

☐

CRITICAL

9.8

Bind Shell Backdoor Detecti...

Backdoors

La prima vulnerabilità che ho affrontato è stata la presenza della backdoor sulla porta 1524 di meta.

```
(alessio@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:/# cd  
bash: cd: HOME not set  
root@metasploitable:/# ls
```

```
1524/tcp open  ingreslock
```

Innanzitutto ho visto quali porte erano aperte con il comando nmap, poi ho visto che la 1524 era aperta (quella con la backdoor come mi aveva detto nessus), ed allora mi sono connesso con il comando netcat alla porta in questione.

```
vim  
vsftpd.conf  
w2m
```

```
(alessio@kali) ~  
$ netcat 192.168.50.101 1524  
  
(alessio@kali) ~  
$ nmap 192.168.50.101
```

Questa è la parte finale dell'esercizio. Non ho riportato tutte le immagini per ogni passaggio perché avrei riempito troppe pagine. Comunque una volta connesso, con il comando ls ho visto che cartelle e file ci fossero all'interno della porta, poi aprendo tutte le cartelle e vedendo il contenuto con ls ho cercato file e elementi che mi facessero nascere qualche sospetto. Nella porta etc, ho trovato il file "vsftpd.conf" che mi ha fatto accendere subito la lampadina, dato che mi ha ricordato del comando letto su internet: `/exploit/unix/ftp/vsftpd_234 backdoor`. Il file mi sembrava sospetto, quindi dalla macchina metasploitable ho cancellato il file in questione.

```
root@metasploitable:/etc# rm vsftpd.conf
```

CRITICAL

VNC Server 'password' Password

```
—(alessio@kali)-[~]
└─$ vncviewer 192.168.50.101
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
```

L'altra vulnerabilità risolta è quella della password weak sulla porta 5900. Mi sono connesso alla porta usando il comando `vncviewer` e sono loggato con la password. Poi con il comando `passwd`, ho provveduto a cambiare la password con una più sicura.

```
root@metasploitable:~# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@metasploitable:~#
```



Questa è l'ultima vulnerabilità che ho risolto. Fondamentalmente su nfs (server per la condivisione file da remoto) permetteva a tutti i client che avevano la possibilità di accedere i privilegi di root. Allora mi sono andato ad informare ed ho scoperto che nel file exports, dentro la cartella etc (dove prima abbiamo eliminato la backdoor), c'era la regola secondo la quale, seguendo qualunque path, ogni cliente aveva questi privilegi, quindi con il cancelletto la sono andato a neutralizzare :

```
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)
#
#_      *(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
```

La regola in questione era l'ultima.