

## **W12D4 -Esame del modulo 3.**

### **Scansione Iniziale con Nessus.**

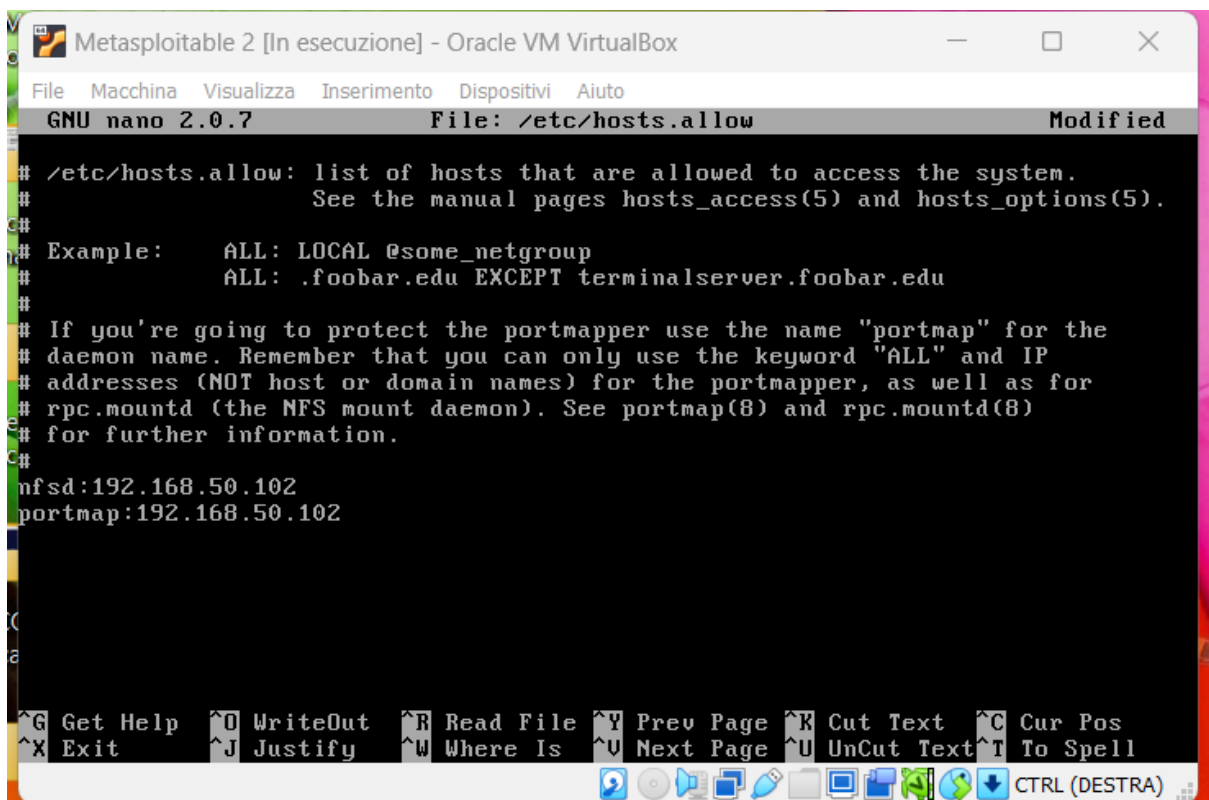
Ho svolto un vulnerability assessment usando Nessus sulla macchina Metasploitable 2 con IP 192.168.50.101. Ho svolto sia una scansione solo sulle porte comuni, sia una scansione su tutte le porte ed allego il report sintetico ed il report dettagliato per entrambe le scansioni. Nemmeno con la scansione su tutte le porte ho trovato la vulnerabilità evidenziata nella consegna, ovvero "Rexced Service Detection" e per questo motivo ho deciso di lavorare in seguito su altre vulnerabilità. Dalla scansione sulle porte comuni sono emerse 7 vulnerabilità critiche, 4 vulnerabilità ad alto rischio, 16 vulnerabilità a medio rischio, 7 vulnerabilità a basso rischio ed infine 69 classificate come "info".

### **Screenshot e spiegazione dei passaggi delle remediation actions.**

#### **NFS Exported Share Information Disclosure**

Questa vulnerabilità riguarda NFS, ovvero Network File system, che è un protocollo che consente di accedere a dei file nella rete come se fossero su un disco locale ed è utile nella condivisione di file tra server e client. Questa vulnerabilità implica il fatto che gli share NFS possono essere visti anche da utenti non autorizzati, i quali possono ricavare informazioni sensibili come specifici file o directory per degli attacchi o possono tentare una privilege escalation, specialmente se l'opzione root squashing non è abilitata e quindi un attaccante può modificare, aggiungere o eliminare file o altri contenuti a suo piacimento. Questa vulnerabilità è pericolosa anche perché dà la possibilità ad un attaccante di compromettere il sistema, di trasferire dati sensibili e di spostarsi su altri file o directory.

**Remediation actions:** è chiara la necessità di configurare correttamente il servizio NFS e i permessi per la condivisione degli NFS shares ed ho quindi agito sui file di configurazione per risolvere questa problematica. Ho deciso di utilizzare TCP Wrappers, che serve per filtrare le connessioni network legate a servizi come NFS e che permette di controllare gli accessi e fare in modo che gli share NFS non siano disponibili per utenti non autorizzati. TCP Wrappers è simile ad un firewall, ma a differenza del firewall serve per controllare le configurazioni e i permessi relativi solo a servizi specifici e permette una personalizzazione maggiore riguardo alla scelta di quale IP può accedere ai dati di un certo servizio. La configurazione di TCP Wrappers avviene con due file di configurazione, ossia /etc/hosts.allow, che indica quali host possono avere accesso ad un particolare servizio, e /etc/hosts.deny, che indica a quali host ed IP deve essere negata la connessione ad un servizio. Ho trovato questi file con `sudo nano /etc/hosts.allow` e `sudo nano /etc/hosts.deny` ed ho configurato il file /etc/hosts.allow indicando che solo l'indirizzo IP 192.168.50.102 di Windows può accedere agli share NFS e al demone di NFS nfsd. Mentre nel file /etc/hosts.deny ho inserito una policy che vieta a tutti gli IP non autorizzati di collegarsi ai servizi come NFS. Gli screenshot che seguono dimostrano la configurazione dei due file di TCP Wrappers.



Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox

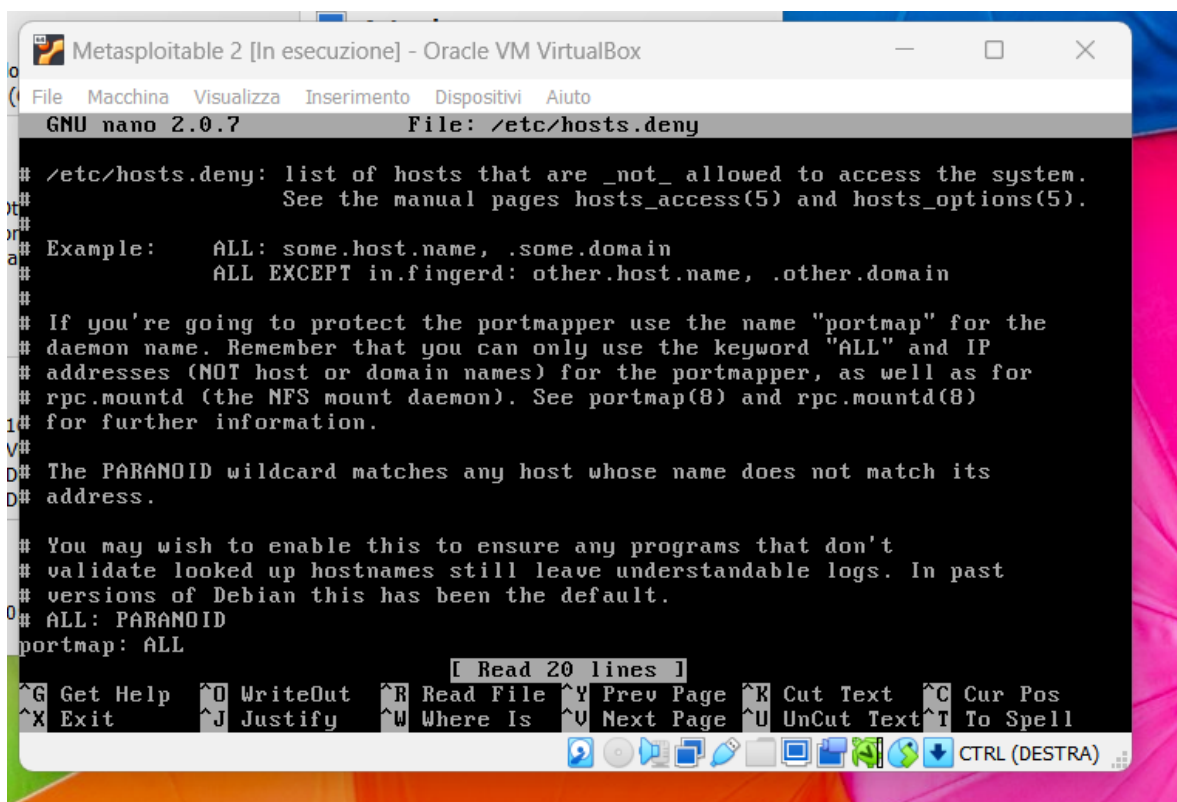
File Macchina Visualizza Inserimento Dispositivi Aiuto

GNU nano 2.0.7 File: /etc/hosts.allow Modified

```
# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: LOCAL @some_netgroup
#              ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
nfsd:192.168.50.102
portmap:192.168.50.102
```

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos  
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell

CTRL (DESTRA)



Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

GNU nano 2.0.7 File: /etc/hosts.deny

```
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: some.host.name, .some.domain
#              ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
portmap: ALL
```

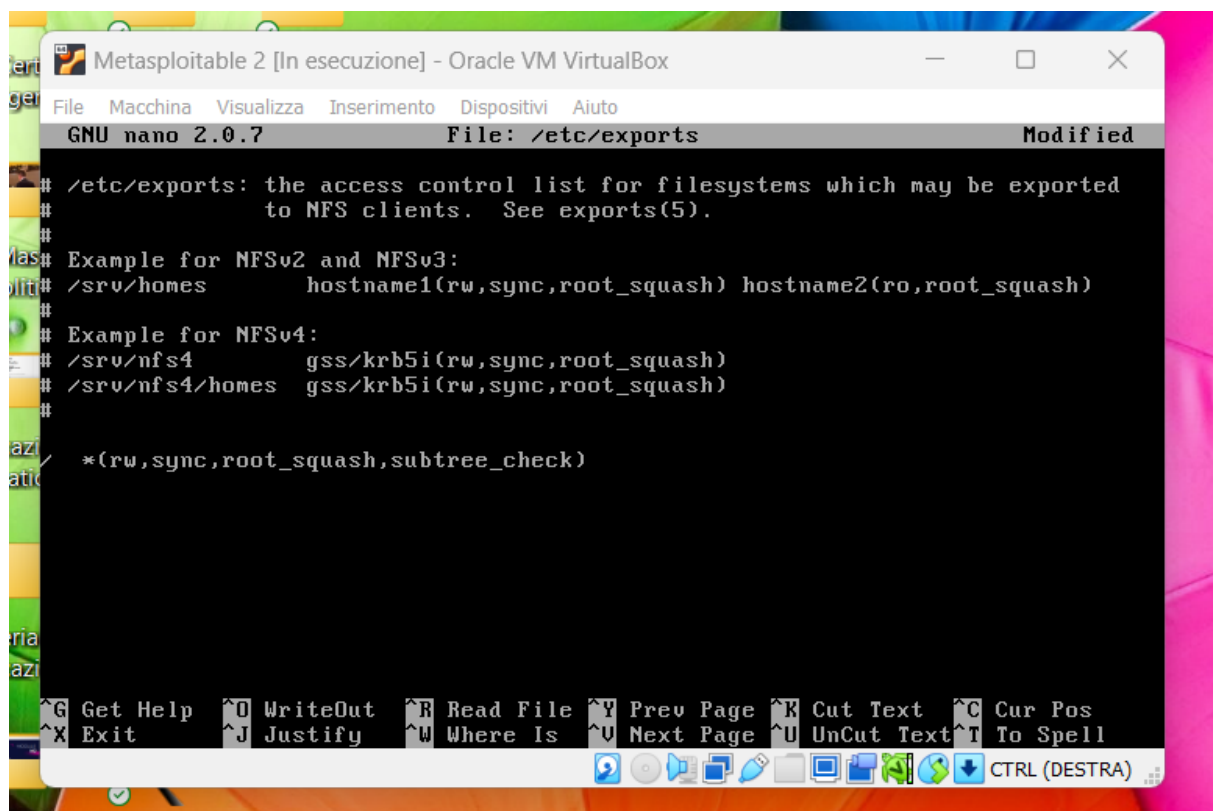
[ Read 20 lines ]

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos  
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell

CTRL (DESTRA)

Ho deciso di rafforzare questa remediation action con un'altra remediation action che riguarda la configurazione dei file `/etc/exports`, che disciplinano le condivisioni degli NFS shares. Ho raggiunto il file da modificare con `sudo nano /etc/exports`. Poi ho configurato i permessi indicando `"root_squash"`, che serve ad evitare una privilege escalation da parte di

utenti con privilegi di root sul client, che in questo modo non possono acquisire privilegi di root anche sul server e "subtree\_check", che previene accessi non autorizzati ai dati. Lo screenshot successivo dimostra la configurazione che ho applicato.



The screenshot shows a window titled "Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox". Inside, the GNU nano 2.0.7 editor is open to 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,root_squash) hostname2(ro,root_squash)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,root_squash)
# /srv/nfs4/homes gss/krb5i(rw,sync,root_squash)
#
*(rw,sync,root_squash,subtree_check)
```

The nano editor interface includes a menu bar with options like File, Macchina, Visualizza, Inserimento, Dispositivi, and Aiuto. At the bottom, there is a toolbar with various editing functions and a status bar showing "CTRL (DESTRA)".

**Soluzione:** L'azione combinata di TCP Wrappers e la giusta configurazione di /etc/exports ha permesso di eliminare questa vulnerabilità e di gestire con cura i permessi per accedere agli share NFS.

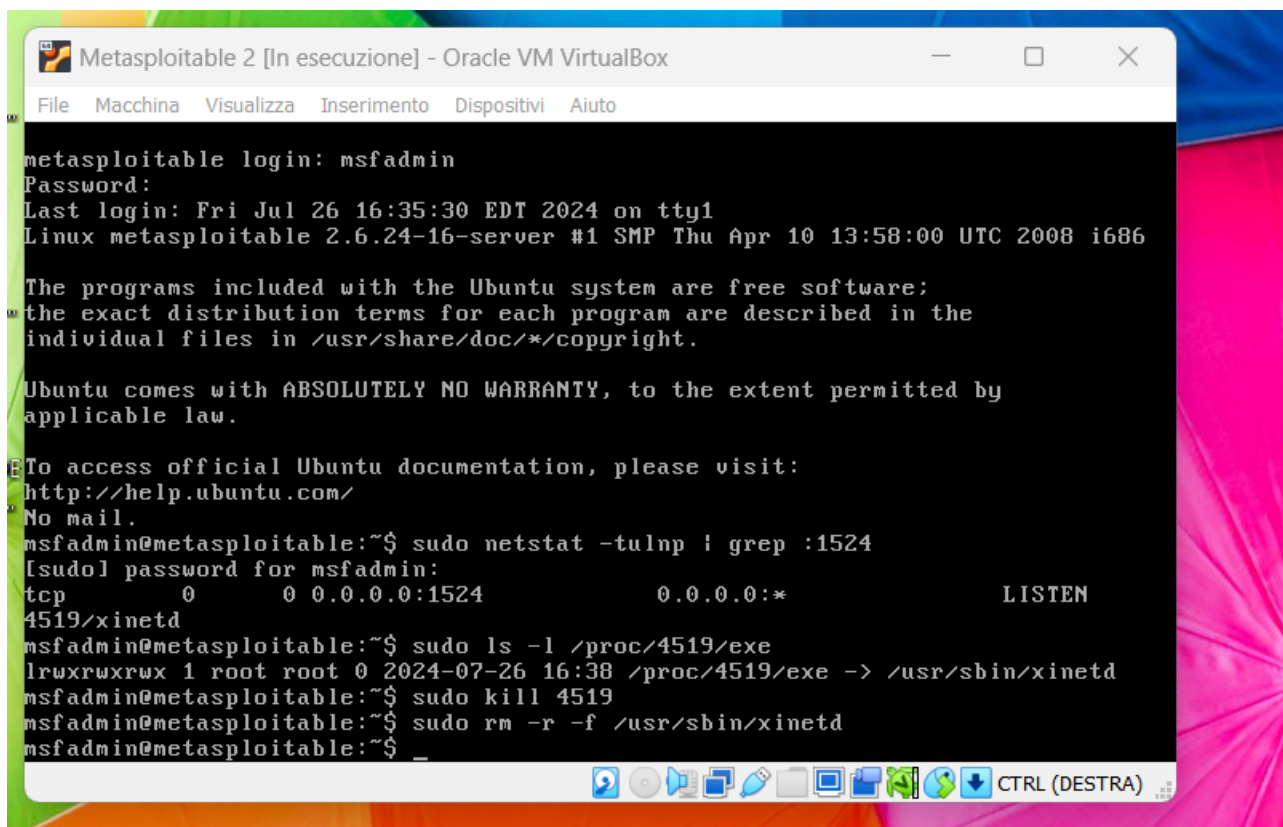
### Bind Shell Backdoor Detection.

È stata individuata una backdoor di tipo bind shell molto pericolosa, perché permette ad un attaccante di connettersi da remoto e di far eseguire del codice malevolo con la shell ottenuta. Solitamente su Metasploitable 2 le shell di questo tipo hanno i privilegi di root, per cui un malintenzionato può agire indisturbato sul sistema, compromettendolo in modo grave senza doversi autenticare.

**Remediation actions:** Ho individuato il processo della bind shell backdoor sulla porta 1524 sia analizzando il report di Nessus in formato CSV, sia ricordando le precedenti scansioni fatte con Nmap con target Metasploitable 2. Lo screenshot che segue dimostra proprio come nella porta 1524 sia presente una bind shell con privilegi di root.

```
root@kali: ~  
File Actions Edit View Help  
root@kali:~# nmap -sV 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 14:57 EDT  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns  
or specify valid servers with --dns-servers  
Nmap scan report for 192.168.50.101  
Host is up (0.00078s latency).  
Not shown: 977 closed tcp ports (reset)  
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  http         Apache Tomcat/Coyote JSP engine 1.1  
MAC Address: 08:00:27:8D:17:A0 (Oracle VirtualBox virtual NIC)  
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 55.99 seconds
```

Con `sudo netstat -tulnp | grep :1524` ho individuato la connessione sulla porta 1524, individuando il PID del processo. Il processo è stato successivamente visualizzato, trovando maggiori dettagli riguardo al processo eseguibile e alla sua posizione con il comando `sudo ls -l /proc/PID/exe`. Il processo della bind shell è stato quindi terminato con `sudo kill PID`, ma killare il processo non è sufficiente, perché in caso di nuova accensione o riavvio si verrebbe a creare di nuovo questa bind shell. È dunque necessario rimuovere definitivamente anche la backdoor con il comando `sudo rm -r -f /usr/sbin/xinetd`, che elimina completamente la backdoor eseguibile e che rende definitiva l'eliminazione della backdoor anche in caso di accensione e riavvio.



```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

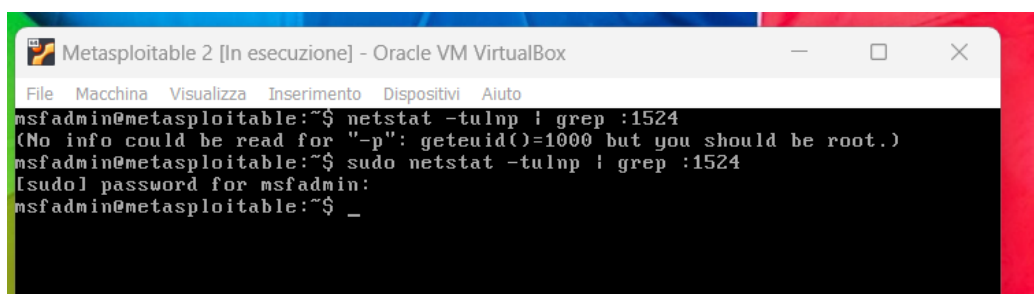
metasploitable login: msfadmin
Password:
Last login: Fri Jul 26 16:35:30 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

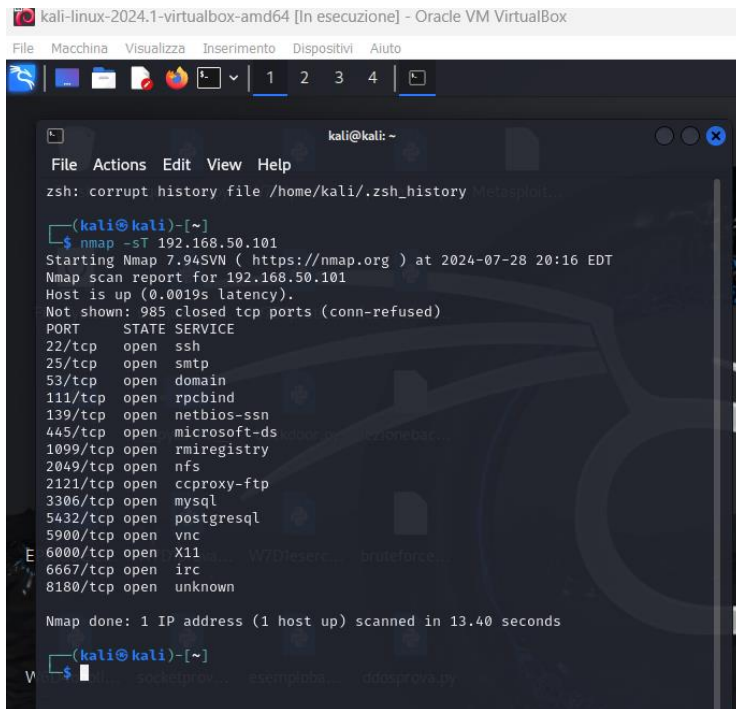
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep :1524
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
4519/xinetd
msfadmin@metasploitable:~$ sudo ls -l /proc/4519/exe
lrwxrwxrwx 1 root root 0 2024-07-26 16:38 /proc/4519/exe -> /usr/sbin/xinetd
msfadmin@metasploitable:~$ sudo kill 4519
msfadmin@metasploitable:~$ sudo rm -r -f /usr/sbin/xinetd
msfadmin@metasploitable:~$ _
```

**Soluzione:** con queste azioni il processo della bind shell è terminato e la backdoor è stata eliminata definitivamente. Per accertarmi di questo, ho svolto una verifica sia da Metasploitable 2, sia una scansione con Nmap da Kali che hanno dimostrato che la rimozione della backdoor ha avuto successo.



```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

msfadmin@metasploitable:~$ netstat -tulnp | grep :1524
(No info could be read for "-p": geteuid()=1000 but you should be root.)
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep :1524
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ _
```

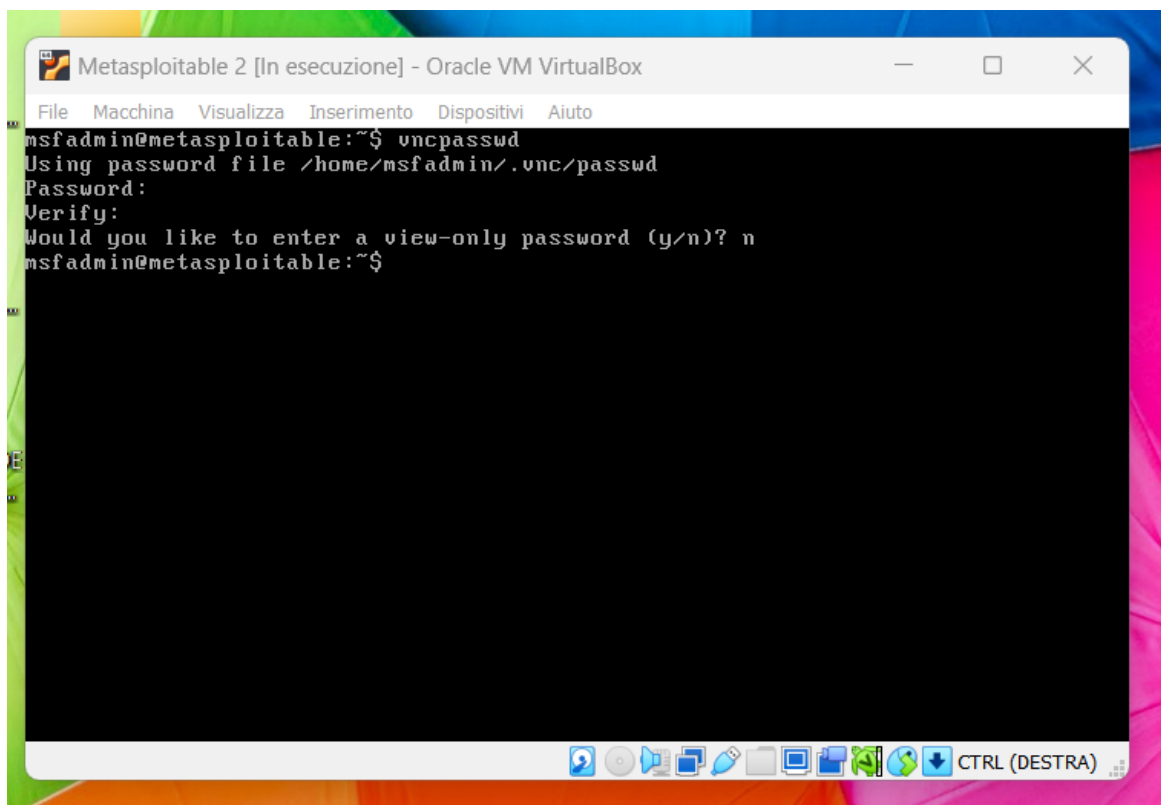


```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
  
kali@kali:~  
$ nmap -sT 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 20:16 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.0019s latency).  
Not shown: 985 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
25/tcp    open  smtp  
53/tcp    open  domain  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
1099/tcp  open  rmiregistry  
2049/tcp  open  nfs  
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  
8180/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds  
  
kali@kali:~  
$
```

## VNC Server "password" Password

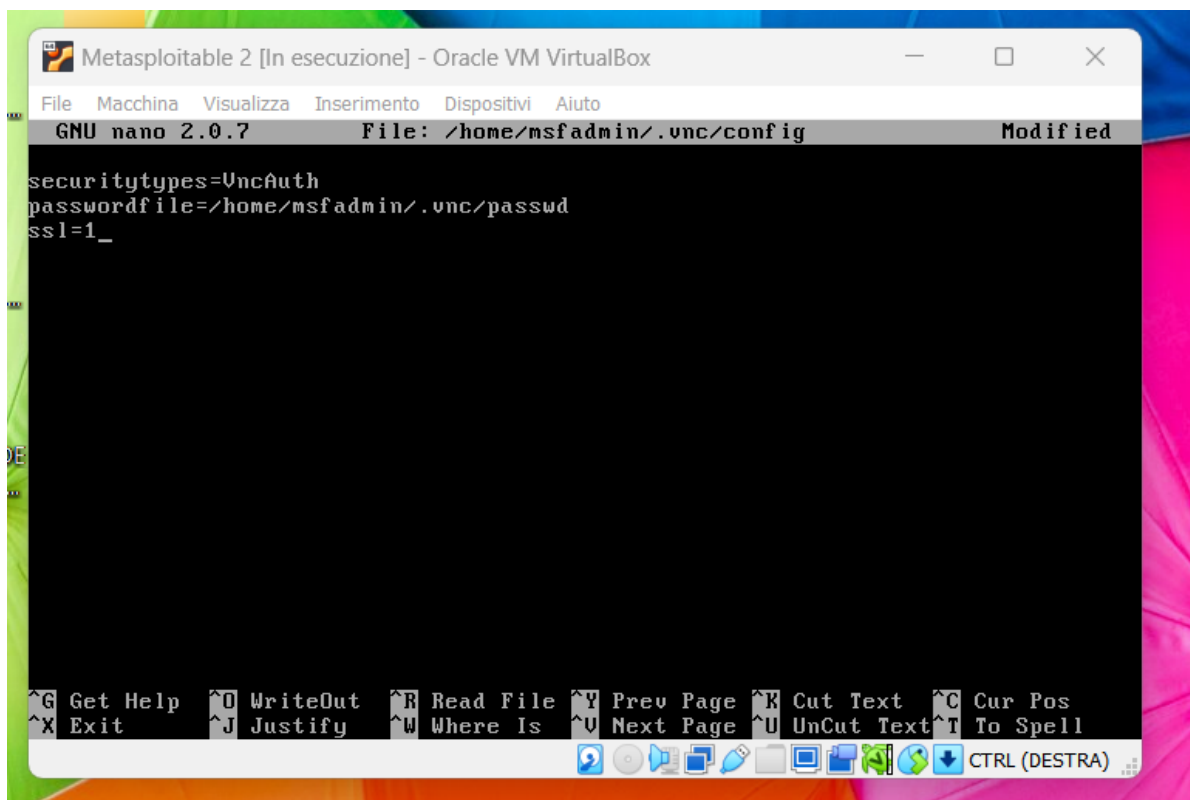
Questa vulnerabilità riguarda il server VNC: VNC significa Virtual Network Computing ed è un sistema di condivisione del desktop grafico che utilizza il protocollo Remote Frame Buffer (RFB) per controllare un altro computer da remoto. È dunque facile immaginare le conseguenze che derivano dall'uso di una password troppo debole ed ovvia come "password" perché un attaccante può facilmente connettersi al server VNC e controllare da remoto il computer, installando e rimuovendo file e cartelle, compromettendo il sistema, rubando dati ed eseguendo malware di vario tipo. La password di questo server è quindi troppo debole e senza crittografia, esponendo la macchina ad un grave rischio.

**Remediation actions:** Per prima cosa, ho impostato la nuova password del server VNC con il comando `vncpasswd`.



```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$
```

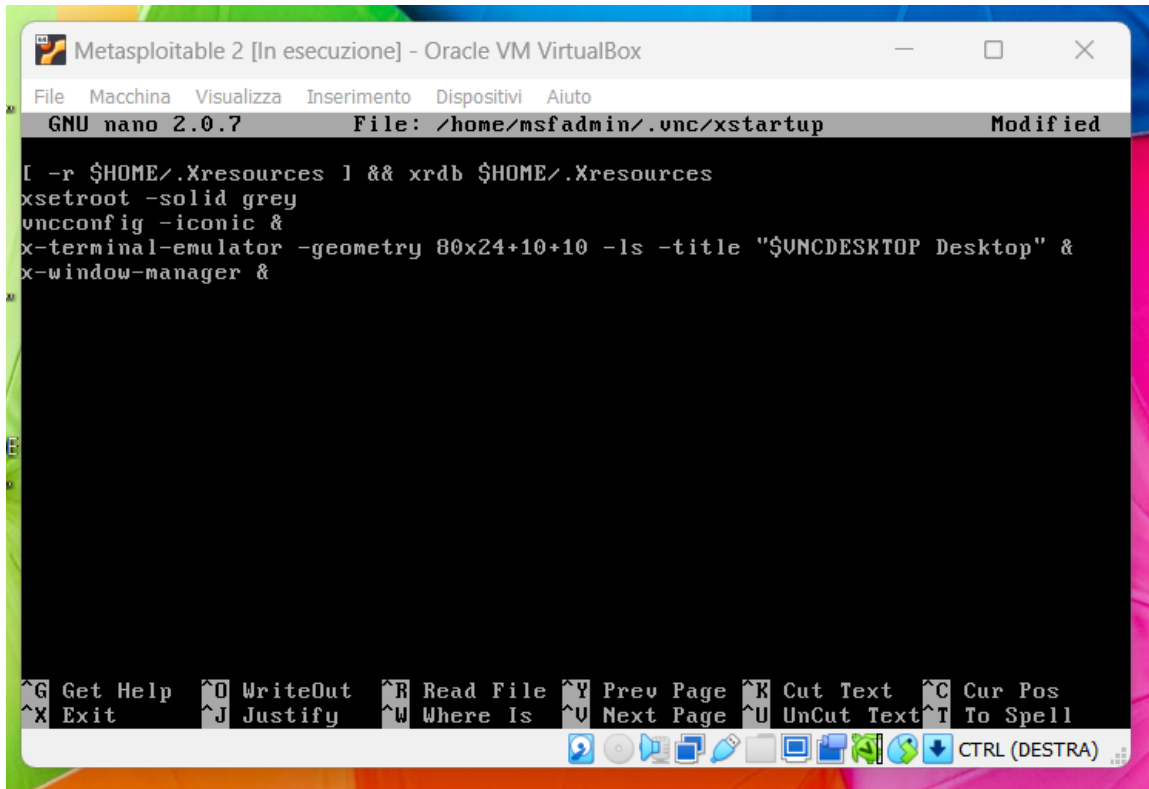
Successivamente ho creato il file di configurazione con `sudo nano /home/msfadmin/.vnc/config`, in cui si indica che l'accesso al server VNC deve avvenire solo tramite autenticazione (prima riga), si specifica il path del file dove è contenuta la password (riga 2) e si abilita la cifratura con protocollo SSL della password (riga 3).



```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7 File: /home/msfadmin/.vnc/config Modified
securitytypes=VncAuth
passwordfile=/home/msfadmin/.vnc/passwd
ssl=1_

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

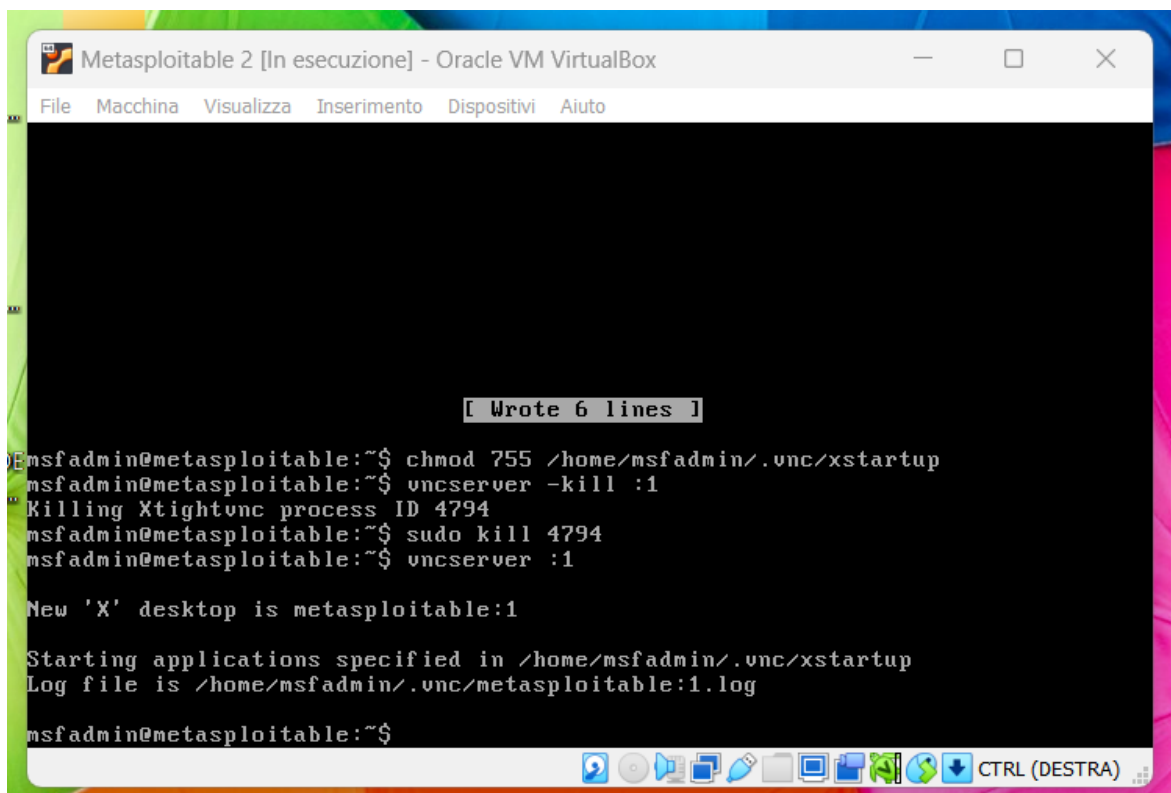
Poi ho modificato il file xstartup con `sudo nano /home/msfadmin/.vnc/xstartup` per indicare cosa avviene quando si avvia una sessione con il server VNC. Viene stabilito come caricare delle risorse (riga 1), il colore della finestra (riga 2), l'avvio di VNC configuration tool (riga 3), l'avvio di un terminal emulator (riga 4) e l'avvio del window manager di default (riga 5).



```
[ -r $HOME/.Xresources ] && xrdp $HOME/.Xresources
xsetroot -solid grey
vncconfig -iconic &
x-terminal-emulator -geometry 80x24+10+10 -ls -title "$UNCDESKTOP Desktop" &
x-window-manager &
```

A questo punto con `chmod` ho dato permessi di lettura, scrittura ed esecuzione all'utente `msfadmin` e permessi di sola lettura ed esecuzione agli altri utenti per il file `xstartup`, rendendo così il file eseguibile. Per poter riavviare VNC ho dovuto terminare il processo dopo averne individuato il PID ed infine ho riavviato il server VNC con il comando `vncserver :1`.





```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

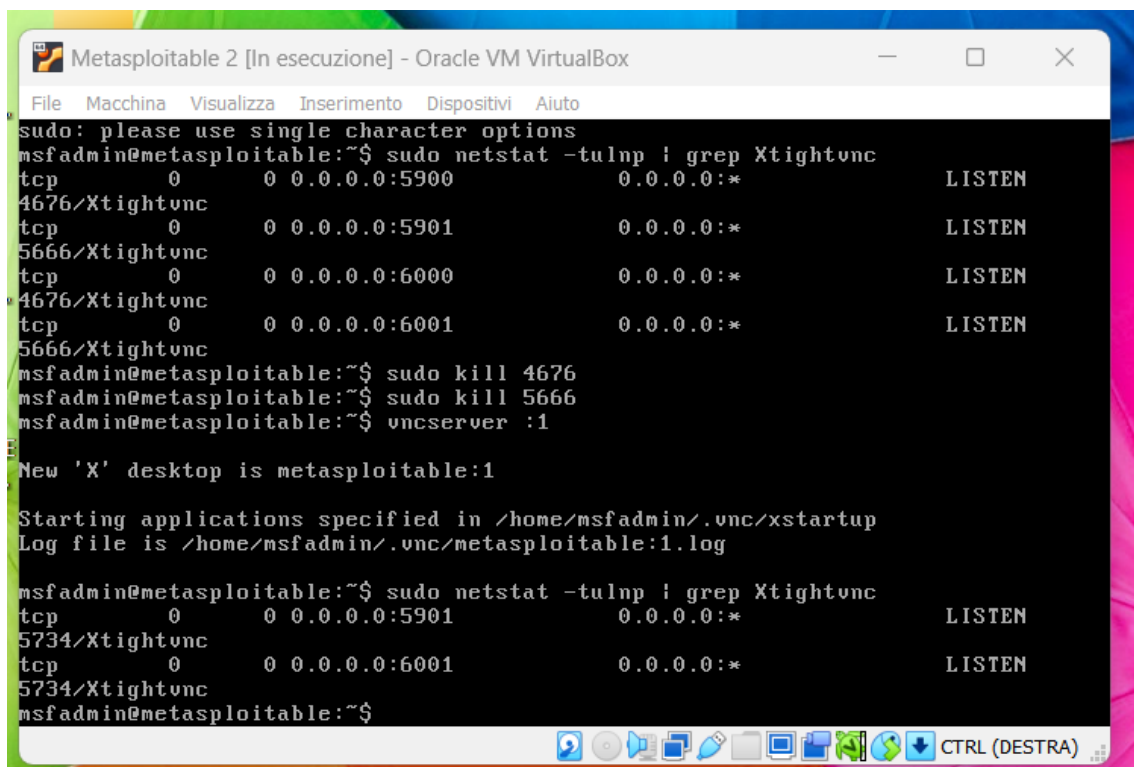
[ Wrote 6 lines ]

msfadmin@metasploitable:~$ chmod 755 /home/msfadmin/.vnc/xstartup
msfadmin@metasploitable:~$ vncserver -kill :1
Killing Xtightvnc process ID 4794
msfadmin@metasploitable:~$ sudo kill 4794
msfadmin@metasploitable:~$ vncserver :1

New 'X' desktop is metasploitable:1

Starting applications specified in /home/msfadmin/.vnc/xstartup
Log file is /home/msfadmin/.vnc/metasploitable:1.log
msfadmin@metasploitable:~$
```

Con `sudo netstat -tulnp | grep Xtightvnc` ho controllato le connessioni attive che riguardano Xtightvnc, che è il processo legato alle sessioni del server TightVNC. Ho ottenuto il PID per terminare le vecchie sessioni con il comando `kill` ed ho avviato una nuova sessione con `vncserver :1`, riavviando il server e verificando che il riavvio sia andato a buon fine con `netstat`.



```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

sudo: please use single character options
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep Xtightvnc
tcp        0      0 0.0.0.0:5900          0.0.0.0:*            LISTEN
4676/Xtightvnc
tcp        0      0 0.0.0.0:5901          0.0.0.0:*            LISTEN
5666/Xtightvnc
tcp        0      0 0.0.0.0:6000          0.0.0.0:*            LISTEN
4676/Xtightvnc
tcp        0      0 0.0.0.0:6001          0.0.0.0:*            LISTEN
5666/Xtightvnc
msfadmin@metasploitable:~$ sudo kill 4676
msfadmin@metasploitable:~$ sudo kill 5666
msfadmin@metasploitable:~$ vncserver :1

New 'X' desktop is metasploitable:1

Starting applications specified in /home/msfadmin/.vnc/xstartup
Log file is /home/msfadmin/.vnc/metasploitable:1.log

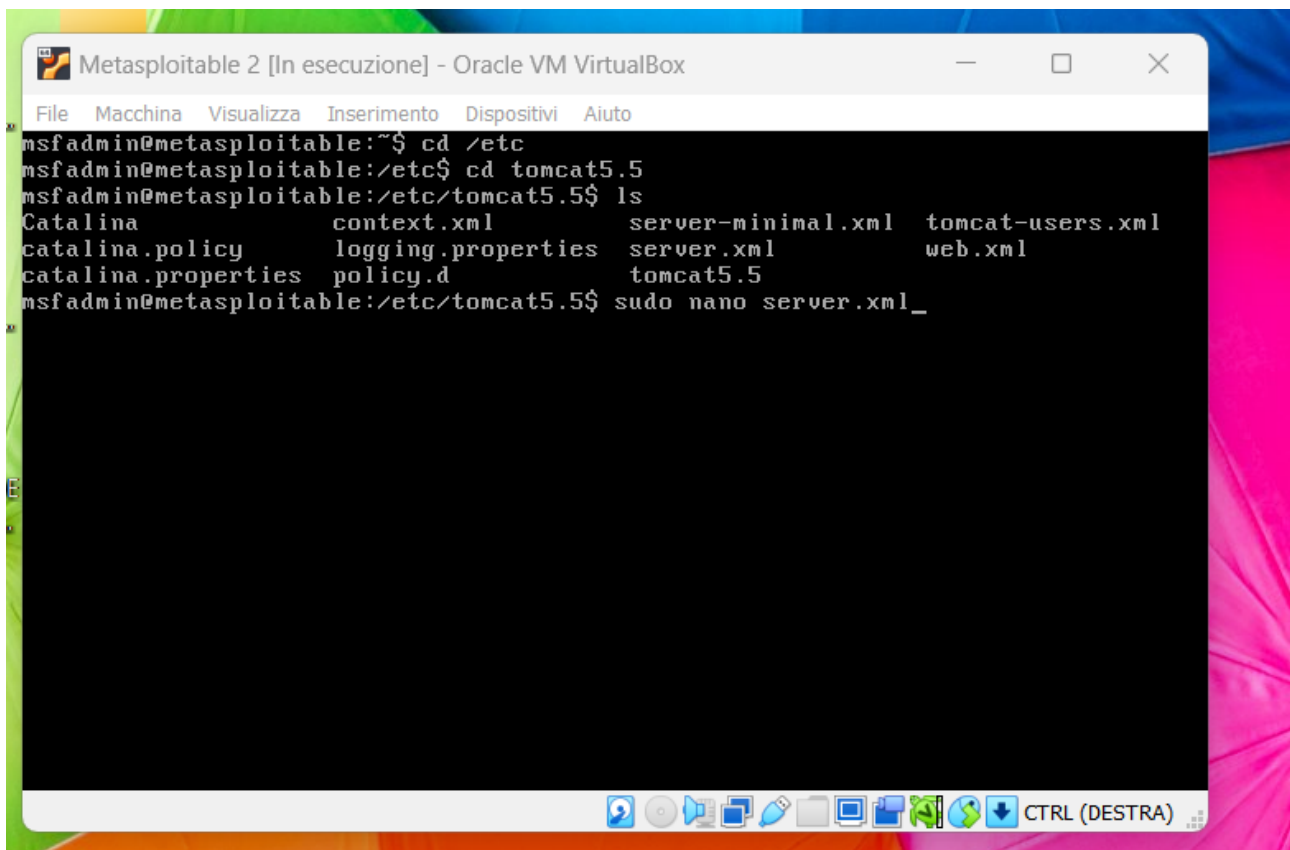
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep Xtightvnc
tcp        0      0 0.0.0.0:5901          0.0.0.0:*            LISTEN
5734/Xtightvnc
tcp        0      0 0.0.0.0:6001          0.0.0.0:*            LISTEN
5734/Xtightvnc
msfadmin@metasploitable:~$
```

**Soluzione:** ora il server VNC ha una password forte, si può accedere solo tramite autenticazione e la password è protetta dalla crittografia, garantendo un maggiore livello di sicurezza.

### Apache Tomcat AJP Connector Request Injection (Ghostcat).

Apache JServ Protocol (AJP) è un protocollo binario che consente il collegamento tra un server web remoto come Apache e un application server come Tomcat. Il connettore AJP serve proprio per far interagire Tomcat con un server Apache. Questa vulnerabilità è dovuta ad una configurazione sbagliata del connettore AJP, in ascolto sulla porta 8009, che permette ad un attaccante di accedere a file sensibili, inviare file JSP (JavaServer Pages) malevoli ed eseguire codici malevoli da remoto sfruttando il connettore AJP. In questo caso AJP accetta connessioni da qualsiasi indirizzo IP, rendendo facile per un attaccante sfruttare questa vulnerabilità.

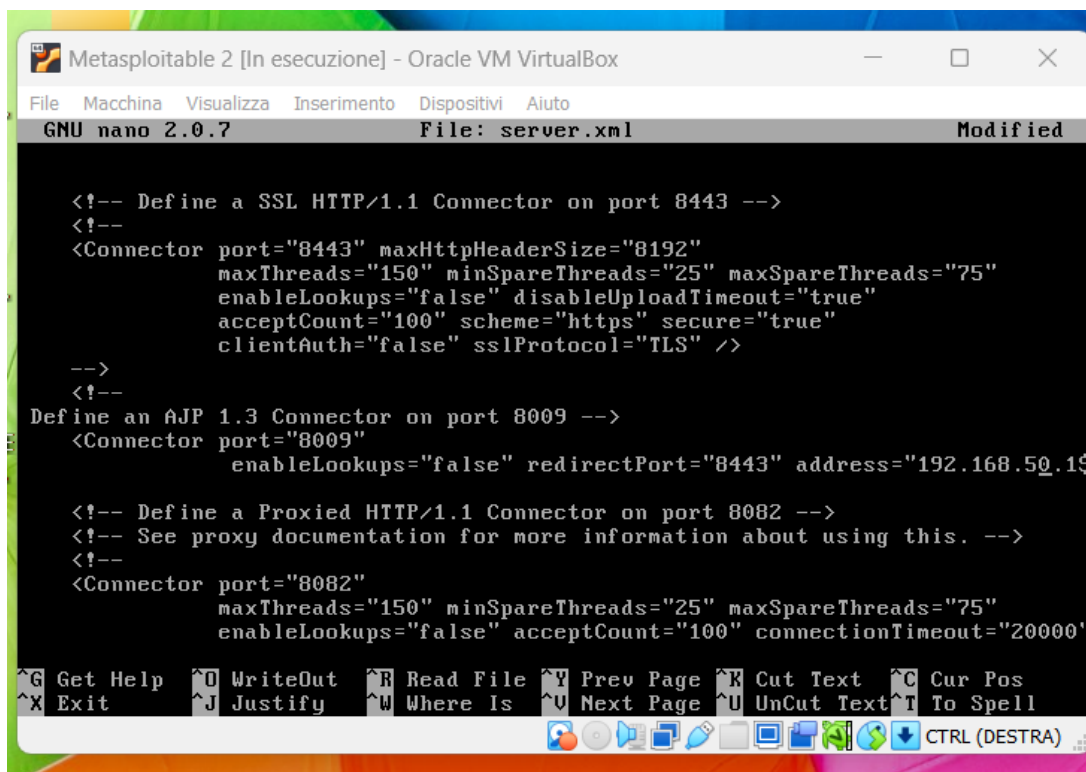
**Remediation actions:** Per prima cosa, ho trovato il file di configurazione di Tomcat per modificarlo. Sono partita dai file di configurazione generali /etc per poi passare ai file di configurazione di Tomcat. Ho trovato il file server.xml, che è il file principale per configurare i vari tipi di connessione e per definire i connettori e l'ho modificato con `sudo nano server.xml`.



```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:~$ cd /etc
msfadmin@metasploitable:/etc$ cd tomcat5.5
msfadmin@metasploitable:/etc/tomcat5.5$ ls
Catalina          context.xml       server-minimal.xml  tomcat-users.xml
catalina.policy   logging.properties  server.xml          web.xml
catalina.properties  policy.d         tomcat5.5
msfadmin@metasploitable:/etc/tomcat5.5$ sudo nano server.xml_
```

Con control + W ho individuato la collocazione esatta della configurazione del connettore AJP nel file di configurazione. A questo punto ho provato due strade per risolvere questa vulnerabilità, ossia applicare delle restrizioni nell'uso di AJP connector per ridurre la

superficie di attacco oppure disabilitare completamente questo connettore. Nel primo caso illustrato dagli screenshot che seguono, ho deciso di limitare l'uso del connettore AJP al solo indirizzo IP indicato, per cui AJP gestirà e risponderà solamente a richieste legate all'indirizzo IP indicato, riducendo significativamente la superficie di attacco e bloccando altri IP che vogliono sfruttare questa vulnerabilità. Questa soluzione è indicata qualora non fosse proprio possibile disabilitare questo AJP connector e fosse necessario mantenerlo. Nei due screenshot che seguono si vede che ho inserito l'IP di Windows per far in modo che AJP connector interagisca solo con l'IP di Windows dato nel file di configurazione.



The screenshot shows a window titled "Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox". Inside, a terminal window is running GNU nano 2.0.7, editing the file "server.xml". The XML content is as follows:

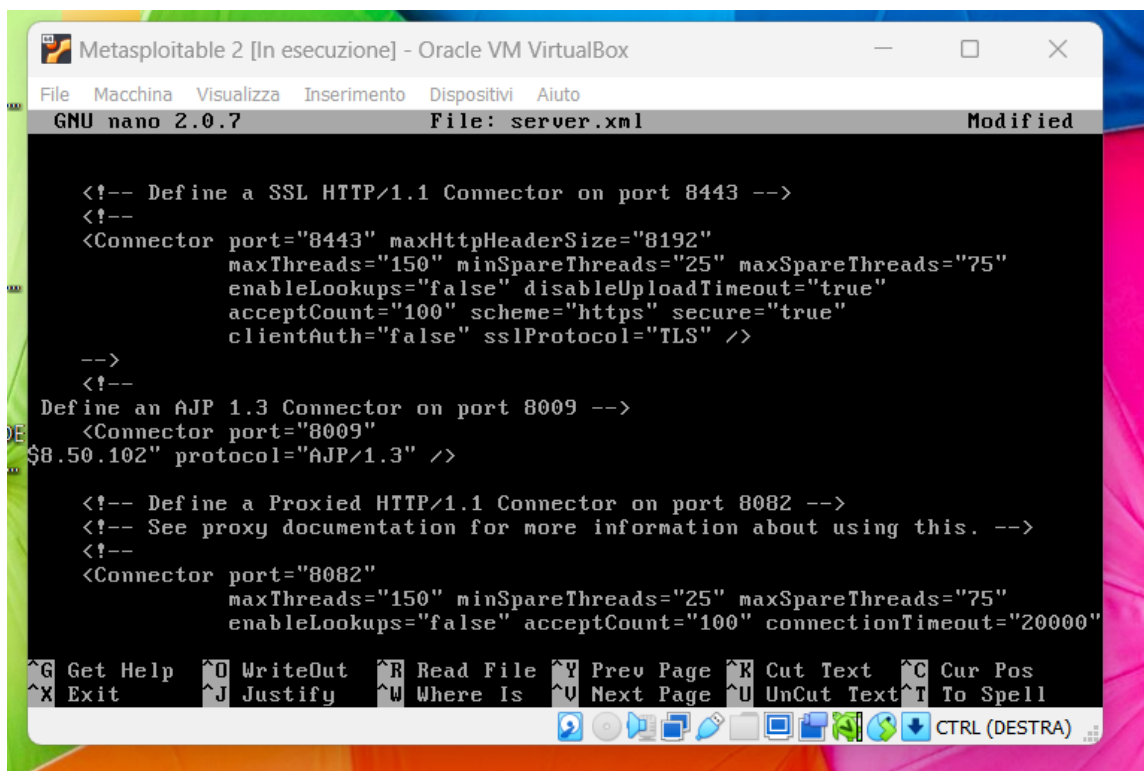
```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" disableUploadTimeout="true"
          acceptCount="100" scheme="https" secure="true"
          clientAuth="false" sslProtocol="TLS" />

-->
<!--
Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
          enableLookups="false" redirectPort="8443" address="192.168.50.15"

-->
<!-- Define a Proxyed HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<!--
<Connector port="8082"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" acceptCount="100" connectionTimeout="20000"

-->
```

The bottom of the terminal window shows a status bar with various keyboard shortcuts like ^G Get Help, ^X Exit, ^O WriteOut, ^J Justify, ^R Read File, ^W Where Is, ^Y Prev Page, ^V Next Page, ^K Cut Text, ^U UnCut Text, ^C Cur Pos, and ^T To Spell. The system tray at the bottom right shows the date and time as 10/10/2014 10:07.



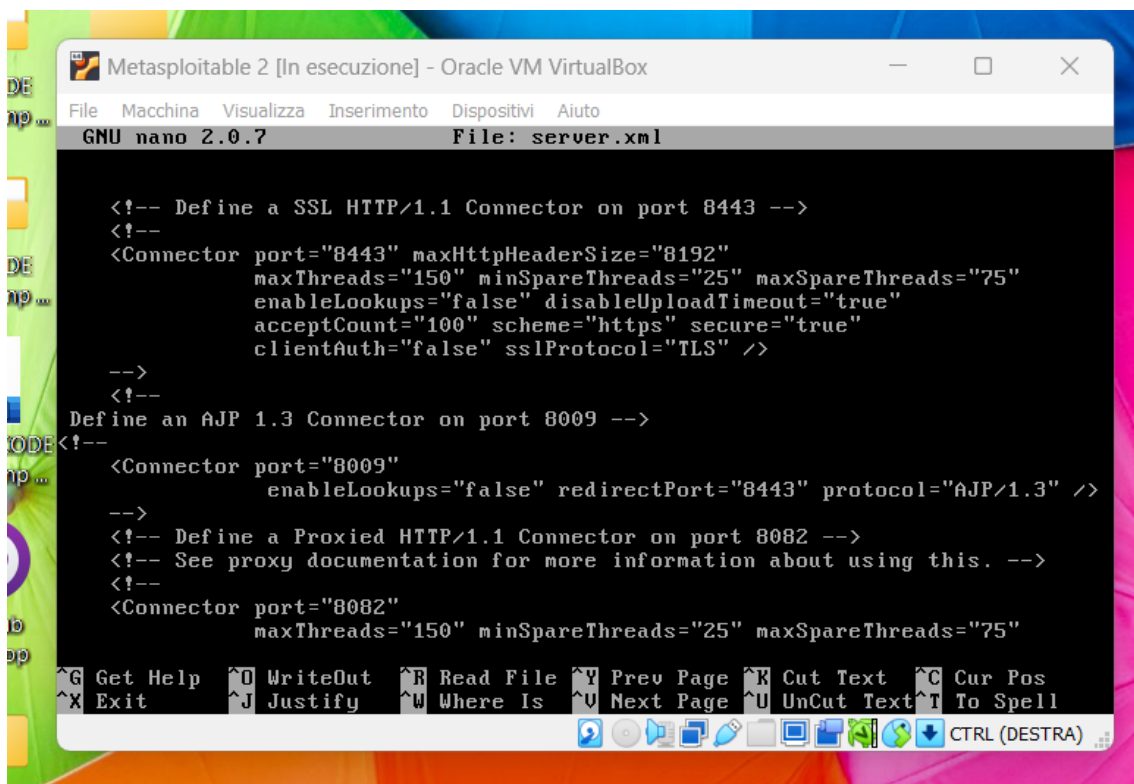
```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: server.xml Modified

<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" disableUploadTimeout="true"
          acceptCount="100" scheme="https" secure="true"
          clientAuth="false" sslProtocol="TLS" />
-->
<!--
Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
$8.50.102" protocol="AJP/1.3" />

<!-- Define a Proxyed HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<!--
<Connector port="8082"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" acceptCount="100" connectionTimeout="20000"
-->

^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

La seconda soluzione è adatta per quei casi in cui non è necessario utilizzare il connettore AJP, perché il connettore AJP viene completamente disabilitato, commentando le sue righe di configurazione con `<!--e -->`. In questo modo, non possono avvenire interazioni usando il protocollo AJP e il connettore AJP in questione, ottenendo una protezione completa da connessioni malevole e proteggendo il connettore AJP. Questa soluzione è indicata solo per chi sa di non avere bisogno del servizio AJP, anche se in ogni momento è possibile modificare la configurazione ed esporsi solamente ad un IP autorizzato. Alla fine, in ogni caso, è sempre consigliabile riavviare Tomcat dopo queste modifiche.



```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: server.xml

<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" disableUploadTimeout="true"
          acceptCount="100" scheme="https" secure="true"
          clientAuth="false" sslProtocol="TLS" />

-->
<!--
Define an AJP 1.3 Connector on port 8009 -->
<!--
<Connector port="8009"
          enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />

-->
<!-- Define a Proxyied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<!--
<Connector port="8082"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

**Soluzione:** modificando la configurazione del connettore AJP in Tomcat, si riesce a risolvere questa vulnerabilità limitando l'accesso al servizio AJP solo ad IP autorizzati oppure disabilitando completamente il connettore AJP.

### Scansione finale con Nessus.

Dopo aver posto in essere delle remediation actions per queste vulnerabilità, ho controllato con una scansione con Nessus se effettivamente queste vulnerabilità erano state corrette. Alla fine, le azioni di rimedio hanno dato i risultati sperati, riducendo il numero di vulnerabilità critiche da 7 a 3. Ora la macchina target Metasploitable 2 ha 3 vulnerabilità critiche, 3 vulnerabilità ad alto rischio, 16 vulnerabilità a medio rischio, 7 a basso rischio e 64 classificate come "info". Allego sia il report sintetico che quello approfondito della scansione generati da Nessus.