

INDICE

1. Introduzione.....	2
1.1. Kali Linux e Metasploitable2.....	2
1.2. Nessus.....	2
2. Scansione delle vulnerabilità trovate attraverso Nessus.....	3
2.1. Riassunto dei risultati ottenuti.....	3
3. Inizio fase “Remediation” delle vulnerabilità.....	4
4. Scansione delle vulnerabilità con Nessus (post-intervento).....	14
4.1. Riassunto dei risultati ottenuti.....	14
5. Conclusione.....	15

1. Introduzione

Il presente report descrive le attività di **vulnerability assessment** (una delle fasi del Penetration Test) condotte all'interno di un contesto simulato, con l'obiettivo di riprodurre un'analisi di sicurezza.

La scansione è stata eseguita utilizzando il tool **Nessus**, installato su una macchina **Kali Linux (192.168.50.100)**, e diretta verso l'host target rappresentato da **Metasploitable2 (192.168.50.101)**, una macchina volutamente vulnerabile utilizzata a scopo didattico.

Le fasi di questa attività sono state:

- identificazione delle vulnerabilità tramite scansione automatizzata (Nessus), e manuale per verificarne che non ci siano “falsi positivi”.
- analisi dei risultati e delle raccomandazioni fornite per la risoluzione delle criticità.
- applicazione delle misure correttive una volta verificato il problema.
- riesecuzione della scansione per verificare l'efficacia degli interventi.

1.1. Kali Linux e Metasploitable2

L'ambiente di test è composto da due macchine virtuali principali, configurate all'interno di una rete isolata:

- **Kali Linux**: è la macchina utilizzata come **host di analisi e scansione**, progettata per test di sicurezza e penetration testing. Include numerosi strumenti preinstallati, tra cui **Nessus**, utilizzato in questo caso per l'identificazione automatica delle vulnerabilità presenti nel sistema target.
- **Metasploitable2** è una macchina virtuale progettata intenzionalmente per contenere numerose vulnerabilità note, al fine di fornire un ambiente controllato per esercitazioni di **penetration testing**, **vulnerability scanning** e **analisi forense**

1.2. Nessus

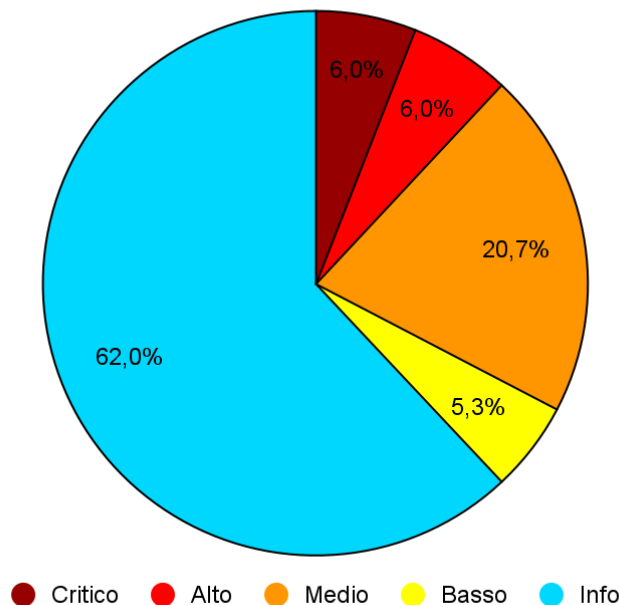
Nessus è un software utilizzato per **scansionare un sistema informatico** e rilevare possibili problemi di sicurezza, chiamati **vulnerabilità**. Questo tipo di analisi viene chiamata **vulnerability assessment**, come detto nell'introduzione, ed è una delle prime fasi che si compiono per valutare la sicurezza di un sistema.

In questo intervento, **Nessus è stato utilizzato dalla macchina Kali Linux per esaminare Metasploitable2**, che funge da sistema vulnerabile. Il risultato della scansione è una lista di vulnerabilità, classificate per gravità, che possono essere rappresentate tramite grafici.

2. Scansione delle vulnerabilità trovate attraverso Nessus

Attraverso la procedura effettuata affinché trovassimo delle criticità, è risultata positiva a determinate mal configurazioni dell'host interessato e servizi abilitati/obsoleti, che possono compromettere le difese della macchina virtuale e permettere ai malintenzionati (black hat) di avere l'accesso ad essa. Qui riporta raffigurato un grafico con i vari "problemi" rilevati:

Vulnerabilità individuate su Metasploitable2



2.1. Riassunto dei risultati ottenuti

Lo stato generale della macchina riporta "come previsto" diverse problematiche dovuto al fatto che la macchina Metasploitable2 è stata progettata così al fine di effettuare interventi che possano attaccare/proteggere la macchina a scopo didattico/esercitazione. In un reale contesto trovare molte criticità sarebbe un rischio elevato non eseguire le adeguate procedure.

Stato delle vulnerabilità ottenute:

Critico	Alto	Medio	Basso	Info
10	9	31	8	93

Esito finale: **Molto vulnerabile.**

Il sistema di punteggio viene calcolato attraverso il CVSS 3.0 :

"Critico: 10.0 - 9.0 / Alto: 8.9 - 7.0 / Medio: 6.9 - 4.0 / Basso: 3.9 - 0.1 / Info: 0.0"

3. Inizio fase “Remediation” delle vulnerabilità

Una volta raccolte tutte le informazioni necessarie, possiamo iniziare la fase di “soluzioni” delle potenziali falle, descrivendole al fine di applicare le giuste “restrizioni” mitigando e/o migliorando la sicurezza della macchina.

Canonical Ubuntu Linux SEoL (8.04.x)

- **Livello criticità: “10.0”**
- **Descrizione:** la versione attuale del sistema ha raggiunto la “End of Life”, ovvero che non riceve alcun aggiornamento di sicurezza dal fornitore perché non più sostenuta da molto tempo.
- **Conseguenza:** le vulnerabilità di sicurezza non “aggiornate” possono essere sfruttate da un malintenzionato per compromettere la sicurezza dell’host.
- **Soluzione:** aggiornare la macchina a una versione supportata, installando l’ultima versione Ubuntu disponibile.

```
msfadmin@metasploitable:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:   Ubuntu 8.04
Release:      8.04
Codename:     hardy
```

:versione obsoleta

Apache Tomcat SEoL (<= 5.5.x)

- **Livello criticità: “10.0”**
- **Descrizione:** la versione attuale del sistema ha raggiunto la “End of Life”, ovvero che non riceve alcun aggiornamento di sicurezza dal fornitore perché non più sostenuta da molto tempo.
- **Conseguenza:** le vulnerabilità di sicurezza non “aggiornate” possono essere sfruttate da un malintenzionato per compromettere la sicurezza dell’host.
- **Soluzione:** aggiornare il servizio a una versione supportata, installando l’ultima versione disponibile.

Si riporta in qui in basso la versione obsoleta:

```
msfadmin@metasploitable:~$ ps aux | grep tomcat
root      4554  0.0  0.0   1928   248 ?        Ss   08:52   0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid
-Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djav
a.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
root      4555  0.0  0.0   1928   476 ?        S    08:52   0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid
-Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djav
a.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
tomcat55  4567  0.2  9.6 377204 99588 ?        Sl   08:52   0:06 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid
-Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djav
a.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
msfadmin  4908  0.0  0.0   1984   752 pts/1    R+   09:31   0:00 grep tomcat
```

- **Soluzione extra:** se per dei motivi, bisogna lasciare aperto il servizio, potremmo avere una criticità in più da risolvere, come spiegato nella vulnerabilità successiva a questa. Altrimenti se l'utilizzo di questo servizio non è necessario, potremmo eliminare 2 criticità, semplicemente usando il comando “kill” sui vari processi attivi di tomcat. In allegato le procedure qui in basso:

Verifica dei processi attivi:

```
msfadmin@metasploitable:~$ ps aux | grep tomcat
root      4564  0.0  0.0  282 148 ?        Ss   08:52   0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
root      4565  0.0  0.0  282 148 ?        Ss   08:52   0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
root      4567  0.2  9.6 37228 9958 ?        Sl   08:52   0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
msfadmin  5048  9.0  0.0  3044  752 pts/1    R+   09:31   0:00 grep tomcat
```

Dopo aver usato il comando: processi non più attivi.

```
msfadmin@metasploitable:~$ sudo kill 4564 4565 4567
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ps aux | grep tomcat
msfadmin  5049  0.0  0.0  3004  756 pts/1    R+   10:07   0:00 grep tomcat
```

- **Attenzione:** al riavvio successivo della macchina metasploitable2, i servizi torneranno a funzionare, questa soluzione è “temporanea”. Per avere il servizio disabilitato permanentemente bisognerà utilizzare un altro comando.

Porte attive:

8009/tcp open ajp13

Apache Jserv (Protocol v1.3)

8180/tcp open http

Apache Tomcat/Coyote JSP engine 1.1

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 08:55 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000066s latency).
Not shown: 977 closed tcp ports (reset)
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  ftp          ProFTPD 1.3.1
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
MAC Address: 08:00:27:CC:EB:61 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 52.41 seconds
```

Porte chiuse:

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.101 -script
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 10:20 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000062s latency).
Not shown: 979 closed tcp ports (reset)
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  ftp          ProFTPD 1.3.1
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
MAC Address: 08:00:27:CC:EB:61 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 36.44 seconds
```

Apache Tomcat AJP Connector Request Injection (Ghostcat)

- **Livello criticità: “9.8”**
- **Descrizione:** la vulnerabilità Ghostcat (CVE-2020-1938) è una problematica di sicurezza critica che riguarda il connector AJP (Apache JServ Protocol) di Apache Tomcat.
- **Conseguenza:** la vulnerabilità consente ad un attaccante remoto e non autenticato di leggere i file delle applicazioni web o, in alcuni casi, eseguire codice arbitrario tramite un attacco di tipo Remote Code Execution (RCE).
- **Soluzione:** se non si utilizza il connettore AJP (che di solito è utilizzato per comunicare tra Apache HTTP Server e Tomcat), la soluzione migliore è disabilitarlo completamente. Si può fare ciò modificando il file di configurazione di Tomcat (server.xml) e commentando o rimuovendo la configurazione del connettore AJP. Aggiungiamo: “<!--” all’inizio e “-->” alla fine della sezione indicata.

In allegato la soluzione:

```
root@metasploitable:/usr/share/tomcat5.5/conf# ls
Catalina          context.xml       server-minimal.xml  tomcat-users.xml
catalina.policy   logging.properties  server.xml          web.xml
catalina.properties  policy.d         tomcat5.5
root@metasploitable:/usr/share/tomcat5.5/conf#

<!-- Define an AJP 1.3 Connector on port 8009 -->
<!-- <Connector port="8009"
      enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />_

<!-- Define an AJP 1.3 Connector on port 8009 -->
<!-- <Connector port="8009"
$3" /> -->_
```

Porta attiva:

8009/tcp open ajp13

Apache Jserv (Protocol v1.3)

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 08:55 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000066s latency).
Not shown: 977 closed tcp ports (reset)
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  ftp            ProFTPD 1.3.1
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
MAC Address: 08:00:27:CC:EB:61 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 52.41 seconds
```

Porta chiusa:

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 10:42 EDT
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.92% done; ETC: 10:43 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.000075s latency).
Not shown: 978 closed tcp ports (reset)
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  ftp            ProFTPD 1.3.1
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
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:CC:EB:61 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 52.43 seconds
```

VNC Server 'password' Password

- **Livello criticità:** “10.0”
- **Descrizione:** il server VNC in esecuzione sull'host remoto è protetto da una password debole. Un aggressore remoto non autenticato potrebbe sfruttare questa vulnerabilità per assumere il controllo del sistema.
- **Conseguenza:** un aggressore remoto non autenticato potrebbe sfruttare questa vulnerabilità per assumere il controllo del sistema.
- **Soluzione:** modificare la password tramite terminale metasploitable2 o tramite kali connettendosi alla VNC.

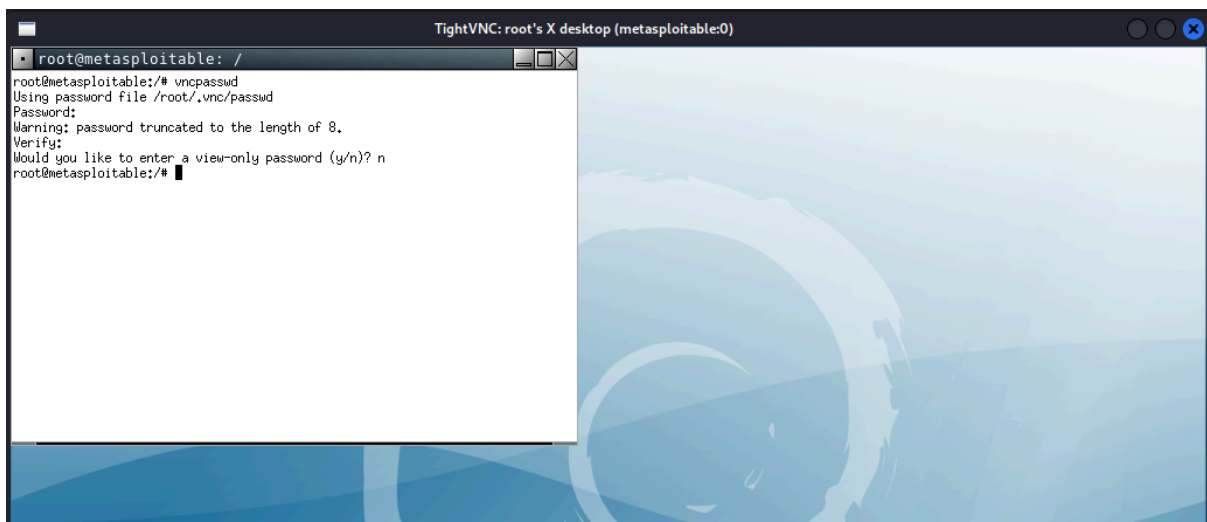
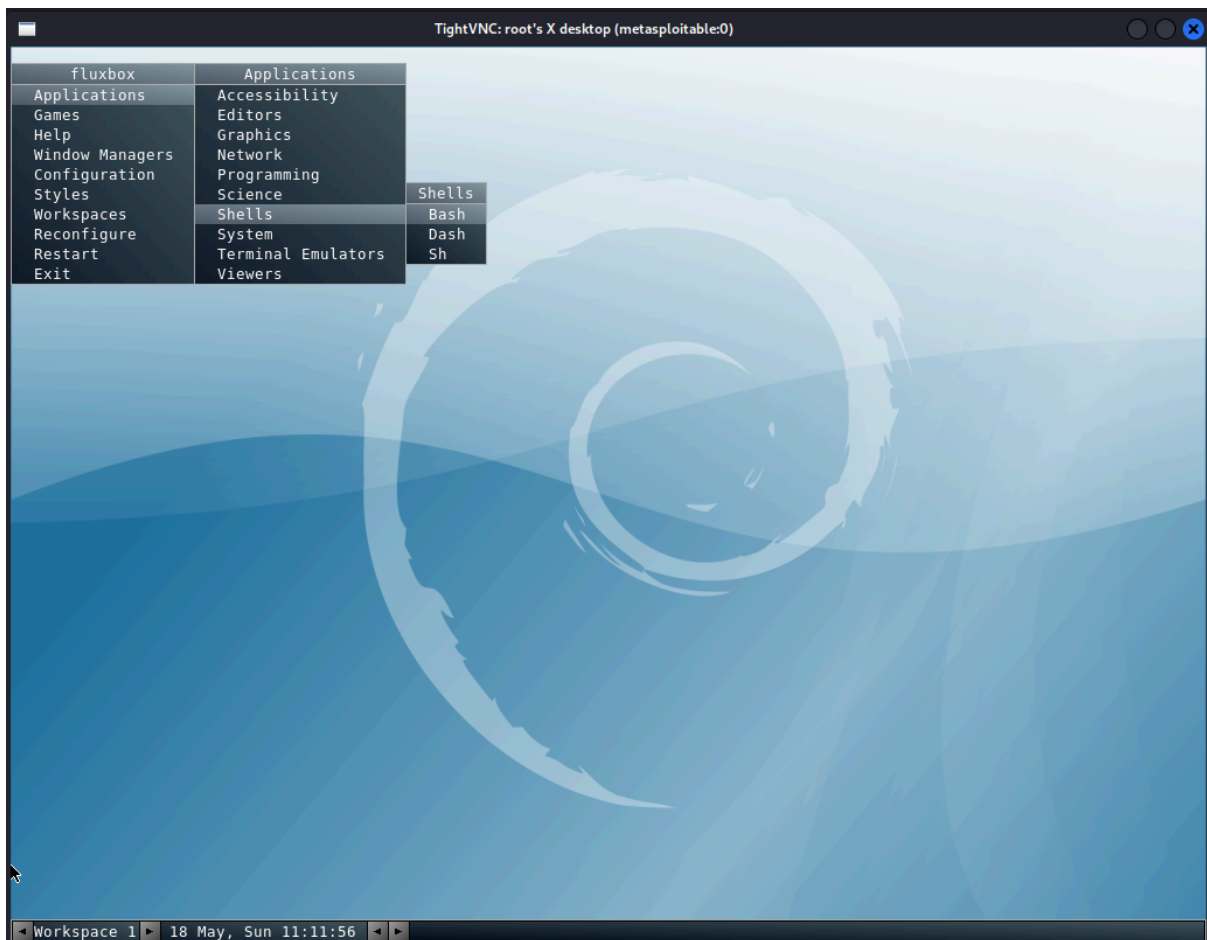
Screenshot dei passaggi da effettuare:

Metasploitable2:

```
root@metasploitable:/# 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)? n
root@metasploitable:/#
```

Kali Linux:

```
(kali@kali)-[~]
$ vncviewer 192.168.50.101:5900
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

Bind Shell Backdoor Detection

- **Livello criticità: “9.8”**
- **Descrizione:** una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione.
- **Conseguenza:** un aggressore potrebbe utilizzarla connettendosi alla porta remota e inviando comandi direttamente.
- **Soluzione:** impedirne l'accesso tramite una regola firewall a chiunque

Screenshot dei passaggi effettuati:

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j drop

msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      tcp  --  anywhere              anywhere
DROP      tcp  --  anywhere              anywhere
DROP      tcp  --  anywhere              anywhere

(kali㉿kali)-[~]
└─$ nmap -p 1524 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 14:21 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00018s latency).
PORT      STATE      SERVICE
1524/tcp  filtered  ingreslock
MAC Address: 08:00:27:CC:EB:61 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

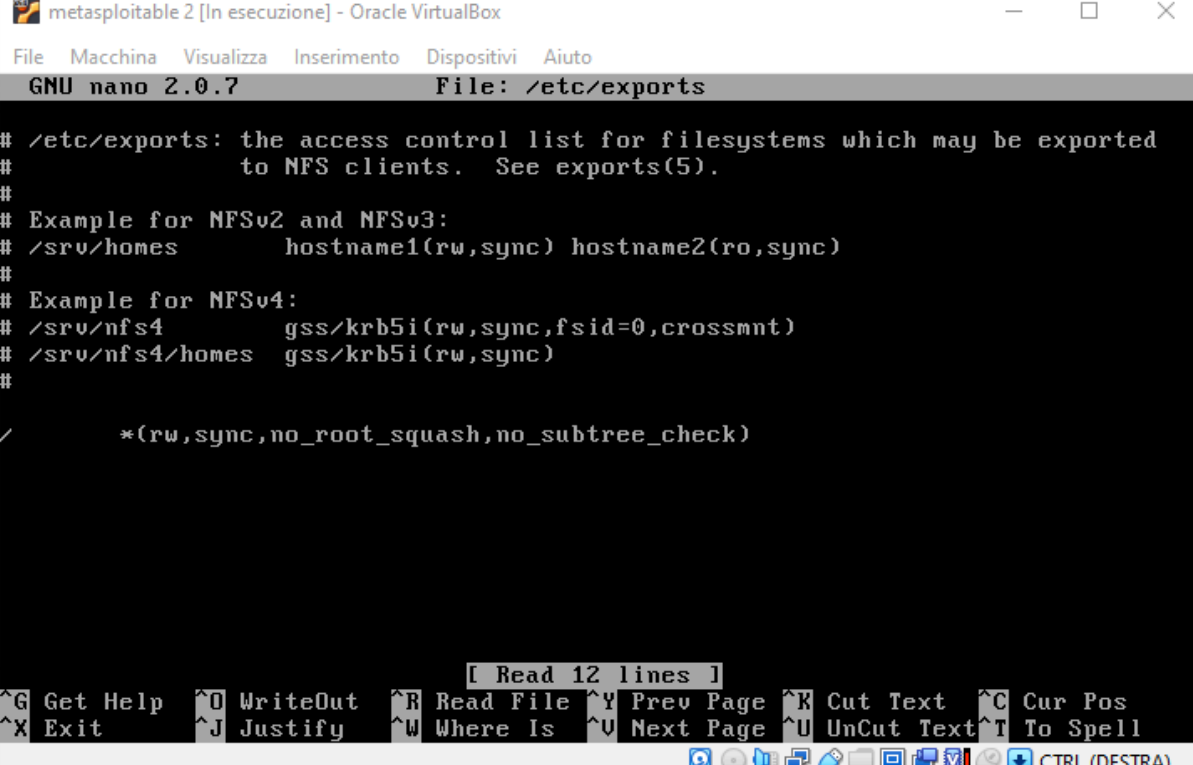
- **Attenzione:** questa è una contromisura temporanea, perché il codice della backdoor è ancora nel sistema e potrebbe aggirare anche l'intervento effettuato. Se la macchina è già appunto compromessa bisognerebbe ripulire l'intero sistema reinstallandolo per essere sicuri che non ci sia più traccia di esso.

NFS Shares World Readable

- **Livello criticità: “7.5”**
- **Descrizione:** il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base al nome host, all'IP o all'intervallo IP).
- **Conseguenza:** senza restrizioni di accesso, un attaccante potrebbe intercettare o manipolare le comunicazioni tra il server NFS e i client, soprattutto se la rete non è protetta o è vulnerabile a questi attacchi.

- **Soluzione:** Impostare le opportune restrizioni su tutte le condivisioni NFS.

In allegato la procedura:



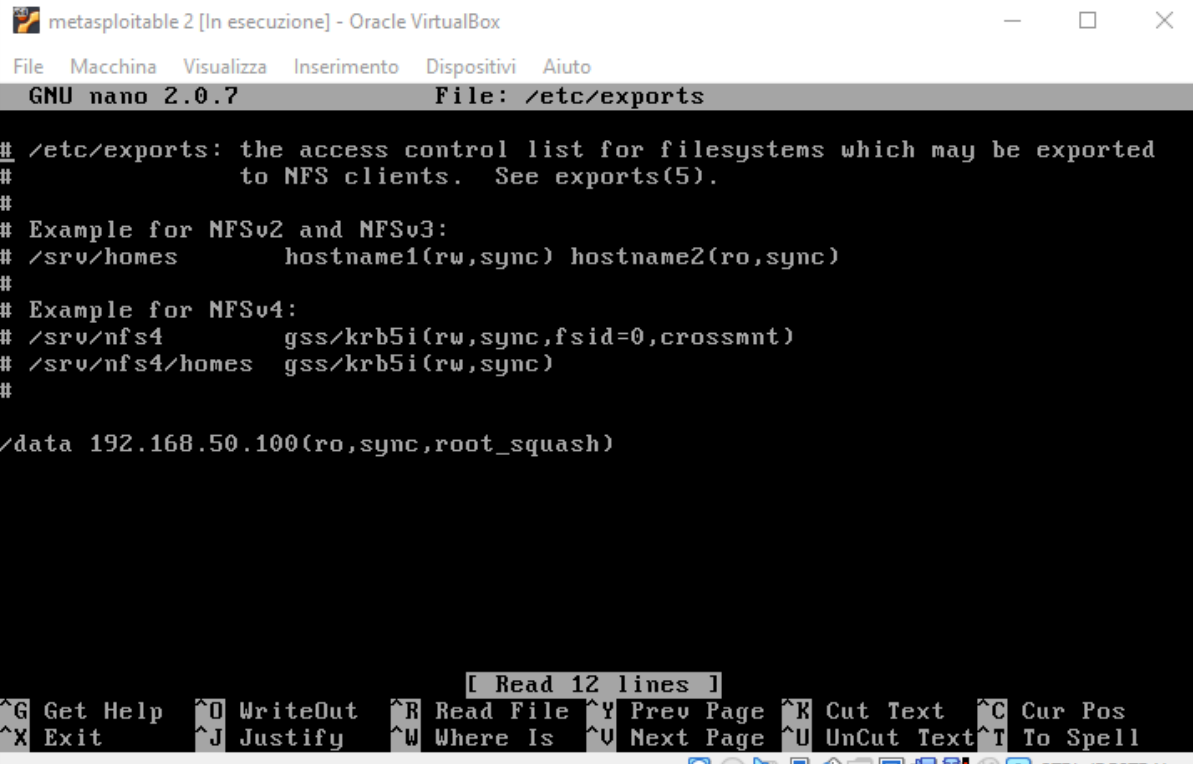
```

metasploitable 2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/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)
#
*/*(rw,sync,no_root_squash,no_subtree_check)

[ Read 12 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
CTRL (DESTRA)

```



```

metasploitable 2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/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)
#
/data 192.168.50.100(ro,sync,root_squash)

[ Read 12 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
CTRL (DESTRA)

```

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

- **Livello criticità: “10.0”**
- **Descrizione:** la chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto alla rimozione da parte di un pacchettizzatore Debian di quasi tutte le fonti di entropia nella versione remota di OpenSSL. Porte interessate: 22, 25, 5432.
- **Conseguenza:** un aggressore può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o per impostare un attacco man-in-the-middle.
- **Soluzione:** si consideri tutto il materiale crittografico generato sull'host remoto come indovicabile. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato. Dato che è irrisolvibile in questi casi per mitigare il più possibile è anche qui necessario usare delle regole firewall, lasciando solamente il libero accesso alla nostra macchina Kali in modo tale da poterci collegare tramite la porta 22, anche se questo comporterebbe che nessun la rilevi come criticità.

Screenshot dei procedimenti eseguiti durante l'intervento:

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.50.100 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 25 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 5432 -j DROP

msfadmin@metasploitable:~$ sudo iptables -L
[sudo] password for msfadmin:
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           tcp dpt:postgresql
DROP       tcp  --  anywhere              anywhere              tcp dpt:smtp
DROP       tcp  --  anywhere              anywhere              tcp dpt:ingreslock
ACCEPT     tcp  --  192.168.50.100        anywhere              tcp dpt:ssh
DROP       tcp  --  anywhere              anywhere              tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)

- **Livello criticità:** “9.8”
- **Descrizione:** in base al numero di versione auto-dichiarato, l'applicazione phpMyAdmin ospitata sul server web remoto è precedente alla 4.8.6. È quindi affetta da una vulnerabilità di tipo SQL injection (SQLi) presente nella funzionalità di progettazione di phpMyAdmin.
- **Conseguenza:** un aggressore remoto non autenticato può sfruttarla per iniettare o manipolare query SQL nel database back-end, con conseguente divulgazione o manipolazione di dati arbitrari.
- **Soluzione:** aggiornare phpMyAdmin alla versione 4.8.6 o successiva. In alternativa, applicare le patch indicate negli avvisi del fornitore.

Riportato qui sotto la “soluzione” alla vulnerabilità all'interno del codice sorgente del fornitore:

```
768 768         $(this).dialog('close');
769 769     };
770 770
771 771     var $form = $('<form action="db_designer.php" method="post" name="save_page" id="save_page" class="ajax"></form>')
772 772         .append('<input type="hidden" name="server" value="' + server + '" />')
773 773         .append('<input type="hidden" name="db" value="' + db + '" />')
774 774         .append('<input type="hidden" name="db" />').val(db))
775 775         .append('<input type="hidden" name="operation" value="savePage" />')
776 776         .append('<input type="hidden" name="save_page" value="new" />')
777 777         .append('<label for="selected_value">' + PMA_messages.strPageName +
778 778             '</label><input type="text" name="selected_value" />');
779 779     $form.on('submit', function (e) {
780 780         e.preventDefault();
781 781         submitSaveDialogAndClose(callback);
```

Apache PHP-CGI Remote Code Execution

- **Livello criticità:** “9.8”
- **Descrizione:** l'installazione di PHP sul server web remoto contiene una falla che potrebbe consentire a un aggressore remoto di passare argomenti della riga di comando come parte di una stringa di query al programma PHP-CGI.
- **Conseguenza:** questo potrebbe essere sfruttato per eseguire codice arbitrario, rivelare il codice sorgente di PHP, causare un crash di sistema, ecc.
- **Soluzione:** aggiornare a PHP 5.3.13 / 5.4.3 o versione successiva, oppure disabilitare il supporto PHP-CGI se non è strettamente necessario.

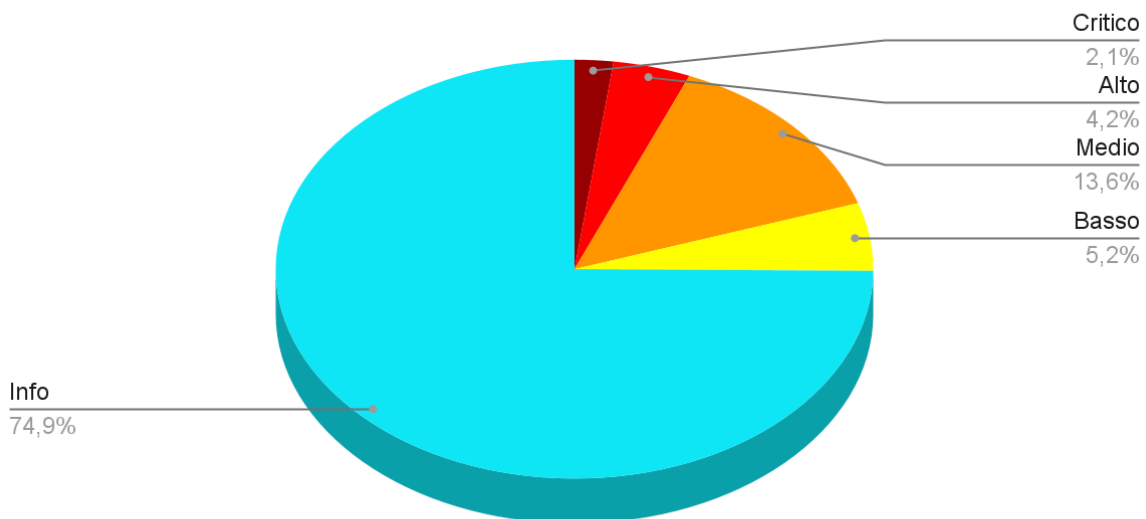
Riportato qui il comando utilizzato:

```
root@metasploitable:/etc/init.d# sudo a2dismod cgi
Module cgi already disabled
```

4. Scansione delle vulnerabilità con Nessus (post-intervento)

Una volta eseguite tutte le accurate modifiche per mitigare le vulnerabilità, si può procedere con la scansione con il tool Nessus alla verifica che essi siano effettivamente risolte o quantomeno mitigate.

Vulnerabilità rimaste su Metasploitable2



4.1. Riassunto dei risultati ottenuti

Come previsto alcune vulnerabilità non sono state risolte del tutto, ma sono state sicuramente mitigate abbastanza per non facilitare troppo i malintenzionati ad accedere alla macchina. Alcune vulnerabilità trovate da nessus sono state:

Canonical Ubuntu Linux SEoL (8.04.x) = “non risolvibile se non usando un'altra versione”

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness = “porta 22 lasciata aperta di proposito ma limitata l’accesso solo all’host kali”

phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3) = “possibile soluzione tramite modifica al codice sorgente dichiarata dal fornitore”

Apache PHP-CGI Remote Code Execution = “aggiornare la versione ad una più supportata, oppure disabilitare i moduli anche se in questo caso non è bastato, ma sicuramente avrà reso la vulnerabilità meno pericolosa.

Critico	Alto	Medio	Basso	Info
4	8	26	10	143

5. Conclusione

L'attività di vulnerability assessment svolta su Metasploitable2 evidenziando numerose vulnerabilità critiche, in linea con le caratteristiche volutamente insicure del sistema target.

La fase di scansione, effettuata con Nessus, ha rilevato un ampio spettro di problematiche, tra cui servizi obsoleti, configurazioni errate e vulnerabilità note e sfruttabili. In seguito, sono state applicate una serie di contromisure mirate, come la disattivazione di servizi inutilizzati, l'introduzione di restrizioni firewall, la modifica delle configurazioni.

La seconda scansione ha confermato una riduzione generale del rischio, pur evidenziando la permanenza di alcune vulnerabilità non completamente risolvibili nel contesto simulato, come quelle legate alla fine del supporto del sistema operativo e di alcuni servizi. Tuttavia, l'implementazione di misure di mitigazione ha comunque migliorato il livello di sicurezza generale.

In conclusione è molto importante eseguire un processo ciclico di valutazione e miglioramento continuo ottimizzando la sicurezza della macchina per ridurre la superficie d'attacco e limitare i rischi.