WARDIERE INC.

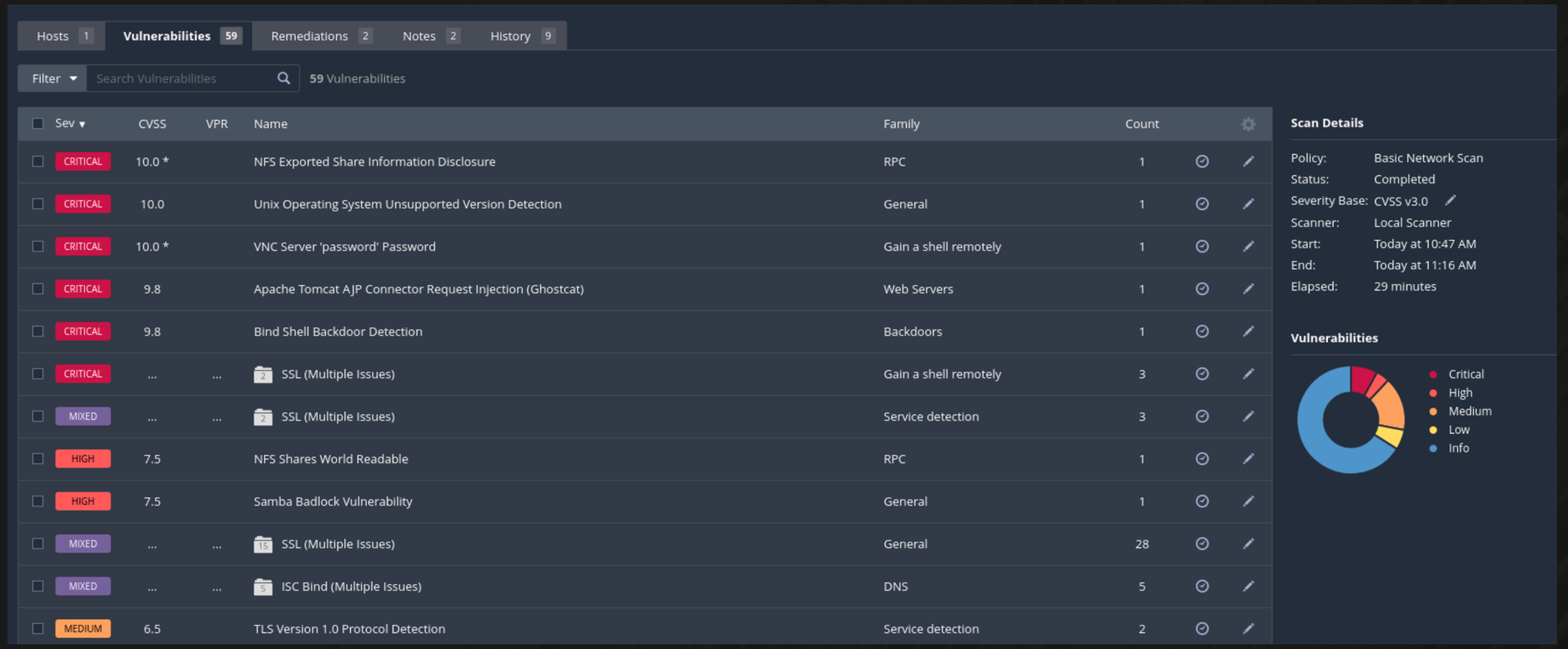
PROGETTO S5 L5

Scansione e remediation su macchina Metasploitable 2

F E R N A N D O C A T R A M B O N E

2022
Company

PRIMO REPORT



Hosts 1 | **Vulnerabilities 59** | Remediations 2 | Notes 2 | History 9

Filter | Search Vulnerabilities | **59** Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *		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		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
MIXED	...	...	2 SSL (Multiple Issues)	Service detection	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5		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 10:47 AM
End:	Today at 11:16 AM
Elapsed:	29 minutes

Vulnerabilities

VNC SERVER 'PASSWORD' PASSWORD

CRITICAL VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Output

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.50.101

In primo luogo ho risolto la vulnerabilità VNC modificando la password di default con il comando vncpasswd

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin# _
```

BIND SHELL BACKDOOR DETECTION

Per risolvere questa vulnerabilità che permette di attivare una bind shell backdoor sulla macchina Metasploitable 2 ho chiuso gli accessi tramite la porta 1524 che veniva indicata nel report di Nessus

CRITICAL Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the
following request :


This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

------------------------------ snip ------------------------------
```

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.50.101

```
root@metasploitable:/home/msfadmin# ufw enable
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin# ufw default ALLOW
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin# ufw deny 1524
Rules updated
```

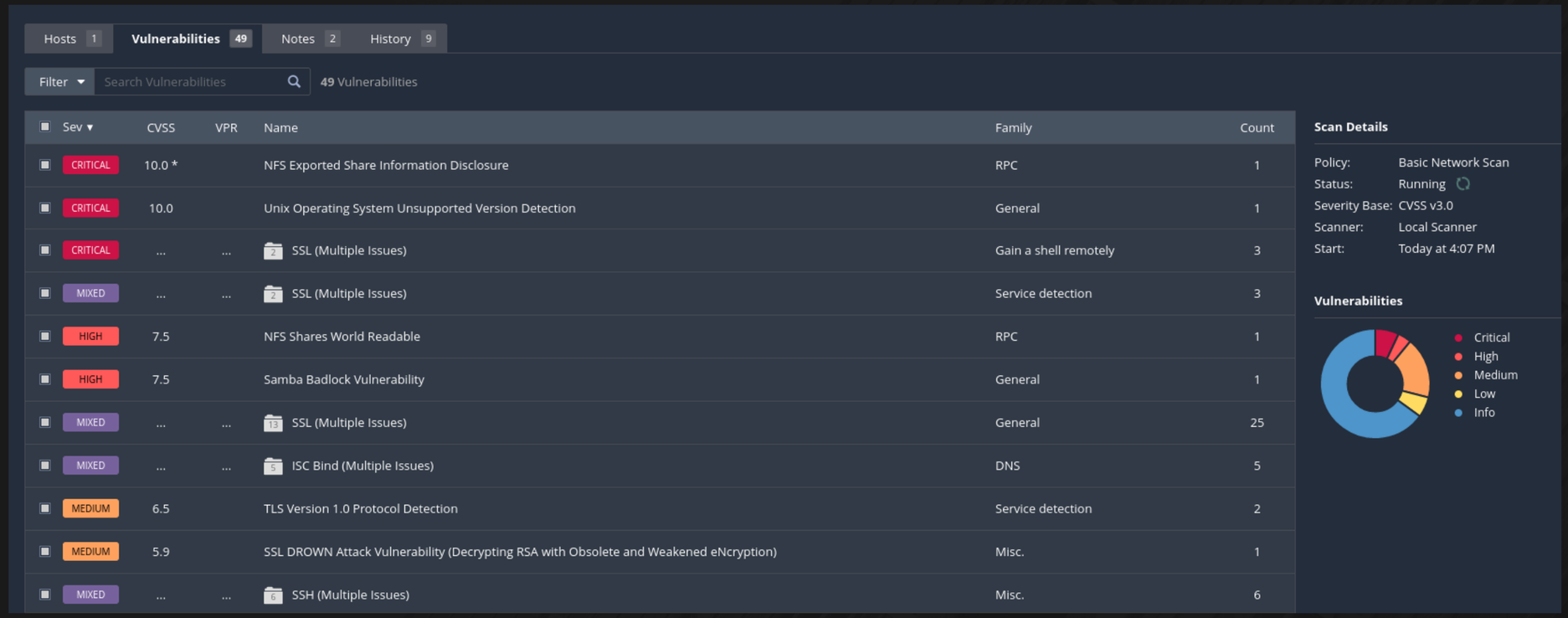
Ufw (Uncomplicated firewall) è l'applicazione predefinita in Ubuntu per la configurazione del firewall. Sviluppato per semplificare la configurazione di iptables, Ufw offre un modo semplice per creare un firewall basato su protocolli IPv4 e IPv6. Ufw è inizialmente disabilitato.

Ho abilitato ufw e bloccato con una nuova regola gli accessi dalla porta 1524

In alternativa si sarebbe potuto configurare iptables ovvero il Firewall di Linux con questo comando:

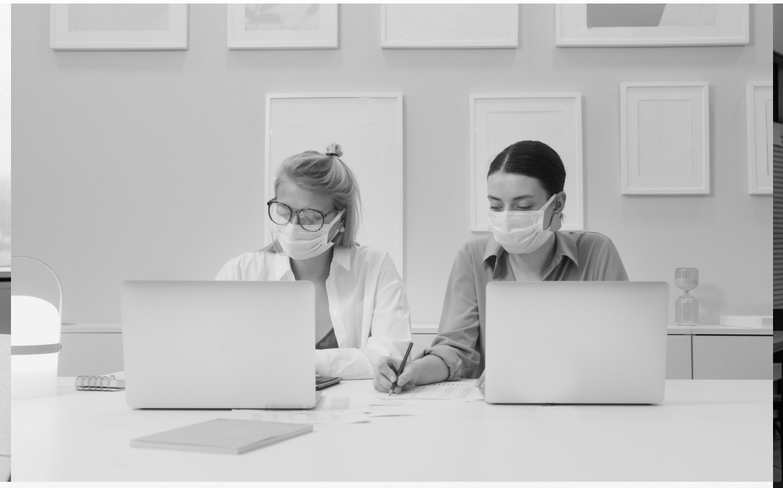
iptables -A INPUT -p tcp --dport 1524 -j DROP

ULTIMO REPORT



Come si può notare dall'ultimo report le vulnerabilità attivando il firewall e impostando password più robuste sono diminuite drasticamente.

CONSIDERAZIONI FINALI



Attivare Firewall e dispositivi di sicurezza

Per mantenere sicura una rete o una macchina è consigliabile utilizzare un buon Firewall e configurarlo con regole che proteggano da potenziali attacchi da malintenzionati.

Impostare password complesse

Per evitare che le password vengano trovate tramite attacchi brute force o a dizionario è consgiliabile scegliere password più robuste e non lasciare quelle di default come ad esempio ‘password’.

Aggiornare il sistema

Per risolvere molte altre vulnerabilità del sistema analizzato sarebbe stato sufficiente aggiornare i software alle versioni più recenti. Si consiglia di aggiornare sempre per evitare di rimanenere esposti a vulnerabilità già note .

GRAZIE