

Remediation delle vulnerabilità

Vulnerabilità risolte:

- NFS Exported Share Information Disclosure
- Bind Shell Backdoor Detection
- VNC server 'password' Password

1. NFS Exported Share Information Disclosures

Per quanto riguarda la prima vulnerabilità, la remediation da applicare è quella di inserire all'interno della sottocartella del root /etc.

La prima cosa da fare è quella di visualizzare all'interno delle sottocartelle del root con "ls -a".

Cerchiamo la directory "/etc" e apriamo il file "exports".

All'interno di questo file, andremo a modificare l'* in fondo alla pagina con l'ip della nostra macchina.

Una volta fatto, riavviamo la macchina.

```
GNU nano 2.0.7      File: exports      Modified
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
/mnt/newdisk      192.168.50.101(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   ^U Next Page  ^U UnCut Text ^T To Spell
```

2. Bind Shell Backdoor Detection

Per quanto riguarda la risoluzione di questa vulnerabilità, ho abilitato il firewall di Metasploitable con il comando “UFW ENABLE”.

Dopodichè, ho detto al firewall di acconsentire a tutte le regole di default con “UFW DEFAULT ALLOW”.

```
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# ufw

Usage: ufw COMMAND

Commands:
  enable                Enables the firewall
  disable               Disables the firewall
  default ARG           set default policy to ALLOW or DENY
  logging ARG           set logging to ON or OFF
  allow|deny RULE       allow or deny RULE
  delete allow|deny RULE delete the allow/deny RULE
  status                show firewall status
  version               display version information

root@metasploitable:/home/msfadmin# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin# ufw deny 1524
```

Ho aggiunto una regola con il comando “UFW DEFAULT 1524” e ho controllato che la porta fosse con lo stato “FILTERED” con una scansione nmap.

```
(kali㉿kali)-[~/Downloads]
$ sudo systemctl start nessusd.service
[sudo] password for kali:
(kali㉿kali)-[~/Downloads]
$ nmap -sT -p 1524 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-05 09:24 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).

PORT      STATE      SERVICE
1524/tcp   filtered  ingreslock

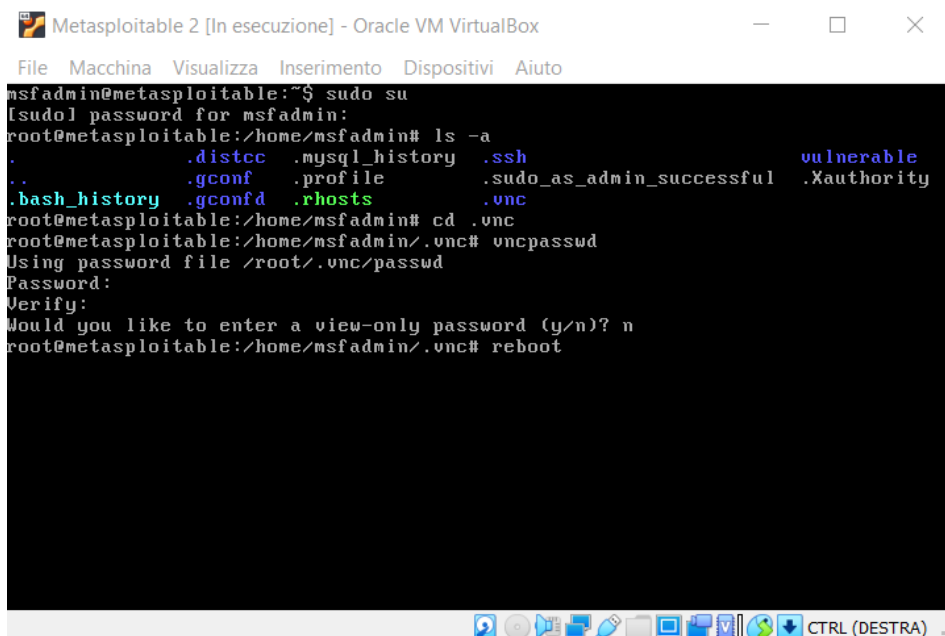
Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds

(kali㉿kali)-[~/Downloads]
$
```

3. VNC Server 'password' Password

Per modificare la password del VNC Server, troviamo all'interno della directory msfadmin, con il comando ls-a, il directory .vnc. All'interno di questa directory, andremo a eseguire il comando "vncpasswd" per cambiare la password.

Alla fine riavviamo la macchina.



```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# ls -la
.                  .distcc  .mysql_history  .ssh          vulnerable
..                 .gconf   .profile        .sudo_as_admin_successful  .Xauthority
.bash_history      .gconfd  .rhosts         .vnc
root@metasploitable:/home/msfadmin# cd .vnc
root@metasploitable:/home/msfadmin/.vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin/.vnc# reboot
```