

Remediation

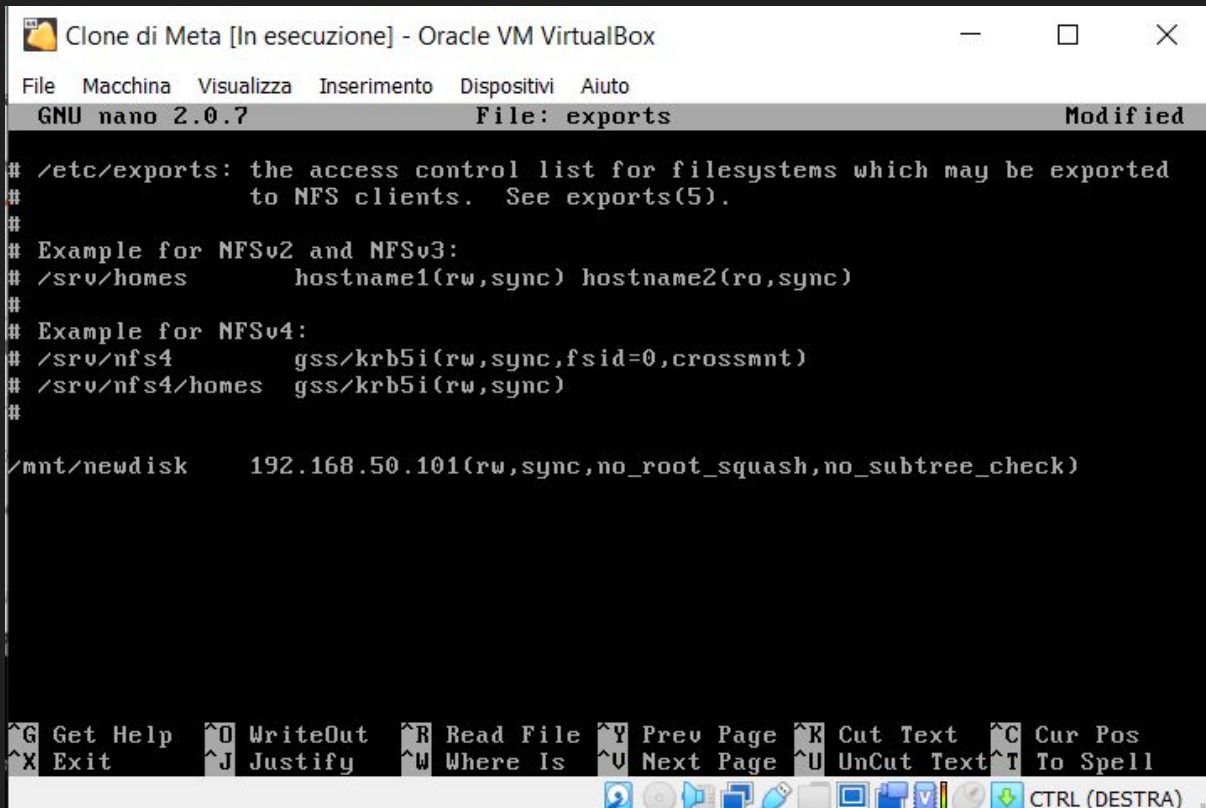


Vulnerability Remediation

NSF Exported Share Information Disclosure

NSF è un protocollo di condivisione file di rete; questa vulnerabilità potrebbe consentire a un potenziale attaccante di ottenere informazioni sensibili o di eseguire operazioni non autorizzate sulle risorse condivise tramite NSF

Remediation:



The screenshot shows a window titled "Clone di Meta [In esecuzione] - Oracle VM VirtualBox". Inside, the GNU nano 2.0.7 text editor is open, editing the file "/etc/exports". The file content is as follows:

```
# /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)
```

The bottom of the window shows a menu bar with various keyboard shortcuts and a status bar with "CTRL (DESTRA)".

Eseguo comandi:

```
sudo su
nano /etc/exports
```

poi modifico l'ultima riga
come in figura così da
dare accesso solo alla
macchina Metasploitable
(inserisco il corrispettivo
indirizzo IP)

VNC Server 'password' Password

Questa vulnerabilità indica la presenza di una password debole associata al server VNC, il VNC è un protocollo di desktop remoto che consente agli utenti di controllare e visualizzare l'interfaccia grafica di un computer da un altro dispositivo

Remediation:

```
Clone di Meta [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security/multiverse/i18n/Translation-en_US.bz2 Could not resolve 'security.ubuntu.com'
W: Some index files failed to download, they have been ignored, or old ones used instead.
W: You may want to run apt-get update to correct these problems
msfadmin@metasploitable:~$ vncpassword
-bash: vncpassword: command not found
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
UNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Warning: password truncated to the length of 8.
Verify:
msfadmin@metasploitable:~$
```

Eseguo il comando:

`vncpasswd`

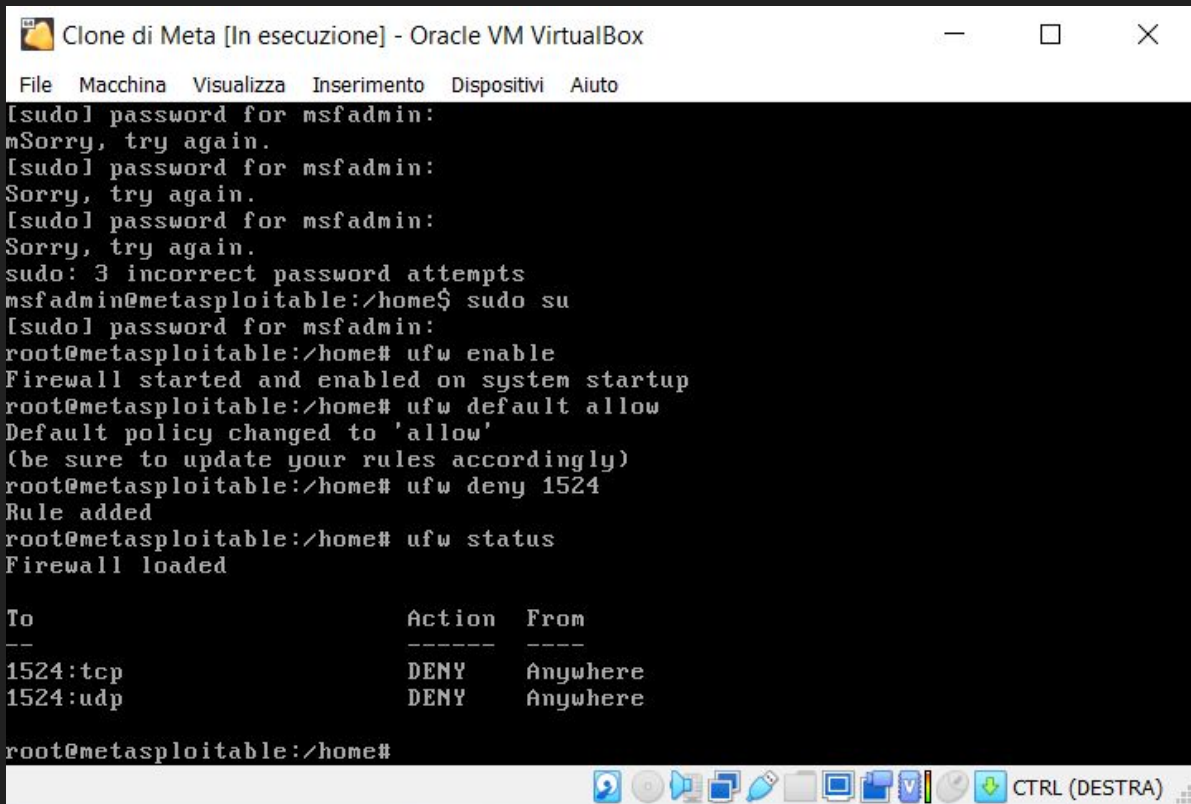
e continuo inserendo una nuova password per poi confermarla reinserendola

Bind Shell Backdoor Detection

Come suggerisce il nome, questa vulnerabilità si tratta di una backdoor scoperta dentro la macchina Metasploitable, in questo caso è presente una porta aperta non filtrata che permetterebbe ad un attaccante di aprire una shell da remoto ed eseguire comandi come se fosse fisicamente presente sulla macchina

in questo caso la porta da filtrare è la 1524

Remediation:



```
[sudo] password for msfadmin:
mSorry, try again.
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
Sorry, try again.
sudo: 3 incorrect password attempts
msfadmin@metasploitable:/home$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home# ufw enable
Firewall started and enabled on system startup
root@metasploitable:/home# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home# ufw deny 1524
Rule added
root@metasploitable:/home# ufw status
Firewall loaded

To Action From
--
1524:tcp DENY Anywhere
1524:udp DENY Anywhere

root@metasploitable:/home#
```

Eseguo comandi:

```
sudo su
ufw enable
ufw default allow
ufw deny 1524 (chiudo la
porta 1524)
```

poi controllo se la porta è
stata chiusa tramite
comando:

```
ufw status
```

Samba Badlock Vulnerability

Vulnerabilità di sicurezza scoperta nel software Samba, le caratteristiche principali includono la possibilità di essere sfruttata per eseguire attacchi Man in the Middle e/o per ottenere credenziali di accesso.

in questo caso le porte associate a Samba sono le 139 e 445

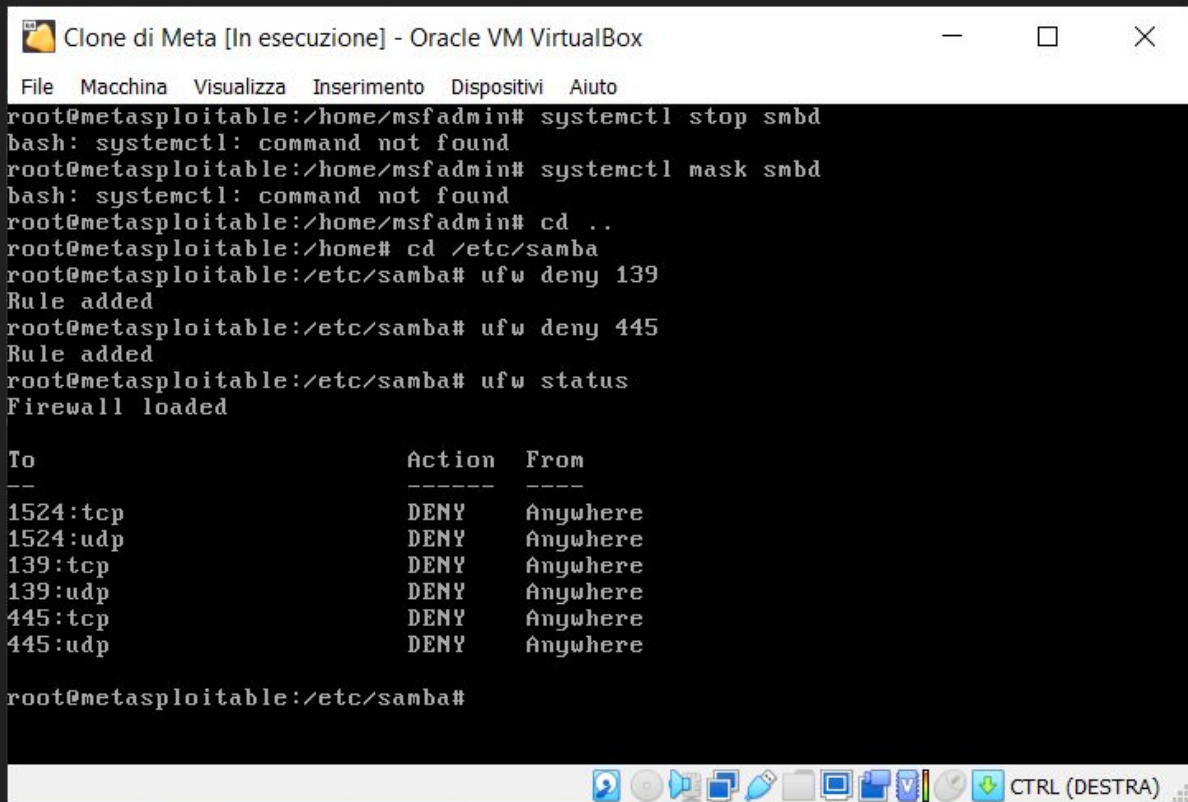
Remediation:

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 03:48 CST
Nmap scan report for 192.168.50.101
Host is up (0.00053s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  unknown
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 185.71 seconds
```

Tramite una scansione sV con Nmap possiamo notare che le porte 139 e 445 sono aperte e sono relative al servizio Samba

Remediation:



```
Clone di Meta [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
root@metasploitable:/home/msfadmin# systemctl stop smbd
bash: systemctl: command not found
root@metasploitable:/home/msfadmin# systemctl mask smbd
bash: systemctl: command not found
root@metasploitable:/home/msfadmin# cd ..
root@metasploitable:/home# cd /etc/samba
root@metasploitable:/etc/samba# ufw deny 139
Rule added
root@metasploitable:/etc/samba# ufw deny 445
Rule added
root@metasploitable:/etc/samba# ufw status
Firewall loaded

To                Action From
--                -
1524:tcp           DENY  Anywhere
1524:udp           DENY  Anywhere
139:tcp            DENY  Anywhere
139:udp            DENY  Anywhere
445:tcp            DENY  Anywhere
445:udp            DENY  Anywhere

root@metasploitable:/etc/samba#
```

Eseguo i comandi:

ufw deny 139

ufw deny 445

così da bloccare le
rispettive porte e mi accerto
dell'effettiva chiusura
tramite comando:

ufw status

Remediation:

```
kali@kali: ~  
(kali@kali)-[~]  
$ sudo systemctl start nessusd.service  
[sudo] password for kali:  
(kali@kali)-[~]  
$ ping 192.168.50.101  
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data:  
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.321 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.426 ms  
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.416 ms  
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.388 ms  
^C  
--- 192.168.50.101 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3025ms  
rtt min/avg/max/mdev = 0.321/0.387/0.426/0.040 ms  
(kali@kali)-[~]  
$ nmap -sV 192.168.50.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-22 16:46 CET  
Nmap scan report for 192.168.50.101  
Host is up (0.0013s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE        VERSION  
21/tcp    open  ftp            vsftpd 2.3.4  
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet         Linux telnetd  
25/tcp    open  smtp           Postfix smtpd  
53/tcp    open  domain         ISC BIND 9.4.2  
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind        rpcbind  
139/tcp   filtered netbios-ssn    netbios-ssn  
445/tcp   filtered microsoft-ds microsoft-ds  
512/tcp   open  exec           netkit-rsh rexecd  
513/tcp   open  login?         netkit-rshd  
514/tcp   open  shell          Netkit rshd  
1099/tcp  open  java-rmi       GNU Classpath grmiregistry  
1524/tcp  filtered ingreslock  
2049/tcp  open  rpcbind        rpcbind  
2121/tcp  open  ftp            ProFTPD 1.3.1  
3306/tcp  open  mysql?         MySQL 5.7.33-0ubuntu0.22.04.1  
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc            VNC (protocol 3.3)  
6000/tcp  open  X11            (access denied)  
6667/tcp  open  irc            UnrealIRCd  
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)  
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Eseguendo di nuovo uno scan
tramite Nmap possiamo notare che
ora le porte 139 e 445 sono filtrate