

# Passaggi di Remediation per le Vulnerabilità Identificate


## Introduzione

- Questo documento descrive i passaggi intrapresi per risolvere le vulnerabilità critiche identificate nella scansione iniziale eseguita su un server con IP 192.168.50.101.

## Riepilogo della Scansione Iniziale

La scansione iniziale ha identificato diverse vulnerabilità critiche. Di seguito sono riportate le vulnerabilità specifiche identificate:

- 1) NFS Exported Share Information Disclosure;
- 2)VNC Server 'password' Password;
- 3) Apache Tomcat AJP Connector Request Injection (Ghostcat);
- 4) SSL Version 2 and 3 Protocol Detection;
- 5) Bind Shell Backdoor Detection;
- 6)Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection
<input type="checkbox"/>	CRITICAL	...	...	 SSL (Multiple Issues)

## 1) NFS Exported Share Information Disclosure

### Descrizione del Problema:

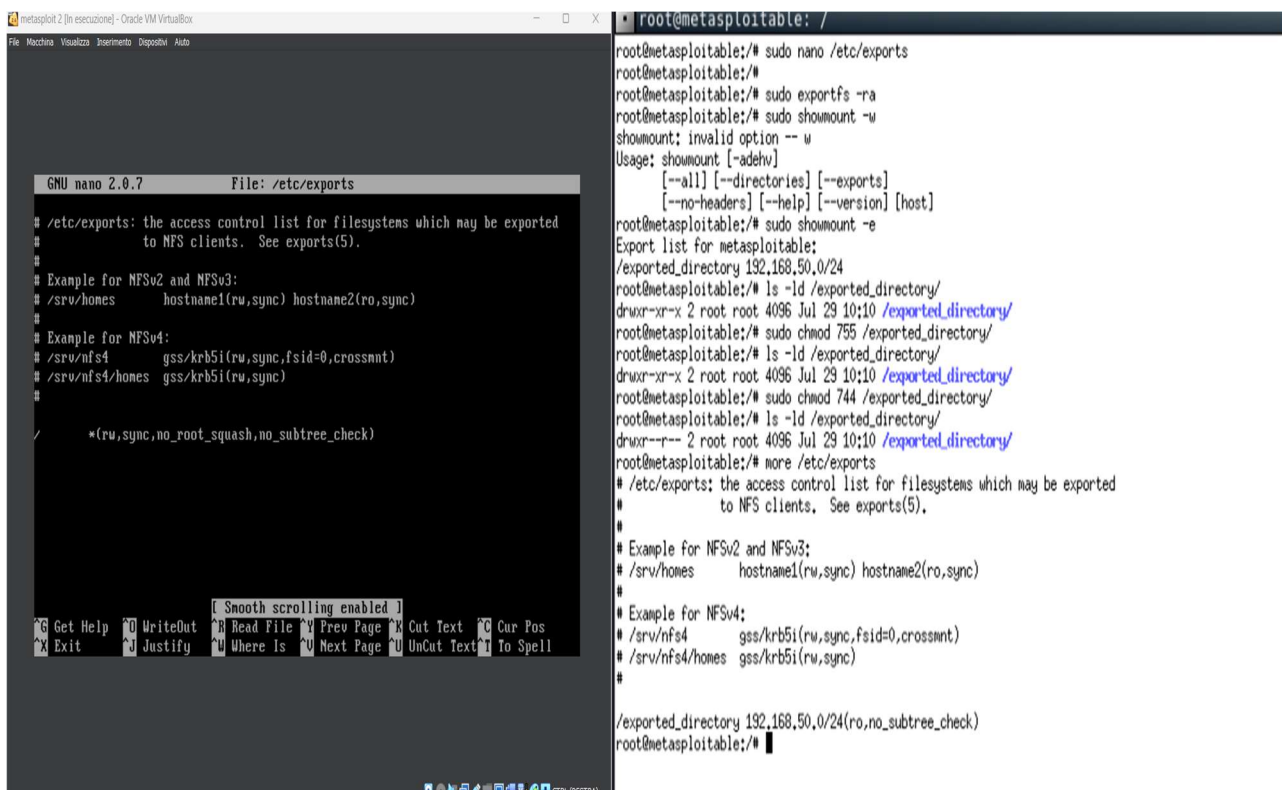
Questa vulnerabilità si verifica quando le condivisioni NFS (Network File System) sono configurate in modo tale da consentire l'accesso non autorizzato alle informazioni condivise. Gli attaccanti possono sfruttare questa configurazione per accedere a dati sensibili.

### Passaggi di Remediation:

- Aggiornamento delle impostazioni di condivisione NFS per limitare l'accesso solo agli utenti autorizzati.
- Configurazione dei permessi corretti per le condivisioni NFS.
- Comando per modifica file del servizio di condivisione: ``sudo nano /etc/exports`` e aggiornamento delle regole di esportazione.
- Nel file è stato poi modificato la riga dove era specificato quale era la cartella da condividere e i privilegi, la modifica è stata la seguente :

``/exported_directory 192.168.50.100(ro, no_subtree_check)``

- Riavvio del servizio NFS: ``sudo exportfs -ra``.
- Con il comando ``showmount -e`` si è visto dopo il riavvio, quale è la cartella condivisa aggiornata.
- Screen vulnerabilità prima e dopo:



```
metasploit 2 [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)
#
/*(rw,sync,no_root_squash,no_subtree_check)

[ Smooth scrolling enabled ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^X Cut Text ^C Cur Pos
^X Exit ^J Justify ^U Where Is ^V Next Page ^U UnCut Text ^I To Spell

root@metasploitable: /
root@metasploitable:/# sudo nano /etc/exports
root@metasploitable:/#
root@metasploitable:/# sudo exportfs -ra
root@metasploitable:/# sudo showmount -w
showmount: invalid option -- w
Usage: showmount [-adehv]
        [--all] [--directories] [--exports]
        [--no-headers] [--help] [--version] [host]
root@metasploitable:/# sudo showmount -e
Export list for metasploitable:
/exported_directory 192.168.50.0/24
root@metasploitable:/# ls -ld /exported_directory/
drwxr-xr-x 2 root root 4096 Jul 29 10:10 /exported_directory/
root@metasploitable:/# sudo chmod 755 /exported_directory/
root@metasploitable:/# ls -ld /exported_directory/
drwxr-xr-x 2 root root 4096 Jul 29 10:10 /exported_directory/
root@metasploitable:/# sudo chmod 744 /exported_directory/
root@metasploitable:/# ls -ld /exported_directory/
drwxr--r-- 2 root root 4096 Jul 29 10:10 /exported_directory/
root@metasploitable:/# more /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)
#
/exported_directory 192.168.50.0/24(ro,no_subtree_check)
root@metasploitable:/#
```

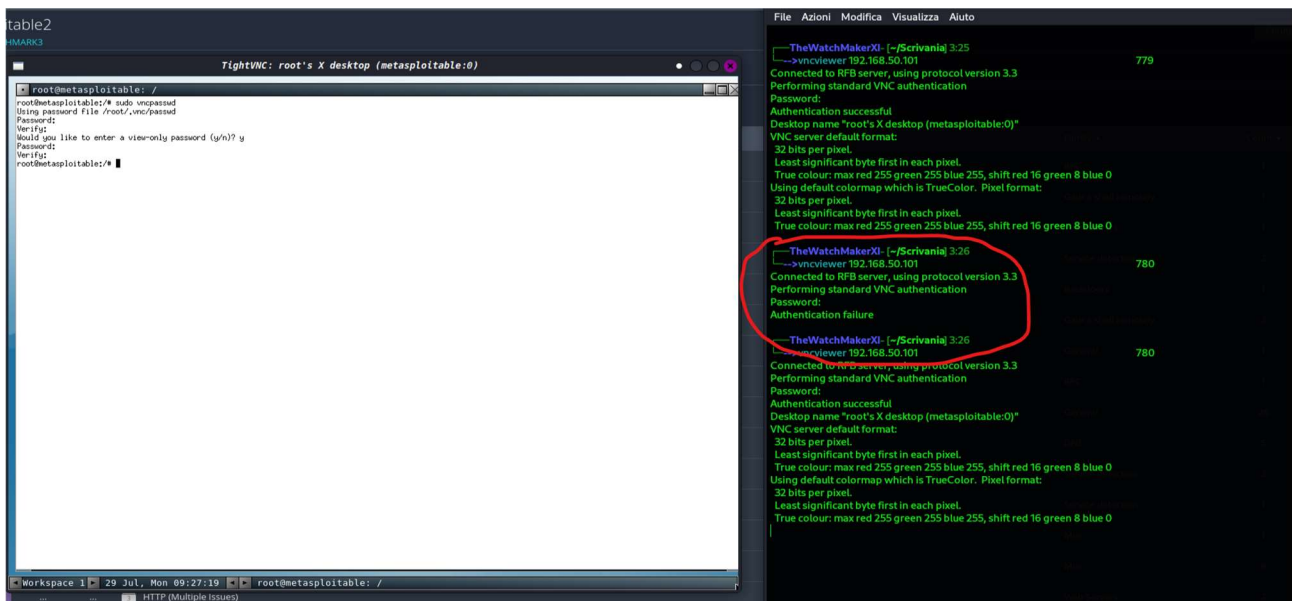
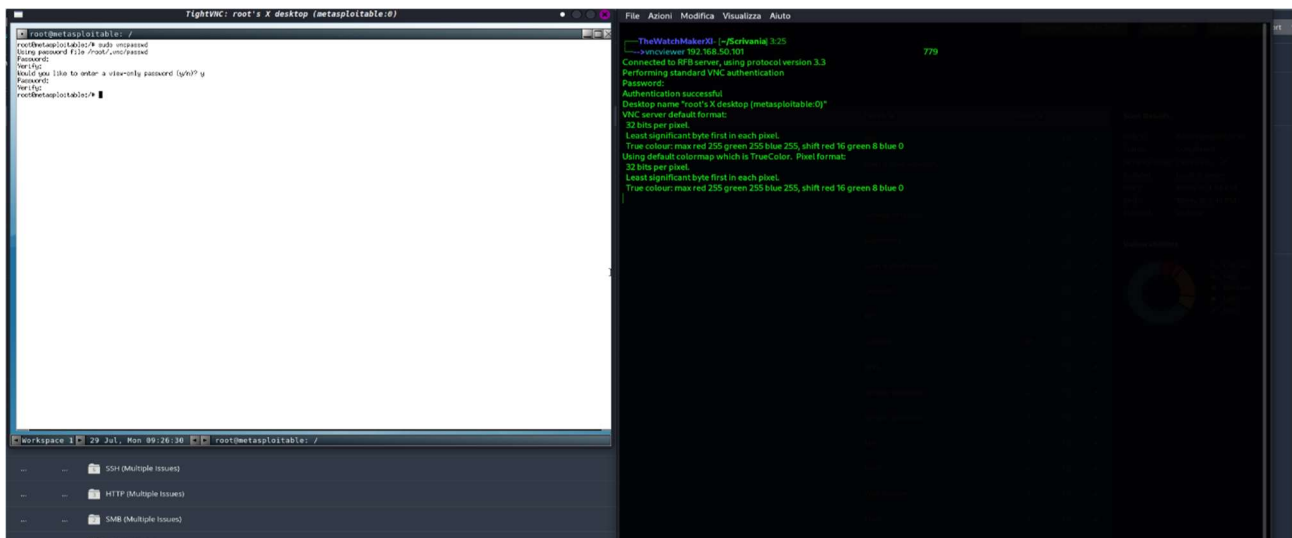
## 2) Password del Server VNC 'password'

### Descrizione del Problema:

- Questa vulnerabilità si verifica quando un server VNC (Virtual Network Computing) è configurato con una password debole o predefinita, consentendo agli attaccanti di accedere facilmente al server remoto.

### Passaggi di Remediation:

- Modifica della password predefinita del server VNC.
- Configurazione di una password complessa e sicura.
- Comando per cambio password: `'sudo vncpasswd'` per cambiare la password VNC.
- Verifica e screen:
  - Connessione al server VNC per assicurarsi che la nuova password sia richiesta e che sia complessa.



### 3) Iniezione di Richieste del Connettore AJP di Apache Tomcat (Ghostcat)

**Descrizione del Problema:**

- Ghostcat è una vulnerabilità che permette l'iniezione di richieste tramite il connettore AJP di Apache Tomcat, consentendo agli attaccanti di leggere il contenuto dei file web applicativi e, in alcuni casi, di eseguire codice arbitrario.

- Passaggi di Remediation:

- Disabilitazione del connettore AJP commentando la riga di attivazione del connettore nel file `server.xml`, per accedere in scrittura al file si è usato il comando

**'sudo nano /etc/tomcat/server.xml'.**

- La riga da commentare per disabilitare il connettore AJP è:

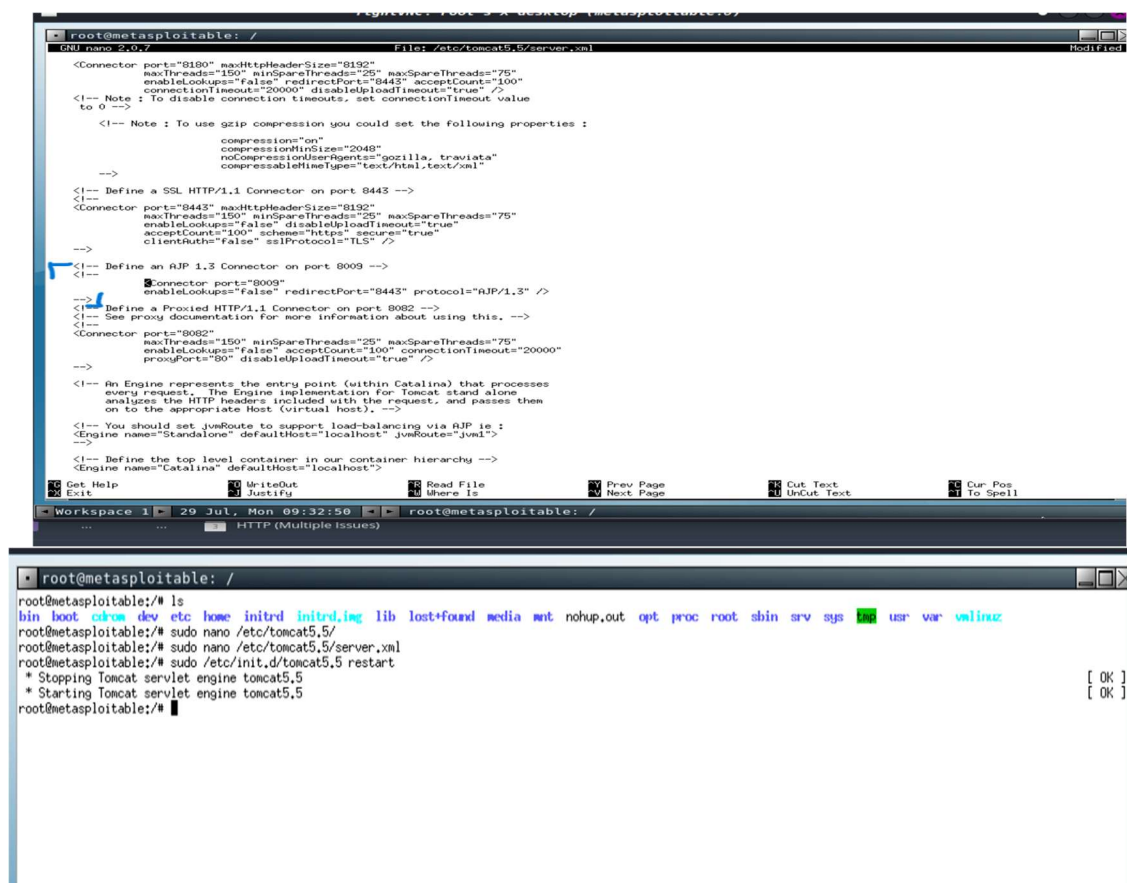
```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

commentandola così:

```
<!--
    <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
-->
```

-Infine con il comando **'sudo /etc/init.d/tomcat5.5 restart'**, si riavvia il servizio con le modifiche apportate al file 'server.xml'.

- Screen:



#### 4) Rilevazione del Protocollo SSL Versione 2 e 3

##### *Descrizione del Problema*

- Le versioni 2 e 3 del protocollo SSL (Secure Sockets Layer) sono obsolete e vulnerabili a diversi tipi di attacchi. L'uso di questi protocolli mette a rischio la sicurezza delle comunicazioni.

##### *Passaggi di Remediation*

Per la risoluzione temporanea del problema, ho configurato due regole firewall tramite iptables. Non essendo riuscito a disattivare né a attivare TLS 1.x, ho preferito non rendere accessibili i servizi sulle porte associate. I passaggi seguiti sono i seguenti:

-Impostazione delle Regole del Firewall, ho configurato le regole del firewall per bloccare l'accesso alle porte specifiche:

```
'sudo iptables -A INPUT -p tcp --dport 25 -j REJECT'
```

```
'sudo iptables -A INPUT -p tcp --dport 5432 -j REJECT'
```

- Salvataggio delle Regole del Firewall: Per assicurarmi che le regole del firewall siano persistenti dopo un riavvio, ho utilizzato il comando iptables-save per salvare le regole in un file:

```
'sudo iptables-save > /etc/iptables/rules.v4'
```

-Per rendere Permanenti le Regole del Firewall ho creato un file eseguibile nel percorso /etc/network/if-pre-up.d/iptables con il seguente contenuto per garantire che le regole del firewall vengano applicate automaticamente ad ogni riavvio del sistema:

```
'#!/bin/sh
```

```
iptables-restore < /etc/iptables/rules.v4'
```

una volta creato l'ho reso eseguibile con il comando:

```
'sudo chmod +x /etc/network/if-pre-up.d/iptables'
```

Screen:

```
msfadmin@metasploitable:/etc/network/if-pre-up.d$ cd
msfadmin@metasploitable:~$ more /etc/iptables/rules.v4
# Generated by iptables-save v1.3.8 on Mon Jul 29 17:12:15 2024
*filter
:INPUT ACCEPT [544:96810]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [835:121163]
- A INPUT -p tcp -m tcp --dport 25 -j REJECT --reject-with icmp-port-unreachable
- A INPUT -p tcp -m tcp --dport 5432 -j REJECT --reject-with icmp-port-unreachabl
e
COMMIT
# Completed on Mon Jul 29 17:12:15 2024
msfadmin@metasploitable:~$
```

```
#!/bin/sh
iptables-restore < /etc/iptables/rules.v4
```

## 5) Rilevazione della Backdoor Bind Shell

### Descrizione del Problema

Una bind shell backdoor permette agli attaccanti di ottenere l'accesso remoto a un sistema attraverso una shell di comando. Questa vulnerabilità è molto pericolosa poiché consente il controllo completo del sistema.

*Passaggi di Remediation : Rimozione della bind shell backdoor.*

-Identificazione del Processo Associato alla Porta 1524 ho utilizzato il comando:

```
'sudo netstat -tulnp | grep 1524'
```

per rilevare il processo associato alla porta 1524. Questo mi ha permesso di trovare il PID del processo, che era 4431.

- Identificazione del File Eseguibile del Processo con il comando:

```
'ls -l /proc/4431/exe'
```

ho individuato il percorso del file eseguibile del processo, che risultava essere:

```
/usr/sbin/xinetd
```

- Arresto del Processo ho terminato il processo con il comando:

```
'sudo kill -9 4431'
```

successivamente, ho eseguito nuovamente il comando netstat per assicurarmi che il processo fosse effettivamente terminato.

- Rimozione del File Eseguibile Per prevenire il riavvio del processo che attivava la backdoor, ho eliminato il file eseguibile con il comando:

```
'sudo rm /usr/sbin/xinetd'
```

Questi passaggi hanno garantito la rimozione della backdoor e impedito la sua riattivazione, ripristinando la sicurezza del sistema.

Screen:



```
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep 1524
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
4431/xinetd
msfadmin@metasploitable:~$ sudo ls -l /proc/4431/exe
lrwxrwxrwx 1 root root 0 2024-07-29 08:35 /proc/4431/exe -> /usr/sbin/xinetd
msfadmin@metasploitable:~$ sudo ps -p 4431 -o comm,args
COMMAND
xinetd      /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_
msfadmin@metasploitable:~$

msfadmin@metasploitable:~$ sudo ls -l /proc/4431/exe
lrwxrwxrwx 1 root root 0 2024-07-29 08:35 /proc/4431/exe -> /usr/sbin/xinetd
msfadmin@metasploitable:~$ sudo kill -9 4431
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep 1524
msfadmin@metasploitable:~$ sudo rm /usr/sbin/xinetd
msfadmin@metasploitable:~$ cd /usr/sbin
msfadmin@metasploitable:/usr/sbin$ ls | grep xinetd
msfadmin@metasploitable:/usr/sbin$ ls
```

## 6)Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

### Descrizione del Problema

Questa vulnerabilità compromette la sicurezza dei sistemi crittografici, inclusi chiavi SSH, certificati SSL, e altre chiavi utilizzate per la crittografia. Le chiavi generate con la versione difettosa di OpenSSL non sono casuali come dovrebbero essere, rendendole prevedibili e quindi vulnerabili ad attacchi di forza bruta o altri tipi di compromissione.

*Passaggi di Remediation: Per risolvere questa vulnerabilità, è necessario rigenerare tutto il materiale crittografico sul sistema*

- Identificare la versione di OpenSSL con il comando:

***'openssl version -a'***

-Installare i Pacchetti aggiornati di sul sistema con i comandi:

***'sudo apt-get update '***

***'sudo apt-get upgrade'***

-Eliminare le Chiavi Interessate con il comando:

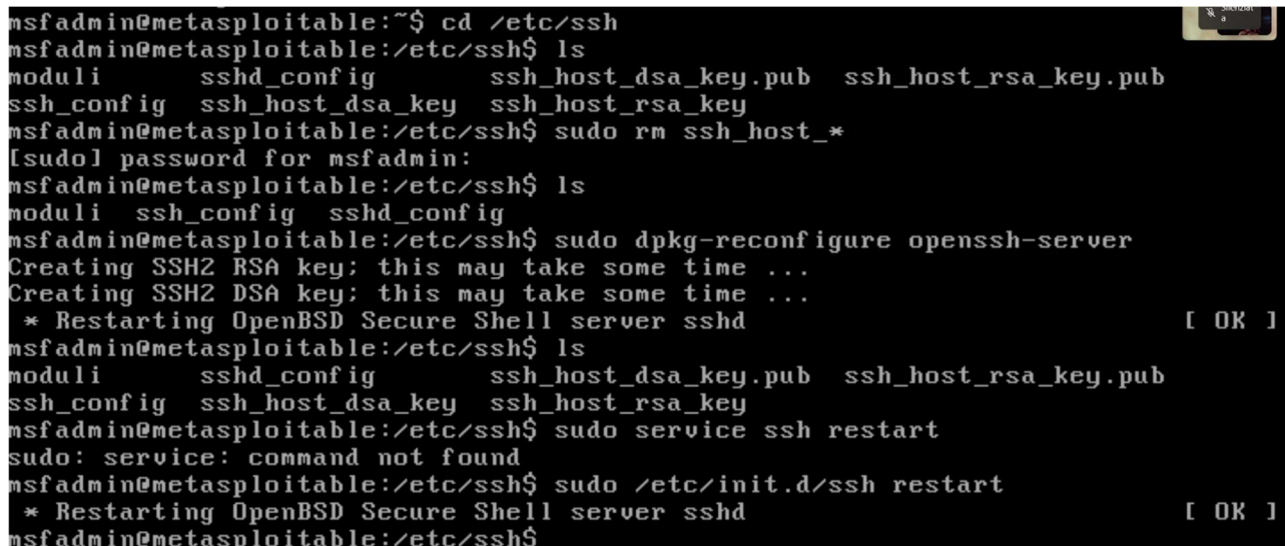
***'sudo rm /etc/ssh/ssh\_host\_\****

-Rigenerare le chiavi SSH con il comando:

***'sudo dpkg-reconfigure openssh-server'***

-Riavvio dei servizi con il comando:

***'sudo /etc/init.d/ssh restart'***



```
msfadmin@metasploitable:~$ cd /etc/ssh
msfadmin@metasploitable:/etc/ssh$ ls
moduli      sshd_config      ssh_host_dsa_key.pub  ssh_host_rsa_key.pub
ssh_config  ssh_host_dsa_key  ssh_host_rsa_key
msfadmin@metasploitable:/etc/ssh$ sudo rm ssh_host_*
[sudo] password for msfadmin:
msfadmin@metasploitable:/etc/ssh$ ls
moduli  ssh_config  sshd_config
msfadmin@metasploitable:/etc/ssh$ sudo dpkg-reconfigure openssh-server
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
* Restarting OpenBSD Secure Shell server sshd [ OK ]
msfadmin@metasploitable:/etc/ssh$ ls
moduli      sshd_config      ssh_host_dsa_key.pub  ssh_host_rsa_key.pub
ssh_config  ssh_host_dsa_key  ssh_host_rsa_key
msfadmin@metasploitable:/etc/ssh$ sudo service ssh restart
sudo: service: command not found
msfadmin@metasploitable:/etc/ssh$ sudo /etc/init.d/ssh restart
* Restarting OpenBSD Secure Shell server sshd [ OK ]
msfadmin@metasploitable:/etc/ssh$
```