Metasploitable Vulnerabily Assesment

CPTP0524 – W12D4

- Vulnerabilità 1: CRITICA

46882 - UnrealIRCd Backdoor Detection

CRITICAL	10.0*	7.4	0.7565	46882	UnrealIRCd Backdoor Detection

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.

Plugin Output

Solution

tcp/6697/irc

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

La Versione Unreal3.2.8.1 Contiene una Backdoor, va rimosso il servizio, vanno rimossi i file correlati e va installata la versione pulita aggiornata.

1.1 Accesso ssh su Metasploitable:

```
ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+ssh-rsa
msfadmin@192.168.51.101
```

1.2 Controllo della versione di unrealircd:

```
sudo unrealircd -v
```

```
msfadmin@metasploitable:~$ sudo unrealircd -v
Unreal3.2.8.1 build 1.1.1.1.2.26 2009/04/13 11:03:55
msfadmin@metasploitable:~$
```

1.3 Ricerca processo attivo di unrealircd con ‘ps’ e controllato la porta in ascolto 6697 con ‘netstat’:

```
ps aux | grep unreal
netstat -tulpn | grep 6697
```

```
msfadmin@metasploitable:~$ ps aux | grep unreal
root      5098  0.0  0.0   8540  2476 ?        S    08:02   0:00 /usr/bin/unrealircd
msfadmin  5412  0.0  0.0   3008   780 pts/1    S+   10:04   0:00 grep unreal
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ netstat -tuln | grep 6697
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN
msfadmin@metasploitable:~$
```

1.4 Chiusura del Processo 5098 (unrealircd) e ricerca nuovamente il processo attivo unrealircd:

```
kill 5098
ps aux | grep unreal
```

```
msfadmin@metasploitable:~$ sudo kill 5098
msfadmin@metasploitable:~$ ps aux | grep unreal
msfadmin  5496  0.0  0.0   3004   772 pts/1    S+   10:30   0:00 grep unreal
msfadmin@metasploitable:~$
```

1.5 Ricerca file e Eliminazione:

find / -name "*unreal*" 2>/dev/null
sudo su
rm /usr/bin/unrealircd
rm -rf /etc/unreal
find / -name "*unreal*" 2>/dev/null

```
msfadmin@metasploitable:~$ find / -name "*unreal*" 2>/dev/null
/usr/bin/unrealircd
/etc/unreal
msfadmin@metasploitable:~$ sudo rm /usr/bin/unrealircd
msfadmin@metasploitable:~$ sudo rm /usr/bin/unrealircd
```

```
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# rm -rf /etc/unreal
root@metasploitable:/home/msfadmin#
```

```
root@metasploitable:/home/msfadmin# find / -name "*unreal*" 2>/dev/null
root@metasploitable:/home/msfadmin#
```

1.6 Riavvio del sistema e ricerca del servizio unrealircd:

```
sudo reboot
```

```
msfadmin@metasploitable:~$ sudo reboot
[sudo] password for msfadmin:

Broadcast message from msfadmin@metasploitable
        (/dev/pts/1) at 11:07 ...

The system is going down for reboot NOW!
msfadmin@metasploitable:~$ Connection to 192.168.51.101 closed by remote host.
Connection to 192.168.51.101 closed.
```

```
ps aux | grep unreal
sudo unrealircd -v
```

```
Last login: Sun Feb  9 09:36:35 2025 from 192.168.50.100
msfadmin@metasploitable:~$ ps aux | grep unreal
msfadmin  5199  0.0  0.0    308   108 pts/1    R+   11:09   0:00 grep unreal
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ sudo unrealircd -v
[sudo] password for msfadmin:
sudo: unrealircd: command not found
msfadmin@metasploitable:~$
```

IL SERVIZIO UNREALIRCD E' STATO RIMOSSO, DOPO IL RIAVVIO, AVENDO ELIMINATO IL BINARIO E FILE CORRELATI, POSSIAMO NOTARE CHE ANCHE IL PROCESSO NON ESISTE PIU'.

- Vulnerabilità 2: CRITICA

51988 - Bind Shell Backdoor Detection

CRITICAL	9.8	-	-	51988	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.

Plugin Output

tcp/1524/wild_shell

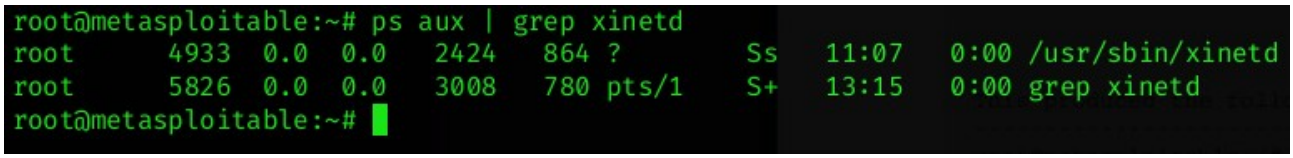
```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.51.101 1524
root@metasploitable:/# pwd
/
root@metasploitable:/# whoami
root
root@metasploitable:/#
```

2.1 Enumerazione:

`netstat -tulnp | grep 1524` (trova il binario in ascolto sulla porta 1524)

Trovato il binario xinetd in ascolto sulla porta 1524

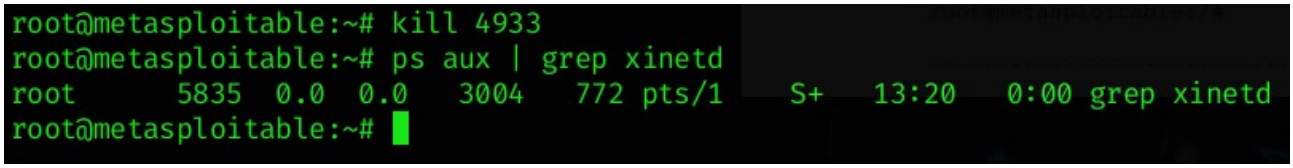
`ps aux | grep xinetd` (trova il processo attivo di xinetd)



Il binario si trova in /usr/sbin

2.2 Chiusura del processo e Eliminazione del servizio

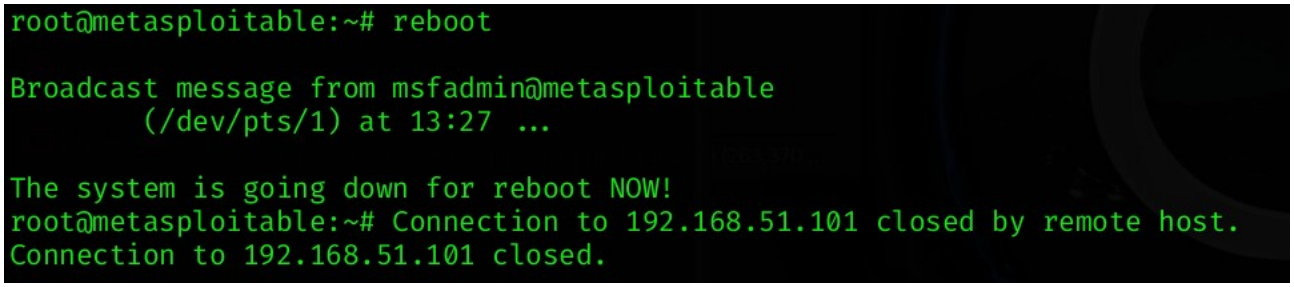
```
kill 4933
ps aux | grep xinetd
```



Il processo xinetd (4933) non è più in esecuzione

```
find / -name xinetd
rm -rf /usr/sbin/xinetd /usr/share/doc/xinetd /etc/init.d/xinetd
/etc/default/xinetd
```

`reboot`



2.3 Ricerca del processo per assicurarmi di aver risolto il problema

```
ps aux | grep xinetd
netstat -tulnp | grep 1524
```

```
msfadmin@metasploitable:~$ ps aux | grep xinetd
msfadmin  5266  0.0  0.0   3004   764 pts/1    S+   14:22   0:00 grep xinetd
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep 1524
msfadmin@metasploitable:~$
```

Con ‘ps’ non troviamo più processi, e con ‘netstat’ non troviamo più servizi con bind sulla porta1524

2.4 Test di accesso

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.51.101 1524
(UNKNOWN) [192.168.51.101] 1524 (ingreslock) : Connection refused

┌──(kali㉿kali)-[~]
└─$
```

- Vulnerabilità 3: CRITICA

62203 - Default Password (user) for 'user' Account

CRITICAL	9.8	7.4	0.013	62203	Default Password (user) for 'user' Account

Description

The account 'user' on the remote host has the password 'user'. An attacker may use it to gain further privileges on this system.

Solution

Change the password for this account or disable it.

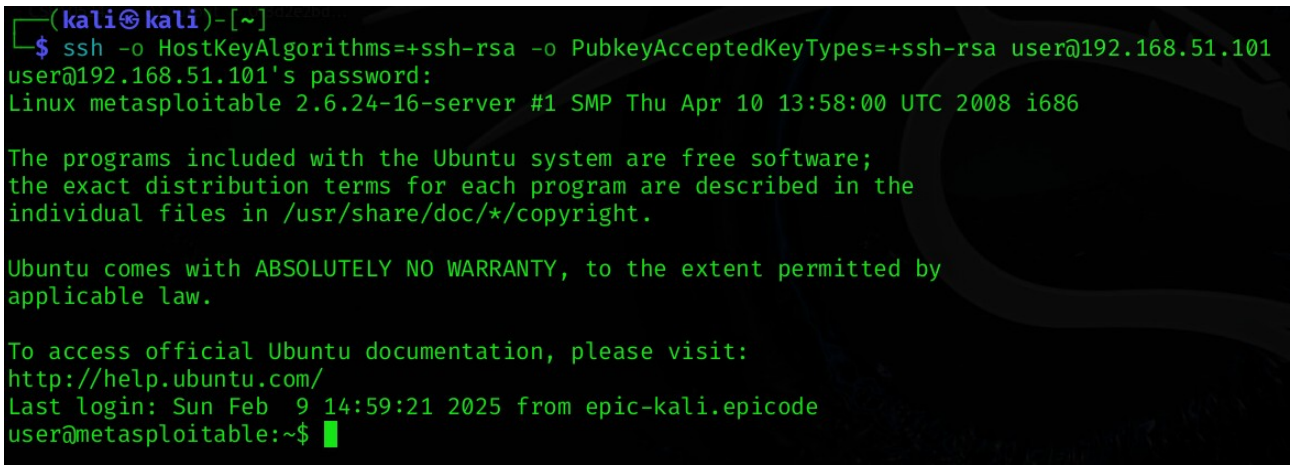
Plugin Output

tcp/22/ssh

```
┌──(kali㉿kali)-[~]
└─$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+
user@192.168.51.101's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sun Feb  9 14:50:07 2025 from epic-kali.epicode
user@metasploitable:~$ pwd
/home/user
user@metasploitable:~$ whoami
user
user@metasploitable:~$
```

3.1 Accesso SSH come utente user e cambio password:

```
ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+ssh-r
user@192.168.51.101
```

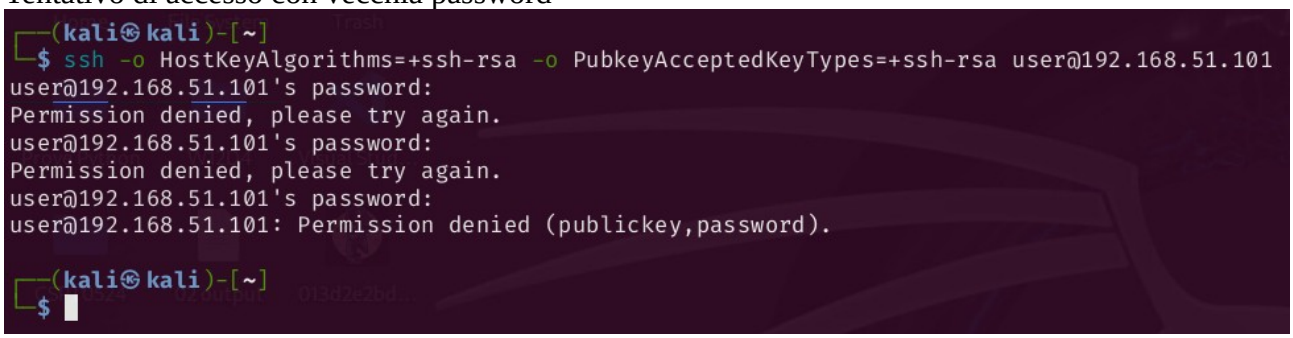


3.2 Cambio Password

```
passwd
```

3.3 Test di Accesso

Tentativo di accesso con vecchia password



Tentativo di accesso con nuova password

```
┌──(kali㉿kali)-[~]
└─$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+ssh-rsa user@192.168.51.101
user@192.168.51.101's password:
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/
Last login: Sun Feb  9 15:08:29 2025 from epic-kali.epicode
user@metasploitable:~$
```

- Vulnerabilità 4: CRITICA

61708 - VNC Server 'password' Password

CRITICAL	10.0*	-	-	61708	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	Plugin Output
Secure the VNC service with a strong password.	tcp/5900/vnc

4.1 Enumerazione su porta 5900

```
netstat -tulnp | grep 5900
ps aux | grep vnc
```

```
root@metasploitable:~# netstat -tulnp | grep 5900
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN      5069/Xtightvnc
root@metasploitable:~#
root@metasploitable:~# _
root@metasploitable:~#
root@metasploitable:~# ps aux | grep vnc
root      5069  0.0  0.3  14628 12676 ?        S    13:24   0:00 Xtightvnc :0 -desktop X -auth /
ty -geometry 1024×768 -depth 24 -rfbwait 120000 -rfbauth /root/.vnc/passwd -rfbport 5900 -fp /us
1/fonts/Type1/,/usr/X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X1
,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/sh
75dpi/,/usr/share/fonts/X11/100dpi/ -co /etc/X11/rgb
root      5076  0.0  0.0   2724  1192 ?        S    13:24   0:00 /bin/sh /root/.vnc/xstartup
root      5580  0.0  0.0   3008   780 pts/1    S+   15:31   0:00 grep vnc
root@metasploitable:~#
```

Abbiamo attenuto il servizio Xtightvnc/xstartup

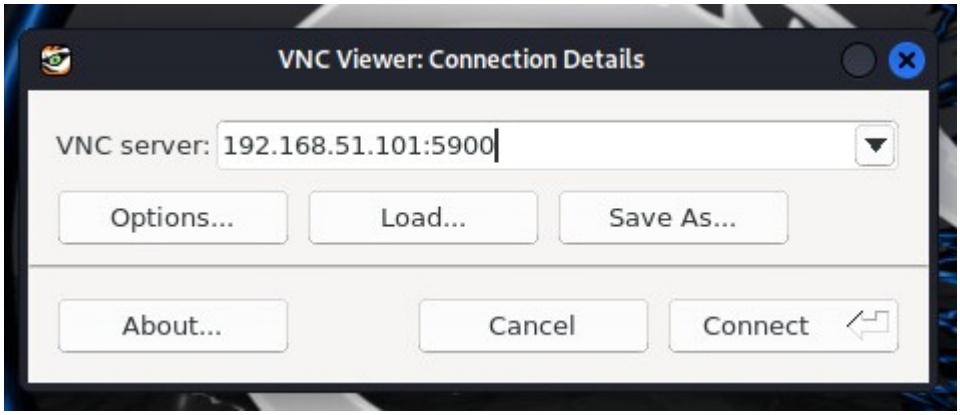
4.2 Cambio password VNC

vncpasswd

```
root@metasploitable:~# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~#
```

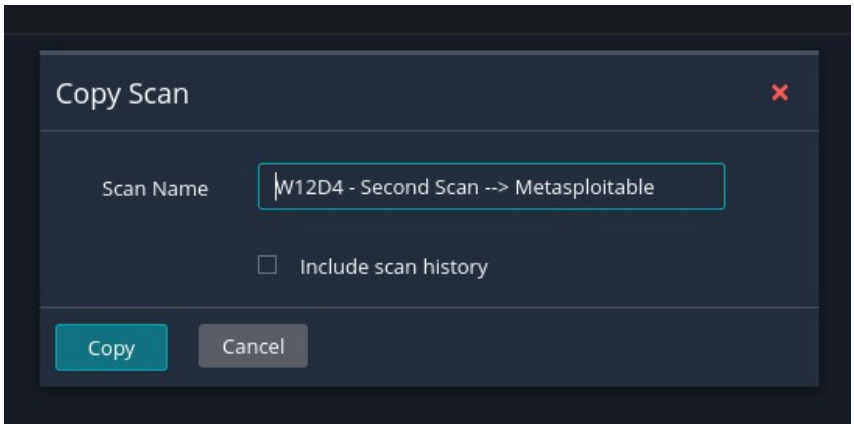
4.3 Test di Accesso VNC

Tentativo di accesso con vecchia password



Accesso con vecchia password Negato!

COPIA SCANSIONE PER EFFETTUARE UNA SCANSIONE IDENTICA



Scansione Iniziale

Epic-Metasploitable.epicode

35	77	115	17	172
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

DNS Name:	Epic-Metasploitable.epicode
Netbios Name:	METASPLOITABLE
IP:	192.168.51.101
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Scansione Finale

Epic-Metasploitable.epicode

30	73	113	16	149
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Sun Feb 9 23:41:15 2025
End time:	Mon Feb 10 04:26:33 2025

Host Information

DNS Name:	Epic-Metasploitable.epicode
Netbios Name:	METASPLOITABLE
IP:	192.168.51.101
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Francesco Rinaldi