

RemediationMeta

PROGETTO S5/L5

di Giuseppe Lupoi



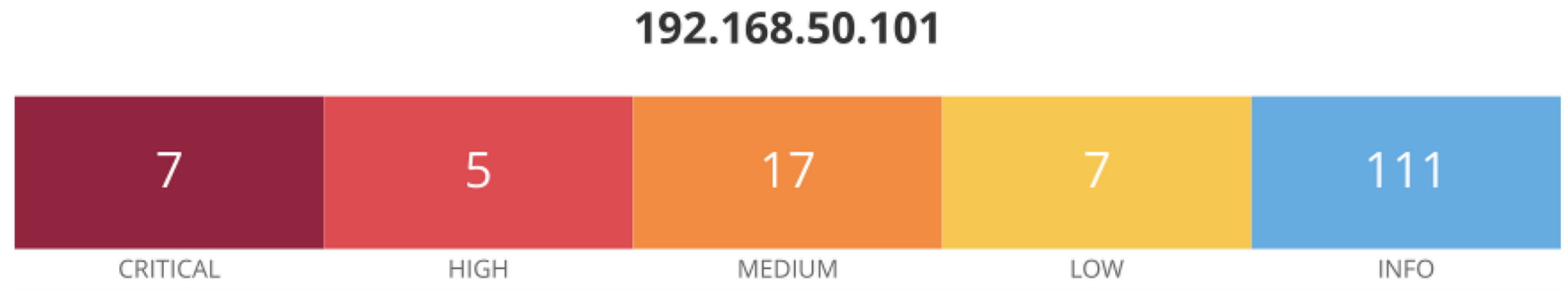
Svolgimento

Come richiesto dalla consegna di questo progetto quest'oggi andremo ad analizzare e risolvere alcune vulnerabilità del nostro target, ovvero Metaploitable.

Proseguirò dunque con un primo scan su Meta per poi andare a risolvere alcune falle del sistema



Risultati primo scan



ScansioneInizio

[Back to My Scans](#)

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 63 Remediations 2 Notes 1 History 3

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.50.101	<div><div>7</div><div>5</div><div>17</div><div>7</div><div>111</div></div>

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 4:40 PM

End: Today at 4:52 PM

Elapsed: 12 minutes

Vulnerabilities

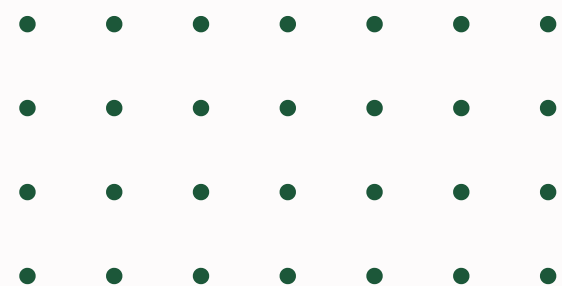
- Critical
- High
- Medium
- Low
- Info

Riguardo le vulnerabilità ho deciso di prendere in considerazione la numero **32314**, **32321**, **61708** e la **11356**.

Dunque ho proceduto come prima cosa con il cambiare le credenziali dell'utente **msfadmin** per rendere più sicuro l'accesso.

Quindi una volta avviata la macchina, ho eseguito il comando “**sudo passwd msfadmin**” per cambiare appunto la password, il sistema ci chiederà di immettere la nuova password due volte per conferma.

```
msfadmin@metasploitable:~$ sudo passwd msfadmin
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:~$
```



Ho deciso di proseguire attivando un servizio **firewall** ovvero **ufw**.

Quindi ho passato i seguenti comandi alla macchina:

- **sudo apt-get update**, per verificare la disponibilità di nuovi pacchetti
- **sudo apt-get install ufw**, per installare il pacchetto del firewall ufw
- **sudo ufw enable**, per attivare il servizio dopo averlo scaricato

```
msfadmin@metasploitable:~$ sudo apt-get update_
msfadmin@metasploitable:~$ sudo apt-get install ufw
[sudo] password for msfadmin:
Building dependency tree
Reading state information... Done

The following packages will be upgraded:
  ufw
1 upgraded, 0 newly installed, 0 to remove and 138 not upgraded
Need to get 23.4kB of archives.
After this operation, 0B of additional disk space will be used.
ufmsfadmin@metasploitable:~$ sudo ufw enable
[sudo] password for msfadmin:
[ 4434.567739] Out of memory: kill process 5115 (jsvc) score 15756 or a
[ 4434.568612] Killed process 5115 (jsvc)
Firewall started and enabled on system startup
msfadmin@metasploitable:~$
```

Ed una volta attivato il servizio ho abilitato le regole di default con il seguente comando:

- **sudo ufw default allow**

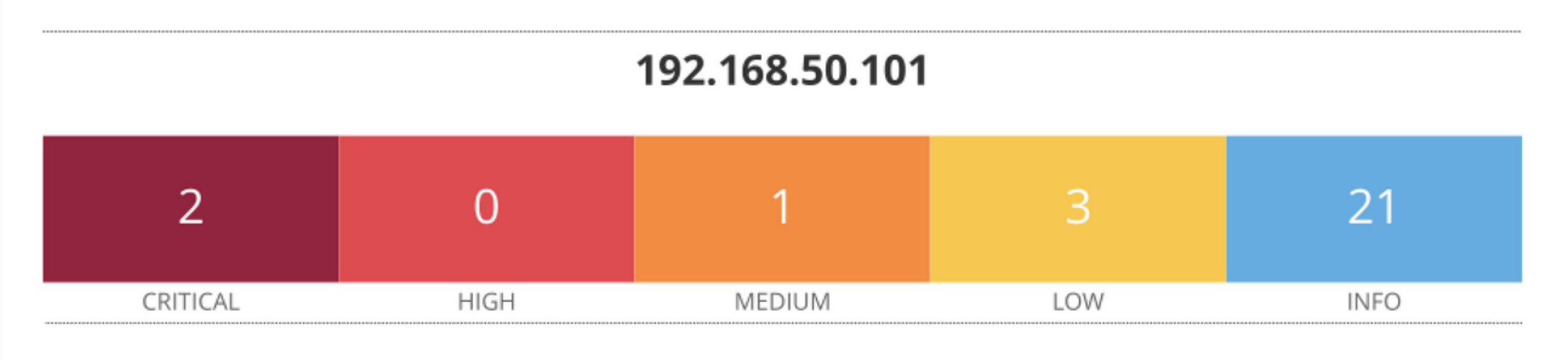
Per essere sicuro delle modifiche apportate ho in seguito controllato lo stato del servizio con:

- **sudo ufw status**

L'output della macchina ci dirà che il servizio è stato caricato correttamente

```
msfadmin@metasploitable:~$ sudo ufw default allow
[ 1649.739644] Out of memory: kill process 5028 (jsvc) score 13938 or a child
[ 1649.740702] Killed process 5028 (jsvc)
Default policy changed to 'allow'
(be sure to update your rules accordingly)
msfadmin@metasploitable:~$ sudo ufw status
[ 1720.666316] Out of memory: kill process 5034 (jsvc) score 13906 or a child
[ 1720.667408] Killed process 5034 (jsvc)
Firewall loaded
```

Ho eseguito dunque un'altro scan dopo le modifiche apportate alla macchina



ScansioneFine

[Back to My Scans](#)

Configure

Audit Trail

Launch

Report

Export

Hosts1

Vulnerabilities19

Notes1

History6

Filter

Search Hosts

1 Host

Host	Vulnerabilities
192.168.50.101	<div><div>2</div><div>1</div><div>3</div><div>21</div></div>

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

December 23 at 1:20 PM

End:

December 23 at 1:28 PM

Elapsed:

8 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Conclusione

Infine possiamo dunque evidenziare le differenze tra i due scan, quello eseguito all'inizio ed il secondo dopo le modifiche, dove si evidenzia appunto che molte vulnerabilità sono state corrette, non solo di livello **critical** e **hard** ma bensì anche quelle di livello **medium** e **low**, semplicemente grazie all'attivazione di un firewall e con il cambio delle credenziali dell'utente rendendole più "forti".