

VULNERABILITY REMEDATION ACTION

#KALI LINUX

#METASPLOITABLE

EFFETTUARE UNA SCANSIONE COMPLETA SUL TARGET:
#METASPLOITABLE.

SCEGLIETE DA UN **MINIMO DI 2 FINO AD UN MASSIMO DI 4 VULNERABILITÀ CRITICHE** E PROVATE AD IMPLEMENTARE DELLE AZIONI DI RIMEDIO.

N.B. LE AZIONI DI RIMEDIO, IN QUESTA FASE, POTREBBERO ANCHE ESSERE DELLE REGOLE **FIREWALL** BEN CONFIGURATE IN MODO DA LIMITARE EVENTUALMENTE LE ESPOSIZIONI DEI SERVIZI VULNERABILI.

VI CONSIGLIAMO TUTTAVIA DI UTILIZZARE MAGARI QUESTO APPROCCIO **PER NON PIÙ DI UNA VULNERABILITÀ.**

PER DIMOSTRARE L'EFFICACIA DELLE AZIONI DI RIMEDIO, ESEGUITE NUOVAMENTE LA SCANSIONE SUL TARGET E CONFRONTATE I RISULTATI CON QUELLI PRECEDENTEMENTE OTTENUTI.

CONSEGNA:

1. SCANSIONE INIZIALE DOVE SI VEDE IL GRAFICO CON TUTTE LE VULNERABILITÀ E LE VULNERABILITÀ DA RISOLVERE (TECNICO, GIÀ RIASSUNTO) - SCANSIONEINIZIO.PDF
 2. SCREENSHOT E SPIEGAZIONE DEI PASSAGGI DELLA REMEDIATION - REMEDIATIONMETA.PDF
 3. SCANSIONE DOPO LE MODIFICHE CHE EVIDENZIA LA RISOLUZIONE DEI PROBLEMI/VULNERABILITÀ (IL GRAFICO CHE MOSTRA TUTTE LE VULNERABILITÀ) - SCANSIONEFINE.PDF OPPURE UN REPORT UNICO, A VOSTRA SCELTA.
- PENSO SIA PIÙ COMODO FARNE TRE COMUNQUE.

NOTA: I REPORT POSSONO ESSERE LASCIATI IN INGLESE, SENZA PROBLEMI. **SE RISOLVETE LE 4 VULNERABILITÀ, POTETE RISOLVERNE UNA QUINTA (A SCELTA),** AD ESEMPIO CON UNA REGOLA DI FIREWALL.

COME ACCENNATO IN PRECEDENZA, PER QUESTO TEST LE MIE MACCHINE SARANNO SULLA STESSA RETE A CAUSA DI CONTINUI ED IMPREVISTI CRASH IN SEGUITO ALL'AVVIO DI 3 VM (KALI, METASPLOITABLE, E PFSENSE) E APERTURA DI NESSUS DAL BROWSER DI KALI.

!LA PRIMA REMEDIATION ACTION INERENTE LA BIND SHELL EFFETTUATA CON NETCAT È STATA EFFETTUATA CON LE DUE MACCHINE ANCORA IMPOSTATE SU RETI DIVERSE (IP METASPLOITABLE **192.168.60.101**, A DIMOSTRAZIONE DEL FATTO CHE PFSENSE FUNZIONASSE), MA POI HO DOVUTO CAMBIARE IN VISTA DELLO SCAN FINALE

UTILIZZIAMO COME TARGET **METASPLOITABLE** CON L'IP **192.168.50.101.**

LA MACCHINA ATTACCANTE SARÀ **KALI LINUX** CON L'IP **192.168.50.100.**

CI SI AVVALE DELLO SCAN EFFETTUATO IN PRECEDENZA CON IL TOOL NESSUS, CHE HA RISCONTRATO LA PRESENZA DI **10 VULNERABILITÀ CRITICHE** DA RISOLVERE.

192.168.50.101



NE SCEGLIAMO ALCUNE DA FIXARE PONENDOCI LE REMEDIATION ACTION NECESSARIE E VERIFICANDO DI CONSEGUENZA L'EFFICACIA ANDANDO AD EFFETTUARE UNO NUOVO SCAN.

#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

Nessus was able to execute the command "id" using the following request :

This produced the following truncated output (limited to 10 lines) :
----- snip -----
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
----- snip -----

192.168.50.101

7

ABBIAMO QUI RISCONTRATO UNA VULNERABILITÀ DI LIVELLO CRITICO CHE CONSISTE NELLA PRESENZA DI UNA PORTA IN ASCOLTO (SI SA CHE È LA N°1524 GRAZIE A NESSUS SCAN) SUL TARGET SENZA ALCUNA NECESSITÀ DI AUTENTICAZIONE. QUESTA PORTA CI DA L'ACCESSO DIRETTAMENTE ALLA SHELL DI COMANDI COI PRIVILEGI DI ROOT SULLA MACCHINA ESPOSTA. VEDIAMO IN SEGUITO COME IDENTIFICARLA UTILIZZANDO NETCAT, SFRUTTARLA E BLOCCARLA CON IPTABLES DA KALI.

```
(django@kali)-[~]
$ nc -nvz 192.168.60.101 1-2000
(UNKNOWN) [192.168.60.101] 1524 (ingreslock) open
(UNKNOWN) [192.168.60.101] 1099 (rmiregistry) open
(UNKNOWN) [192.168.60.101] 514 (shell) open
(UNKNOWN) [192.168.60.101] 513 (login) open
(UNKNOWN) [192.168.60.101] 512 (exec) open
(UNKNOWN) [192.168.60.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.60.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.60.101] 111 (sunrpc) open
(UNKNOWN) [192.168.60.101] 80 (http) open
(UNKNOWN) [192.168.60.101] 53 (domain) open
(UNKNOWN) [192.168.60.101] 25 (smtp) open
(UNKNOWN) [192.168.60.101] 23 (telnet) open
(UNKNOWN) [192.168.60.101] 22 (ssh) open
(UNKNOWN) [192.168.60.101] 21 (ftp) open
```

```
(django@kali)-[~]
$ netcat 192.168.60.101 1524
root@metasploitable:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:dc:03:d4
          inet addr:192.168.60.101  Bcast:192.168.60.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fedc:3d4/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2072 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2161 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:161120 (157.3 KB)  TX bytes:124772 (121.8 KB)
          Base address:0xd020  Memory:f0200000-f0220000

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:244 errors:0 dropped:0 overruns:0 frame:0
          TX packets:244 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:90425 (88.3 KB)  TX bytes:90425 (88.3 KB)

(django@kali)-[~]
$ netcat 192.168.60.101 1524
root@metasploitable:/# sudo iptables -I INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/# ^C
```

```
(django@kali)-[~]
$ ping 192.168.60.101
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data.
64 bytes from 192.168.60.101: icmp_seq=1 ttl=63 time=1.81 ms
64 bytes from 192.168.60.101: icmp_seq=2 ttl=63 time=3.17 ms

— 192.168.60.101 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.806/2.485/3.165/0.679 ms

(django@kali)-[~]
$ nc -nvz 192.168.60.101 1-2000
(UNKNOWN) [192.168.60.101] 1524 (ingreslock) : Connection timed out
(UNKNOWN) [192.168.60.101] 1099 (rmiregistry) open
(UNKNOWN) [192.168.60.101] 514 (shell) open
(UNKNOWN) [192.168.60.101] 513 (login) open
(UNKNOWN) [192.168.60.101] 512 (exec) open
(UNKNOWN) [192.168.60.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.60.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.60.101] 111 (sunrpc) open
(UNKNOWN) [192.168.60.101] 80 (http) open
(UNKNOWN) [192.168.60.101] 53 (domain) open
(UNKNOWN) [192.168.60.101] 25 (smtp) open
(UNKNOWN) [192.168.60.101] 23 (telnet) open
(UNKNOWN) [192.168.60.101] 22 (ssh) open
(UNKNOWN) [192.168.60.101] 21 (ftp) open
```

#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: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".

192.168.50.101

21

VNC (VIRTUAL NETWORK COMPUTING) SI BASA SUL PROTOCOLLO RFB CHE PERMETTE DI CONTROLLARE IL COMPUTER DA UNA "REMOTE LOCATION", GESTISCE LA CONNESSIONE SERVER TO CLIENT E PERMETTE DI INVIARE IMMAGINI SUL DESKTOP. UNO DEI SOFTWARE PIÙ RINOMATI CHE UTILIZZANO VNC È TEAM-VIEWER. ABBIAMO QUI RISCONTRATO UNA VULNERABILITÀ DI LIVELLO CRITICO CHE CONSISTE NELLA PRESENZA DI UNA PASSWORD DI ACCESSO TROPPO FACILE DA IDENTIFICARE, PER FIXARE QUESTA VULNERABILITÀ QUINDI SAREBBE OPPORTUNO CAMBIARE PASSWORD IN UNA PIÙ COMPLESSA.

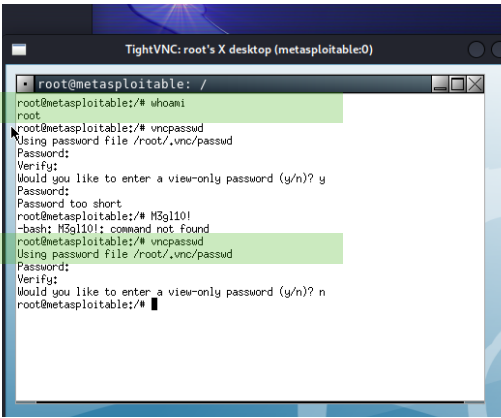
```
(django@kali)-[~]
$ nc -nvz 192.168.60.101 4000-6000
(UNKNOWN) [192.168.60.101] 6000 (x11) open
(UNKNOWN) [192.168.60.101] 5900 (?) open
(UNKNOWN) [192.168.60.101] 5432 (postgresql) open

^C
(django@kali)-[~]
$ nmap -A 192.168.60.101 -p 5900
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-27 15:38 EST
Nmap scan report for 192.168.60.101
Host is up (0.00085s latency).

PORT      STATE SERVICE VERSION
5900/tcp  open  vnc      VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_   VNC Authentication (2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds

(django@kali)-[~]
$ vncviewer 192.168.60.101
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```



MI CONNETTO ALL'EDITOR GRAFICO DI VNC SU METASPLOITABLE COI PRIVILEGI DI ROOT TRAMITE LA PASSWORD "PASSWORD" RIVELATA DA NESSUS, E LA AGGIORNO IN M3g110! INFATTI SE PROVO A RICONNETTERMI CON LA PWD VECCHIA L'AUTENTICAZIONE FALLISCE

```
(django@kali)-[~]
$ vncviewer 192.168.60.101
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure

(django@kali)-[~]
$ vncviewer 192.168.60.101
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0

(django@kali)-[~]
$
```

#VULNERABILITÀ N°3: NFS EXPORTED SHARE INFO 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

The following NFS shares could be mounted :

- + /
- + Contents of / :
- .
- ..
- bin
- boot
- cdrom
- dev
- etc
- home
- initrd
- initrd.img
- lib
- lost+found
- media
- mnt
- nohup.out
- opt
- proc
- root
- sbin
- srv
- sys
- tmp
- usr
- var
- vmlinuz

NFS (NETWORK FILE SYSTEM) È UN PROTOCOLLO DI RETE, UN FILE SYSTEM CHE CONSENTE A COMPUTER CLIENT DI UTILIZZARE LA RETE PER ACCEDERE A DIRECTORY CONDIVISE TRAMITE UN PUNTO DI MONTAGGIO DA SERVER REMOTI COME FOSSE-RO DISPONIBILI IN LOCALE. È SPESSO ASSOCIATO A SISTEMI UNIX. ABBIAMO QUI UN PROBLEMA CHE RIGUARDA LA POSSIBILITÀ DI ACCESSO LIBERO DA PARTE DEI MALINTENZIONATI AD ALMENO UN PUNTO DI MONTAGGIO, COSA CHE PERMETTE DI LEGGERE/SCRIVERE FILE SULLA NOSTRA MACCHINA. LA SOLUZIONE STA NEL RIUSCIRE A CONFIGURARE NFS IN MODO TALE CHE SOLO UTENTI AUTORIZZATI POSSANO ACCEDERVI.

RILANCIO UNO SCAN AGGRESSIVO E VERBOSO SULLE PORTE:

```
File Actions Edit View Help
(django@kali)-[~]
$ nmap -p 1-65535 -T4 -A -v 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-28 07:43 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:43
Completed NSE at 07:43, 0.00s elapsed
Initiating NSE at 07:43
Completed NSE at 07:43, 0.00s elapsed
Initiating NSE at 07:43
Completed NSE at 07:43, 0.00s elapsed
Initiating Ping Scan at 07:43
Scanning 192.168.50.101 [2 ports]
Completed Ping Scan at 07:43, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:43
Completed Parallel DNS resolution of 1 host. at 07:43, 0.05s elapsed
Initiating Connect Scan at 07:43
Scanning 192.168.50.101 [65535 ports]
Discovered open port 139/tcp on 192.168.50.101
Discovered open port 23/tcp on 192.168.50.101
Discovered open port 80/tcp on 192.168.50.101
Discovered open port 21/tcp on 192.168.50.101
Discovered open port 25/tcp on 192.168.50.101
Discovered open port 5900/tcp on 192.168.50.101
Discovered open port 3306/tcp on 192.168.50.101
Discovered open port 111/tcp on 192.168.50.101
Discovered open port 22/tcp on 192.168.50.101
Discovered open port 445/tcp on 192.168.50.101
Discovered open port 53/tcp on 192.168.50.101
Discovered open port 44698/tcp on 192.168.50.101
Discovered open port 6697/tcp on 192.168.50.101
Discovered open port 6667/tcp on 192.168.50.101
Discovered open port 1524/tcp on 192.168.50.101
Discovered open port 2049/tcp on 192.168.50.101
Discovered open port 36725/tcp on 192.168.50.101
Discovered open port 3632/tcp on 192.168.50.101
Discovered open port 6000/tcp on 192.168.50.101
Discovered open port 8009/tcp on 192.168.50.101
Discovered open port 8787/tcp on 192.168.50.101
Discovered open port 514/tcp on 192.168.50.101
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_ 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATU
SCODES, 8BITIME, DSN
53/tcp open domain ISC BIND 9.4.2
|_dns-nsid:
|_ bind.version: 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/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 6e 65 a\5*t Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
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
|_mysql-info:
|_ Protocol: 10
|_ Version: 5.0.51a-3ubuntu5
|_ Thread ID: 71
|_ Capabilities flags: 43564
|_ Some Capabilities: Support41Auth, SupportsTransactions, ConnectWithDatabase, LongColumnFlag, Speaks41Pr
otocolNew, SwitchToSSLAfterHandshake, SupportsCompression
|_ Status: Autocommit
|_ Salt: <v\[)Zi!dWg"o+"s?}x
3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-01-28T12:46:33+00:00; -2s from scanner time.
```

#VULNERABILITÀ N°3: NFS EXPORTED SHARE INFO DISCLOSURE

CHIAMO IL PROGRAMMA CON **RPC** (REMOTE PROCEDURAL CALL) CHE MI RESTITUISCE LE SEGUENTI INFORMAZIONI: NFS È IN ASCOLTO SIA SULLE PORTE TCP CHE UDP.

```
(django@kali)-[~]
$ rpcinfo -p 192.168.50.101 | grep nfs
100003      2      udp      2049     nfs
100003      3      udp      2049     nfs
100003      4      udp      2049     nfs
100003      2      tcp      2049     nfs
100003      3      tcp      2049     nfs
100003      4      tcp      2049     nfs
```

IL COMANDO **SHOWMOUNT** MOSTRA INFORMAZIONI SU UN SERVER NFS. QUESTE INFORMAZIONI SONO MANTENUTE DAL SERVER MOUNTD SULL'HOST. SI TROVA DI SOLITO IN /usr/sbin, CHE NON È NEL PERCORSO DI RICERCA PREDEFINITO.

-e / -exports: STAMPA L'ELENCO DEI FILESYSTEM ESPORTATI. VEDIAMO "/" CHE STA AD INDICARE IL FILESYSTEM DI PROPRIETÀ DI ROOT PER LA MAGGIOR PARTE DELLE VERSIONI DI UNIX E LINUX. PERMETTERE A CHIUNQUE DI MONTARE SUL FILE SYSTEM "/" APRE LE PORTE A UNA QUANTITÀ ILLIMITATA DI EXPLOIT. MONTIAMO LA DIR **/mnt**

SAPPIAMO CHE IL FILE DI CONFIGURAZIONE DELLA CARTELLA CONDIVISA È **/etc/exports** QUINDI VADO A MODIFICARLO DA METASPLOITABLE E VERIFICO L'ACCESSO DA KALI

```
(django@kali)-[~]
$ showmount -e 192.168.50.101
Export list for 192.168.50.101:
/ *
```

```
(root@kali)-[~/ssh]
# cd /

(root@kali)-[/]
# mount -t nfs 192.168.50.101:/ /mnt -o nolock

(root@kali)-[/]
# df -k
Filesystem            1K-blocks      Used Available Use% Mounted on
udev                   3348472         0    3348472   0% /dev
tmpfs                   677768       1036     676732   1% /run
/dev/sda1              81000912  19086084    57754216  25% /
tmpfs                  3388820         0    3388820   0% /dev/shm
tmpfs                   5120          0       5120    0% /run/lock
tmpfs                  677764        112     677652   1% /run/user/1000
192.168.50.101:/      7282176  1484032    5431040  22% /mnt
```

```
root@kali: /mnt/etc
File Actions Edit View Help
# mount -t nfs 192.168.50.101:/ /mnt
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service → /lib/systemd/system/rpc-statd.service.

(root@kali)-[~]
# cd /mnt/

(root@kali)-[/mnt]
# ls
bin  cdrom  etc  initrd  lib  lost+found  media  nohup.out  proc  sbin  sys  usr  vmlinuz
boot dev  home  initrd.img  mnt  opt  root  srv  temp  var

(root@kali)-[/mnt]
# cd etc

(root@kali)-[/mnt/etc]
# ls
X11                  fdmount.conf      lsb-base           rc.local
adduser.conf         firefox-3.0        lsb-base-logging.sh rc0.d
adjtime              fonts             lsb-release        rc1.d
aliases              fstab             ltrace.conf        rc2.d
aliases.db           ftpchroot         lvm                rc3.d
alternatives         fuse.conf         magic              rc4.d
apache2              gai.conf          magic.mime         rc5.d
apm                  gdm               mailcap            rc6.d
apparmor             gdm               mailcap.order     rc5.d
apparmor.d           groff             manpath.config    resolv.conf
apt                  group             mediaprm           resolvconf
at.deny              group-            menu               rmt
bash.bashrc          grub.d            menu-methods      rpc
bash_completion     gshadow           mime.types         samba
bash_completion.d   gshadow-          mke2fs.conf       screenrc
belocs               gssapi_mech.conf modprobe.d         security
bind                 gtk-2.0           modules            services
bindresvport.blacklist hdparm.conf      motd               sgml
blkid.tab            hesiod.conf       motd.tail          shadow
blkid.tab.old        host.conf         mtab               shadow
calendar             hostname          mysql              shells
chatscripts          hosts            nanorc            skel
console-setup        hosts.allow       network            ssh
console-tools        hosts.deny        networks           ssl
cowpoke.conf         hosts.equiv       nsswitch.conf     su-to-rootrc
cron.d               idmapd.conf       opt               sudoers
cron.daily           inetd.conf        pam.conf           sysctl.conf
cron.hourly          init.d            pango             syslog.conf
cron.monthly         inittab           passwd            terminfo
cron.weekly          initramfs-tools  pango             timezone
crontab              inputrc          pcmcia            tomcat5.5
cups                 iproute2         perl              ucf.conf
debconf.conf         issue            perl5             udev
debian_version       java             popularity-contest.conf ufw
default              jvm              postfix           unreal
defoma               jvm.d            postgresql         update-manager
deluser.conf         kernel-img.conf  postgresql-common updatedb.conf
depmod.d             ld.so.cache      ppp               vim
devscripts          ld.so.conf       printcap          vsftpd.conf
dhcp3                ld.so.conf.d     profile.d         w3m
distcc               ldap             proftpd           wgetrc
dpkg                 locale.alias     protocols         wpa_supplicant
e2fsck.conf          localtime        python            xinetd.conf
emacs                logcheck         python2.5         xinetd.d
environment          login.defs       zsh_command_not_found
esound               logrotate.conf
event.d              logrotate.d
exports
```

```
(root@kali)-[/mnt/etc]
# cat exports
# /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)
#
/ 192.168.50.101(r)

(root@kali)-[/mnt/etc]
# nano exports
```

MODIFICO IL FILE DA METASPLOITABLE:

```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/exports

/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)

[ Read 12 lines ]
Get Help WriteOut Read File Prev Page Cut Text Cur Pos
Exit Justify Where Is Next Page UnCut Text To Spell
Ctrl destro

Metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/exports

/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)

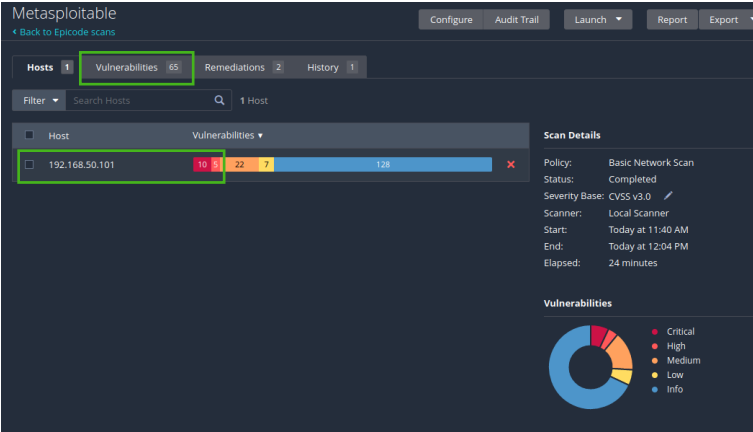
192.168.50.101(r)

[ Wrote 12 lines ]
Get Help WriteOut Read File Prev Page Cut Text Cur Pos
Exit Justify Where Is Next Page UnCut Text To Spell
Ctrl destro
```

#SCANSIONE DIMOSTRATIVA CON NESSUS

LO SCAN EFFETTUATO CON NESSUS DIMOSTRA L'EFFICACIA DELLE REMEDIATION ACTIONS INTRAPRESE

PRIMA: 65 VULNERABILITÀ / 10 CRITICHE



DOPO: 31 VULNERABILITÀ / 4 CRITICHE

