VULNERABILITY REMEDIATION 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.

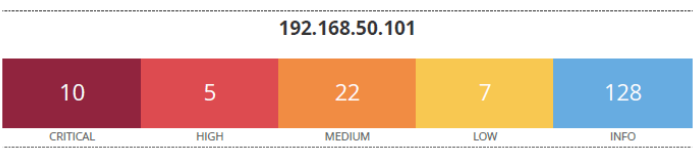
CONSEGNA:
1. SCANSIONE INIZIALE DOVE SI VEDE IL GRAFICO CON TUTTE LE VULNERABILITÀ E LE VULNERABILITÀ DA RISOLVERE (TECNICO, GIÀ RIASSUNTO) - SCANSIONEINIZIO.PDF
2. SCREENSHOT E SPIEGAZIONE DEI PASSAGGI DELLA REMEDIATION - REMEDIATIONMETA.PDF
3. SCANSIONE DOPO LE MODIFICHE CHE EVIDENZIA LA RISOLUZIONE 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 COTINUI ED IMPREVISTI CRASH IN SEGUITO ALL'AVVIO DI 3 VM (KALI, METASPLOITABLE, E PFSENSE) E APERTURA DI NESSUS DAL BROWSER DI KALI.
!.A 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 DIMOSTRAZIUOINE 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 EFFETUATO IN PRECEDENZA CON IL TOOL NESSUS, CHE HA RISCONTRATO LA PRESENZA DI 10 VULNERABILITÀ CRITICHE DA RISOLVERE.



NE SCEGLIAMO ALCUNE DA FIXARE PONENDOVI 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

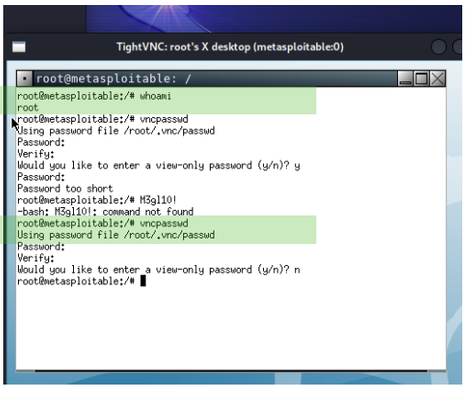
```
Nessus logged in using a password of "password".
```

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 TEAMVIEWER. ABBIAMO QUI RISCONTRATO UNA VULNERABILITÀ DI LIVELLO CRITICO CHE CONSISTE NELLA PRESENZA DI UNA PASSWORD DI ACCESSO TROPPO FACILE DA IDENTFICARE, 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 M3gl10! 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 FOSSERO 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:

```
django@kali: ~
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, ENHANCEDSTATUSCODES, 8BITMIME, 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 @\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, Speaks41ProtocolNew, 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
SAPPPIAMO 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         media  nohup.out  proc  sbin  sys  usr  vmlinuz
boot  dev    home  initrd.img  lost+found  mnt    opt        root  srv   tmp  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            ftpusers          magic                   rc4.d
apache2                 fuse.conf         magic.mime              rc5.d
apm                     gai.conf          mailcap                 rc6.d
apparmor                gconf             mailcap.order           rcS.d
apparmor.d              gdm               mailname                resolv.conf
apt                     groff             manpath.config          resolvconf
at.deny                 group             mediaprm                rmt
bash.bashrc             group-            menu                    rpc
bash_completion         grub.d            menu-methods            samba
bash_completion.d       gshadow           mime.types              screenrc
belocs                  gshadow-          mke2fs.conf             securetty
bind                    gssapi_mech.conf  modprobe.d              security
bindresvport.blacklist  gtk-2.0           modules                 services
blkid.tab               hdparm.conf       motd                    sgml
blkid.tab.old           hesiod.conf       motd.tail               shadow
calendar                host.conf         mtab                    shadow-
chatscripts             hostname          mysql                   shells
console-setup           hosts             nanorc                  skel
console-tools           hosts.allow       network                 ssh
cowpoke.conf            hosts.deny        networks                ssl
cron.d                  hosts.equiv       nsswitch.conf           su-to-rootrc
cron.daily              idmapd.conf       opt                     sudoers
cron.hourly             inetd.conf        pam.conf                sysctl.conf
cron.monthly            init.d            pam.d                   syslog.conf
cron.weekly             initramfs-tools   pango                   terminfo
crontab                 inputrc           passwd                  timezone
cups                    iproute2          passwd-                 tomcat5.5
debconf.conf            issue             pcmcia                  ucf.conf
debian_version          issue.net         perl                    udev
default                 java              php5                    ufw
defoma                  jvm               popularity-contest.conf unreal
deluser.conf            jvm.d             postfix                 update-manager
depmod.d                kernel-img.conf   postgresql              updatedb.conf
devscripts.conf         ld.so.cache       postgresql-common       vim
dhcp3                   ld.so.conf        ppp                     vsftpd.conf
distcc                  ld.so.conf.d      printcap                w3m
dpkg                    ldap              profile                 wgetrc
e2fsck.conf             locale.alias      profile.d               wpa_supplicant
emacs                   localtime         proftpd                 xinetd.conf
environment             logcheck          protocols               xinetd.d
esound                  login.defs        purple                  zsh_command_not_found
event.d                 logrotate.conf    python
exports                 logrotate.d       python2.5

┌──(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 ]
^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
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 ]
^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
Ctrl destro
```

#VULNERABILITÀ N°4:
UPDATE THE A JP CONFIGURATION TO REQUIRE AUTHORIZATION

IL SEGUENTE METODO ABILITA IL CONNETTORE APACHE AJP IN MODO CHE VENGA AVVIATO CON FATTORE DI SICUREZZA ABILITATA. SO CHE IL FILE DA CORREGGERE È SERVER.XML CHE SI TROVA IN /ETC/TOMCAT5.5
VADO AD APRIRLO CON L'EDITOR NANO ED AGGIUNGO LE SEGUENTI STRINGHE VICINO ALLA STRINGA 8009:

- secretRequired="true": se impostato su true, indica che il connettore AJP verrà avviato solo se l'attributo secret è incluso e definito con un valore appropriato (vedere di seguito). Il valore vero è fortemente consigliato per garantire che al connettore accedano solo i lavoratori nel cluster di bilanciamento del carico che forniscono il valore segreto.
- secret= "<string>": qualsiasi valore di stringa diverso da null e con lunghezza diversa da zero. I lavoratori nel cluster di bilanciamento del carico devono fornire questo stesso stringo quando effettuano richieste; in caso contrario, le loro richieste vengono respinte.

SALVO IL FILE E RIAVVIO IL SERVIZIO APACHE TOMCAT.

```
dpkg                    mailname                sudoers
e2fsck.conf             manpath.config          su-to-rootrc
emacs                   mediaprm                sysctl.conf
environment             menu                    syslog.conf
esound                  menu-methods            terminfo
event.d                 mime.types              timezone
exports                 mke2fs.conf             tomcat5.5
fdmount.conf            modprobe.d              ucf.conf
firefox-3.0             modules                 udev
fonts                   motd                    ufw
fstab                   motd.tail               unreal
ftpchroot               mtab                    updatedb.conf
ftpusers                mysql                   update-manager
fuse.conf               nanorc                  vim
gai.conf                network                 vsftpd.conf
gconf                   networks                w3m
gdm                     nsswitch.conf           wgetrc
groff                   opt                     wpa_supplicant
group                   pam.conf                X11
group-                  pam.d                   xinetd.conf
grub.d                  pango                   xinetd.d
gshadow                 passwd                  zsh_command_not_found
gshadow-                passwd-
gssapi_mech.conf        pcmcia
msfadmin@metasploitable:/etc/tomcat5.5$ ls
Catalina            context.xml          server-minimal.xml  tomcat-users.xml
catalina.policy     logging.properties   server.xml          web.xml
catalina.properties policy.d             tomcat5.5
```

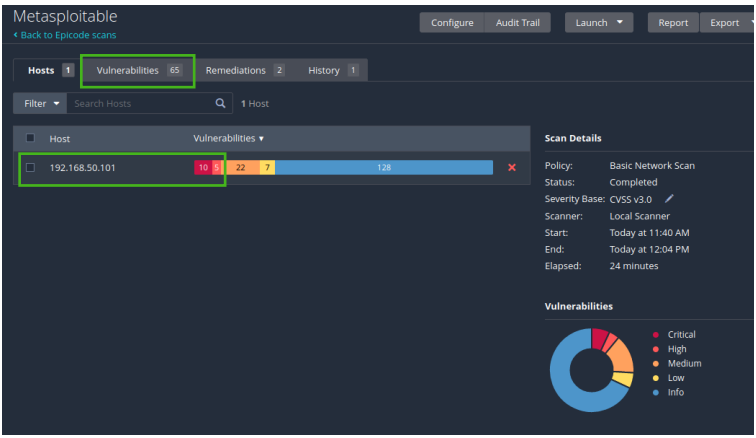
```
 GNU nano 2.0.7                File: server.xml                          Modified

                         noCompressionUserAgents="gozilla, traviata"
                         compressableMimeType="text/html,text/xml"
        -->

    <!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
    <!--
    <Connector port="8443" maxHttpHeaderSize="8192"
               maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
               enableLookups="false" disableUploadTimeout="true"
               acceptCount="100" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS" />
    -->

    <!-- Define an AJP 1.3 Connector on port 8009 -->
    <Connector port="8009"
$8443" protocol="AJP/1.3" secret="<string>" />

    <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
    <!-- See proxy documentation for more information about using this. -->
    <!--

^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
```

```
 GNU nano 2.0.7                File: server.xml

                         noCompressionUserAgents="gozilla, traviata"
                         compressableMimeType="text/html,text/xml"
        -->

    <!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
    <!--
    <Connector port="8443" maxHttpHeaderSize="8192"
               maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
               enableLookups="false" disableUploadTimeout="true"
               acceptCount="100" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS" />
    -->

    <!-- Define an AJP 1.3 Connector on port 8009 -->
    <Connector port="8009"
               enableLookups="false" secretRequired="true" redirectPort="8443" 

    <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
    <!-- See proxy documentation for more information about using this. -->
    <!--
                            [ Wrote 384 lines ]
^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 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