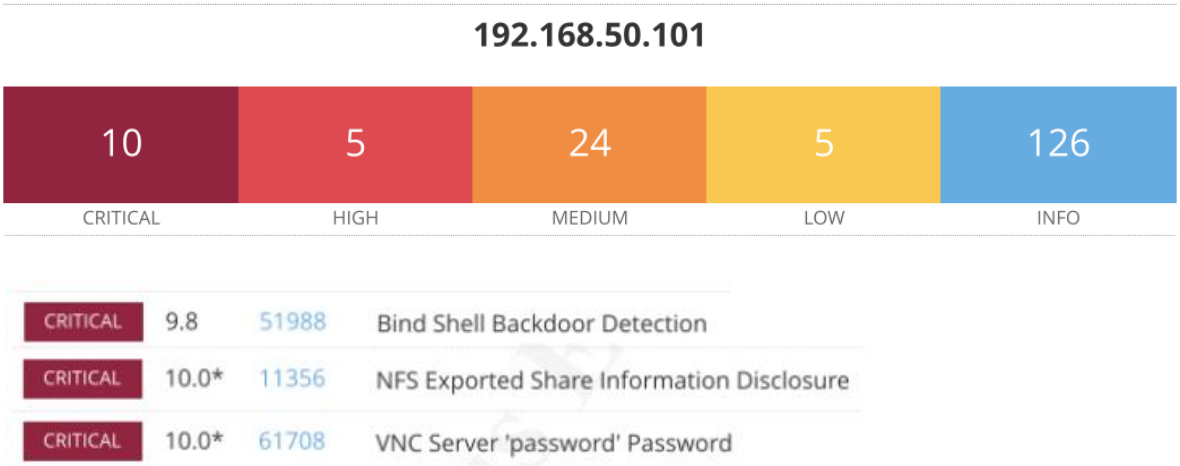
Esercizio 24-02

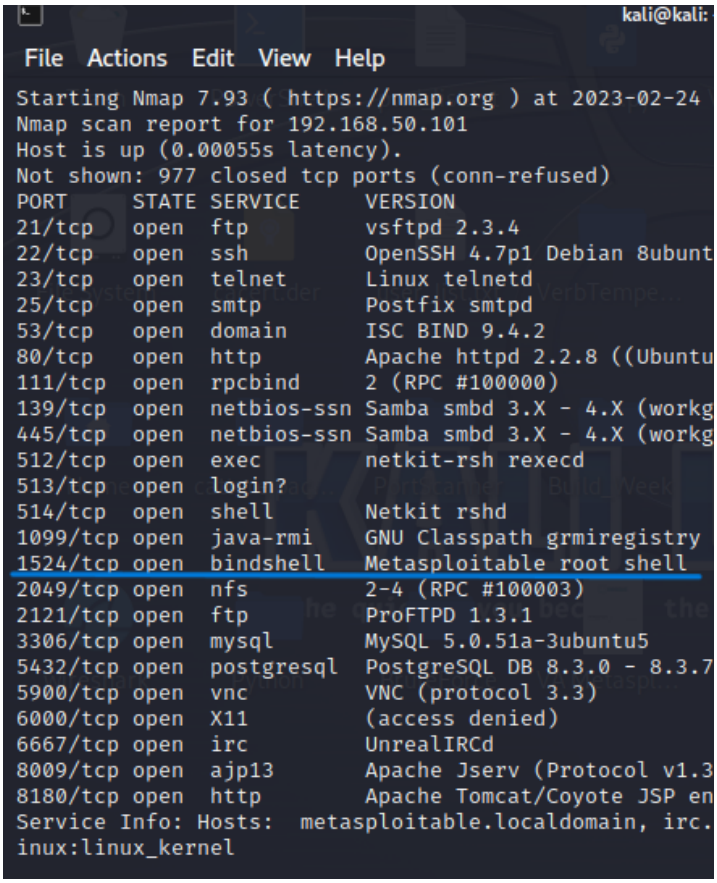
Traccia: effettuare una scansione delle vulnerabilità sulla macchina Metasploitable e risolvere da un minimo di 2 a un massimo di 4/5 vulnerabilità di livello critico tra quelle trovate.

Indicazioni: le soluzioni non possono essere raggiunte aggiornando sistemi/applicazioni a versioni più recenti, devono essere operazioni manuali da dentro la macchina. l'utilizzo di regole Firewall vale per un massimo di 1 soluzione.



Correzione errore 51988

Effettuando una scansione nmap da Kali verso l'indirizzo di Metasploitable troviamo una porta con servizio attivo "bindshell", porta 1524.



Tento di connettermi al servizio con il comando netcat IP di Metasploitable e 1524 (porta)

```
┌──(kali㉿kali)-[~]
└─$ netcat 192.168.50.101 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# hostname
metasploitable
root@metasploitable:/# pwd
/
root@metasploitable:/# echo $$
5108
root@metasploitable:/# isof -p
bash: isof: command not found
root@metasploitable:/# lsfo -p $
bash: lsfo: command not found
root@metasploitable:/# sudo lsof -p $
lsof: illegal process ID: $
lsof 4.78
 latest revision: ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/
 latest FAQ: ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/FAQ
 latest man page: ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/lsof_man
 usage: [-?abhlnNoOPRstUvVX] [+|-c c] [+|-d s] [+D D] [+|-f]
 [-F [f]] [-g [s]] [-i [i]] [+|-L [l]] [+m [m]] [+|-M] [-o [o]]
 [-p s] [+|-r [t]] [-S [t]] [-T [t]] [-u s] [+|-w] [-x [fl]] [--] [names]
Use the ``-h'' option to get more help information.
root@metasploitable:/# readlink/proc/$/exe
bash: readlink/proc/$/exe: No such file or directory
root@metasploitable:/# readlink /proc/$/exe
root@metasploitable:/# readlink /proc/$/exe
root@metasploitable:/# md5sum readlink /proc/$/exe
md5sum: readlink: No such file or directory
md5sum: /proc/$/exe: No such file or directory
root@metasploitable:/#
```

Dopo essere riuscito a connettermi eseguo qualche comando per testare le funzionalità che mi concede la backdoor.

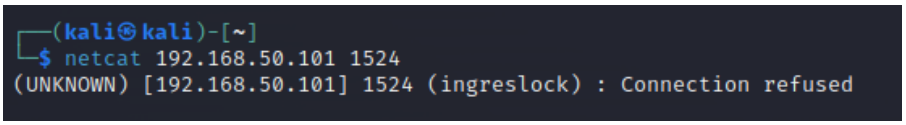
Da terminale di Metasploitable mi muovo nella cartella /etc e cerco la backdoor.

```
  GNU nano 2.0.7                File: inetd.conf

##<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
```

Utilizzo del comando sudo nano inetd.conf, la backdoor, e commentando le righe di codice la rendiamo “vuota”.

Ritento l’accesso alla backdoor da kali


┌──(kali㉿kali)-[~]
└─$ netcat 192.168.50.101 1524
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection refused

Connessione rifiutata, per sicurezza lancio di nuovo una scansione nmap.

La porta 1524 non è più tra le porte aperte.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-24 08:36 EST
Nmap scan report for 192.168.50.101
Host is up (0.00067s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1099/tcp open  java-rmi    GNU Classpath grmiregistry
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN;
inux:linux_kernel
```

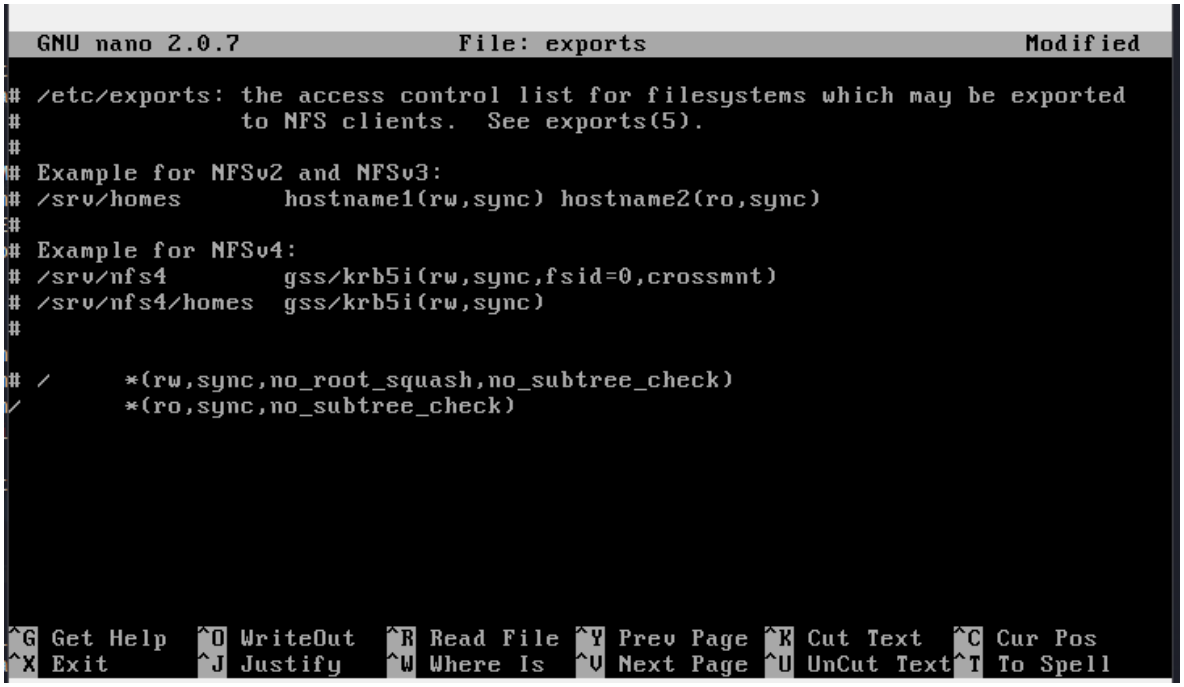
Correzione errore 11356

Mi sposto nella cartella /etc alla ricerca del file exports.

Utilizzo del comando ls -l | less per movimento verticale nella lista.

```
-rw-r--r--  1 root     root      724 2008-04-08 14:02 crontab
drwxr-xr-x  2 root     root     4096 2010-03-16 19:11 cron.weekly
drwxr-xr-x  2 root     root     4096 2010-03-04 05:01 cups
-rw-r--r--  1 root     root     2969 2008-03-11 11:51 debconf.conf
-rw-r--r--  1 root     root       10 2007-10-20 07:51 debian_version
drwxr-xr-x  2 root     root     4096 2012-05-13 23:35 default
drwxr-xr-x  4 root     root     4096 2010-03-23 17:54 defoma
-rw-r--r--  1 root     root      600 2007-10-23 11:01 deluser.conf
drwxr-xr-x  2 root     root     4096 2010-03-16 19:00 depmod.d
-rw-r--r--  1 root     root    15280 2010-04-28 00:06 devscripts.conf
drwxr-xr-x  4 root     root     4096 2010-03-16 19:01 dhcp3
drwxr-xr-x  2 root     root     4096 2010-04-17 13:31 distcc
drwxr-xr-x  3 root     root     4096 2010-03-23 17:55 dpkg
-rw-r--r--  1 root     root       34 2008-02-18 23:33 e2fsck.conf
drwxr-xr-x  3 root     root     4096 2010-04-28 00:07 emacs
-rw-r--r--  1 root     root       79 2010-03-16 18:59 environment
drwxr-xr-x  2 root     root     4096 2012-05-20 15:07 esound
drwxr-xr-x  2 root     root     4096 2010-03-16 18:59 event.d
-rw-r--r--  1 root     root      399 2023-02-24 06:04 exports
-rw-r--r--  1 root     root      354 2007-03-05 01:54 fdmount.conf
drwxr-xr-x  4 root     root     4096 2012-05-20 15:07 firefox-3.0
drwxr-xr-x  4 root     root     4096 2010-03-23 17:54 fonts
-rw-r--r--  1 root     root      534 2012-05-20 14:59 fstab
-rw-r--r--  1 root     root       76 2007-10-27 23:37 ftpchroot
```

Apertura del file con editor di testo con comando sudo nano exports.

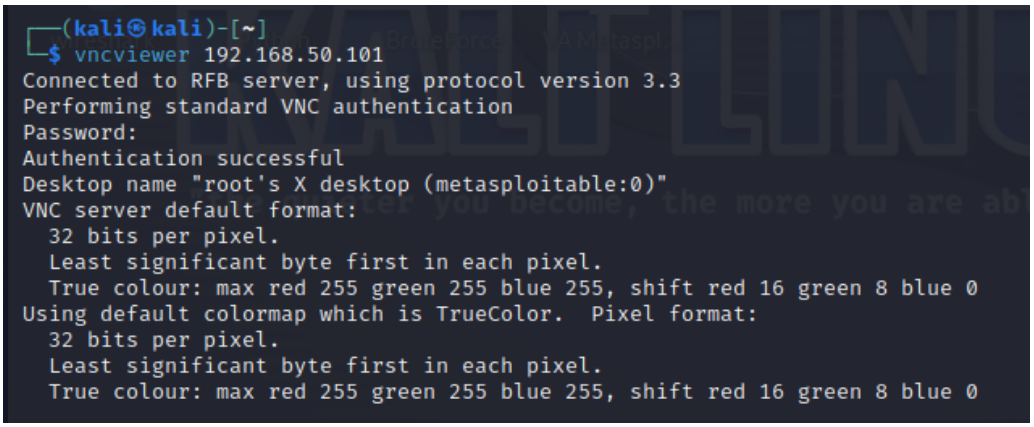


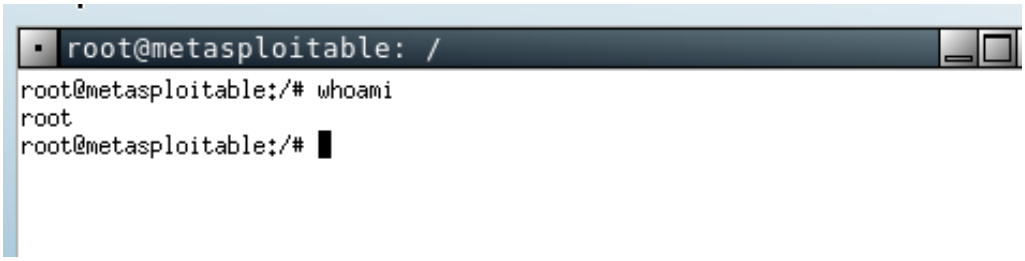
La penultima riga conferiva l'accesso da qualunque directory, lettura e scrittura file, privilegi amministratore. Commentata così da rendere nulla e aggiunta una nuova riga che conferisce sola lettura a chi accede.

Correzione errore 61708

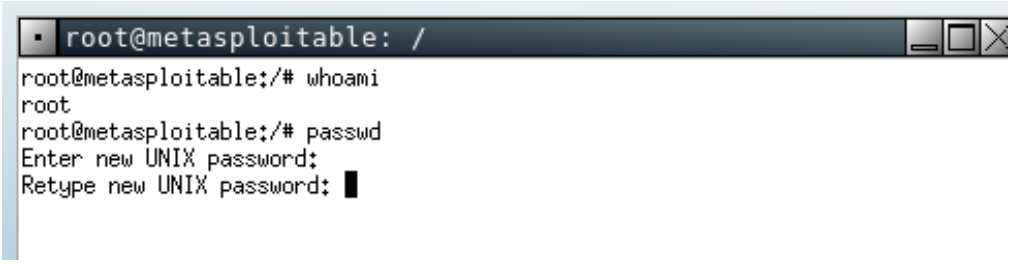
Nessus indica questa vulnerabilità critica perchè con l'utilizzo della password "password" ha effettuato il login.

Provo a effettuare la login con password "password", login riuscita.





Procedo con la sostituzione per una password più sicura.



Ritento l'accesso con password "password", login fallito.

La nuova password è "25PASSword"

Risultati dello scan Nessus post remediation actions.