

1. Introduzione

Questo progetto ha come obiettivo quello di simulare un'attività reale di **Vulnerability Assessment**, partendo dall'analisi di un sistema volutamente vulnerabile fino all'applicazione di alcune **remediation**, per poi verificarne l'efficacia tramite una nuova scansione.

Il lavoro è stato svolto in un ambiente di laboratorio isolato, senza alcuna esposizione verso reti reali, così da poter sperimentare liberamente senza rischi.

Lo scopo non è “mettere in sicurezza Metasploitable” (cosa impossibile), ma **capire come ragiona un analista di sicurezza**, come valuta le vulnerabilità e come decide cosa e come mitigare.

Nota sull'approccio iniziale

Inizialmente era stato previsto l'utilizzo di **pfSense** come firewall di rete per gestire le remediations. Tuttavia, nel corso delle prove di laboratorio, la sua configurazione si è rivelata decisamente più impegnativa del previsto, introducendo una serie di problematiche che hanno reso il laboratorio inutilmente complesso.

Dopo numerosi tentativi e verifiche, si è scelto di **mettere da parte pfSense** per evitare di perdere ulteriore tempo su configurazioni che andavano oltre gli obiettivi del progetto.

L'adozione di **iptables** ha consentito di semplificare l'ambiente, mantenere il controllo diretto sulle mitigazioni applicate e, soprattutto, preservare la sanità mentale dello studente (cioè io) durante lo svolgimento del lavoro.

2. Ambiente di laboratorio

L'ambiente utilizzato è composto da due macchine virtuali:

- **Kali Linux**
IP: 192.168.50.100
Utilizzata come macchina di attacco e di scansione
- **Metasploitable 2**
IP: 192.168.50.101
Utilizzata come macchina target vulnerabile

Le macchine sono collegate alla stessa rete interna per consentire la comunicazione diretta. Per l'analisi delle vulnerabilità è stato utilizzato **Nessus Essentials**, mentre per le remediations

è stato scelto di intervenire direttamente sulla macchina target tramite **iptables**, simulando un approccio realistico di hardening.

3. Scansione iniziale delle vulnerabilità

La prima fase del progetto ha previsto l'esecuzione di una **scansione di rete completa** con Nessus sulla macchina Metasploitable.

Già dalla prima scansione risulta evidente come il sistema presenti **numerose vulnerabilità**, molte delle quali classificate come *Critical* e *High*. Questo è coerente con la natura di Metasploitable, progettata appositamente per essere insicura.

Tra le principali criticità emerse si notano:

- sistema operativo obsoleto e non più supportato
- servizi esposti con configurazioni deboli
- presenza di backdoor e servizi di accesso remoto
- utilizzo di protocolli di cifratura obsoleti

The screenshot shows the Nessus interface after a scan. The main title is "PROGETTO DI FINE MODULO M3". On the left, there's a sidebar with "Folders" (My Scans, All Scans, Trash) and "Resources" (Policies, Plugin Rules). The main area has tabs for "Hosts" (1), "Vulnerabilities" (63), "Remediations" (2), "Notes" (2), and "History" (1). A search bar filters for "1 Host". Below it is a table with one host entry: "192.168.50.101" with status "Fail". To the right, the "Scan Details" pane shows the policy was a "Basic Network Scan", completed at 8:41 PM today, with a duration of 26 minutes. The "Vulnerabilities" section includes a pie chart showing the distribution of severity levels: Critical (~1%), High (~10%), Medium (~30%), Low (~40%), and Info (~15%).

This screenshot shows a detailed view of the vulnerabilities found in the previous scan. The title is "PROGETTO DI FINE MODULO M3". The left sidebar and tabs are identical to the previous screenshot. The main table lists 63 vulnerabilities, each with columns for Severity (CVSS, VPR, EPSS), Name, Family, and Count. Some examples include "Canonical Ubuntu Linux SEOL (8.04.x)" with a CVSS of 10.0, "VNC Server password: Password" with a CVSS of 10.0, and "Apache Tomcat AJP Connector Request Injection (Ghostcat)" with a CVSS of 9.8. The "Scan Details" pane on the right is identical to the first screenshot, showing the same completion details. The "Vulnerabilities" section also includes a pie chart showing the distribution of severity levels: Critical (~1%), High (~10%), Medium (~30%), Low (~40%), and Info (~15%).

4. Analisi delle vulnerabilità

Analizzando i risultati della scansione, è stato necessario fare una distinzione tra:

- vulnerabilità **realisticamente mitigabili**
- vulnerabilità **non risolvibili direttamente** su Metasploitable

Alcune criticità, come l'End Of Life del sistema operativo, non possono essere risolte senza una reinstallazione completa. In questi casi la gestione del rischio consiste nel **riconoscere il problema e documentarlo**, non nel forzare una soluzione inesistente.

L'attenzione è stata quindi posta su quelle vulnerabilità che potevano essere **mitigate riducendo la superficie di attacco**, in particolare intervenendo a livello di rete.

5. Fase di remediation

Scelta dell'approccio

Per le remediation è stato scelto di utilizzare **iptables** anziché strumenti grafici o firewall esterni.

Questo approccio consente di:

- lavorare direttamente sul sistema
 - capire cosa viene realmente bloccato
 - simulare un contesto più vicino a quello reale
-

5.1 Remediation 1 – Blocco del servizio VNC (porta 5900)

Una delle vulnerabilità critiche individuate riguardava il servizio **VNC**, accessibile con password debole.

Questa vulnerabilità riguarda l'esposizione del servizio VNC con una password estremamente debole. Un attaccante potrebbe accedere facilmente all'interfaccia grafica del sistema, ottenendo il controllo completo della macchina senza particolari competenze tecniche.

Per mitigare il rischio è stata creata una regola iptables che **blocca completamente il traffico in ingresso sulla porta 5900**, impedendo l'accesso remoto al servizio.

La regola è stata verificata tramite test con nc e nmap, che hanno confermato l'impossibilità di raggiungere il servizio dopo l'applicazione della regola.

```
metasploitable login: msfadmin
Password:
Last login: Tue Dec 16 10:19:38 EST 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/**/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

msfadmin@metasploitable:~$ sudo loadkeys it
[sudo] password for msfadmin:
Loading /usr/share/keymaps/it.map.bz2
msfadmin@metasploitable:~$ sudo netstat -tulpn | grep 5900
tcp        0      0 0.0.0.0:5900          0.0.0.0:*                  LISTEN
4606/Xtightvnc
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport 5900 -s 192.168.50.100 -j DROP
msfadmin@metasploitable:~$
```

```
(pireddone㉿kali)-[~]
└─$ sudo nmap -p 5900 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-18 17:22 CET
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).

PORT      STATE      SERVICE
5900/tcp  filtered  vnc
MAC Address: 08:00:27:C7:D0:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.27 seconds
```

5.2 Remediation 2 – Blocco Bind Shell Backdoor (porta 1524)

Nessus ha rilevato la presenza di una **bind shell backdoor**, una delle vulnerabilità più note di Metasploitable.

La presenza di una bind shell indica una backdoor attiva che permette a un attaccante di ottenere una shell remota collegandosi a una specifica porta. Questo tipo di vulnerabilità consente l'accesso diretto al sistema senza autenticazione.

Anche in questo caso è stata applicata una regola iptables per bloccare il traffico verso la porta utilizzata dalla backdoor, riducendo drasticamente il rischio di accesso remoto non autorizzato.

```

and is deactivated.
25/12/18@11:49:00: DEBUG: 4780 {cnf_start_services} mask_max = 0, services_start
ed = 0
25/12/18@11:49:00: CRITICAL: 4780 {init_services} no services. Exiting...
msfadmin@metasploitable:/etc$ sudo service xinetd stop
sudo: service: command not found
msfadmin@metasploitable:/etc$ sudo iptables -A INPUT -p tcp -s 192.168.50.100 --dport 1524 -j DROP
msfadmin@metasploitable:/etc$ sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 363 packets, 121K bytes)
 pkts bytes target     prot opt in     out     source               destination
      2    88  DROP      tcp  --  *      *       192.168.50.100    0.0.0.0/0
      0     0  DROP      tcp  --  *      *       192.168.50.100    0.0.0.0/0
      0     0  DROP      tcp  --  *      *       192.168.50.100    0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 373 packets, 122K bytes)
 pkts bytes target     prot opt in     out     source               destination

msfadmin@metasploitable:/etc$
```

```

└─(pireddone㉿kali)-[~]
└─$ sudo nmap -p 1524 192.168.50.101
[sudo] password for pireddone:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-18 17:54 CET
Nmap scan report for 192.168.50.101
Host is up (0.0016s latency).

PORT      STATE      SERVICE
1524/tcp  filtered  ingreslock
MAC Address: 08:00:27:C7:D0:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

5.3 Remediation 3 – Riduzione dei servizi esposti

Sono state applicate ulteriori regole firewall per limitare l'esposizione di servizi non strettamente necessari all'interno del laboratorio.

Questo intervento segue il principio del **least privilege**, secondo cui un sistema dovrebbe esporre solo ciò che è realmente necessario.

R-SERVICES (rexec, rlogin, rsh)

I servizi rexec, rlogin e rsh sono protocolli legacy che trasmettono dati in chiaro e non prevedono meccanismi di sicurezza adeguati. La loro esposizione può consentire intercettazioni o accessi non autorizzati al sistema.

```

msfadmin@metasploitable:/etc$ sudo iptables -A INPUT -p tcp --dport 513 -j DROP
msfadmin@metasploitable:/etc$ sudo iptables -A INPUT -p tcp --dport 514 -j DROP
msfadmin@metasploitable:/etc$ sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 424 packets, 147K bytes)
pkts bytes target     prot opt in     out    source          destination
      2     88 DROP       tcp  --  *      *      192.168.50.100   0.0.0.0/0
      2     88 DROP       tcp  --  *      *      192.168.50.100   0.0.0.0/0
      0     0  DROP      tcp  --  *      *      0.0.0.0/0        0.0.0.0/0
      0     0  DROP      tcp  --  *      *      0.0.0.0/0        0.0.0.0/0
      0     0  DROP      tcp  --  *      *      0.0.0.0/0        0.0.0.0/0
      0     0  DROP      tcp  --  *      *      0.0.0.0/0        0.0.0.0/0
      0     0  DROP      tcp  --  *      *      0.0.0.0/0        0.0.0.0/0
      0     0  DROP      tcp  --  *      *      0.0.0.0/0        0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source          destination

Chain OUTPUT (policy ACCEPT 431 packets, 148K bytes)
pkts bytes target     prot opt in     out    source          destination

msfadmin@metasploitable:/etc$
```

```

└─(pireddone㉿kali)-[~]
$ sudo nmap -p 512,513,514 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-18 18:06 CET
Nmap scan report for 192.168.50.101
Host is up (0.0014s latency).

PORT      STATE SERVICE
512/tcp    filtered exec
513/tcp    filtered login
514/tcp    filtered shell
MAC Address: 08:00:27:C7:D0:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.84 seconds
```

NFS ESPOSTO

Un servizio NFS esposto può permettere a utenti non autorizzati di accedere a file e directory condivise. Questo può portare alla lettura o modifica di dati sensibili presenti sul sistema.

```

msfadmin@metasploitable:/etc$ sudo /etc/init.d/nfs-kernel-server stop
* Stopping NFS kernel daemon                                         [ OK ]
* Unexporting directories for NFS kernel daemon...                  [ OK ]
msfadmin@metasploitable:/etc$ sudo /etc/init.d/portmap stop
* Stopping portmap daemon...                                         [ OK ]
msfadmin@metasploitable:/etc$
```

```

└─(pireddone㉿kali)-[~]
$ sudo nmap -p 2049 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-18 18:10 CET
Nmap scan report for 192.168.50.101
Host is up (0.0020s latency).

PORT      STATE SERVICE
2049/tcp  closed nfs
MAC Address: 08:00:27:C7:D0:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.38 seconds
```

5.4 Vulnerabilità non mitigabili

Alcune vulnerabilità critiche, come:

- **Ubuntu Linux 8.04 End Of Life**
- **protocolli SSL obsoleti**

non sono risolvibili direttamente su Metasploitable.

In questi casi la soluzione corretta è teorica: aggiornamento o migrazione del sistema.

Queste vulnerabilità sono state quindi **documentate e accettate**, come avverrebbe in un contesto reale con sistemi legacy.

L'utilizzo di un sistema operativo non più supportato implica l'assenza di aggiornamenti di sicurezza. Eventuali vulnerabilità note rimangono quindi sfruttabili, aumentando significativamente il rischio complessivo del sistema.

6. Scansione finale di verifica

Dopo aver applicato le remediation, è stata eseguita una **seconda scansione Nessus** sulla macchina target.

La scansione finale ha permesso di:

- verificare l'efficacia delle regole iptables
- confrontare lo stato del sistema prima e dopo le mitigazioni
- osservare una riduzione dell'esposizione dei servizi

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 6:16 PM
- End: Today at 6:41 PM
- Elapsed: 25 minutes

Vulnerabilities

Severity	Count
Critical	1
High	4
Medium	21
Low	7
Info	191

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 6:16 PM
- End: Today at 6:41 PM
- Elapsed: 25 minutes

Vulnerabilities

Severity	Count
Critical	1
High	1
Medium	28
Low	5
Info	3

7. Conclusioni

Questo progetto ha permesso di comprendere in modo pratico come si svolge un’attività di **Vulnerability Assessment**, evidenziando che la sicurezza non è solo “patchare tutto”, ma anche **capire cosa è realmente mitigabile e come gestire il rischio**.

L’uso di iptables ha dimostrato come sia possibile ridurre l’impatto di vulnerabilità anche su sistemi obsoleti, adottando un approccio pragmatico e consapevole.

L’esperienza ha inoltre sottolineato l’importanza della documentazione e della verifica post-remediation, elementi fondamentali nel lavoro di un analista di sicurezza.