


Oggi come compito c'era da effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.

Progetto SS/L5 - PDF

 **EPICODE**

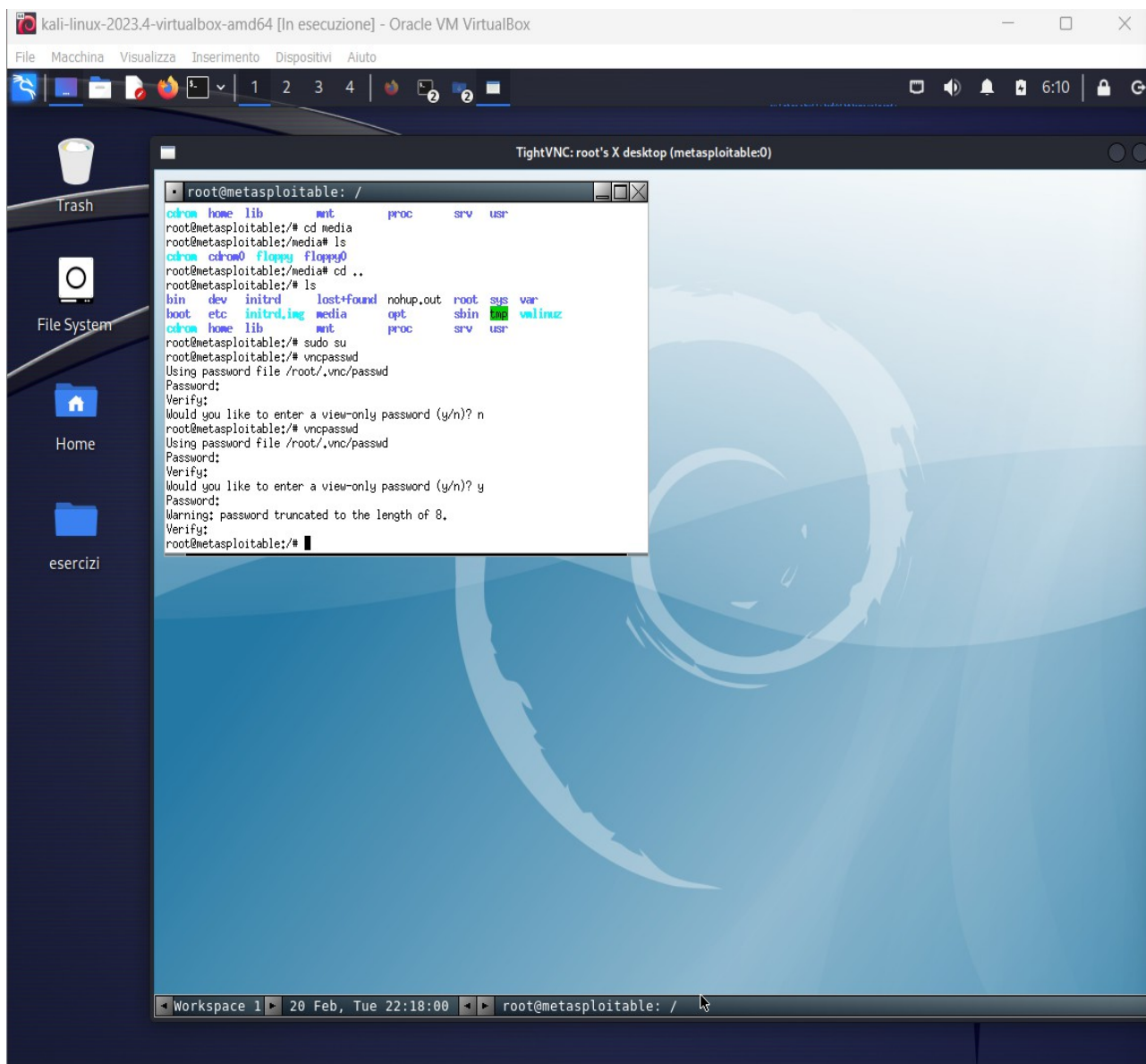
Esercizio
Traccia e requisiti

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Exported Share Information Disclosure
<input type="checkbox"/>	CRITICAL	10.0 *	rexecd Service Detection
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server 'password' Password
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor Detection

3

Siamo andati a vedere vnc server 'password' password per vedere e dimostrare la vulnerabilità mostrata

```
kali@kali: ~  
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').  
  
$ nc 192.168.49.101 5900  
RFB 003.003  
^C  
  
$ 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 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
```



una soluzione per la vnc server 'password' password: e avere una password complessa.

Qui siamo andati a vedere la vulnerabilità NFS exported share information disclosure

una soluzione per risolvere questa criticità configurare le NFS sul server remoto in modo che solo i computer autorizzati possano accedere e utilizzare le cartelle condivise.

```
(root@kali)-[/home/kali]
# sudo nmap -p 111,2049 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 06:42 EST
Nmap scan report for 192.168.49.101
Host is up (0.0014s latency).

PORT      STATE SERVICE
111/tcp    open  rpcbind
2049/tcp   open  nfs
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

```
root@kali: /mnt
File Actions Edit View Help
(root@kali)-[/mnt]
# ls
metasploit

(root@kali)-[/mnt]
# ls -la
total 12
drwxr-xr-x  3 root root 4096 Feb 23 06:53 .
drwxr-xr-x 19 root root 4096 Feb 23 06:53 ..
drwxr-xr-x  2 root root 4096 Feb 23 06:53 metasploit

(root@kali)-[/mnt]
# rm metasploit
rm: cannot remove 'metasploit': Is a directory

(root@kali)-[/mnt]
# rmdir metasploit

(root@kali)-[/mnt]
# ls

(root@kali)-[/mnt]
# mkdir -p /mnt/metasploit_share

(root@kali)-[/mnt]
# ls
metasploit_share

(root@kali)-[/mnt]
# ls -la
total 12
drwxr-xr-x  3 root root 4096 Feb 23 06:56 .
drwxr-xr-x 19 root root 4096 Feb 23 06:53 ..
drwxr-xr-x  2 root root 4096 Feb 23 06:56 metasploit_share

(root@kali)-[/mnt]
#
```

```
root@kali: /mnt/metasploit_share
File Actions Edit View Help

(root@kali)-[/mnt]
# ls -la
total 12
drwxr-xr-x  3 root root 4096 Feb 23 06:56 .
drwxr-xr-x 19 root root 4096 Feb 23 06:53 ..
drwxr-xr-x 21 root root 4096 May 20 2012 metasploit_share

(root@kali)-[/mnt]
# cd metasploit_share

(root@kali)-[/mnt/metasploit_share]
# ls -la
total 104
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x  3 root root 4096 Feb 23 06:56 ..
drwxr-xr-x  2 root root 4096 May 13 2012 bin
drwxr-xr-x  3 root root 4096 Apr 28 2010 boot
lrwxrwxrwx  1 root root    11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x  2 root root 4096 Apr 28 2010 dev
drwxr-xr-x 94 root root 4096 Feb 20 10:22 etc
drwxr-xr-x  6 root root 4096 Apr 16 2010 home
drwxr-xr-x  2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx  1 root root    32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwx----- 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x  4 root root 4096 Mar 16 2010 media
drwxr-xr-x  3 root root 4096 Apr 28 2010 mnt
-rw----- 1 root root 6542 Feb 20 10:22 nohup.out
drwxr-xr-x  2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x  2 root root 4096 Apr 28 2010 proc
drwxr-xr-x 13 root root 4096 Feb 20 10:22 root
drwxr-xr-x  2 root root 4096 May 13 2012/sbin
drwxr-xr-x  2 root root 4096 Mar 16 2010/srv
drwxr-xr-x  2 root root 4096 Apr 28 2010/sys
drwxrwxrwt  4 root root 4096 Feb 20 16:10 tmp
drwxr-xr-x 12 root root 4096 Apr 28 2010/usr
drwxr-xr-x 14 root root 4096 Mar 17 2010/var
lrwxrwxrwx  1 root root    29 Apr 28 2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server

6-server

(root@kali)-[/mnt/metasploit_share]
```

```
root@kali: /mnt/metasploit_share/root/.ssh
File Actions Edit View Help

(root@kali)-[/mnt/metasploit_share/root]
# cd .ssh

(root@kali)-[/mnt/metasploit_share/root/.ssh]
# ls -lh
authorized_keys  known_hosts  this to

(root@kali)-[/mnt/metasploit_share/root/.ssh]
# cd ..

(root@kali)-[/mnt/metasploit_share/root]
# ls -la
.          .config      .gconf       .profile     .ssh
..         Desktop    .gconfd      .purple      .vnc
.bash_history .filezilla  .gstreamer-0.10 reset_logs.sh vnc.log
.bashrc     .fluxbox    .mozilla     .rhosts      .Xauthority

(root@kali)-[/mnt/metasploit_share/root]
# cd .ssh

(root@kali)-[/mnt/metasploit_share/root/.ssh]
# cat
^C

(root@kali)-[/mnt/metasploit_share/root/.ssh]
# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNL0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70
lShHQqldJkcteZZdPFSbw76IUipR00h+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2q0ffdo
mVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8
FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73
KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w=
msfadmin@metasploitale

(root@kali)-[/mnt/metasploit_share/root/.ssh]
# nano authorized_keys

(root@kali)-[/mnt/metasploit_share/root/.ssh]
# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNL0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70
lShHQqldJkcteZZdPFSbw76IUipR00h+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2q0ffdo
mVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8
FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73
KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w=
kali@kali

(root@kali)-[/mnt/metasploit_share/root/.ssh]
#
```

<https://medium.com/r3d-buck3t/exploiting-a-misconfigured-nfs-share-5a7e01e7a42f>

su questo sito ci stanno i passi che volevo fare per dimostrare questa criticità avendo provato a fare un collegamento alla macchina come root. Non riuscendoci . Ho trovato un grande problema con la parte .ssh .

