

RIMEDI ALLE VULNERABILITA' CRITICHE DI METASPLOTABLE

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	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1	
HIGH	7.5		NFS Shares World Readable	RPC	1	

1) **Critical: VNC Server "password" password.**

CRITICAL VNC Server 'password' Password

Per rimediare a questa vulnerabilità, data per l'inefficacia della password, ho impostato una password alternando numeri e caratteri con il comando:

`vncpasswd`

la password richiede massimo

8 caratteri: `M3t4spl-`

```

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Fri Jun 28 03:53:48 EDT 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:~$ 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)? n
msfadmin@metasploitable:~$

```

`vncserver -kill :1`

2) **Critical: Blind Shell Backdoor Detection.**

CRITICAL Bind Shell Backdoor Detection

Per rimuovere la backdoor, toccherà capire quale porta è in ascolto alla 1524 tcp/vnc,

Per fare ciò eseguiamo il comando:

```
sudo netstat -tulnp | grep 1524
```

troverà la porta in ascolto 4495 che andremo a chiudere con il comando:

```
sudo kill -9 4495
```

```
metasploitable login: msfadmin
Password:
Login incorrect
metasploitable login: msfadmin
Password:
Last login: Fri Jun 28 04:21:27 EDT 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:~$ sudo netstat -tulnp | grep 1524
(sudo) password for msfadmin:
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
4495/xinetd
msfadmin@metasploitable:~$ sudo kill -9 4495
msfadmin@metasploitable:~$
```

```
sudo nano /etc/inetd.conf
```

```
#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/tcpd
telnet                stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/tcpd
#<off># ftp             stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/tcpd
#ftp                 dgram  udp      wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tftpd
shell                stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
login                stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
exec                 stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
ingreslock stream tcp nowait root /bin/bash bash -i
```

Ed eliminare la riga: **Shell stream** e salvare.

3) **Critical: NFS exported s.i disclosure**

Severity	Score	CVSS Vector	Exploitability	Impact	Service	Protocol
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Infor...	RPC		

Entrare sulla cartella **/etc** e modificare il file

```
/  *(rw, sync, no_root_squash,no_subtree_check)
```

aggiungendo un commento #

```

GNU nano 2.0.7          File: 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/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)

```

```
#/ *(rw, sync, no_root_squash, no_subtree_check) e salvare.
```

