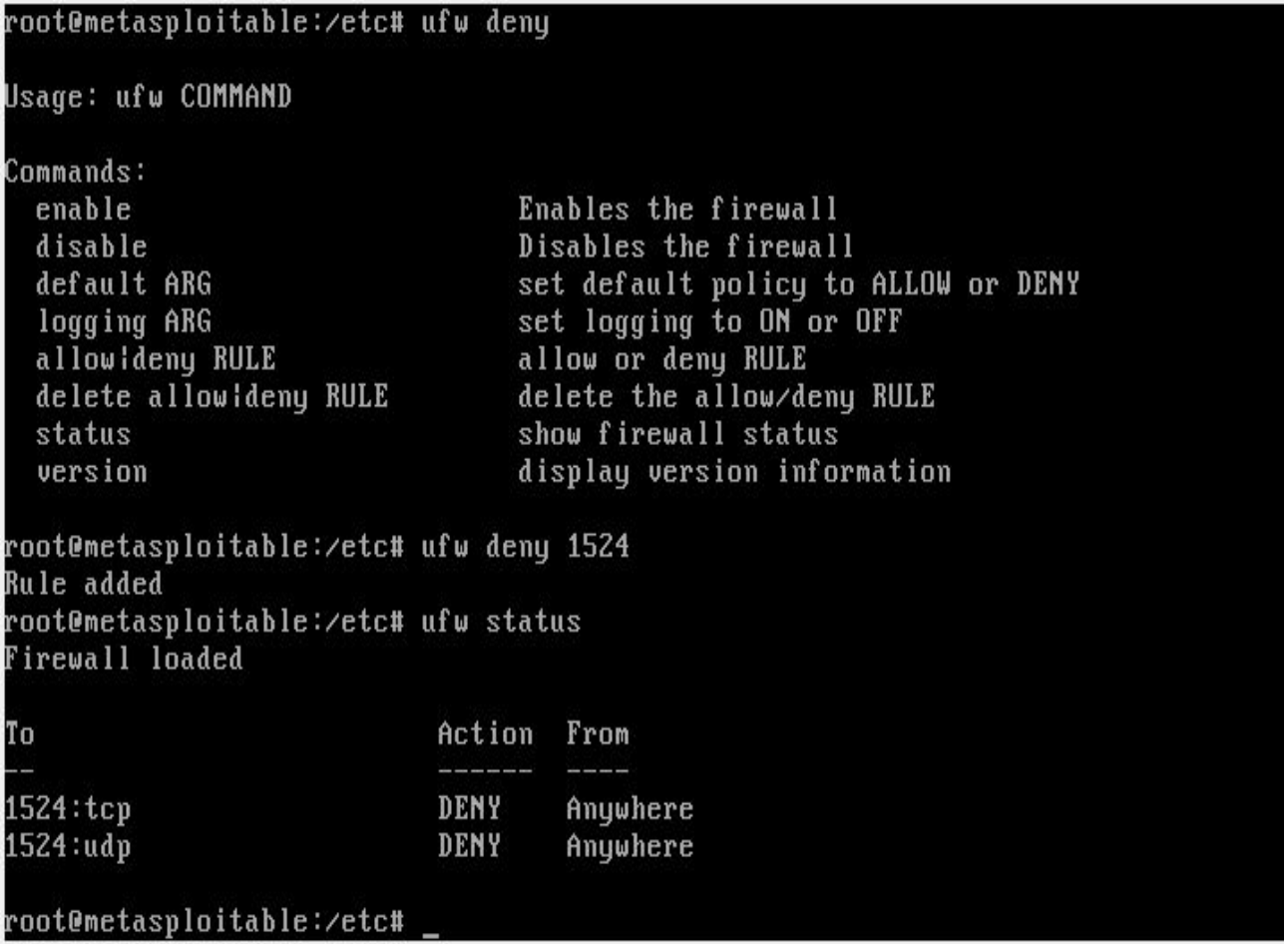


```
From 192.168.1.102 icmp_seq=3 Destination Host Unreachable
From 192.168.1.102 icmp_seq=4 Destination Host Unreachable
From 192.168.1.102 icmp_seq=5 Destination Host Unreachable
From 192.168.1.102 icmp_seq=6 Destination Host Unreachable

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 vulnerabita 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 vulnerabiltà

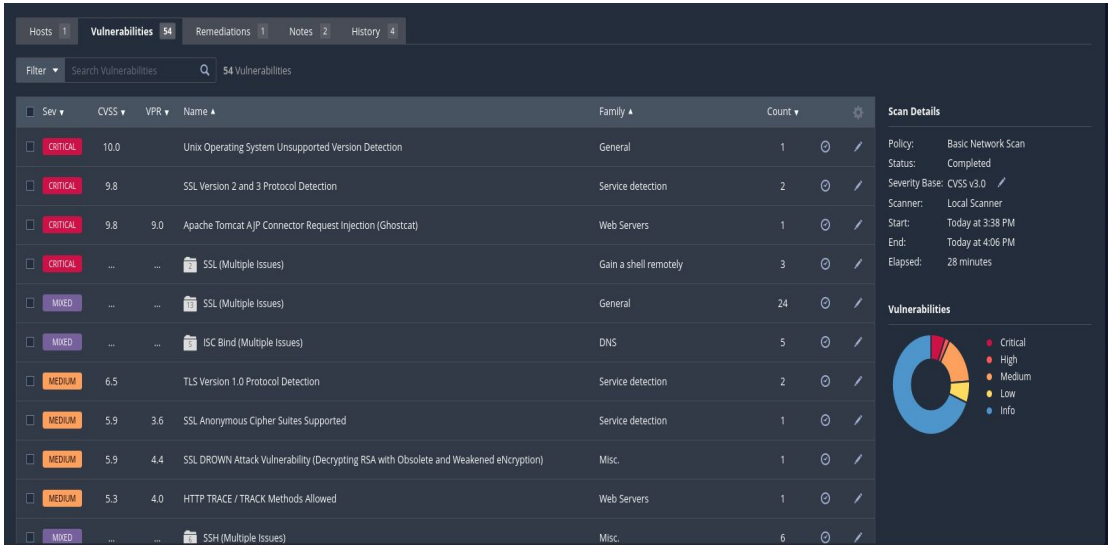


abbiamo modificato le regole del firewall per riuscire ad eliminare le vulnerabilità qui vediamo l utilizzo delle porte trovate in precedenza su nmap

```
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


GNU nano 2.0.7 File: exports
/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#



vediamo che non sono più presenti le vulnerabilità che volevamo eliminare