

la vulnerabilita 1

nella prima foto ho semplicmetne aggiornato la password perchè era torppo facile da penetrare e nessun lo specifica nella critica su tenable

la vulnerabilitata2

nella seconda ho aggiornato alcuni programmi perchè alcune vulnerabilità nessun le ha date sugli aggiornamenti tenable dice di aggiornare e qui ho fatto cio

```
Kali [in execution] - Oracle VM VirtualBox
File Machine Visuals Inspectors Devices Auto
Applications Places Terminal
Aug 25 10:18

kali@kali: /mnt/metasploitable_share

kali@kali:~$ mkdir -p /mnt/metasploitable_share
kali@kali:~$ cd /mnt
kali@kali:~/mnt$ ls -la
ls: cannot access 'la': No such file or directory
kali@kali:~/mnt$ ls -la
total 12
drwxr-xr-x 3 root root 4096 Aug 25 09:25 .
drwxr-xr-x 19 root root 4096 Aug 1 09:16 ..
drwxr-xr-x 2 root root 4096 Aug 25 09:25 metasploitable_share
kali@kali:~/mnt$ sudo mount -o noexec 192.168.1.4:/mnt/metasploitable_share
[sudo] password for kali:
kali@kali:~/mnt$ ls -la
total 12
drwxr-xr-x 3 root root 4096 Aug 25 09:25 .
drwxr-xr-x 19 root root 4096 Aug 1 09:16 ..
drwxr-xr-x 21 root root 4096 May 20 2012 metasploitable_share
kali@kali:~/mnt$ cd metasploitable_share
kali@kali:~/mnt/metasploitable_share$ ls -la
total 188
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x 3 root root 4096 Aug 25 09:25 ..
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 96 root root 4096 Aug 25 08:17 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 1 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
```

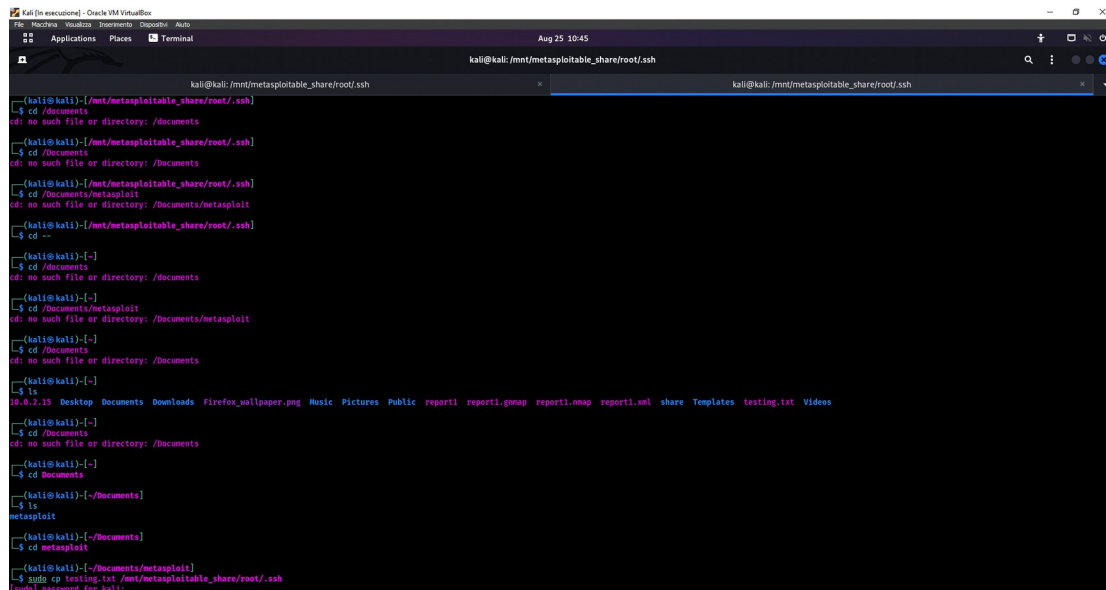
```
Kali [in execution] - Oracle VM VirtualBox
File Machine Visuals Inspectors Devices Auto
Applications Places Terminal
Aug 25 10:19

kali@kali: /mnt/metasploitable_share

kali@kali:~/mnt$ ls -la
total 12
drwxr-xr-x 3 root root 4096 Aug 25 09:25 .
drwxr-xr-x 19 root root 4096 Aug 1 09:16 ..
drwxr-xr-x 21 root root 4096 May 20 2012 metasploitable_share
kali@kali:~/mnt$ cd metasploitable_share
kali@kali:~/mnt/metasploitable_share$ ls -la
total 188
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x 3 root root 4096 Aug 25 09:25 ..
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 96 root root 4096 Aug 25 08:17 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 11369 Aug 25 08:17 mshup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
drwxr-xr-x 2 root root 4096 Apr 28 2010 proc
drwxr-xr-x 13 root root 4096 Aug 25 08:17 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
drwxr-xr-x 4 root root 4096 Aug 25 08:53 tmp
drwxr-xr-x 12 root root 4096 Apr 28 2010 usr
drwxr-xr-x 16 root root 4096 May 17 2010 var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vulnmap -> boot/vulnmap-2.6.24-16-server
kali@kali:~/mnt/metasploitable_share$ cat authorized_keys
cat: authorized: No such file or directory
cat: keys: No such file or directory
kali@kali:~/mnt/metasploitable_share$
```







```
kali [in esecuzione] - Oracle VM VirtualBox
File Hosts/Network -> Hosts/Network -> Desktop -> Auto
Applications Places Terminal
Aug 25 10:45
kali@kali: /mnt/metasploitable_share/root/.ssh

kali@kali: /mnt/metasploitable_share/root/.ssh
└─$ cd /documents
cd: no such file or directory: /documents

kali@kali: /mnt/metasploitable_share/root/.ssh
└─$ cd /documents
cd: no such file or directory: /documents

kali@kali: /mnt/metasploitable_share/root/.ssh
└─$ cd /documents/metasploit
cd: no such file or directory: /documents/metasploit

kali@kali: /mnt/metasploitable_share/root/.ssh
└─$ cd --
└─$ cd /documents
cd: no such file or directory: /documents

kali@kali: /mnt/metasploitable_share/root/.ssh
└─$ cd /documents/metasploit
cd: no such file or directory: /documents/metasploit

kali@kali: /mnt/metasploitable_share/root/.ssh
└─$ cd /documents
cd: no such file or directory: /documents

kali@kali: /mnt/metasploitable_share/root/.ssh
└─$ ls
10.0.2.15 Desktop Documents Downloads Firefox_wallpaper.png Music Pictures Public report1 report1.gmap report1.mmap report1.xml share Templates testing.txt Videos

kali@kali: /mnt/metasploitable_share/root/.ssh
└─$ cd /documents
cd: no such file or directory: /documents

kali@kali: /mnt/metasploitable_share/root/.ssh
└─$ cd Documents
└─$ ls
metasploit

kali@kali: /mnt/metasploitable_share/root/.ssh
└─$ cd metasploit
└─$ cp testing.txt /mnt/metasploitable_share/root/.ssh
[undo] password for kali:
```

le foto di questa vulnerabilita non sono tutte messe in ordine ma non la ho completata per il fatto che è stata molto dura la nfs da fare e alla fine ho riscontrato un problema altrimenti era completamente risolta infatti da come si nota tutti i passaggi sono stati svolti manca solo il finale

il tutto era copiare un file dove ci mettevi la chiave pubblica per gli host che si vogliono ammettere perchè il problema è che l'host era compromesso e questa vulnerabilita poteva essere aggiustata