

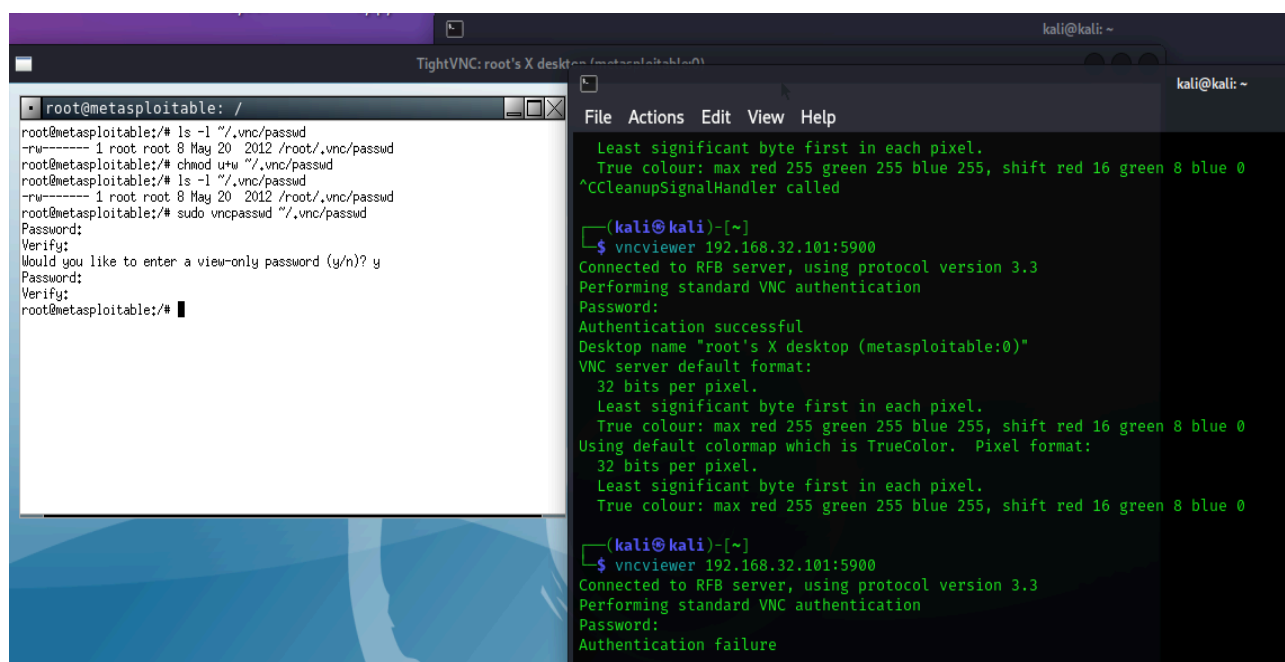
RISOLUZIONE DELLE VULNERABILITA'

Gelosa Matteo

- VNC Server 'password' Password

Per correggere questa vulnerabilità ho cambiato la password dell'accesso al server VNC.

Con il comando **vncpasswd ~/.vnc/passwd** ho potuto modificare la password rendendola più complessa e sicura, in modo che un malintenzionato non sia in grado di individuarla facilmente.



The image contains two terminal screenshots. The left screenshot shows a root user on a machine named 'metasploitable' running the command 'vncpasswd ~/.vnc/passwd'. The command prompts for a new password and verification, and the user enters 'password'. The right screenshot shows a Kali Linux terminal with a vncviewer window. It shows a successful connection to the RFB server at 192.168.32.101:5900 using protocol version 3.3. The terminal output includes details about the VNC server default format (32 bits per pixel, TrueColor) and the authentication process. The password 'password' is entered, and the connection is successful.

```
root@metasploitable: /
root@metasploitable:~# ls -l ~/.vnc/passwd
-rw-r--r-- 1 root root 8 May 20 2012 /root/.vnc/passwd
root@metasploitable:~# chmod u+w ~/.vnc/passwd
root@metasploitable:~# ls -l ~/.vnc/passwd
-rw-r--r-- 1 root root 8 May 20 2012 /root/.vnc/passwd
root@metasploitable:~# sudo vncpasswd ~/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:~#
```

```
(kali@kali)~[~]
$ vncviewer 192.168.32.101:5900
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

(kali@kali)~[~]
$ vncviewer 192.168.32.101:5900
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure
```

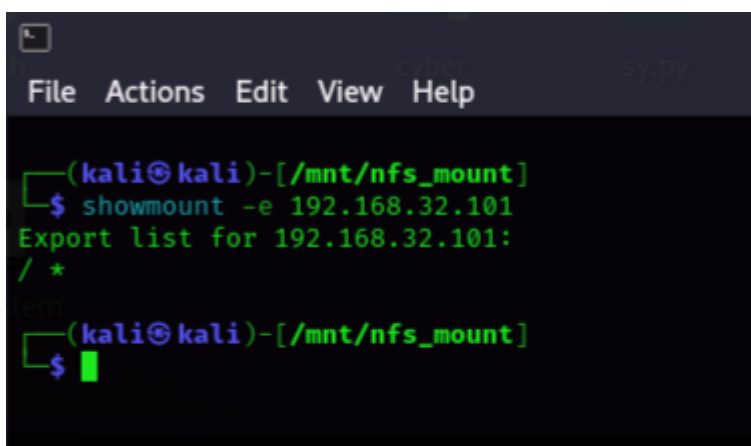
Nella figura a sinistra si possono vedere i passaggi che ho effettuato per modificare la password.

Nella figura di destra si nota come inizialmente la connessione è avvenuta utilizzando '**password**' come password e successivamente a password cambiata l'accesso fallito '**Authentication failure**'.

- **NFS Exported Share Information Disclosure**

Per questa vulnerabilità sono riuscito a connettermi al server nfs dalla macchina kali al servizio esposto su metasploitable alla porta 2049. In questo caso ho creato una cartella **/mnt/nfs_mount** in caso volessi fare il “mount” dei file sul server.

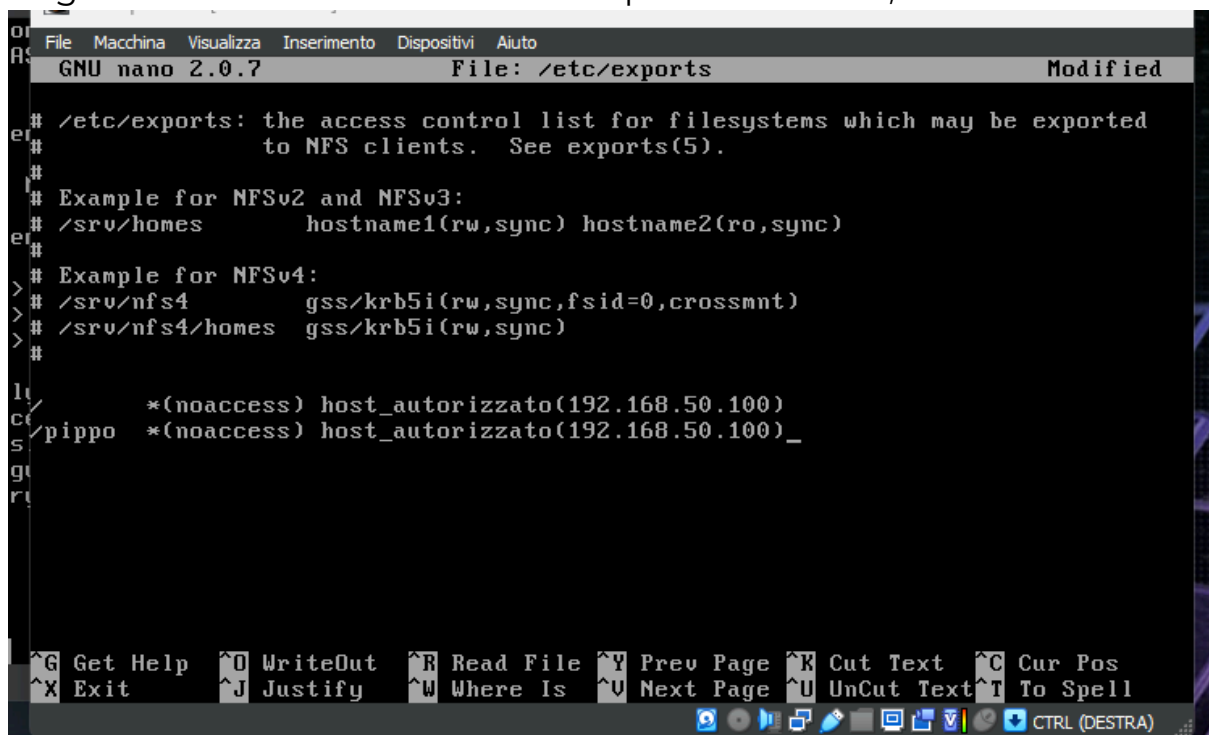
Successivamente ho eseguito il comando **showmount -e** per mostrare le esportazioni nfs disponibili.



```
(kali㉿kali)-[/mnt/nfs_mount]
$ showmount -e 192.168.32.101
Export list for 192.168.32.101:
/ *
```

Successivamente per testare il tutto ho creato un file **‘pippo’** sulla macchina metasploitable ed inserito nel percorso **/etc/exports** per appunto essere esportato.

Ho modificato il file **/etc/exports** in modo tale che possa essere eseguito il mount solo dall’indirizzo ip 192.168.50.100, ovvero kali linux.



```
GNU nano 2.0.7 File: /etc/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)
#
/*(noaccess) host_authorized(192.168.50.100)
/pippo *(noaccess) host_authorized(192.168.50.100)_
```

In questo caso con il comando ***(noaccess)** nego l'accesso a tutti, mentre specificando l'ip in **host_authorized** do il consenso a quella macchina di potervi accedere.

```
(kali㉿kali)-[/mnt/nfs_mount]
$ showmount -e 192.168.32.101
Export list for 192.168.32.101:
/          *
/pippo    *

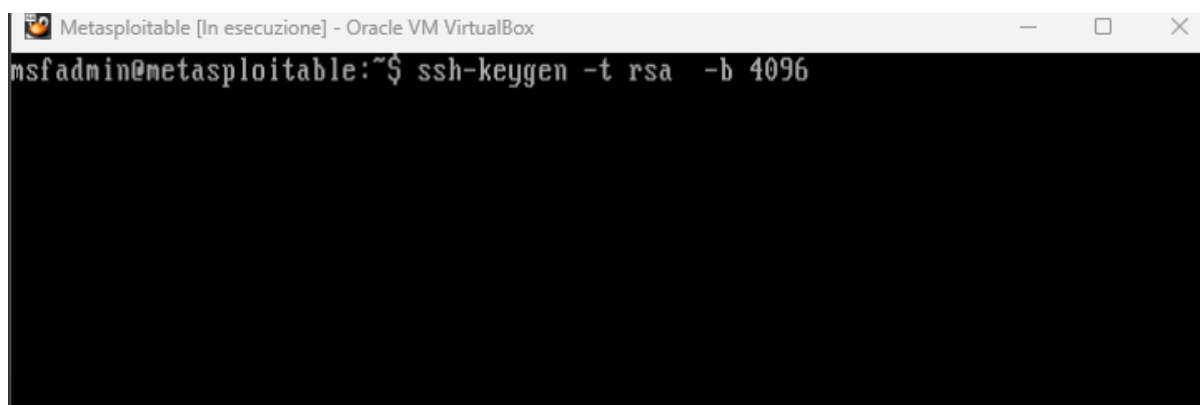
(kali㉿kali)-[/mnt/nfs_mount]
$ sudo mount -t nfs 192.168.32.101:/pippo /mnt/nfs_mount
[sudo] password for kali:
```

Mount eseguito dalla macchina Kali per il file **'pippo'**.

- **kal32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**

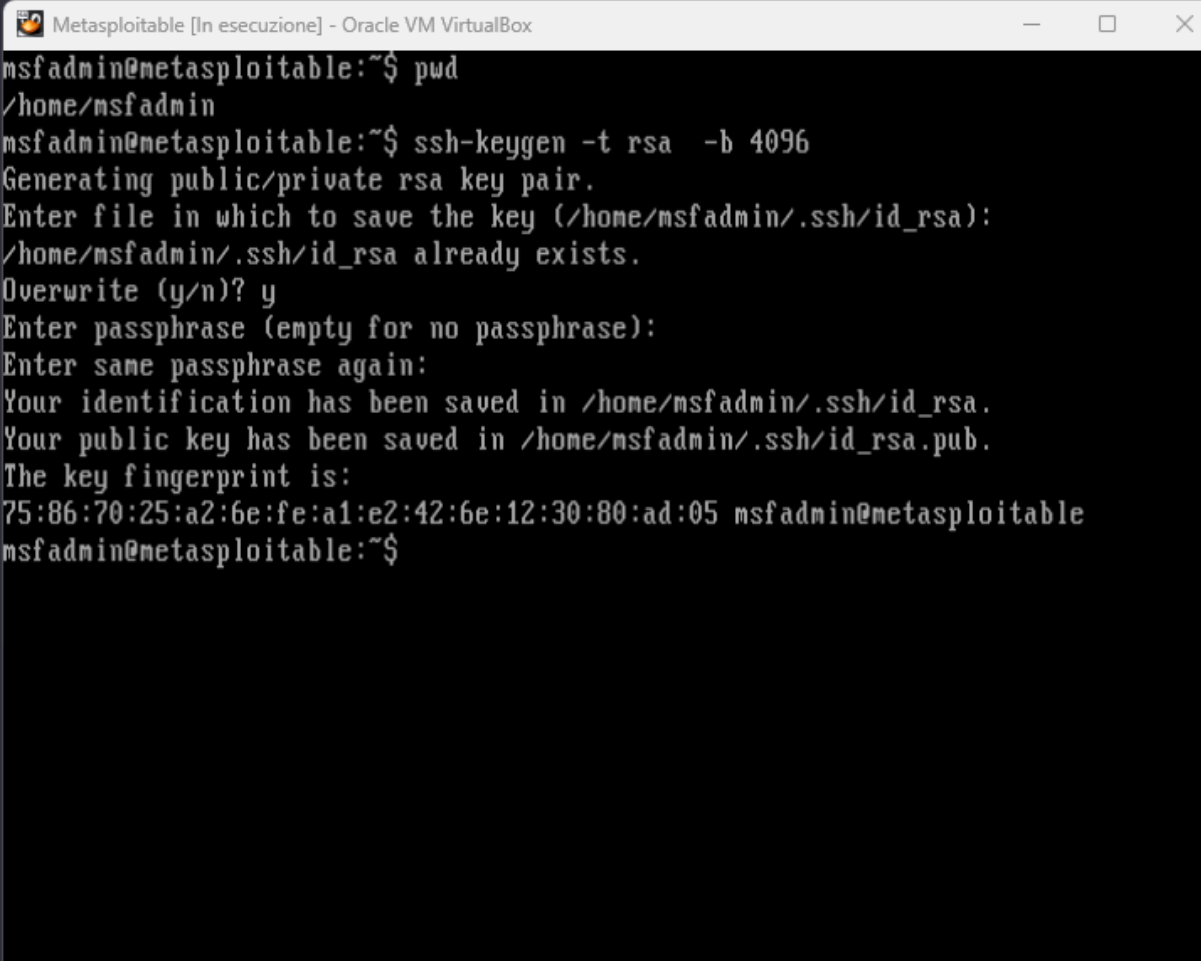
Per questa vulnerabilità ho dovuto aggiornare la chiave d'accesso vecchia perchè risultava datata ed insicura, con una nuova ed aggiornata.

per fare questo ho creato manualmente la chiave in questo modo:



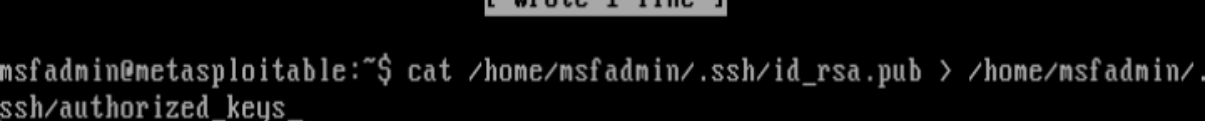
```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
msfadmin@metasploitable:~$ ssh-keygen -t rsa -b 4096
```

Ssh-keygen permette di generare nuove chiavi sicure e dal peso che vogliamo, in questo caso 4096 byte.



```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/msfadmin/.ssh/id_rsa):
/home/msfadmin/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/msfadmin/.ssh/id_rsa.
Your public key has been saved in /home/msfadmin/.ssh/id_rsa.pub.
The key fingerprint is:
75:86:70:25:a2:6e:fe:a1:e2:42:6e:12:30:80:ad:05 msfadmin@metasploitable
msfadmin@metasploitable:~$
```

Successivamente ho passato il contenuto del file di destinazione della chiave al file in cui verrà eseguita la chiave.



```
msfadmin@metasploitable:~$ cat /home/msfadmin/.ssh/id_rsa.pub > /home/msfadmin/.ssh/authorized_keys_
```

Successivamente ho provato l'accesso ed in seguito mi è stata richiesta la password locale per accedere .



```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
msfadmin@metasploitable:~$ ssh -i ~/.ssh/id_rsa msfadmin@192.168.32.101
msfadmin@192.168.32.101's password: _
```

- **Apache Tomcat AJP Connector Request Injection**

Per correggere questa vulnerabilità era necessario aggiornare TomCat.

Per prima cosa ho scaricato dalla macchina Kali Linux il file tar di TomCat e successivamente l'ho caricato sul server Apache locale.

```
(kali@kali)-[~/Downloads]
$ pwd
/home/kali/Downloads

(kali@kali)-[~/Downloads]
$ sudo cp /home/kali/Downloads/apache-tomcat-9.0.85.tar.gz /var/www/html/

(kali@kali)-[~/Downloads]
$ █
```

Successivamente con il comando wget ho scaricato il file sulla macchina meta per facilitare le operazioni.

```
root@metasploitable:~# cd /var/www/html
-bash: cd: /var/www/html: No such file or directory
root@metasploitable:~# wget http://192.168.50.100/apache-tomcat-9.0.85.tar.gz
--11:44:44-- http://192.168.50.100/apache-tomcat-9.0.85.tar.gz
=> 'apache-tomcat-9.0.85.tar.gz'
Connecting to 192.168.50.100:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11,809,177 (11M) [application/x-gzip]

100%[=====] 11,809,177 --.-K/s

11:44:44 (95.85 MB/s) - 'apache-tomcat-9.0.85.tar.gz' saved [11809177/11809177]
root@metasploitable:~# █
```

I

Si può notare che ho effettuato la connessione all'indirizzo di kali ed infine ho aggiunto il path per scaricare il file necessario.

Una volta scaricato l'ho estratto in quanto era in formato tar.gz.

```
root@metasploitable: /home/msfadmin
root@metasploitable:/home/msfadmin# ls
apache-tomcat-10.1.18.tar.gz.asc  apache-tomcat-9.0.85.tar.gz
apache-tomcat-10.1.18.tar.gz.asc.1  vulnerable
root@metasploitable:/home/msfadmin# tar -zxvf apache-tomcat-9.0.85.tar.gz
apache-tomcat-9.0.85/conf/
apache-tomcat-9.0.85/conf/catalina.policy
apache-tomcat-9.0.85/conf/catalina.properties
apache-tomcat-9.0.85/conf/context.xml
apache-tomcat-9.0.85/conf/jaspic-providers.xml
apache-tomcat-9.0.85/conf/jaspic-providers.xsd
apache-tomcat-9.0.85/conf/logging.properties
apache-tomcat-9.0.85/conf/server.xml
apache-tomcat-9.0.85/conf/tomcat-users.xml
```

Successivamente ho rimosso completamente i file della versione vecchia di TomCat per poter installare quella nuova.

```
root@metasploitable: /var/lib/tomcat5.5
root@metasploitable:/home/msfadmin# sudo rm -r /var/lib/tomcat7/
rm: cannot remove '/var/lib/tomcat7/': No such file or directory
root@metasploitable:/home/msfadmin# cd /var/lib
root@metasploitable:/var/lib# ls
apparmor  dhcp3          libuid         mysql-cluster  samba          update-manager
apt       dpkg           locales        nfs             security        urandom
aptitude  gcj-4.2        logrotate      nfs             sgml-base       vim
belocs    gconf          misc           postfix         tomcat5.5       x11
bind      initramfs-tools mlocate        postgresql      ucf             xkb
defoma    initscripts    mysql          python-support  ufw
root@metasploitable:/var/lib# cd tomcat5.5
root@metasploitable:/var/lib/tomcat5.5# ls
conf  logs  shared  temp  webapps  work
root@metasploitable:/var/lib/tomcat5.5# sudo rm -r /var/lib/tomcat5.5/
root@metasploitable:/var/lib/tomcat5.5#
```

Ho poi spostato il file estratto nella cartella /var/bin/tomcat7 , tomcat7 creata da me.

```
root@metasploitable: /home/msfadmin
apt      dpkg      locales   nfs        security   vim
aptitude gcj-4.2    logrotate php5        sgml-base  x11
belocs    gconf     misc      postfix    ucf         xkb
bind      initramfs-tools mlocate   postgresql ufw
defoma    initscripts mysql      python-support update-manager
root@metasploitable:/var/lib# cd
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# cd Desktop
root@metasploitable:~/Desktop# ls
root@metasploitable:~/Desktop# cd
root@metasploitable:~# cd /home
root@metasploitable:/home# ls
ftp  msfadmin  service  user
root@metasploitable:/home# cd /msfadmin
-bash: cd: /msfadmin: No such file or directory
root@metasploitable:/home# cd /home/msfadmin
root@metasploitable:/home/msfadmin# ls
apache-tomcat-10.1.18.tar.gz.asc  apache-tomcat-9.0.85  vulnerable
apache-tomcat-10.1.18.tar.gz.asc.1  apache-tomcat-9.0.85.tar.gz
root@metasploitable:/home/msfadmin# pwd
/home/msfadmin
root@metasploitable:/home/msfadmin# sudo cp -r /home/msfadmin/apache-tomcat-9.0.85 /var/lib/tomcat7/
```

Infine ho avviato il servizio di netcat.

- **57608 - SMB Signing not required (vulnerabilità a scelta)**

Per aggirare la vulnerabilità ho impostato delle regole specifiche con iptables.

Ho messo una regola che accetta unicamente l'indirizzo ip di meta al server samba , ovvero il 192.168.23.101.

Ho messo una seconda regola in cui rifiuta tutti gli altri ip non uguali a quello di metasploitable.

```
root@metasploitable: ~
root@metasploitable:~# sudo iptables -A INPUT -p tcp --dport 445 -s 192.168.32.101 -j ACCEPT
root@metasploitable:~# sudo iptables -A input -p tcp --dport 445 -j DROP
iptables: No chain/target/match by that name
root@metasploitable:~# sudo iptables -A INPUT -p tcp --dport 445 -j DROP
root@metasploitable:~#
```

```
root@metasploitable: ~
root@metasploitable:~# sudo iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
ACCEPT    tcp  --  192.168.32.101         anywhere        tcp dpt:microsoft-d
s
DROP      tcp  --  anywhere              anywhere        tcp dpt:microsoft-d
s

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
root@metasploitable:~#
```

Effettuando una scan anche da kali linux la porta 445 risulta effettivamente filtrata.

```
(kali㉿kali)-[~]  
└─$ sudo nmap -sS 192.168.32.101  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-28 12:30 EST  
Nmap scan report for 192.168.32.101  
Host is up (0.00093s latency).  
Not shown: 980 closed tcp ports (reset)  
PORT      STATE      SERVICE  
21/tcp    open      ftp  
22/tcp    open      ssh  
23/tcp    open      telnet  
25/tcp    open      smtp  
53/tcp    open      domain  
80/tcp    open      http  
111/tcp   open      rpcbind  
139/tcp   open      netbios-ssn  
445/tcp   filtered  microsoft-ds  
512/tcp   open      exec  
513/tcp   open      login  
514/tcp   open      shell  
1099/tcp  open      rmiregistry  
1524/tcp  open      ingreslock  
2121/tcp  open      ccproxy-ftp  
3306/tcp  open      mysql  
5432/tcp  open      postgresql  
5900/tcp  open      vnc  
6000/tcp  open      X11  
6667/tcp  open      irc  
  
Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
```