

# REPORT PROGETTO Vulnerability/Remediation

NOME DEL PROGETTO	Vulnerability/Remediation	PROGETTO N.	001
RESPONSABILE DI PROGETTO	PERIODO COPERTO	DATA DI INSERIMENTO DELLO STATO	DATA PREVISTA DI COMPLETAMENTO
Simone Cisbaglia	Week 12	06/05/2024	10/05/2024

## SINTESI DEL PROGETTO

In un ambiente virtuale composta da 3 macchine virtuali: Kali linux (IP 192.168.1.100) Metasploitable (IP 192.168.50.100) e Pfsense. Esegirò una scansione da Kali con il tool Nessus sulla macchina Metasploitable e una volta scoperte le vulnerabilità critiche, ne risolverò 5 sia intervenendo direttamente in Metasploitable sia con l'aiuto di Pfsense e poi eseguirò una nuova scansione per verificare la risoluzione delle vulnerabilità.

## PANORAMICA DEL PROGETTO

CATEGORIA	STATO	DETTAGLI	COMMENTI
Creazione Ambiente	Eseguito	Test comunicazione tra macchine	Ambiente funzionante e pronto
Scansione Nessus	Eseguito	La scansione rivelà vulnerabilità	Analisi delle vulnerabilità critiche
Azioni di rimedio	Eseguito	Selezione di 5 vulnerabilità critiche	Avvio azioni di rimedio
Nuova scansione Nessus	Eseguito	Verifica della risoluzione	Vulnerabilità risolte con successo
Stesura report	Eseguito	Creazione report onnicomprensivo	Sintesi di tutte le lavorazioni



## RISCHI E PROBLEMI CHIAVE

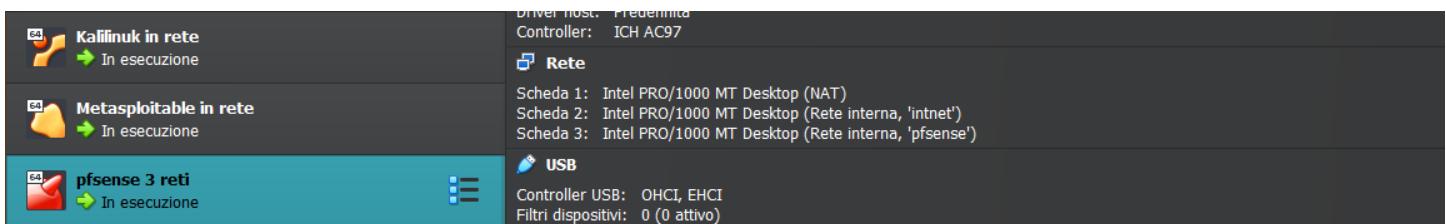
NOME DEL RISCHIO	STATO	SISTEMA	DESCRIZIONE
Bind Shell Backdoor Detection	Risolto	Metasploitable	Backdoor
VNC Server 'password' Password	Risolto	Metasploitable	Gain a shell remotely
NFS Exported Share Information Disclosure	Risolto	Metasploitable	RPC

Apache Tomcat AJP Connector Request Injection (Ghostcat)	Risolto	Metasploitable	Web Servers
UnrealIRCd Backdoor Detection	Risolto	Metasploitable	Backdoors

## Creazione Ambiente

Creo un ambiente virtuale composta da 3 macchine virtuali:

1. Kali linux (IP 192.168.1.100)
2. Metasploitable (IP 192.168.50.100)
3. PfSense



## Scansione nessus:

Testo l'ambiente e una volta assicurandomi della corretta comunicazione tra le macchine avvio il tool Nessus da Kali linux impostando come target Metasploitable, ecco i risultati:

**192.168.50.100**



### Host Information

Netbios Name: METASPLOITABLE  
 IP: 192.168.50.100  
 OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Analizzo i risultati, seleziono 5 vulnerabilità su cui intervenire e avvio le azioni correttive dopo le opportune ricerche

FOLDERS  
My Scans  
All Scans  
Trash

RESOURCES  
Policies  
Plugin Rules  
Terrascan

Tenable News  
CyberPower  
PowerPanel  
Enterprise Power  
Device Netw...

Metasploitable / 192.168.50.100  
[Back to Hosts](#)

Vulnerabilities 104

Filter ▾ Search Vulnerabilities 104 Vulnerabilities (5 Selected) [Clear Selected Items](#)

Sev	CVSS	VPR	Name	Family	Count	Actions
<span style="background-color: red; color: white;">CRITICAL</span>	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1	<span style="color: #ccc;">Snooze</span> <span style="color: #ccc;">Modify</span> <span style="color: #ccc;">Configure</span> <span style="color: #ccc;">Audit Trail</span> <span style="color: #ccc;">Launch</span> <span style="color: #ccc;">Report</span> <span style="color: #ccc;">Export</span>
<span style="background-color: red; color: white;">CRITICAL</span>	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	<span style="color: #ccc;">Snooze</span> <span style="color: #ccc;">Modify</span> <span style="color: #ccc;">Configure</span> <span style="color: #ccc;">Audit Trail</span> <span style="color: #ccc;">Launch</span> <span style="color: #ccc;">Report</span> <span style="color: #ccc;">Export</span>
<span style="background-color: lightgray;">CRITICAL</span>	10.0		Unix Operating System Unsupported Version Detection	General	1	<span style="color: #ccc;">Snooze</span> <span style="color: #ccc;">Modify</span> <span style="color: #ccc;">Configure</span> <span style="color: #ccc;">Audit Trail</span> <span style="color: #ccc;">Launch</span> <span style="color: #ccc;">Report</span> <span style="color: #ccc;">Export</span>
<span style="background-color: red; color: white;">CRITICAL</span>	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	<span style="color: #ccc;">Snooze</span> <span style="color: #ccc;">Modify</span> <span style="color: #ccc;">Configure</span> <span style="color: #ccc;">Audit Trail</span> <span style="color: #ccc;">Launch</span> <span style="color: #ccc;">Report</span> <span style="color: #ccc;">Export</span>
<span style="background-color: red; color: white;">CRITICAL</span>	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	<span style="color: #ccc;">Snooze</span> <span style="color: #ccc;">Modify</span> <span style="color: #ccc;">Configure</span> <span style="color: #ccc;">Audit Trail</span> <span style="color: #ccc;">Launch</span> <span style="color: #ccc;">Report</span> <span style="color: #ccc;">Export</span>
<span style="background-color: lightgray;">CRITICAL</span>	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	<span style="color: #ccc;">Snooze</span> <span style="color: #ccc;">Modify</span> <span style="color: #ccc;">Configure</span> <span style="color: #ccc;">Audit Trail</span> <span style="color: #ccc;">Launch</span> <span style="color: #ccc;">Report</span> <span style="color: #ccc;">Export</span>
<span style="background-color: red; color: white;">CRITICAL</span>	9.8		Bind Shell Backdoor Detection	Backdoors	1	<span style="color: #ccc;">Snooze</span> <span style="color: #ccc;">Modify</span> <span style="color: #ccc;">Configure</span> <span style="color: #ccc;">Audit Trail</span> <span style="color: #ccc;">Launch</span> <span style="color: #ccc;">Report</span> <span style="color: #ccc;">Export</span>
<span style="background-color: purple;">MIXED</span>	...	...	Phpmyadmin (Multiple Issues)	CGI abuses	4	<span style="color: #ccc;">Snooze</span> <span style="color: #ccc;">Modify</span> <span style="color: #ccc;">Configure</span> <span style="color: #ccc;">Audit Trail</span> <span style="color: #ccc;">Launch</span> <span style="color: #ccc;">Report</span> <span style="color: #ccc;">Export</span>
<span style="background-color: lightgray;">CRITICAL</span>	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	<span style="color: #ccc;">Snooze</span> <span style="color: #ccc;">Modify</span> <span style="color: #ccc;">Configure</span> <span style="color: #ccc;">Audit Trail</span> <span style="color: #ccc;">Launch</span> <span style="color: #ccc;">Report</span> <span style="color: #ccc;">Export</span>
<span style="background-color: purple;">MIXED</span>	...	...	PHP (Multiple Issues)	CGI abuses	3	<span style="color: #ccc;">Snooze</span> <span style="color: #ccc;">Modify</span> <span style="color: #ccc;">Configure</span> <span style="color: #ccc;">Audit Trail</span> <span style="color: #ccc;">Launch</span> <span style="color: #ccc;">Report</span> <span style="color: #ccc;">Export</span>
<span style="background-color: red; color: white;">HIGH</span>	8.3		CGI Generic SQL Injection (blind)	CGI abuses	1	<span style="color: #ccc;">Snooze</span> <span style="color: #ccc;">Modify</span> <span style="color: #ccc;">Configure</span> <span style="color: #ccc;">Audit Trail</span> <span style="color: #ccc;">Launch</span> <span style="color: #ccc;">Report</span> <span style="color: #ccc;">Export</span>

Host Details  
IP: 192.168.50.100  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)  
Start: May 7 at 6:32 PM  
End: May 7 at 7:48 PM  
Elapsed: an hour  
KB: [Download](#)

Vulnerabilities

Critical: 10%, High: 20%, Medium: 30%, Low: 20%, Info: 20%

## Azioni correttive:

### VULNERABILITÀ N°1: BIND SHELL BACKDOOR DETECTION

#### 51988 - Bind Shell Backdoor Detection

##### Synopsis

The remote host may have been compromised.

##### 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.

##### Risk Factor

Critical

##### CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

##### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

##### Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

##### Plugin Output

tcp/1524/wild\_shell

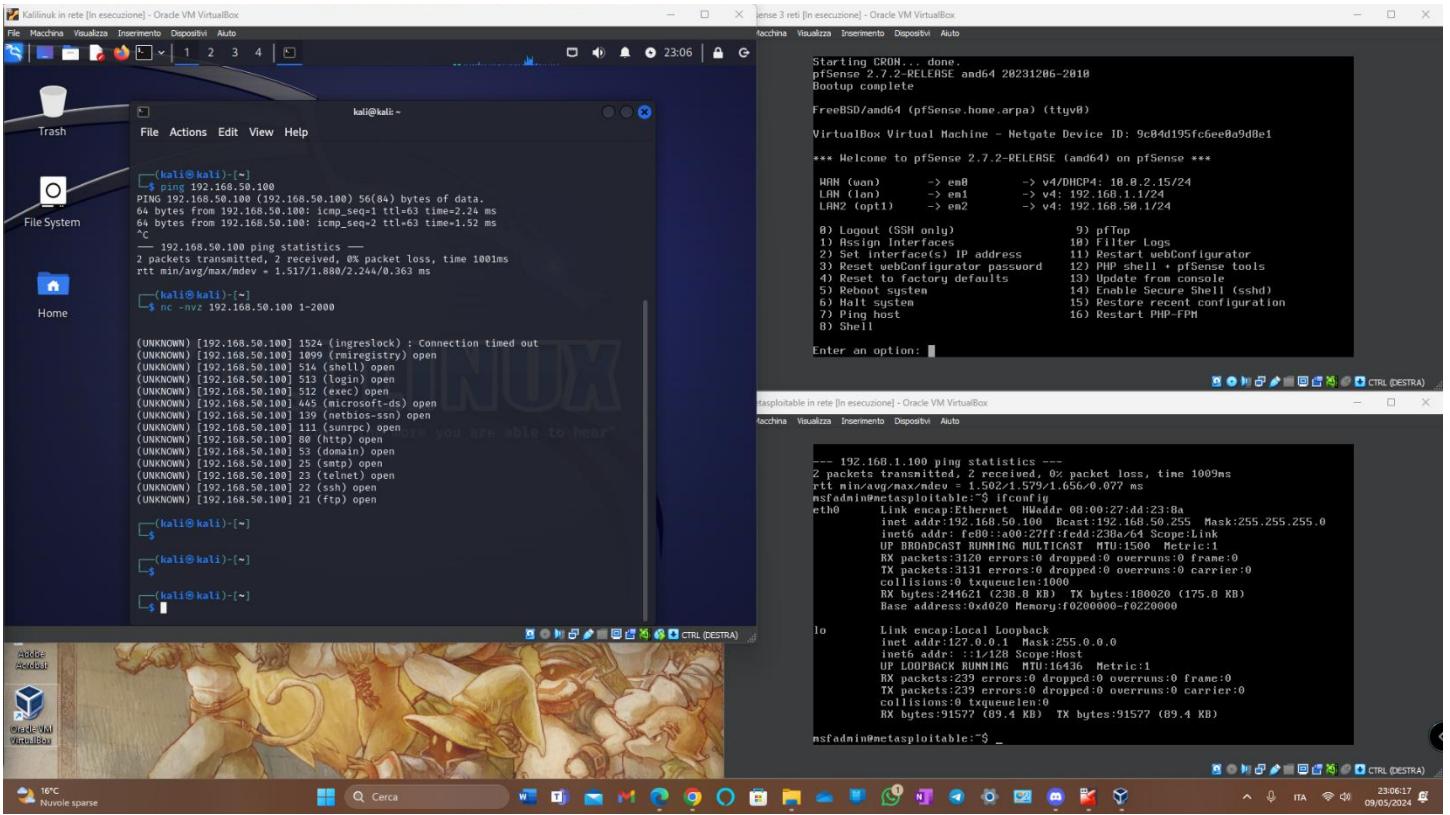
Ho scoperto una vulnerabilità critica relativa alla presenza di una porta in ascolto, identificata come porta numero 1524 attraverso la scansione con Nessus. Questa porta permette l'accesso diretto alla shell di comandi

con privilegi di root senza richiedere autenticazione, esponendo la macchina a rischi significativi. Nei prossimi passi, mostrerò come identificare, sfruttare e infine bloccare questa vulnerabilità utilizzando Netcat e IPTables su Kali Linux.

The screenshot shows a Kali Linux desktop environment with several windows open:

- KaliLinux in rete [In esecuzione] - Oracle VM VirtualBox**: A terminal window showing network statistics and a ping command to 192.168.50.100.
- Metasploitable in rete [In esecuzione] - Oracle VM VirtualBox**: A terminal window showing a welcome message for pfSense 2.7.2-RELESE and64 on pfSense. It lists various configuration options like pftop, filter logs, and web configurator.
- KaliLinux in rete [In esecuzione] - Oracle VM VirtualBox**: A terminal window showing a netstat -an output, listing many open ports on 192.168.50.100, including 1524 (ingreslock), 1099 (rmiregistry), 513 (login), 443 (microsoft-ds), 139 (netbios-ssn), 80 (http), 25 (smtp), 23 (telnet), 22 (ssh), and 21 (ftp).
- Metasploitable in rete [In esecuzione] - Oracle VM VirtualBox**: A terminal window showing a ping statistics output for 192.168.1.100.
- KaliLinux in rete [In esecuzione] - Oracle VM VirtualBox**: A terminal window showing a netcat command to port 1524 on the Metasploitable host.
- Metasploitable in rete [In esecuzione] - Oracle VM VirtualBox**: A terminal window showing a ping statistics output for 192.168.1.100.

The desktop background features a painting of a scene from Final Fantasy VII.



Ho iniziato eseguendo una scansione delle porte con **nmap** sulla mia macchina locale, notando che la porta 1524 era aperta. Dopo aver confermato le configurazioni della mia interfaccia di rete con **ifconfig**, ho deciso di bloccare l'accesso a questa porta vulnerabile utilizzando **iptables**.

Il comando che ho usato per rifiutare il traffico in entrata su questa porta è stato:

```
sudo iptables -I INPUT -p tcp --dport 1524 -j DROP
```

Per verificare l'efficacia di questa regola, ho tentato di connettermi nuovamente alla porta 1524 e ho riscontrato che la connessione era effettivamente bloccata, come confermato dall'output di **nmap** che mostrava "Connection timed out". Ho anche effettuato un ping verso un indirizzo IP per assicurarmi che la connettività di rete fosse ancora attiva, confermando che il blocco era specifico per la porta 1524 e non influenzava altre connessioni.

## VULNERABILITÀ N°2: VNC SERVER "password" PASSWORD

### 61708 - VNC Server 'password' Password

#### Synopsis

A VNC server running on the remote host is secured with a weak 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.

#### Risk Factor

Critical

#### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:I/C:A:C)

#### Plugin Information

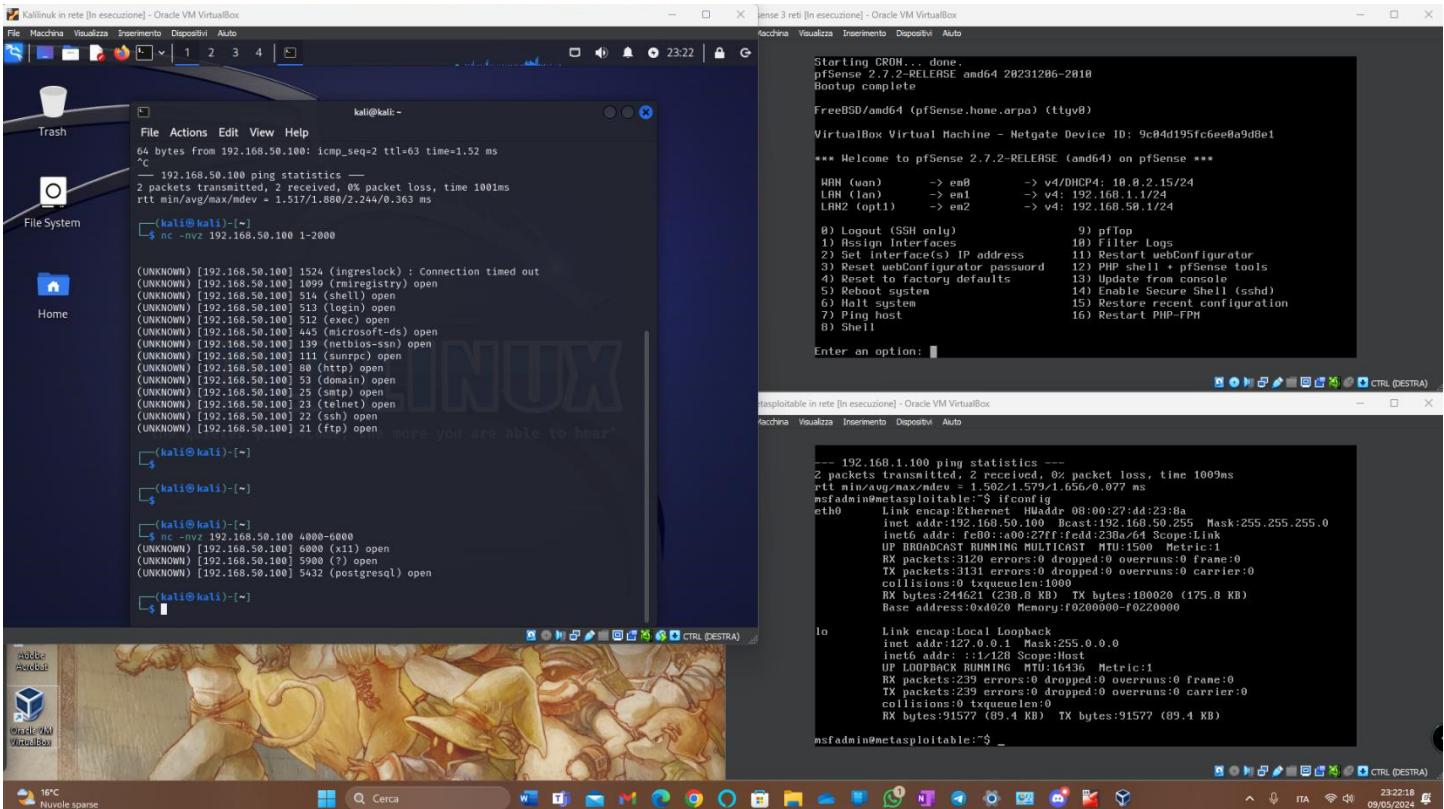
Published: 2012/08/29, Modified: 2015/09/24

#### Plugin Output

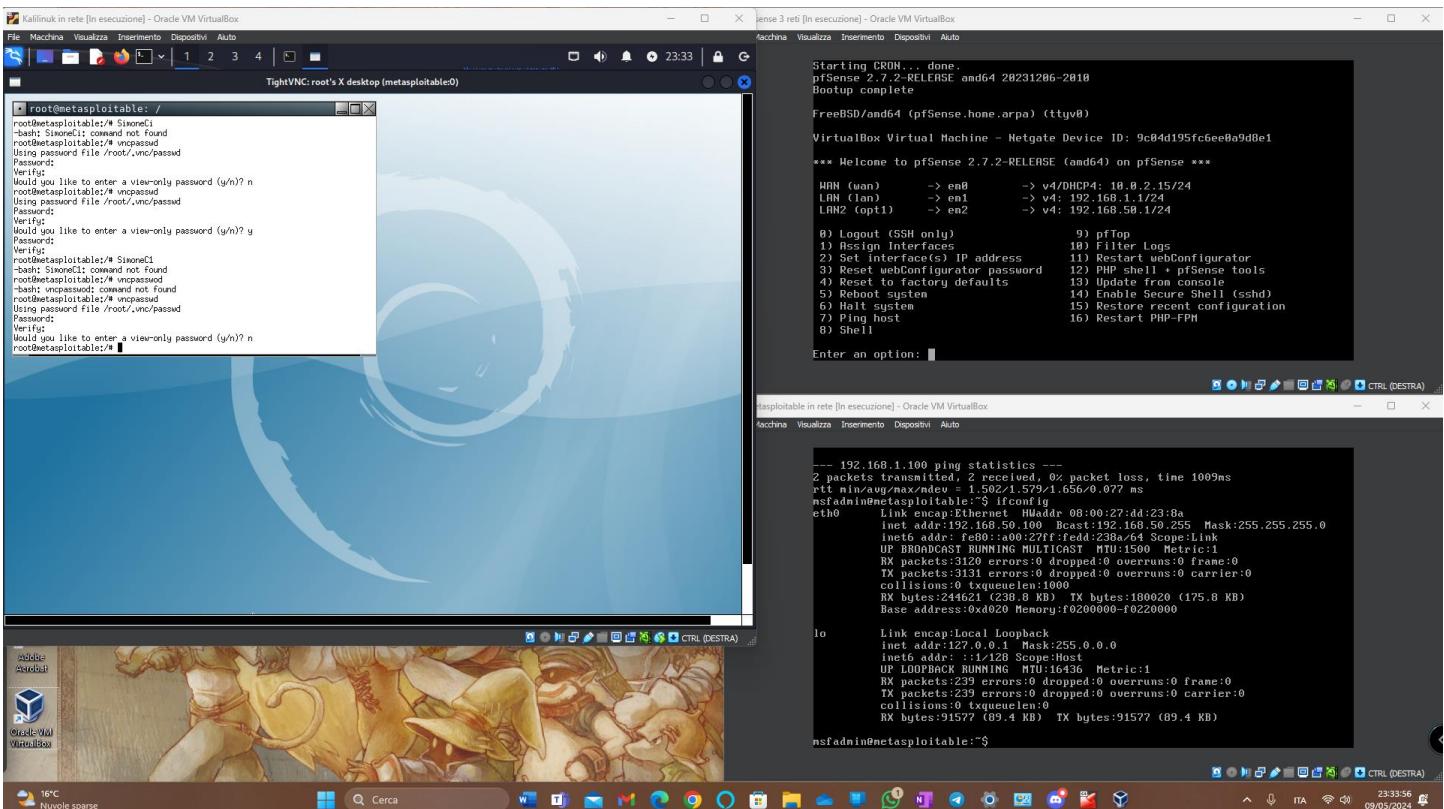
tcp/5900/vnc

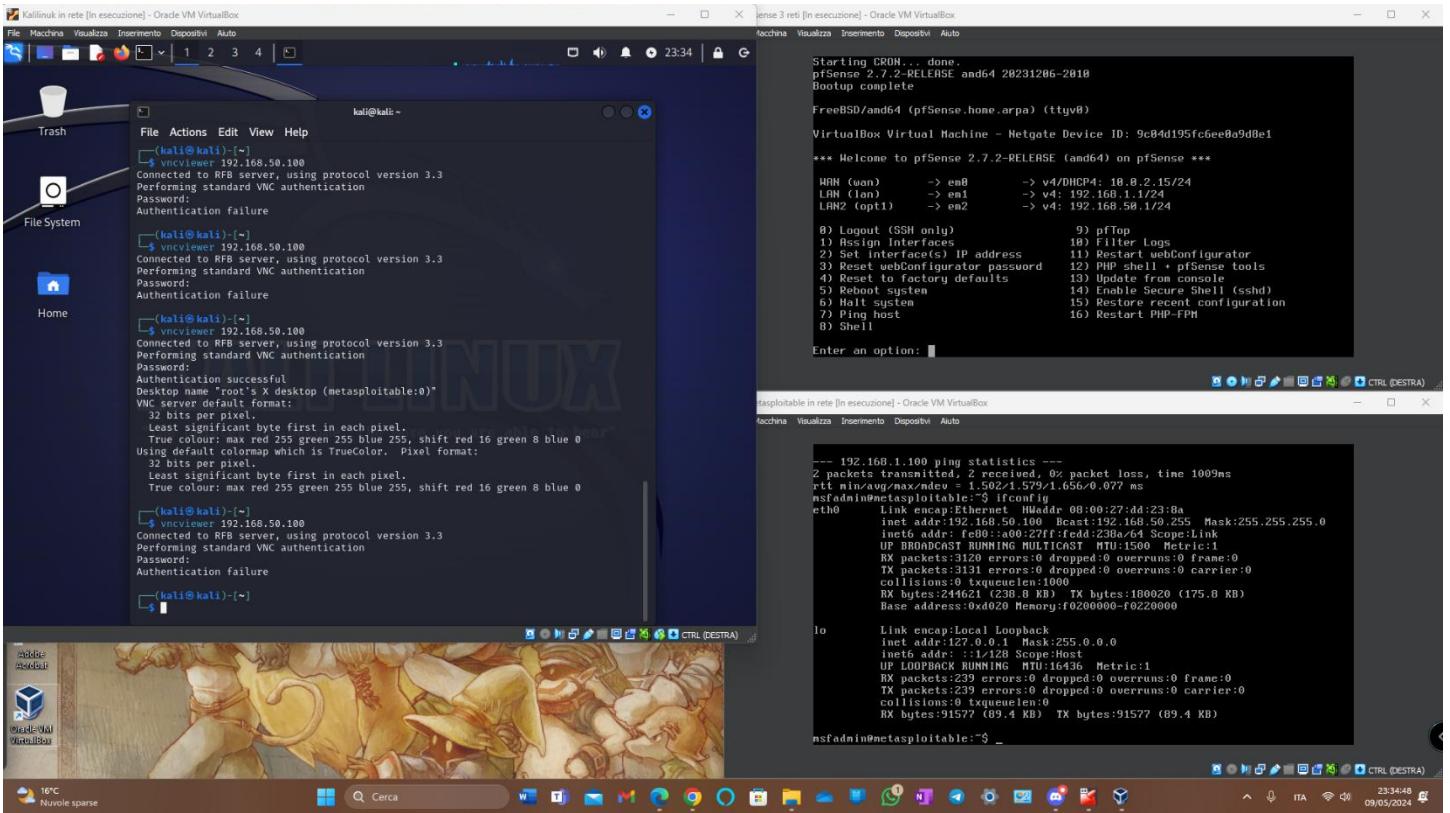
Nessus logged in using a password of "password".

La seconda vulnerabilità che ho scelto di risolvere riguarda il VNC, basato sul protocollo RFB, che permette il controllo di un computer da una posizione remota. Un software noto che sfrutta questa tecnologia è TeamViewer. Questa vulnerabilità è particolarmente critica perché è legata alla presenza di una password di accesso troppo semplice da decifrare. Per mitigare questo rischio, ho deciso di cambiare la password attuale con una più complessa.



Ho iniziato eseguendo una scansione con **nmap** sulla porta 5900 di un indirizzo IP specifico per identificare la presenza di un servizio VNC. La scansione ha confermato che la porta era aperta e che il servizio VNC era attivo con protocollo versione 3.3. Dopo aver scoperto il servizio, mi sono connesso utilizzando un client VNC, inserendo le credenziali che sono state accettate, permettendomi così l'accesso al desktop remoto.





Mi sono connesso all'editor grafico di VNC su Metasploitable con i privilegi di root utilizzando la password "password", rivelata da una scansione Nessus. Successivamente, ho aggiornato la password in "SimoneC1". Per testare la modifica, ho tentato di riconnettermi con la vecchia password e l'autenticazione è fallita, confermando così che l'aggiornamento della password è stato efficace.

## VULNERABILITÀ N°3: NFS EXPORTED SHARE INFORMATION DISCLOSURE

### 11356 - NFS Exported Share Information Disclosure

#### Synopsis

It is possible to access NFS shares on the remote host.

#### 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.

#### Risk Factor

Critical

#### VPR Score

5.9

#### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

#### References

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

#### Exploitable With

Metasploit (true)

#### Plugin Information

Published: 2003/03/12, Modified: 2023/08/30

#### Plugin Output

udp/2049/rpc-nfs

La terza vulnerabilità che ho selezionato riguarda il NFS (Network File System), un protocollo di rete utilizzato spesso in sistemi UNIX, che permette ai computer client di accedere a directory condivise tramite un punto di accesso da server remoti come se fossero locali. Ho scoperto che esiste la possibilità per i malintenzionati di accedere liberamente ad almeno un punto di accesso, consentendo loro di leggere e scrivere file sul nostro sistema. Per mitigare questo rischio, è essenziale riconfigurare NFS in modo che solo utenti autorizzati possano accedere, garantendo così la sicurezza dei nostri dati condivisi.

KaliLinux in rete [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimenti Dispositivi Auto

File Actions Edit View Help

Authentication failure

```
[kali㉿kali]:~$ nmap -p 1-65535 -T4 -A -v 192.168.50.100
Starting Nmap 7.94SNM ( https://nmap.org ) at 2024-05-09 23:39 CEST
NSE: Loaded 156 scripts for scanning.
Initiating NSE at 23:39
Completed NSE at 23:39. 0.00s elapsed
Initiating NSE at 23:39
Completed NSE at 23:39. 0.00s elapsed
Initiating NSE at 23:39
Completed NSE at 23:39. 0.00s elapsed
Initiating Ping Scan at 23:39
Scanning 192.168.50.100 [2 ports]
Completed Ping Scan at 23:39. 0.00s elapsed (1 total hosts)
Parallel DNS resolution of 1 host. at 23:39
Completed Parallel DNS resolution of 1 host. at 23:39. 0.00s elapsed
Initiating Connect Scan at 23:39
Scanning 192.168.50.100 [65535 ports]
Discovered open port 22/tcp on 192.168.50.100
Discovered open port 3306/tcp on 192.168.50.100
Discovered open port 443/tcp on 192.168.50.100
Discovered open port 53/tcp on 192.168.50.100
Discovered open port 111/tcp on 192.168.50.100
Discovered open port 445/tcp on 192.168.50.100
Discovered open port 21/tcp on 192.168.50.100
Discovered open port 5900/tcp on 192.168.50.100
Discovered open port 80/tcp on 192.168.50.100
Discovered open port 8000/tcp on 192.168.50.100
Discovered open port 3632/tcp on 192.168.50.100
Discovered open port 8180/tcp on 192.168.50.100
Discovered open port 5479/tcp on 192.168.50.100
Discovered open port 8787/tcp on 192.168.50.100
Discovered open port 3824/tcp on 192.168.50.100
Discovered open port 1699/tcp on 192.168.50.100

```

File System

Home

12°C Variabile

Tecniche Visualizza Inserimenti Dispositivi Auto

Starting CRON... done.

pfSense 2.7.2-RELEASE amd64 20231206-2018

Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 9c04d195fc6ee8a9d0e1

\*\*\* Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense \*\*\*

```
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
Lan1 (lan)     -> em1      -> v4: 192.168.1.1/24
Lan2 (opt1)    -> em2      -> v4: 192.168.50.1/24

B) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set Interface(s) IP Address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Enter an option: 1

File System

Home

12°C Variabile

Tecniche Visualizza Inserimenti Dispositivi Auto

--- 192.168.1.100 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 1009ms

rtt min/avg/max/mdev = 1.579/1.579/1.656/0.077 ms

nsfadmin@metasploitable:~\$ ifconfig

eth0 Link encap:Ethernet HWaddr 08:00:27:ad:23:8a  
inet addr:192.168.50.100 Bcast:192.168.50.255 Mask:255.255.255.0  
inet6 addr: fe80::a00:27ff:fedd:23a/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:3120 errors:0 dropped:0 overruns:0 frame:0  
TX packets:3120 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:244621 (238.8 KB) TX bytes:100020 (175.8 KB)  
Base address:0xd020 Memory:f0200000-f0220900

lo Link encap:Local Loopback  
inet addr:127.0.0.1 Mask:255.0.0.0  
inet6 addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING MTU:1500 Metric:1  
RX packets:239 errors:0 dropped:0 overruns:0 frame:0  
TX packets:239 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:91577 (89.4 KB) TX bytes:91577 (89.4 KB)

nsfadmin@metasploitable:~\$

File System

Home

12°C Variabile

Tecniche Visualizza Inserimenti Dispositivi Auto

Starting CRON... done.

pfSense 2.7.2-RELEASE amd64 20231206-2018

Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 9c04d195fc6ee8a9d0e1

\*\*\* Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense \*\*\*

```
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
Lan1 (lan)     -> em1      -> v4: 192.168.1.1/24
Lan2 (opt1)    -> em2      -> v4: 192.168.50.1/24

B) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set Interface(s) IP Address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Enter an option: 1

File System

Home

12°C Variabile

Tecniche Visualizza Inserimenti Dispositivi Auto

--- 192.168.1.100 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 1009ms

rtt min/avg/max/mdev = 1.502/1.579/1.656/0.077 ms

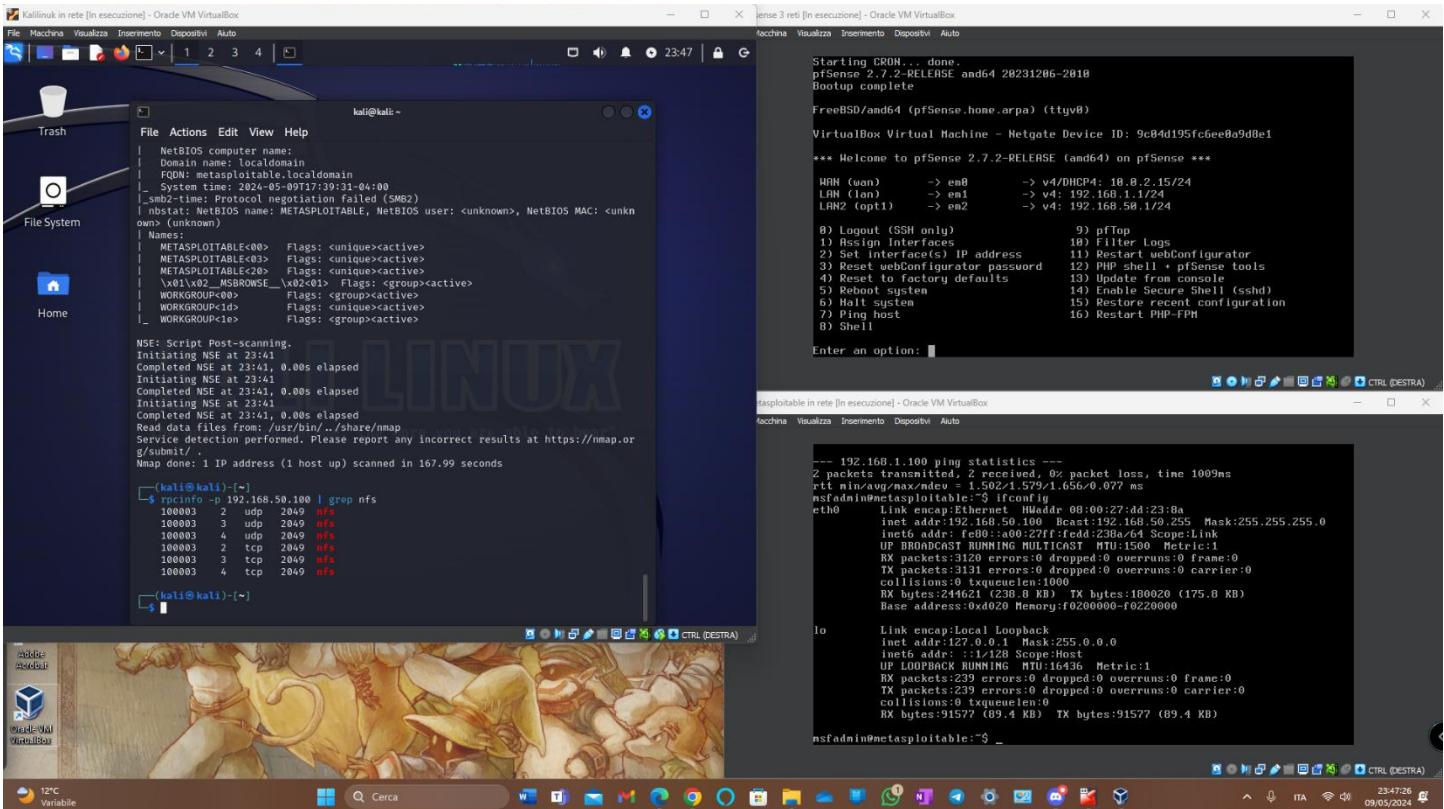
nsfadmin@metasploitable:~\$ ifconfig

eth0 Link encap:Ethernet HWaddr 08:00:27:ad:23:8a  
inet addr:192.168.50.100 Bcast:192.168.50.255 Mask:255.255.255.0  
inet6 addr: fe80::a00:27ff:fedd:23a/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:239 errors:0 dropped:0 overruns:0 frame:0  
TX packets:239 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:244621 (238.8 KB) TX bytes:100020 (175.8 KB)  
Base address:0xd020 Memory:f0200000-f0220900

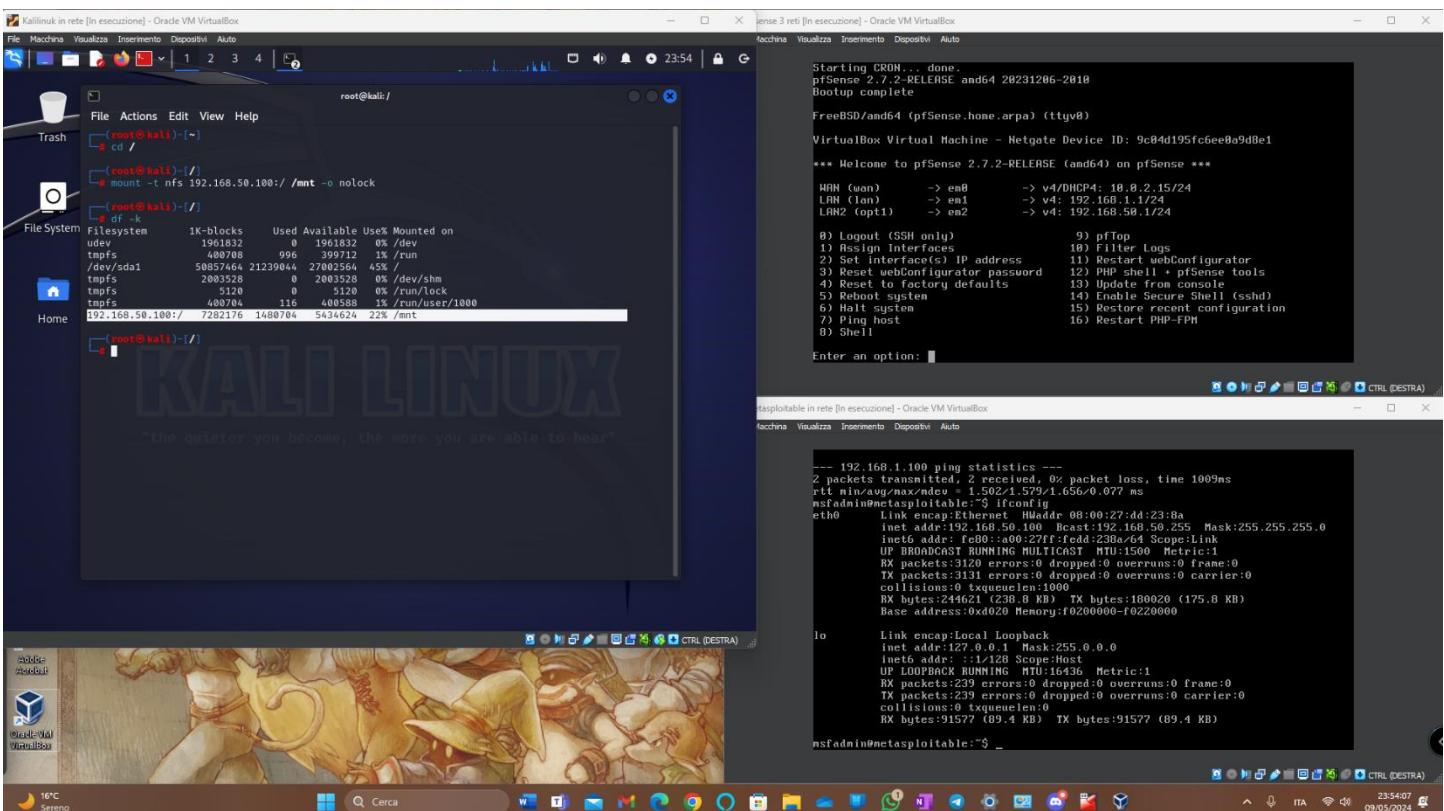
lo Link encap:Local Loopback  
inet addr:127.0.0.1 Mask:255.0.0.0  
inet6 addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING MTU:1500 Metric:1  
RX packets:239 errors:0 dropped:0 overruns:0 frame:0  
TX packets:239 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:91577 (89.4 KB) TX bytes:91577 (89.4 KB)

nsfadmin@metasploitable:~\$

Nello scan che ho eseguito, mi sono concentrato particolarmente sulla porta 2049, notando che era aperta. Questa porta è tipicamente utilizzata da NFS (Network File System) per permettere l'accesso ai file su reti distribuite. La mia attenzione su questa porta è stata motivata dalla necessità di verificare le potenziali vulnerabilità legate a NFS, dato che l'accesso non autorizzato attraverso questa porta può permettere a un attaccante di leggere o scrivere file sul server in modo indesiderato.



Ho utilizzato un tool con RPC (Remote Procedural Call) che mi ha restituito informazioni dettagliate, indicando che NFS è in ascolto sia sulle porte TCP che UDP.



KaliLinux in rete [In esecuzione] - Oracle VM VirtualBox

```
File Macchina Visualizza Inserimento Dispositivi Auto
File Actions Edit View Help
ls
bin cpio etc initrd lib media nohup.out proc sbin sys usr vmlinuz
boot dev home initrd.img lost+found mnt opt root srv tmp var
[root@kali]~[~/mnt/etc]
```

File System

```
File Macchina Visualizza Inserimento Dispositivi Auto
File Actions Edit View Help
ls
X11 fdmount.conf lsb-base rc.local
adduser.conf firefox-3.0 lsb-base-logging.sh rc0.d
adjtime lsb-release rc1.d
atd lsplash rc2.d
aliases.db lptrace.conf rc3.d
alternatives fpcchroot live rc4.d
apache2 fpuusers magic rc5.d
apm gal.conf mailcap rc6.d
apparmor gconf mailcap.order rc7.d
apparmor.d gpm mailname resolv.conf
apt gruff manpage.config resolvconf
at_deny group menu resolv.conf
bash bashrc group menu-methods
bash_completion bash_completion.d grub.d menu mime.types
bash_completion.d shadow mke2fs.conf
blocos gshadow modprobe.d
bin gshadow-noshell modules
bind gshadow-noshell.conf motd.tail
blkid.tab hdparm.conf mtab
blkid.tab.old host.conf hostname mysql
calendar hosts nanorc
chatscripts hosts network
console-setup host.allow networks
console-tools host.allow networks
cron cron.d nscswitch.conf
cron.daily idmapd.conf opt
cron.hourly inetd.conf pam.conf
cron.monthly init.d pam.d
cron.weekly initramfs-tools pam
cubrid jwm postfix
cups passwd pam
debcnf.conf issue perl
debian_version issue.net php5
default java popularity-contest.conf
defoma jwm postfix
deluser.conf jwm.d update-manager
demodm.d kernel-img.conf postgresql
devscripts.conf ld.so.cache postgresql-common
dhcpc ld.so.conf printcap
distcc ld.so.conf.profile wgetc
dpkg locale.alias profile.d
e2fsck.conf wpa_supplicant
```

File Macchina Visualizza Inserimento Dispositivi Auto

```
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2810
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 9c04d195fc6ee8a9d8e1

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN1 (lan)     -> em1      -> v4: 192.168.1.1/24
LAN2 (opt1)    -> em2      -> v4: 192.168.50.1/24

B) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set Interface(s) IP Address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: s
```

Metasploitable in rete [In esecuzione] - Oracle VM VirtualBox

```
File Macchina Visualizza Inserimento Dispositivi Auto
File Actions Edit View Help
ping 192.168.1.100
--- 192.168.1.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.000/0.000/0.000/0.007 ms
nsadmin@metasploitable:~$ ifconfig
eth0  Link encap:Ethernet HWaddr 08:00:27:4d:23:8a
      inet addr:192.168.50.100  Bcast:192.168.50.255  Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fedd:238a/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:3120 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1311 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:244621 (238.8 KB)  TX bytes:180020 (175.8 KB)
      Base address:0xd020 Memory:f0200000-f0220900

lo  Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:239 errors:0 dropped:0 overruns:0 frame:0
      TX packets:239 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:91577 (89.4 KB)  TX bytes:91577 (89.4 KB)

nsadmin@metasploitable:~$ _
```

File Macchina Visualizza Inserimento Dispositivi Auto

```
235545
09/05/2024
```

KaliLinux in rete [In esecuzione] - Oracle VM VirtualBox

```
File Macchina Visualizza Inserimento Dispositivi Auto
File Actions Edit View Help
root@kali:~/mnt/etc
GNU nano 7.2
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/names hostname(ro,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)
```

File System

Home

File Macchina Visualizza Inserimento Dispositivi Auto

```
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2810
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 9c04d195fc6ee8a9d8e1

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN1 (lan)     -> em1      -> v4: 192.168.1.1/24
LAN2 (opt1)    -> em2      -> v4: 192.168.50.1/24

B) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set Interface(s) IP Address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: s
```

File Macchina Visualizza Inserimento Dispositivi Auto

```
GNU nano 2.0.7  File: /etc/exports  Modified
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/names hostname(ro,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)
```

File Macchina Visualizza Inserimento Dispositivi Auto

```
192.168.50.100(r)_
```

File Macchina Visualizza Inserimento Dispositivi Auto

```
001349
10/05/2024
```

Ho utilizzato il comando showmount per verificare le informazioni NFS su un server, notando che il filesystem radice "/" era accessibile a tutti, un notevole rischio di sicurezza. Questo comando, situato in /usr/sbin, mostra dettagli mantenuti dal server mountd. Per risolvere, ho modificato la directory /mnt e aggiornato il file /etc(exports su Metasploitable per restringere l'accesso, poi ho controllato le modifiche da Kali Linux per confermare che solo utenti autorizzati potessero accedere al filesystem.

## VULNERABILITÀ N°4: Apache Tomcat AJP Connector Request Injection (Ghostcat)

### 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

#### Synopsis

There is a vulnerable AJP connector listening on the remote host.

#### Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

#### See Also

<http://www.nessus.org/u?8ebe6246>

<http://www.nessus.org/u?4e287adb>

<http://www.nessus.org/u?cbc3d54e>

<https://access.redhat.com/security/cve/CVE-2020-1745>

<https://access.redhat.com/solutions/4851251>

<http://www.nessus.org/u?dd218234>

<http://www.nessus.org/u?dd772531>

<http://www.nessus.org/u?2a01d6bf>

<http://www.nessus.org/u?3b5af27e>

<http://www.nessus.org/u?9dab109f>

<http://www.nessus.org/u?5eacf70>

#### Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

#### Risk Factor

High

#### CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

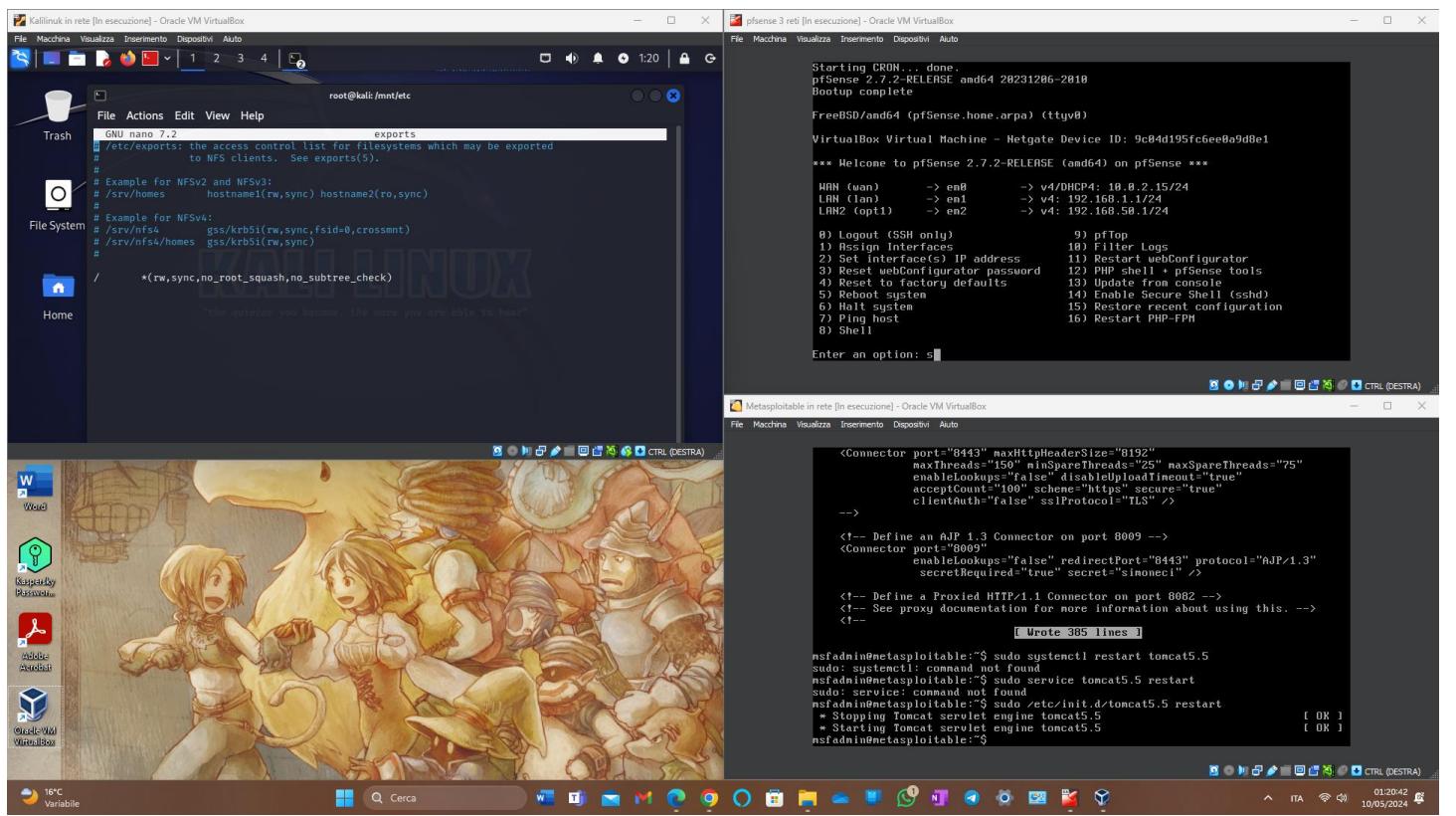
#### Plugin Output

tcp/8009/ajp13

Nella quarta vulnerabilità che ho selezionato, ho deciso di concentrarmi su un'importante questione di sicurezza relativa al connettore Apache AJP in Tomcat. Dopo le opportune ricerche, ho scoperto che il file da modificare è **server.xml**, situato in **/etc/tomcat5.5**. Questa vulnerabilità riguarda la potenziale esposizione a rischi di sicurezza se il connettore AJP non è adeguatamente protetto, permettendo così accessi non autorizzati ai dati sensibili del server.

Per risolvere questo problema, ho aperto il file con l'editor nano e vicino alla porta 8009 ho aggiunto le seguenti stringhe per rafforzare la sicurezza:

- **secretRequired="true"**: impostando questo attributo su true, garantisco che il connettore AJP sarà avviato solo se l'attributo **secret** è incluso e definito con un valore appropriato. Questa misura è fortemente consigliata per assicurare che solo gli utenti autorizzati che forniscono il valore segreto possano accedere al connettore.
- **secret="simonec1"**: ho scelto "simonec1" come valore segreto, un valore di stringa specifico e valido. Gli utenti devono utilizzare esattamente "simonec1" per autenticare le loro richieste. Se non corrisponde, l'accesso verrà negato.



## VULNERABILITÀ N°5: UnrealIRCd Backdoor Detection

### 46882 - UnrealIRCd Backdoor Detection

#### Synopsis

The remote IRC server contains a backdoor.

#### Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

#### See Also

<https://seclists.org/fulldisclosure/2010/Jun/277>

<https://seclists.org/fulldisclosure/2010/Jun/284>

<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

#### Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

#### Risk Factor

Critical

#### VPR Score

7.4

#### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

#### CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

#### Plugin Output

tcp/6667/irc

Nella quinta vulnerabilità che ho selezionato, mi sono imbattuto in un problema serio riguardante il server IRC. IRC, che sta per Internet Relay Chat, è un protocollo di comunicazione in tempo reale utilizzato principalmente per la chat di gruppo in canali, ma anche per la comunicazione uno-a-uno.

Il server in questione è una versione di UnrealIRCd che contiene una backdoor. Questo tipo di vulnerabilità è estremamente critico perché permette agli attaccanti di eseguire codice arbitrario sul host colpito, dando loro la possibilità di prendere il controllo completo del sistema. Questo potrebbe consentire loro di manipolare o distruggere dati, installare malware, avviare attacchi verso altri sistemi nella rete e sottrarre informazioni riservate.

The screenshot displays three windows from a Windows host:

- Kalinuk in rete [In esecuzione] - Oracle VM VirtualBox:** A browser window showing the pfSense firewall rules page at [https://192.168.1.1/firewall\\_rules.php?if=opt1](https://192.168.1.1/firewall_rules.php?if=opt1). It shows a table of rules, with one rule for port 6667 marked as deleted (red X). A message at the top says: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager."
- Inse 3 reti [In esecuzione] - Oracle VM VirtualBox:** A terminal window on a Kali Linux VM titled "FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)". It shows a welcome message for pfSense 2.7.2-RELEASE (amd64) on pfSense. The user has logged in via SSH. The terminal lists various configuration options (1-16) and ends with a prompt: "Enter an option: s". Below the prompt, it shows a successful login message: "php-fpm[397]: /Index.php: Successful login for user 'admin' from: 192.168.1.100 (Local Database)".
- asplitable in rete [In esecuzione] - Oracle VM VirtualBox:** A terminal window on a Metasploitable VM titled "msfadmin@metasploitable:~\$". It shows a series of commands run in the Metasploit framework, including "ifconfig" and "netstat -an". The output includes network interface details like "inet addr:192.168.50.100 Bcast:192.168.50.255 Mask:255.255.255.0" and "RX bytes:234597 (229.0 KB) TX bytes:234597 (229.0 KB)".

Utilizzando pfSense come firewall, ho creato e applicato una nuova regola specifica per bloccare tutto il traffico in ingresso e uscita sulla porta 6667. Questo passo è cruciale per prevenire accessi non autorizzati o attacchi tramite questa porta comunemente usata dai server IRC, proteggendo così ulteriormente il sistema Metasploitable da potenziali minacce.

## Nuova scansione nessus:

Matesploitable2Scansione / 192.168.50.100

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to Hosts](#)

**Vulnerabilities 59**

Filter ▾ Search Vulnerabilities 59 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	⋮
Critical	10.0		Unix Operating System Unsupported Version Detection	General	1	
Critical	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	
High	7.5 *	5.9	rlogin Service Detection	Service detection	1	
High	7.5 *	5.9	rsh Service Detection	Service detection	1	
High	7.5	5.9	Samba Badlock Vulnerability	General	1	
Medium	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	
Medium	6.5		Unencrypted Telnet Server	Misc.	1	
Medium	5.9	4.4	SSL Anonymous Cipher Suites Supported	Service detection	1	
Medium	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	
Low	3.7	3.9	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1	
Low	2.6 *		X Server Detection	Service detection	1	
Info	2.1 *	4.2	ICMP Timestamp Request Remote Date Disclosure	General	1	

**Host Details**

IP: 192.168.50.100  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)  
Start: Today at 10:29 AM  
End: Today at 10:39 AM  
Elapsed: 10 minutes  
KB: [Download](#)

**Vulnerabilities**

● Critical  
● High  
● Medium  
● Low  
● Info

### RISCHI E PROBLEMI CHIAVE

NOME DEL RISCHIO	STATO	SISTEMA	DESCRIZIONE
Bind Shell Backdoor Detection	Risolto	Metasploitable	Backdoor
VNC Server 'password' Password	Risolto	Metasploitable	Gain a shell remotely
NFS Exported Share Information Disclosure	Risolto	Metasploitable	RPC
Apache Tomcat AJP Connector Request Injection (Ghostcat)	Risolto	Metasploitable	Web Servers
UnrealIRCd Backdoor Detection	Risolto	Metasploitable	Backdoors

### Conclusioni

La nuova scansione eseguita con Nessus ha confermato la risoluzione delle 5 vulnerabilità sopra citate. In questa esercitazione ho compreso l'importanza di un VA (Vulnerability Assessment) che già da solo può, se fatto in maniera completa e approfondita contribuire a mettere in sicurezza i sistemi segnalando vulnerabilità che possono essere sfuggite in fase di programmazione oppure per scarsa manutenzione e avviare azioni correttive per poterle risolvere.

Grazie

Simone Cisbaglia