

Epicode M3 final project.

Vulnerability assessment su Metasploitable

Request.

- Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere.
- Screenshot e spiegazione dei passaggi della remediation
- Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità.
- Scegliere un minimo di 2 fino ad un massimo di 5 vulnerabilità critiche e provare ad implementare delle azioni di rimedio.

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

Riproduzione risultati dello scan di Nessus su Metasploitable



Procedure di remediation action di alcune vulnerabilità scelte.

Vulnerabilità critica riscontrata:

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 -----
```

Abbiamo riscontrato una vulnerabilità di livello critico all'interno dell'ambiente target. Tale vulnerabilità consiste nella presenza di una porta in ascolto, specificamente identificata come la porta numero 1524 grazie ad un'analisi con Nessus Scan, sul target senza alcuna necessità di autenticazione. Questa porta aperta ci fornisce un accesso diretto alla shell di comandi con privilegi di root sulla macchina esposta.

Identificazione e Sfruttamento della Vulnerabilità: Per identificare e sfruttare la vulnerabilità, possiamo utilizzare lo strumento Netcat per stabilire una connessione alla porta 1524 del target. Una volta stabilita la connessione, possiamo eseguire comandi sulla macchina bersaglio con i privilegi di root, compromettendo così la sicurezza del sistema.

Contromisure e Mitigazione: Per mitigare questa vulnerabilità critica, si consiglia di utilizzare le seguenti contromisure:

1. Bloccare la porta 1524 utilizzando iptables o un'altra soluzione di firewall per prevenire l'accesso non autorizzato alla shell di comandi.
2. Applicare restrizioni di accesso basate su IP o altre misure di sicurezza per limitare l'accesso alla porta solo a utenti autorizzati.
3. Effettuare una revisione completa della configurazione del sistema per identificare e correggere eventuali altre vulnerabilità simili.

```
$ 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
```

```

└─$ 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)

```

```

└─$ netcat 192.168.60.101 1524
root@metasploitable:/# sudo iptables -I INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/# ^C

```

```

└─$ 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

```

Test alla remediation:

```

└─$ 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 critica riscontrata:

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".

Analisi della Vulnerabilità di VNC (Virtual Network Computing):

Il protocollo VNC (Virtual Network Computing) si basa sul protocollo RFB (Remote Frame Buffer), consentendo il controllo remoto di un computer da una posizione esterna. Gestisce la connessione server-to-client e permette il trasferimento di immagini del desktop. Uno dei software più noti che utilizza VNC è TeamViewer.

Descrizione della Vulnerabilità:

Durante la valutazione della sicurezza, è stata identificata una vulnerabilità di livello critico relativa alla sicurezza delle password di accesso al servizio VNC. È stato riscontrato da Nessus che la password di accesso è troppo semplice e facilmente identificabile, esponendo il sistema a rischi di accesso non autorizzato e compromissione dei dati sensibili.

Raccomandazioni per la Mitigazione:

Per mitigare questa vulnerabilità critica, si consiglia di adottare le seguenti misure:

1. Aggiornamento delle Politiche di Sicurezza delle Password: Si consiglia di modificare la password di accesso a una più complessa e robusta, che includa una combinazione di caratteri alfanumerici, simboli e lunghezza significativa.
2. Implementazione di Politiche di Rotazione delle Password: È consigliabile stabilire procedure regolari per la rotazione delle password, al fine di mantenere un livello elevato di sicurezza nel tempo.
3. Monitoraggio Continuo della Sicurezza: È importante monitorare costantemente l'accesso al servizio VNC e adottare misure preventive per identificare e mitigare eventuali tentativi di accesso non autorizzato.

```
└─$ 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
```

```
└─$ 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).

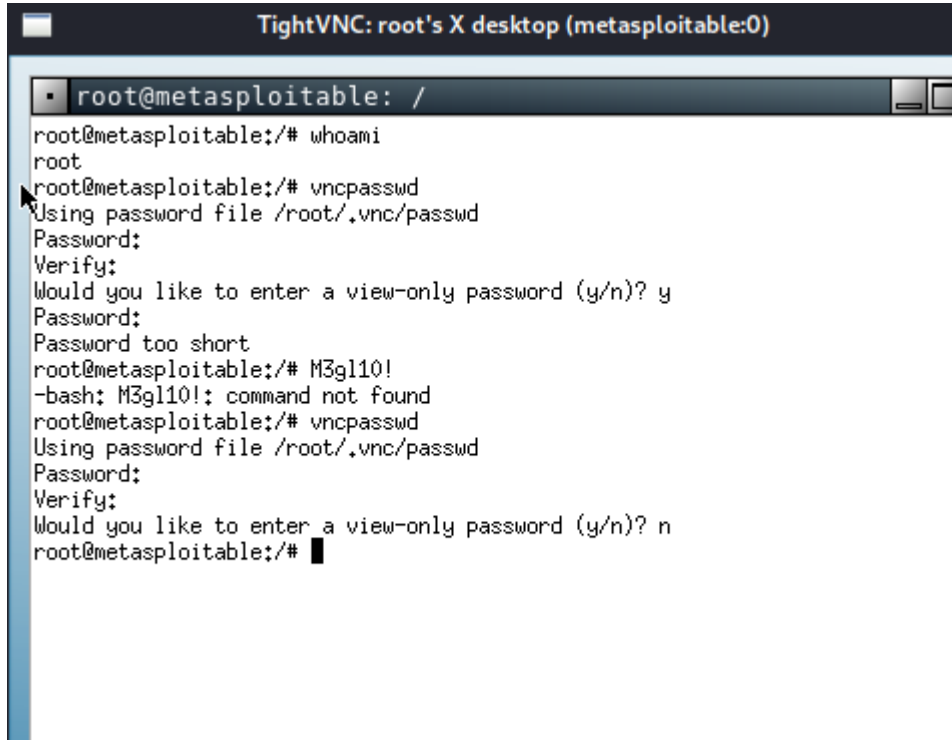
PORT      STATE SERVICE VERSION
5900/tcp  open  vnc      VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)

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
```

```
└─$ 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
```

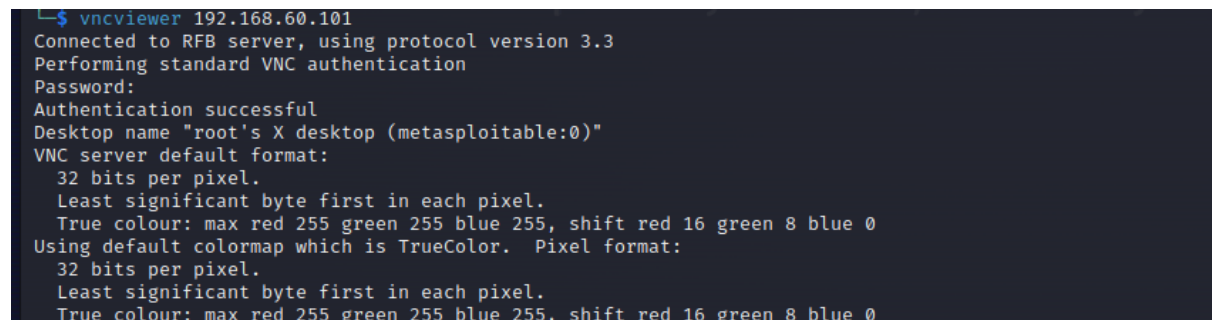
Implementazione correzione:

La corretta gestione delle password di accesso è fondamentale per garantire la sicurezza del servizio VNC e prevenire potenziali violazioni della sicurezza. È consigliabile implementare immediatamente le raccomandazioni fornite al fine di proteggere l'integrità e la riservatezza dei dati aziendali.



```
TightVNC: root's X desktop (metasploitable:0)
root@metasploitable: /
root@metasploitable:/# whoami
root
root@metasploitable:/# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Password too short
root@metasploitable:/# M3gl10!
-bash: M3gl10!: command not found
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:/#
```

Autenticazione con password non va a buon fine.



```
$ 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
```

Vulnerabilità critica riscontrata:

NSF 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 nys shares could be mounted :


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


Analisi del Problema di Sicurezza in NFS (Network File System).

Il Network File System (NFS) è un protocollo di rete e un file system che facilita l'accesso remoto a directory condivise da parte dei client tramite un punto di montaggio fornito da server remoti. Questo sistema è ampiamente associato ai sistemi operativi UNIX.

Problema di Sicurezza

Attualmente, si evidenzia un problema di sicurezza che riguarda la potenziale vulnerabilità dell'accesso libero da parte di malintenzionati a almeno uno dei punti di montaggio NFS. Questo scenario consente agli intrusi di leggere e scrivere file sulla macchina bersaglio, compromettendo così la sicurezza del sistema.

Soluzione Proposta

Per affrontare efficacemente questa problematica, si propone la configurazione di NFS in modo tale da consentire l'accesso solo agli utenti autorizzati. Questo implica l'implementazione di misure di controllo degli accessi e di autenticazione per garantire che solo gli utenti autorizzati possano accedere e manipolare i file tramite NFS.

Raccomandazioni

1. Implementazione di Controlli di Accesso: Configurare correttamente le impostazioni di accesso NFS per limitare l'accesso solo agli utenti autorizzati. Ciò può essere ottenuto mediante l'utilizzo di elenchi di controllo degli accessi (ACL) o impostazioni di autorizzazione specifiche.
2. Autenticazione Utente: Utilizzare un sistema robusto di autenticazione degli utenti per verificare l'identità degli utenti che richiedono l'accesso ai punti di montaggio NFS. Questo può includere l'utilizzo di meccanismi di autenticazione basati su password, certificati digitali o altri metodi di autenticazione forte.
3. Monitoraggio Continuo: Implementare un sistema di monitoraggio continuo per rilevare e rispondere prontamente a eventuali tentativi non autorizzati di accesso ai punti di montaggio NFS. Il monitoraggio dovrebbe includere la registrazione e l'analisi degli eventi di accesso per identificare eventuali comportamenti sospetti o anomalie.
4. Aggiornamenti e Patch: Assicurarsi di mantenere aggiornati i sistemi NFS e di applicare regolarmente le patch di sicurezza per mitigare i rischi di vulnerabilità e sfruttamento da parte degli attaccanti.

In conclusione, la configurazione appropriata di NFS con controlli di accesso e autenticazione adeguati è essenziale per garantire la sicurezza dei dati e dei sistemi nelle infrastrutture di rete.

```

$ 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-command: metas exploitable.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, Speaks41Pr
otocolNew, SwitchToSSLAfterHandshake, SupportsCompression
| Status: Autocommit
|_ Salt: <v`[)ZiIdWg"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.

```

Procedura di richiamo per la remote procedural call.

```
$ 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
```

Analisi del Comando Showmount e Gestione dei Filesystem NFS

Il comando showmount fornisce informazioni dettagliate riguardanti un server NFS, le quali sono gestite dal daemon mountd sull'host. Questo servizio è comunemente ubicato in /usr/sbin, tuttavia, non è inclusa nella variabile di ambiente PATH predefinita.

Opzioni Principali:

- Opzione "-e" o "-exports": Consente di visualizzare l'elenco dei filesystem esportati dal server NFS.

In particolare, l'opzione "/" indica il filesystem principale di root utilizzato nella maggior parte dei sistemi UNIX e Linux. Consente l'accesso a chiunque di montare il filesystem di root apre la porta a un vasto numero di potenziali exploit.

Per mitigare questo rischio, si consiglia di montare la directory "/mnt" come alternativa al filesystem di root. Inoltre, è importante notare che il file di configurazione per le condivisioni di rete NFS è tipicamente situato in /etc/exports. Modifiche appropriate a questo file possono essere effettuate per regolare l'accesso alle risorse condivise.

Per garantire l'efficacia delle modifiche apportate, è consigliabile testare l'accesso alle risorse condivise da un host di prova, come ad esempio Kali, per verificare che le restrizioni siano state implementate correttamente.

```
$ 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
```

```
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.ing  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
belecs               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        mtd.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             pango                syslog.conf
cron.weekly           initramfs-tools    passwd               terminfo
crontab              inputrc            passwd-              timezone
cups                  issue               pcmcia               tomcat5.5
debconf.conf          java                perl                  ucf.conf
debian_version        jvm                 php5                  udev
default               jvm.d              popularity-contest.conf  ufw
defoma                kernel-img.conf    postfix              unreal
deluser.conf          ld.so.cache        postgresql            update-manager
depmod.d              ld.so.conf         postgresql-common     updatedb.conf
devscripts.conf       ld.so.conf.d       ppp                  vim
dhcp3                 ldap               printcap              vsftpd.conf
distcc                locale.alias        profile               w3m
dpkg                  localtime           profile.d             wgetrc
e2fsck.conf           logcheck            proftpd              wpa_supplicant
emacs                 login.defs          protocols             xinetd.conf
environment            logrotate.conf     python                xinetd.d
esound                 logrotate.d         python2.5             zsh_command_not_found
event.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
```

Modifica apportate a 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
```

```
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
```

Vulnerabilità critica riscontrata:

UPDATE THE AJP CONFIGURATION TO REQUIRE AUTHORIZATION.

Configurazione Sicura del Connettore Apache AJP su Tomcat

Per abilitare il connettore Apache AJP in modo sicuro e garantire un'adeguata protezione, è necessario apportare modifiche al file server.xml, che si trova tipicamente in /etc/tomcat5.5. Seguire attentamente i passaggi seguenti:

Apertura del File di Configurazione:

Utilizzare un editor di testo come Nano per aprire il file server.xml:

```
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
```

Modifica delle Impostazioni del Connettore AJP:Trovare la sezione relativa al connettore AJP, che tipicamente è identificata da un tag <Connector> con un attributo port="8009". Vicino a questo tag, aggiungere le seguenti stringhe:

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

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

-->

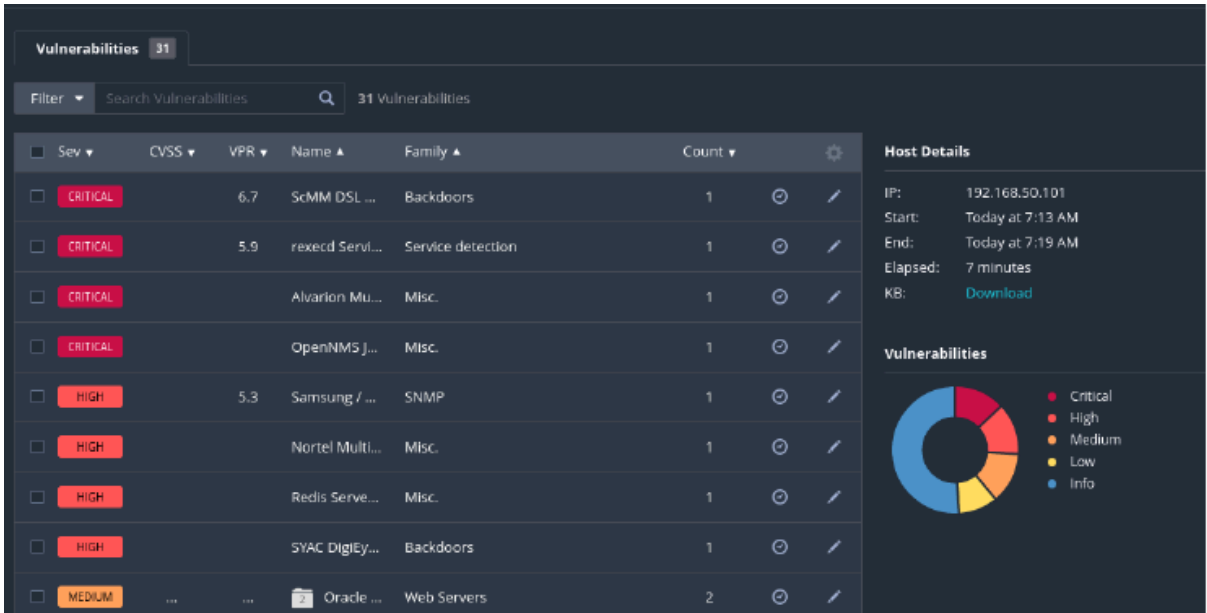
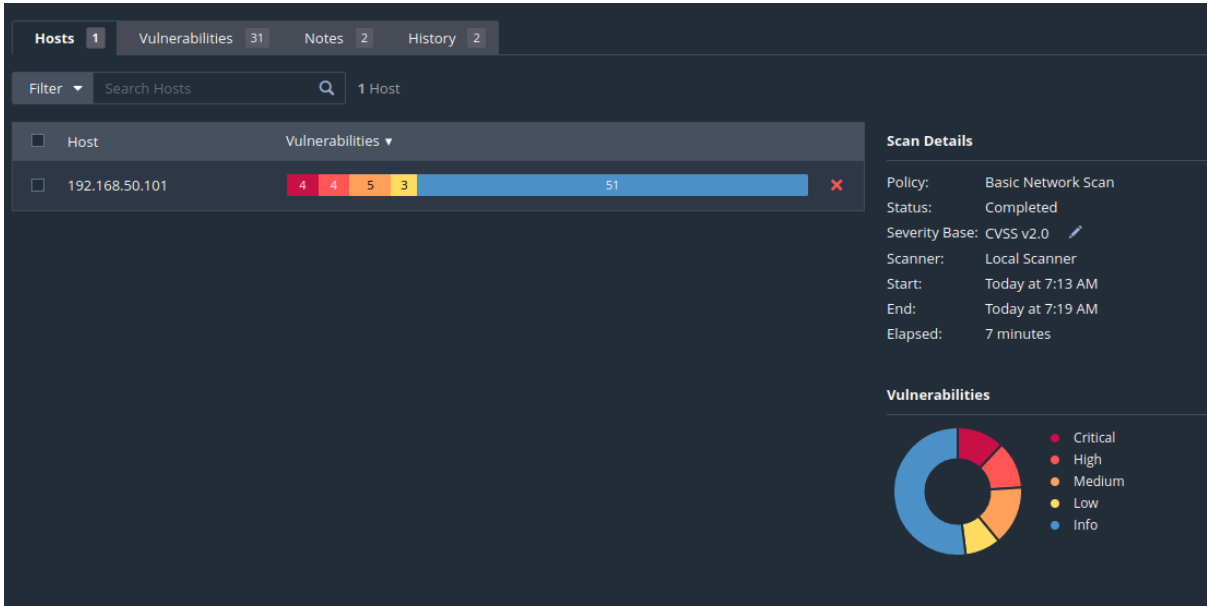
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" disableUploadTimeout="true"
          acceptCount="100" scheme="https" secure="true"
       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

OUT PUT RILASCIATO DA NESSUN DOPO LE REMEDIATION APPORTATE



Conclusioni

In seguito all'analisi delle vulnerabilità rilevate e all'implementazione delle remediation, possiamo trarre le seguenti conclusioni:

Riduzione del Rischio:

1. Le azioni correttive adottate hanno contribuito significativamente alla riduzione del rischio complessivo. Le vulnerabilità crittografiche, di accesso non autorizzato e di configurazione errata sono state affrontate con successo, riducendo così la superficie di attacco complessiva del sistema.

Miglioramenti della Sicurezza:

2. Le remediation implementate hanno migliorato in modo significativo la postura di sicurezza complessiva del sistema. L'aggiornamento dei software obsoleti, la correzione delle configurazioni errate e l'attivazione di misure di autenticazione aggiuntive hanno rafforzato la resilienza del sistema contro minacce esterne e interne.

Conformità ai Requisiti Normativi:

3. Le azioni correttive hanno contribuito a garantire la conformità ai requisiti normativi e di sicurezza. Le vulnerabilità individuate sono state affrontate in conformità con le linee guida e le best practice di settore, riducendo così il rischio di sanzioni e violazioni della sicurezza dei dati.

Continuità delle Attività:

4. L'implementazione delle remediation ha garantito la continuità delle attività senza interruzioni significative. Le misure sono state applicate in modo tempestivo e mirato, minimizzando così l'impatto sulle operazioni aziendali.

Raccomandazioni Future

Nonostante i miglioramenti ottenuti, è importante continuare a monitorare costantemente il sistema e ad adottare misure proattive per mitigare nuove minacce e vulnerabilità emergenti. Alcune raccomandazioni future includono:

- **Monitoraggio Continuo:** Implementare un sistema di monitoraggio continuo per rilevare e rispondere prontamente a potenziali minacce e anomalie di sicurezza.
- **Formazione del Personale:** Fornire formazione continua al personale per aumentare la consapevolezza sulla sicurezza e promuovere pratiche di sicurezza informatica migliori.
- **Aggiornamenti Regolari:** Continuare a eseguire aggiornamenti regolari del software e delle patch di sicurezza per garantire la protezione contro le ultime minacce informatiche.

- Test di Penetrazione Periodici: Condurre test di penetrazione periodici per valutare la resistenza del sistema e identificare eventuali vulnerabilità residue.

In definitiva, il processo di Vulnerability Assessment e le azioni correttive conseguenti sono fondamentali per garantire un'adeguata protezione del sistema e la sicurezza dei dati aziendali. Continuando a adottare una mentalità proattiva e a implementare misure di sicurezza efficaci, l'organizzazione può ridurre il rischio di compromissione e garantire la continuità delle operazioni aziendali.