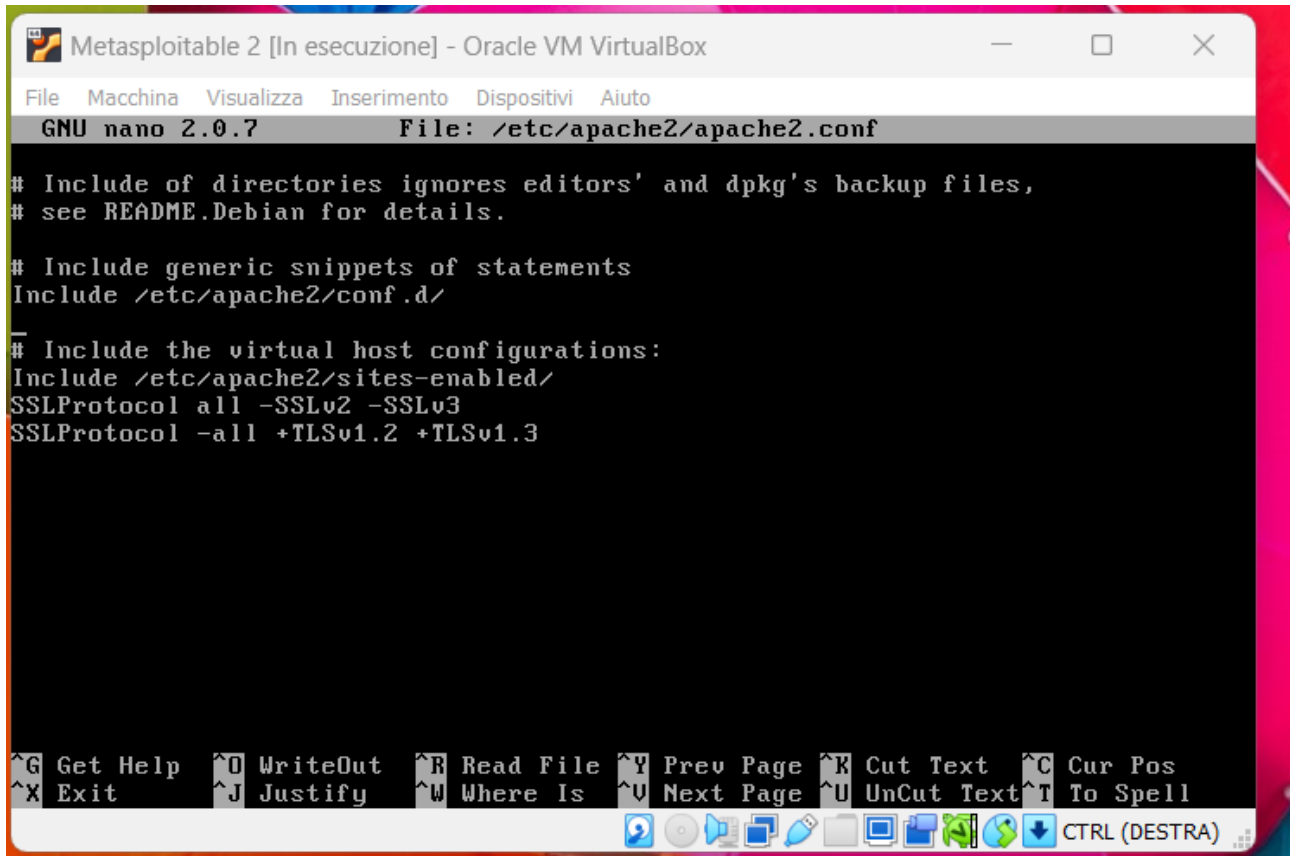


Appendice: tentativi di risoluzione della quinta vulnerabilità.

Ho tentato di correggere la vulnerabilità riguardo all'utilizzo dei protocolli SSLv2 ed SSLv3 seguendo varie strategie. Ho modificato la configurazione del server Apache2 per evitare che utilizzi questi due protocolli SSL.



The screenshot shows a terminal window titled "Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox". The terminal is running the GNU nano 2.0.7 editor, editing the file /etc/apache2/apache2.conf. The visible content of the file is as follows:

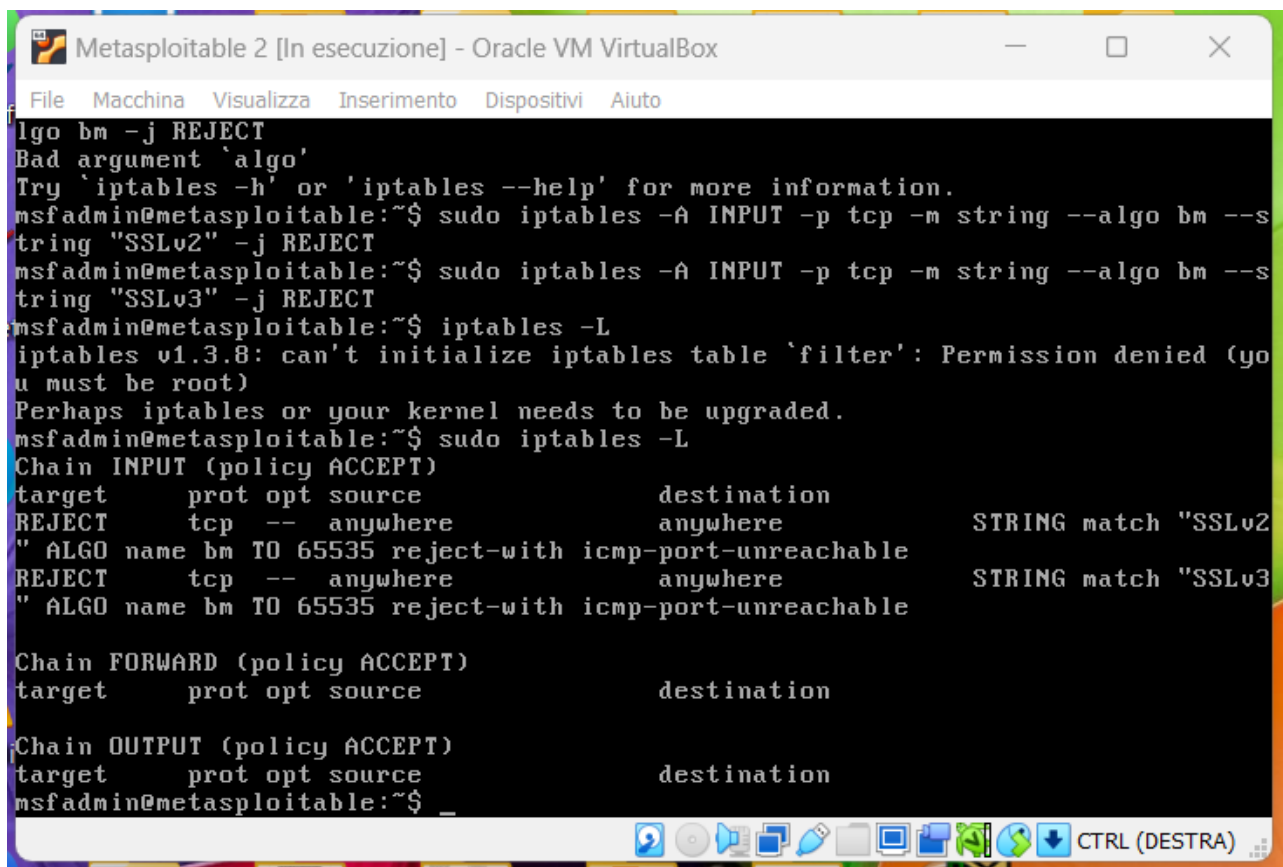
```
# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

# Include generic snippets of statements
Include /etc/apache2/conf.d/

# Include the virtual host configurations:
Include /etc/apache2/sites-enabled/
SSLProtocol all -SSLv2 -SSLv3
SSLProtocol -all +TLSv1.2 +TLSv1.3
```

At the bottom of the terminal, there is a status bar with various keyboard shortcuts: ^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, and a button for CTRL (DESTRA).

Ho provato anche ad inserire una regola nel firewall iptables per rigettare qualsiasi connessione in entrata che utilizza questi protocolli.



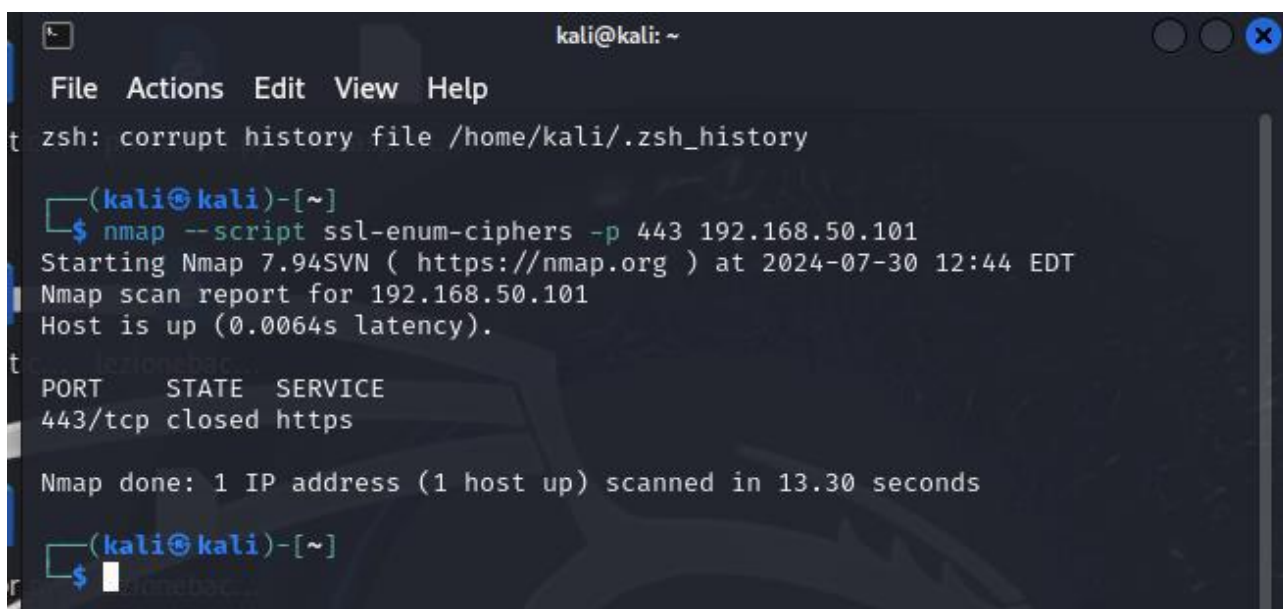
```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

lgo bm -j REJECT
Bad argument 'algo'
Try 'iptables -h' or 'iptables --help' for more information.
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp -m string --algo bm --s
tring "SSLv2" -j REJECT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp -m string --algo bm --s
tring "SSLv3" -j REJECT
msfadmin@metasploitable:~$ iptables -L
iptables v1.3.8: can't initialize iptables table 'filter': Permission denied (yo
u must be root)
Perhaps iptables or your kernel needs to be upgraded.
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
REJECT     tcp  --  anywhere               anywhere           STRING match "SSLv2"
" ALGO name bm TO 65535 reject-with icmp-port-unreachable
REJECT     tcp  --  anywhere               anywhere           STRING match "SSLv3"
" ALGO name bm TO 65535 reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
msfadmin@metasploitable:~$ _
```

Ho cercato di fare un test preliminare per verificare se questi protocolli fossero effettivamente disabilitati e se venissero utilizzati protocolli con livelli di cifratura più sicuri.



```
kali@kali: ~
File  Actions  Edit  View  Help

t zsh: corrupt history file /home/kali/.zsh_history

(kali@kali)-[~]
$ nmap --script ssl-enum-ciphers -p 443 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-30 12:44 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0064s latency).

PORT      STATE SERVICE
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds

(kali@kali)-[~]
$
```

Nonostante questo, non sono riuscita a sistemare questa vulnerabilità con queste remediation actions.