

S5L5

Gli obiettivi dell'esercizio di oggi riguarda nello specifico la risoluzione di alcune criticità scoperte tramite Nessus della macchina virtuale Metasploitable.

Nello specifico ho deciso di risolvere due criticità riscontrate sulla mia macchina virtuale:

- VNC server password password
- NFS Exported share information disclosure

Prima criticità:

Il problema della prima criticità riguarda la debolezza delle password del DNC da cui si può accedere alla shell di Metasploitable come mostrato nelle seguenti immagini.

```

File  Actions  Edit  View  Help

-n          numeric-only IP addresses, no DNS
-o file     hex dump of traffic
-p port     local port number
-r          randomize local and remote ports
-q secs     quit after EOF on stdin and delay of secs
-s addr     local source address
-T tos      set Type Of Service
-t          answer TELNET negotiation
-u          UDP mode
-v          verbose [use twice to be more verbose]
-W secs     timeout for connects and final net reads
-c          Send CRLF as line-ending
-z          zero-I/O mode [used for scanning]

port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp[-data]').

(kali@kali)~#
$ nc 192.168.49.101 5900
RFB 003.003
^C

(kali@kali)~#
$ vncviewer 192.168.49.101
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 TrueColour. 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

```

La risoluzione di questa criticità consiste nel cambiare le password della macchina di Metasploitable da remoto secondo i seguenti parametri

- Password di almeno otto caratteri
- Presenza di almeno un numero
- Presenza di almeno un carattere inusuale
- Presenza di almeno una lettera maiuscola

```

root@metasploitable: /
cd /home/lib          mtnt      proc      srv      usr
root@metasploitable:/* cd media
root@metasploitable:/media# ls
cd /home/cdr0 floppy floppyo
root@metasploitable:/media# cd ..
root@metasploitable:/* ls
bin dev initrd lost+found nohup.out root sys var
boot etc initrd.img media opt/sbin 1111 vmlinuz
cd /home/lib          mtnt      proc      srv      usr
root@metasploitable:/* sudo su
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:/* vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Warning: password truncated to the length of 8.
Verify:
root@metasploitable:/* █

```

Seconda criticità:

La seconda criticità riguarda invece l'accesso o la modifica da remoto ad informazioni riguardo il Network File System, che riguardano anche le password associate ad un nome utente, oppure può consentire ad un attaccante di accedere alla shell di un sistema. Questo si può confermare tramite i seguenti passaggi:

- 1) Inizio con il creare una sottodirectory che chiamerò "metasploitable_share" all'interno della directory già esistente "/mnt"
- 2) Utilizzo il comando mount per accedere da remoto al NFS
- 3) Per avere conferma di ciò ho provato a copiare un file di testo nella cartella ".ssh".
- 4) Poi genero una chiave SSH sulla macchina usata per il test.
- 5) Dopo ho creato un file "authorized_keys" nella macchina attaccante e ho eliminato il contenuto del file "id_rsa.pub".
- 6) Infine, subito dopo aver copiato il file nella directory ".ssh", mi sono connesso alla macchina di Metasploitable con la chiave SSH creata in precedenza nel punto 4)

Per risolvere questa criticità basta:

- Restringere gli indirizzi IP che possono accedere alle directory NFS.
- Imporre solo il permesso di lettura dei file.