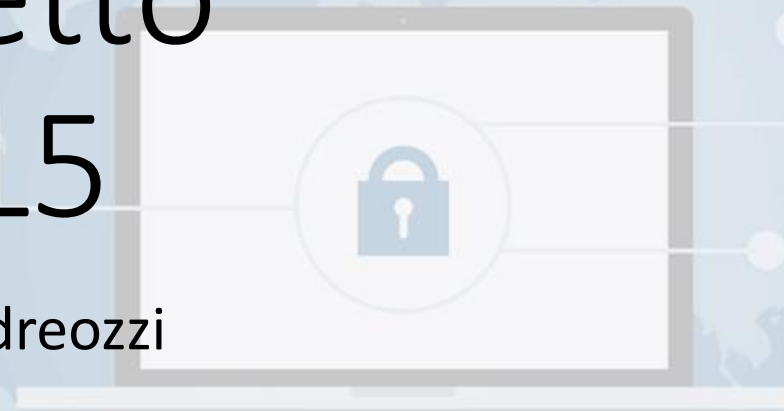


# Progetto S5 L5

Davide Andreozzi



# Scansione tramite Nessus e selezione delle vulnerabilità

Ho effettuato tramite Nessus un Vulnerability Scan completo sulla macchina target con ip 192.168.50.101 (Metasploitable 2).

Finita la scansione sono andato a fare un check delle vulnerabilità riscontrate e come da traccia del progetto ne ho scelte 3.

- (CRITICAL) VNC Server 'password' Password
- (CRITICAL) Bind Shell Backdoor Detection
- (HIGH) rlogin Service Detection

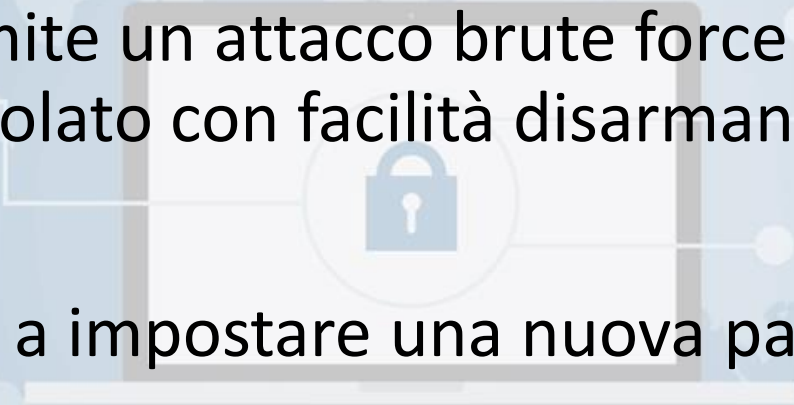
# Output prima scansione

<input type="checkbox"/> Sev ▼	CVSS	VPR	Name	Family	Count	⌚	⚙
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	⌚	✎
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	⌚	✎
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	⌚	✎
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	⌚	✎
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	⌚	✎
<input type="checkbox"/> MIXED	...	...	📅 4 Apache Tomcat (Multiple Issues)	Web Servers	4	⌚	✎
<input type="checkbox"/> CRITICAL	...	...	📅 2 SSL (Multiple Issues)	Gain a shell remotely	3	⌚	✎
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable	RPC	1	⌚	✎
<input type="checkbox"/> HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1	⌚	✎
<input type="checkbox"/> HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	⌚	✎
<input type="checkbox"/> MIXED	...	...	📅 15 SSL (Multiple Issues)	General	28	⌚	✎

# (CRITICAL) VNC Server 'password' Password

Il tipo di problematica è dovuta dal fatto che il Server VNC ha la password di default «password», tramite un attacco brute force – dizionario questo accesso verrebbe violato con facilità disarmante.

Per risolvere il problema sono andato a impostare una nuova password tramite il comando ***vncpasswd***



```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)?
msfadmin@metasploitable:~$
```

# (CRITICAL) Bind Shell Backdoor Detection

Questa criticità rappresenta una backdoor.

Precisamente una shell in ascolto sulla porta 1524.

Ho eseguito un nmap per verificare ulteriormente, successivamente per verificare la vulnerabilità ho avviato una connessione telnet su quella porta.

La slide successiva mostrerà l'output di nmap e l'accesso tramite telnet.

Per risolvere questa criticità sono andato a creare una regola tramite il firewall integrato in Linux – iptables per bloccare la porta 1524

Ho eseguito il seguente comando: `iptables -A INPUT -p tcp -dport 1524 -j DROP`

Questo comando rifiuterà ogni connessione (tcp) in ingresso sulla porta 1524

```
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-11 14:50 CET
Nmap scan report for 192.168.50.101
Host is up (0.00075s latency).
```

```
PORT      STATE SERVICE
1524/tcp  open  ingreslock
MAC Address: 08:00:27:23:71:C8 (Oracle VirtualBox virtual NIC)
```

```
Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds
```

```
(kali㉿kali)-[~]
```

```
$ telnet 192.168.50.101 1524
```

```
Trying 192.168.50.101...
```

```
Connected to 192.168.50.101.
```

```
Escape character is '^]'.  
root@metasploitable:/# ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:23:71:c8  
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0  
          inet6 addr: 2002:9547:339f:0:a00:27ff:fe23:71c8/64 Scope:Global  
          inet6 addr: fe80::a00:27ff:fe23:71c8/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:3806 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:75 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:251232 (245.3 KB)  TX bytes:11164 (10.9 KB)  
          Base address:0xd020 Memory:f0200000-f0220000
```

```
192.168.50.101: icmp_seq=1 ttl=64 time=1.57 ms
```

```
lo 50.101: Link encap:Local Loopback  0.0 ms
```

```
192.168.50.101: inet addr:127.0.0.1  Mask:255.0.0.0
```

```
192.168.50.101: inet6 addr: ::1/128 Scope:Host
```

```
192.168.50.101: UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

```
192.168.50.101: RX packets:298 errors:0 dropped:0 overruns:0 frame:0
```

```
192.168.50.101: TX packets:298 errors:0 dropped:0 overruns:0 carrier:0
```

```
192.168.50.101: collisions:0 txqueuelen:0  0.0 ms
```

```
192.168.50.101: RX bytes:120469 (117.6 KB)  TX bytes:120469 (117.6 KB)
```

```
root@metasploitable:/# root@metasploitable:/# reboot
```

```
ed, 9 received, 0% packet loss, time 8100ms
```

```
r = 0.379/0.717/1.572/0.379 ms
```

# Regola firewall iptables

```
Meta [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Perhaps iptables or your kernel needs to be upgraded.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@metasploitable:/home/msfadmin# sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      tcp  --  anywhere              anywhere            tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@metasploitable:/home/msfadmin#
```

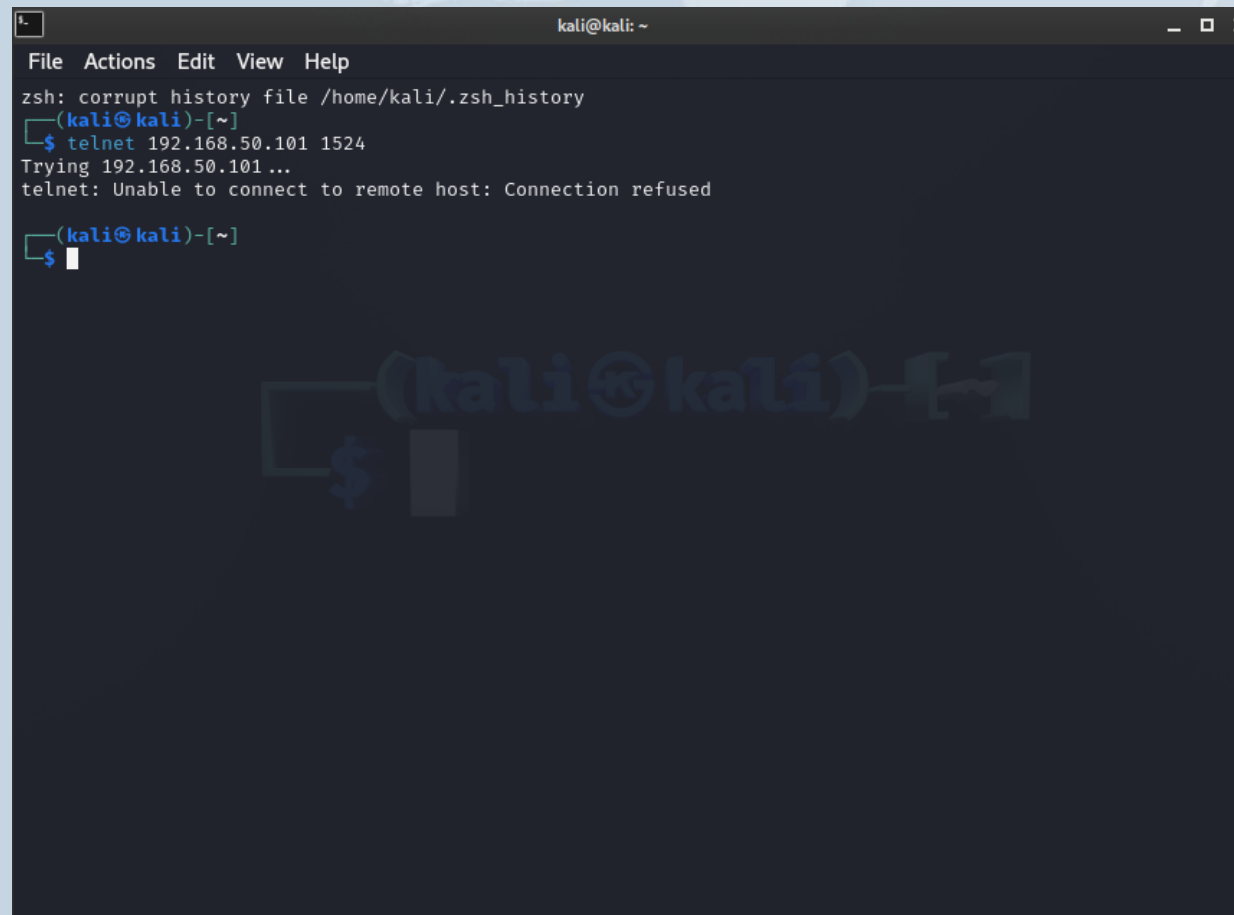
Nmap successivo = porta su «filtered» e non più «open»

```
(root@kali)-[/home/kali]
# nmap -Pn -T5 -sS -p 1524 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 11:37 CET
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).

PORT      STATE      SERVICE
1524/tcp  filtered  ingreslock
MAC Address: 08:00:27:23:71:C8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
```

# Successivamente riproviamo l'accesso con telnet. Fallito!

A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The terminal shows a message 'zsh: corrupt history file /home/kali/.zsh\_history', followed by the prompt '(kali@kali)-[~]'. The user enters '\$ telnet 192.168.50.101 1524'. The output shows 'Trying 192.168.50.101 ...' and 'telnet: Unable to connect to remote host: Connection refused'. The prompt returns to '(kali@kali)-[~]'.

```
kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ telnet 192.168.50.101 1524
Trying 192.168.50.101 ...
telnet: Unable to connect to remote host: Connection refused
(kali@kali)-[~]
$
```



# (HIGH) rlogin Service Detection

In questo servizio non abbiamo una cifratura dei dati di login, cioè sono in chiaro

In sintesi, il servizio rlogin è considerato obsoleto e insicuro in quanto trasmette dati in chiaro sulla rete e presenta varie vulnerabilità che possono essere sfruttate dagli attaccanti. Per migliorare la sicurezza ho deciso di modificare il file `inetd.conf` e commentare la riga `login`, disabilitandolo.

```
GNU nano 2.0.7      File: inetd.conf      Modified
#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet               stream  tcp    nowait  telnetd  /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp                 dgram  udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tf$
shell                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
#login               stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
exec                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i

^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
```

# Scansione Secondaria – Test della risoluzione delle soluzioni sulle vulnerabilities

Scansione secondaria / 192.168.50.101

[Back to Hosts](#)

ConfigureAudit TrailLaunchReportExport

Vulnerabilities67

FilterSearch Vulnerabilities67 Vulnerabilities

<input type="checkbox"/>	Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	🔄	✎
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	🔄	✎
<input type="checkbox"/>	MIXED	...	...	📁 Apache Tomcat (Multiple Issues)	Web Servers	4	🔄	✎
<input type="checkbox"/>	CRITICAL	...	...	📁 SSL (Multiple Issues)	Gain a shell remotely	3	🔄	✎
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1	🔄	✎
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	🔄	✎
<input type="checkbox"/>	MIXED	...	...	📁 SSL (Multiple Issues)	General	28	🔄	✎
<input type="checkbox"/>	MIXED	...	...	📁 ISC Bind (Multiple Issues)	DNS	5	🔄	✎
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	🔄	✎
<input type="checkbox"/>	MEDIUM	6.5		Unencrypted Telnet Server	Misc.	1	🔄	✎
<input type="checkbox"/>	MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1	🔄	✎
<input type="checkbox"/>	MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	🔄	✎

Host Details

IP: 192.168.50.101  
MAC: 08:00:27:23:71:C8  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)  
Start: Today at 12:44 PM  
End: Today at 1:11 PM  
Elapsed: 26 minutes  
KB: [Download](#)

Vulnerabilities

Critical

High

Medium

Low

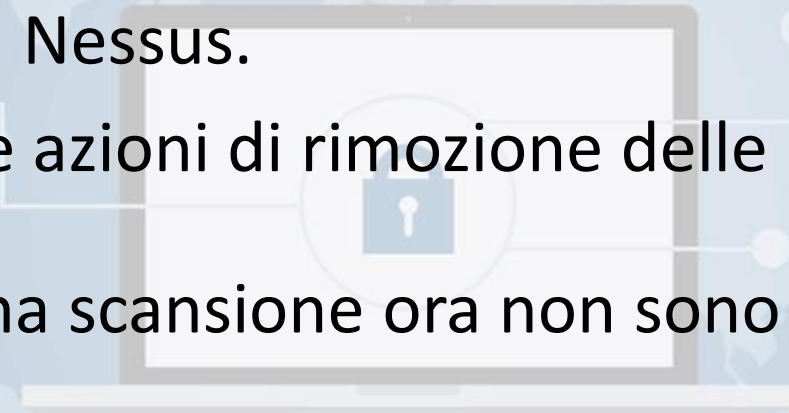
Info

# Scansione Secondaria – Test della risoluzione delle soluzioni sulle vulnerabilities

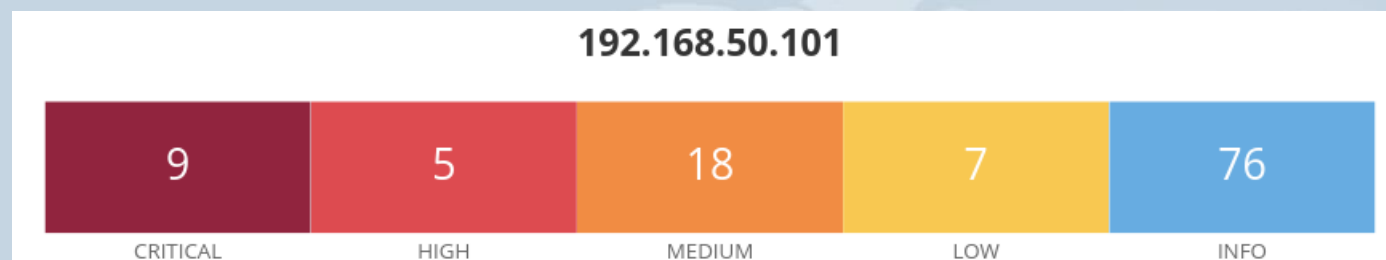
Per testare l'efficacia delle soluzioni trovate e implementate ho effettuato una seconda scansione con Nessus.

Dal risultato possiamo vedere come le azioni di rimozione delle vulnerabilità abbiano avuto successo.

Le tre vulnerabilità presenti nella prima scansione ora non sono presenti nella seconda.



1 Scansione



2 Scansione

