

# **Report remediation Target Metasploitable**

Autore: Fabio Benevento

Il seguente documento descrive le remediation applicate per la risoluzione delle seguenti vulnerabilità critiche:

- 61708 - VNC Server 'password' Password
- 11356 - NFS Exported Share Information Disclosure
- 134862 - Apache Tomcat A JP Connector Request Injection (Ghostcat)
- 51988 - Bind Shell Backdoor Detection
- 20007 - SSL Version 2 and 3 Protocol Detection (2 servizi - parzialmente risolta su 1 servizio)

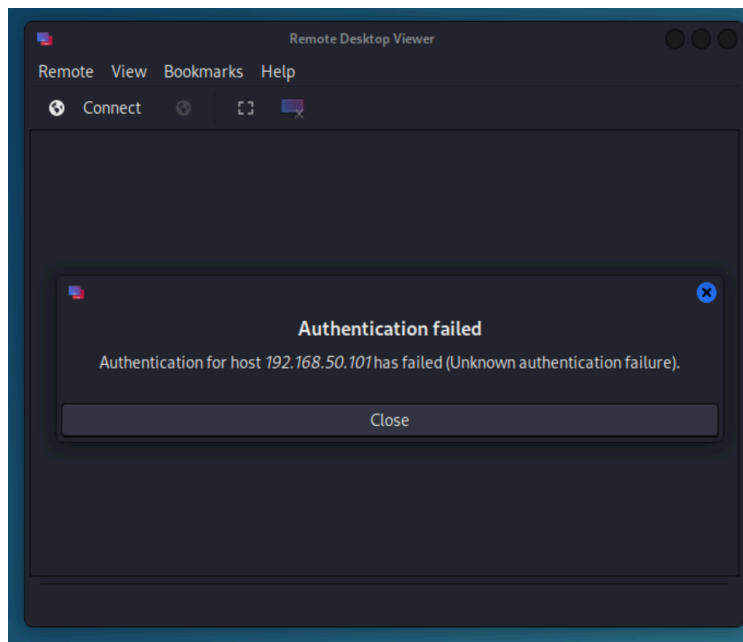
### 61708 - VNC Server 'password' Password

Come indicato dalla descrizione della vulnerabilità, la password del server VNC è la parola 'password', che quindi molto facile da individuare da un hacker.

La risoluzione consiste nel cambiare la password con una più sicura. Per fare ciò, una volta acquisito l'accesso come root, tramite il comando `sudo su`, è stato eseguito il comando `vncpasswd` e configurata una nuova password più sicura.

```
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
```

Connettendosi quindi con un client VNC come in figura (è stato usato il client Vinagre installato in precedenza) e provando ad utilizzare la password 'password' viene infatti ora mostrato un messaggio di errore, cosa che non avveniva in precedenza.

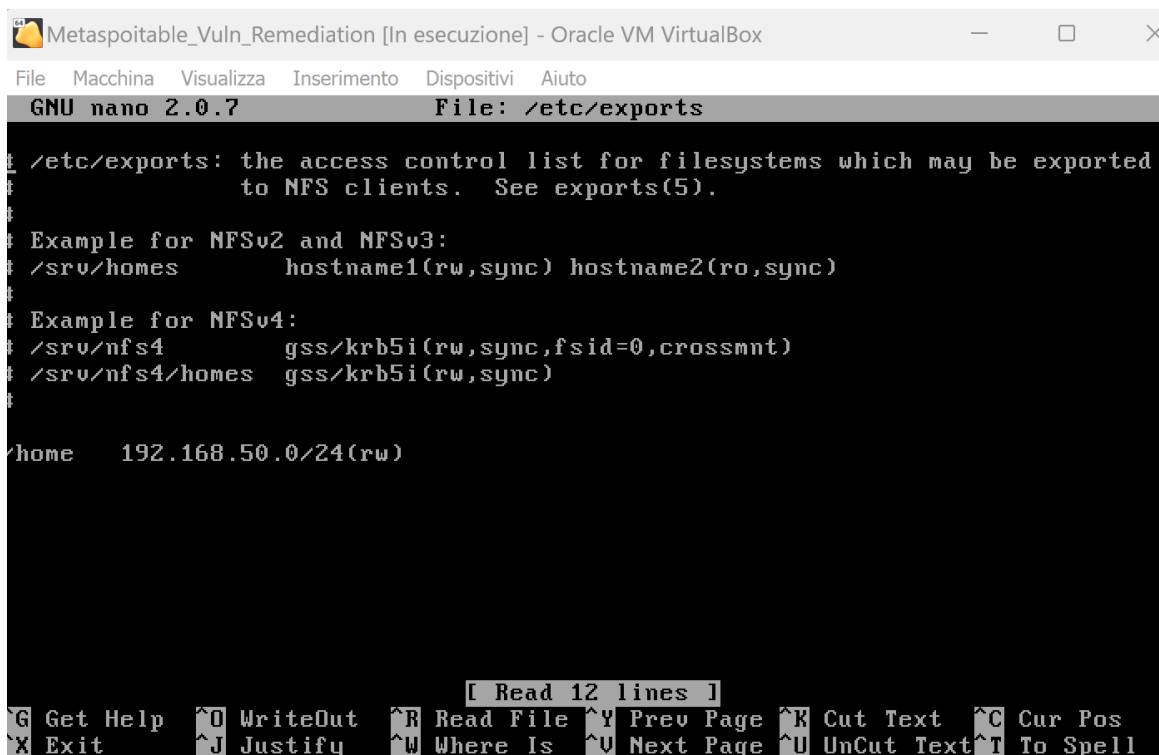


### 11356 - NFS Exported Share Information Disclosure

Il protocollo NFS (porta 2049), è un protocollo per lo scambio e la condivisione di file. La vulnerabilità indica la possibilità da parte di un qualsiasi host remoto di montare il file system ed accederne al contenuto. Il file di configurazione del servizio, costituito dal file `/etc/exports`, prevede infatti la possibilità di montare tutto il file system ('/') da parte di qualsiasi host (\*) in modalità lettura/scrittura ('rw').

```
# /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)
#
# *(rw,sync,no_root_squash,no_subtree_check)
```

La soluzione è costituita nel modificare il file di configurazione `/etc/exports` al fine di limitarne l'accesso alla sola directory `/home` e alle sole macchine appartenenti alla sottorete `192.168.50.x` come mostrato nella figura seguente



```
Metasploitable_Vuln_Remediation [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/exports

/etc/exports: the access control list for filesystems which may be exported
to NFS clients. See exports(5).

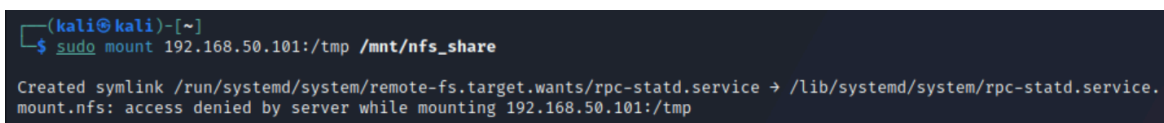
Example for NFSv2 and NFSv3:
/srv/homes hostname1(rw, sync) hostname2(ro, sync)

Example for NFSv4:
/srv/nfs4 gss/krb5i(rw, sync, fsid=0, crossmnt)
/srv/nfs4/homes gss/krb5i(rw, sync)

/home 192.168.50.0/24(rw)

[ Read 12 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
```

Tentando ora di montare il file system da una macchina appartenente alla sottorete `192.168.40.x` (Kali Linux) e/o indicando una cartella non prevista (nel caso in esame la directory `/tmp`) viene quindi mostrato il messaggio di errore seguente.



```
(kali@kali)-[~]
$ sudo mount 192.168.50.101:/tmp /mnt/nfs_share

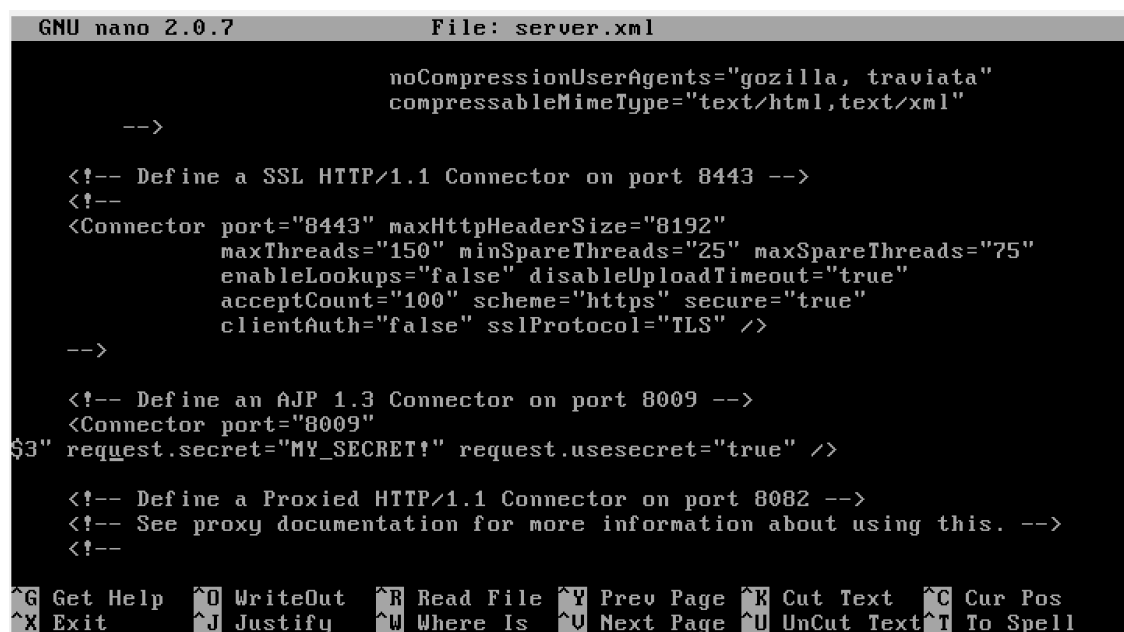
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service → /lib/systemd/system/rpc-statd.service.
mount.nfs: access denied by server while mounting 192.168.50.101:/tmp
```

## 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Questa vulnerabilità è stata individuata in diverse versioni di Tomcat, relativamente al connettore AJP, porta 8009, il quale, se non correttamente configurato, permetterebbe ad un utente di effettuare l'upload di file senza richiesta di nessuna autenticazione. La soluzione indicata da Nessus consiste nel modificare il file di configurazione al fine di richiedere l'autorizzazione dell'utente e/o di effettuare l'upgrade di Tomcat a a 7.0.100, 8.5.51, 9.0.31 o successivo, 9.0.31 o successivo.

La soluzione adottata è stata la prima (modifica del file di configurazione) che permette di mitigare il problema in maniera veloce e con un minor effort rispetto alla soluzione di upgrade di Tomcat, la quale richiederebbe la riconfigurazione ed il test delle applicazione che usufruiscono di Tomcat.

Nello specifico la soluzione è consistita nel modificare la sezione <Connector port="8009"... presente nel file di configurazione di Tomcat (presente sotto /usr/share/tomcat5.5/conf/server.xml) aggiungendo i parametri request.usesecret="true" e request.secret="[CHIAVE]" che rispettivamente abilitano l'uso della chiave segreta e specificano il valore della chiave previsto.



```
GNU nano 2.0.7 File: server.xml

noCompressionUserAgents="gozilla, traviata"
compressableMimeType="text/html,text/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"
request.secret="MY_SECRET!" request.usesecret="true" />

<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<!--
```

Maggiori dettagli sono presenti al seguente indirizzo da cui sono state reperite le informazioni per la risoluzione.

<https://www.tenable.com/blog/cve-2020-1938-ghostcat-apache-tomcat-ajp-file-reading-vulnerability-cnvd-2020-10487>

Di seguito è mostrato per comodità un estratto della pagina.

If your site is not actively using the AJP Connector, simply comment it out from the `/conf/server.xml` file:

```
114
115     <!-- Define an AJP 1.3 Connector on port 8009 -->
116     <!--
117     <Connector protocol="AJP/1.3"
118             address="::1"
119             port="8009"
120             redirectPort="8443" />
121     -->
```

However, if you are using the AJP Connector on your site, you'll need to ensure the AJP Connector contains the **requiredSecret** attribute, which is akin to a password, so it needs to be strong and unique.

```
114
115     <!-- Define an AJP 1.3 Connector on port 8009 -->
116     <Connector protocol="AJP/1.3"
117             address="TOMCAT_IP_ADDRESS"
118             port="8009"
119             redirectPort="8443"
120             requiredSecret="YOUR_AJP_SECRET_GOES_HERE" />
121
```

**UPDATE 02/23/2020:** The above section has been updated to reference the correct attribute, `requiredSecret`.

La soluzione fa comunque riferimento a versioni più recenti rispetto alla versione Tomcat 5.5 della macchina sotto analisi, in cui il parametro per impostare la chiave è diverso (`requestSecret` invece di `request.secret` - vedere parte evidenziata)  
E' stato quindi necessario risalire ai parametri corretti accedendo alla documentazione di Tomcat 5.5 (sezione AJP Connector) al link di seguito

[Apache Tomcat Configuration Reference - The AJP Connector](#)

Il seguente screenshot della pagina mostra i parametri utilizzati

port	The TCP port number on which this <b>Connector</b> will create a server socket and await incoming connections. Your operating system will allow only one server application to listen to a particular port number on a particular IP address.
request.secret	Only requests from workers with this secret keyword will be accepted.
request.shutdownEnabled	If true and a secret has been configured, a correctly formatted AJP request (that includes the secret) will shutdown the Tomcat instance associated with this connector. This is set to <code>false</code> by default.
request.useSecret	If set to true, then a random value for <code>request.secret</code> will be generated. It is for use with <code>request.shutdownEnabled</code> . This is set to <code>false</code> by default.

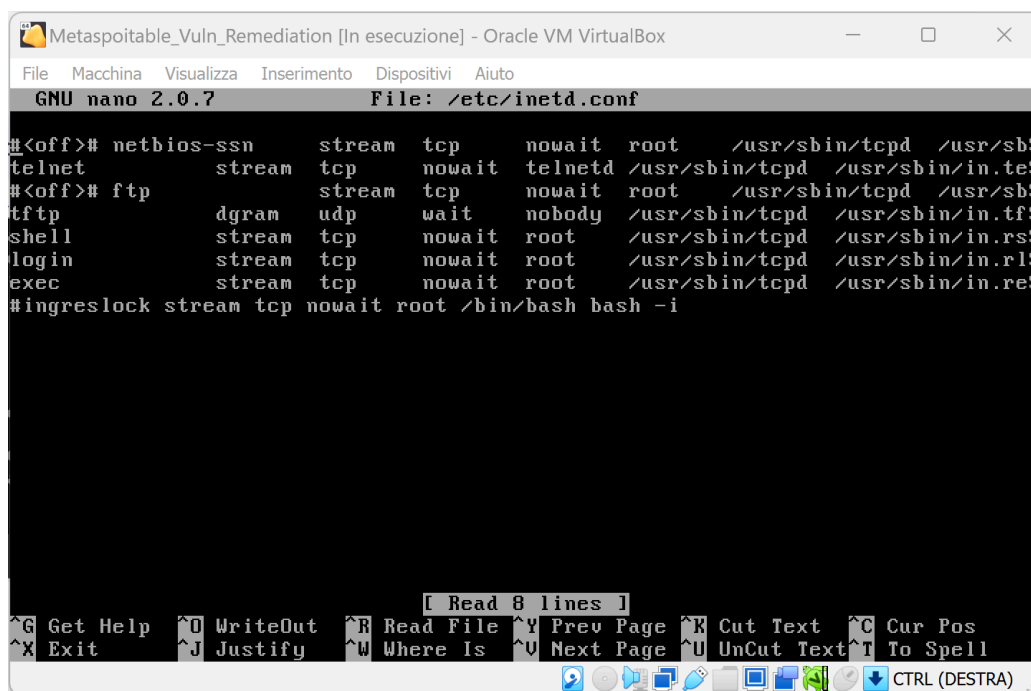
## 51988 - Bind Shell Backdoor Detection

La vulnerabilità riguarda la presenza di una backdoor aperta sulla porta 1524 che consente l'accesso non autorizzato al sistema ad utenti malevoli.

La porta 1524 sul sistema in esame è legata al meccanismo ingreslock del database Ingres, il quale è avviato come servizio dal processo dal demone `inetd` la cui configurazione è presente nel file `/etc/inetd.conf`

### - Soluzione Adottata:

La soluzione adottata è costituita dal modificare il file `/etc/inetd.conf` commentando la riga `'ingreslock stream tcp nowait root /bin/bash bash -i'` al fine di eliminare la backdoor al riavvio del servizio



```
Metasploitable_Vuln_Remediation [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/inetd.conf

#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/tcpd
telnet      stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp             stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
tftp        dgram   udp      wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tftpd
shell       stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
login       stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
exec        stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
#ingreslock stream  tcp      nowait  root    /bin/bash bash -i

[ Read 8 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   ^V Next Page  ^U UnCut Text  ^T To Spell
CTRL (DESTRA)
```

### - Soluzione alternativa tramite iptable:

In alternativa sarebbe stato possibile adottare apposite regole di firewall per limitare l'accesso alla porta 2049 come indicato di seguito.

```
iptables -A INPUT ! -s 192.168.50.0/24 -p udp --dport 2049 -m
state --state NEW,ESTABLISHED -j DROP
```

```
iptables -A INPUT ! -s 192.168.50.0/24 -p tcp --dport 2049 -m
state --state NEW,ESTABLISHED -j DROP
iptables -A OUTPUT ! -d 192.168.50.0/24 -p udp --ports 2049 -m
state --state NEW,ESTABLISHED -j DROP
iptables -A OUTPUT ! -d 192.168.1.0/24 -p tcp --ports 2049 -m
state --state NEW,ESTABLISHED -j DROP
```

## 20007 - SSL Version 2 and 3 Protocol Detection

La vulnerabilità rilevata consiste nell'adozione da parte di alcuni servizi dei protocolli di crittografia SSLv2 e SSLv3, i quali sono stati dichiarati non più sicuri e sostituiti in favore di altri protocolli come TLS.

Nella macchina in esame, come evidenziato nel report dettagliato fornito da Nessus, i servizi affetti da questa vulnerabilità sono 2:

- SMTP (porta 25)
- PostgreSQL (porta 5432 - database)

La soluzione consiste nel configurare correttamente questi servizi al fine di limitarli all'utilizzo del protocollo solo TLS per la crittografia

### Postgresql

La versione di postgresql presente sulla macchina è la 8.3. La modifica ha riguardato la sezione "Security e authentication" del file di configurazione presente sotto /etc/postgresql/8.3/main/postgresql.conf.

Nello specifico è stato configurato il parametro `ssl_ciphers` secondo quanto segue:

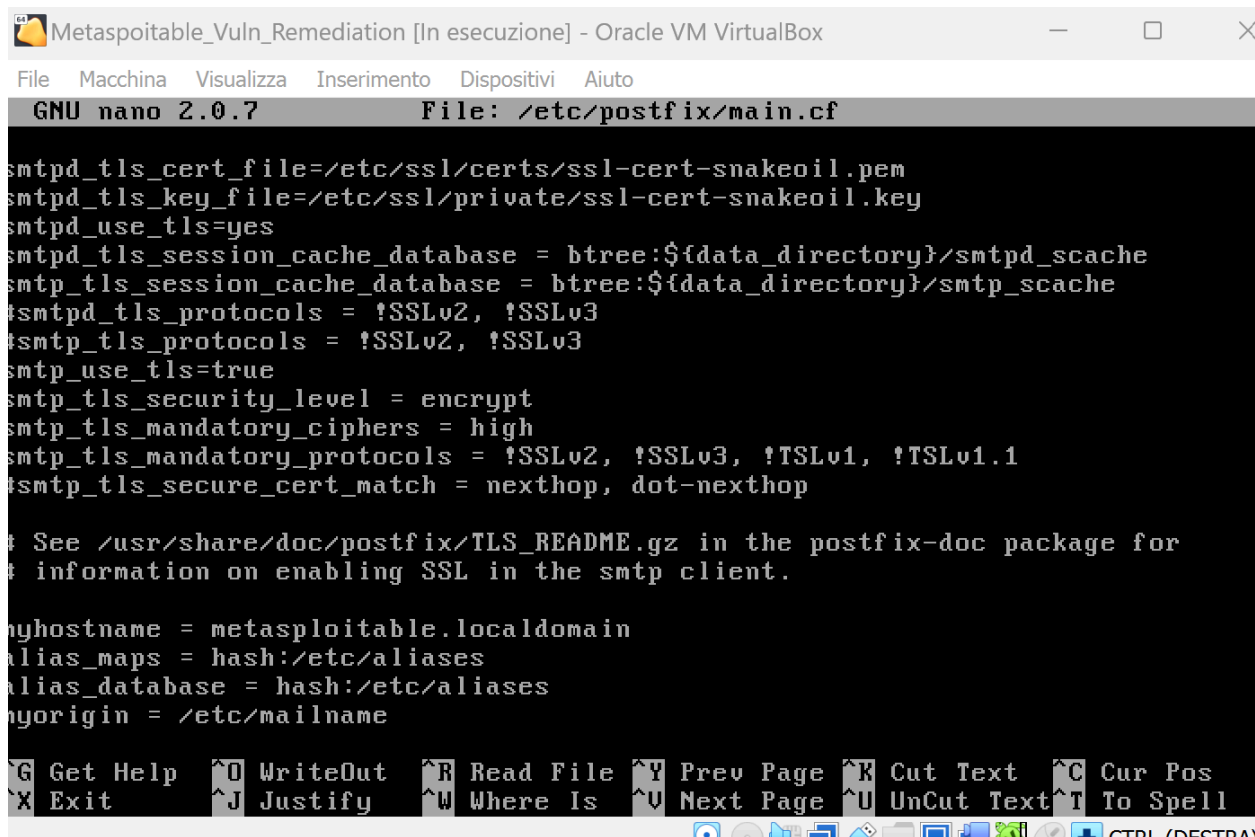
```
# - Security and Authentication -
#authentication_timeout = 1min          # 1s-600s
ssl = true                             # (change requires restart)
ssl_ciphers = 'HIGH:MEDIUM:+3DES:!aNULL:!SSLv2:!SSLv3' # allowed SSL ciphers
                                                # (change requires restart)
```



## SMTP

Il servizio SMTP nella macchina analizzata è fornito dal server di posta Postfix, versione 2.5.1

Per la risoluzione è stato modificato il file di configurazione di Postfix presente sotto `/etc/postfix/main.cf` effettuando diversi tentativi di intervento agendo sui parametri `smtp_tls_security_level`, `smtp_tls_mandatory_ciphers`, `smtp_tls_mandatory_protocols` come evidenziato in figura



The screenshot shows a terminal window titled "Metasploitable\_Vuln\_Remediation [In esecuzione] - Oracle VM VirtualBox". The terminal is running the GNU nano 2.0.7 text editor, editing the file `/etc/postfix/main.cf`. The configuration file contains the following settings:

```
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
smtpd_tls_protocols = !SSLv2, !SSLv3
smtp_tls_protocols = !SSLv2, !SSLv3
smtp_use_tls=true
smtp_tls_security_level = encrypt
smtp_tls_mandatory_ciphers = high
smtp_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1
smtp_tls_secure_cert_match = nexthop, dot-nexthop

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

myhostname = metasploitable.localdomain
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
```

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`, `^U Next Page`, `^U UnCut Text`, `^T To Spell`.

secondo quanto indicato nella documentazione ufficiale presente al seguente link [https://www.postfix.org/postconf.5.html#smtp\\_tls\\_mandatory\\_protocols](https://www.postfix.org/postconf.5.html#smtp_tls_mandatory_protocols) di cui si riporta uno screenshot per comodità.

← ↻ 🏠 [https://www.postfix.org/postconf.5.html#smtp\\_tls\\_mandatory\\_protocols](https://www.postfix.org/postconf.5.html#smtp_tls_mandatory_protocols)

parameter. The default matching rule is that a server certificate matches when its name is equal to or is a sub-  
for systems delivering mail to the Internet.

Examples:

```
# No TLS. Formerly: smtp_use_tls=no and smtp_enforce_tls=no.  
smtp_tls_security_level = none  
  
# Opportunistic TLS.  
smtp_tls_security_level = may  
# Do not tweak opportunistic ciphers or protocols unless it is essential  
# to do so (if a security vulnerability is found in the SSL library that  
# can be mitigated by disabling a particular protocol or raising the  
# cipher grade).  
smtp_tls_ciphers = medium  
smtp_tls_protocols = >=TLSv1  
# Legacy (Postfix < 3.6) syntax:  
smtp_tls_protocols = !SSLv2, !SSLv3  
  
# Mandatory (high-grade) TLS encryption.  
smtp_tls_security_level = encrypt  
smtp_tls_mandatory_ciphers = high  
  
# Authenticated TLS 1.2 or better matching the nexthop domain or a  
# subdomain.  
smtp_tls_security_level = secure  
smtp_tls_mandatory_ciphers = high  
smtp_tls_mandatory_protocols = >=TLSv1.2  
smtp_tls_secure_cert_match = nexthop, dot-nexthop  
  
# Certificate fingerprint verification (Postfix ≥ 2.5).  
# The CA-less "fingerprint" security level only scales to a limited  
# number of destinations. As a global default rather than a per-site  
# setting, this is practical only when mail for all recipients is sent  
# to a central mail hub.  
relayhost = [mailhub.example.com]  
smtp_tls_security_level = fingerprint  
smtp_tls_mandatory_protocols = >=TLSv1.2  
smtp_tls_mandatory_ciphers = high  
smtp_tls_fingerprint_cert_match =  
    3D:95:34:51:....:40:99:C0:C1  
    EC:3B:2D:B0:....:A3:9D:72:F6
```

This feature is available in Postfix 2.3 and later.

La remediation adottata non è risultata al momento risolutiva.