

```
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server restart
* Stopping NFS kernel daemon [ OK ]
* Unexporting directories for NFS kernel daemon... [ OK ]
* Exporting directories for NFS kernel daemon... [ OK ]
* Starting NFS kernel daemon [ OK ]
msfadmin@metasploitable:~$
```

2) Debian Open SSH/OpenSSL Package Random Number Generator Weakness

E' a vulnerabilità del **generatore** di **numeri casuali** nei **pacchetti** OpenSSH/OpenSSL. Un generatore di numeri casuali debole potrebbe **comportare** la **sicurezza** di diverse implementazioni crittografiche, rendendo più facile per un **attaccante** **compromettere** i **sistemi** vulnerabili e **sfruttare** questa **vulnerabilità** per effettuare attacchi di tipo "man-in-the-middle", **decifrare** le **comunicazioni criptate** o **eseguire** altre **attività dannose**.

SOLUZIONE: Rigeneriamo tutte le chiavi utilizzate sul server.

1) Procediamo cancellando le chiavi esistenti
comando: `sudo rm /etc/ssh/ssh_host_`

```
msfadmin@metasploitable:~$ sudo rm /etc/ssh/ssh
ssh_config      ssh_host_dsa_key      ssh_host_rsa_key
sshd_config      ssh_host_dsa_key.pub  ssh_host_rsa_key.pub
msfadmin@metasploitable:~$ sudo rm /etc/ssh/ssh_host_dsa_key
msfadmin@metasploitable:~$ sudo rm /etc/ssh/ssh_host_dsa_key.pub
msfadmin@metasploitable:~$ sudo rm /etc/ssh/ssh_host_rsa_key
msfadmin@metasploitable:~$ sudo rm /etc/ssh/ssh_host_rsa_key.pub
msfadmin@metasploitable:~$ 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:~$ sudo rm /etc/ssh/ssh
ssh_config      ssh_host_dsa_key      ssh_host_rsa_key
sshd_config      ssh_host_dsa_key.pub  ssh_host_rsa_key.pub
```

2) Riconfiguriamo le chiavi
comando: `sudo dpkg-reconfigure openssh-server`

```
msfadmin@metasploitable:~$ sudo dpkg-reconfigure openssh-server
msfadmin@metasploitable:~$ sudo /etc/init.d/ssh restart
* Restarting OpenBSD Secure Shell server sshd [ OK ]
msfadmin@metasploitable:~$ sudo /etc/init.d/apache2 restart
* Restarting web server apache2 [ OK ]
msfadmin@metasploitable:~$
```

3) Restart del servizio
comando: `sudo /etc/init.d/ssh restart`

4) Restart del di Apache 2 per il servizio SSL
comando `sudo /etc/init.d/apache2 restart`

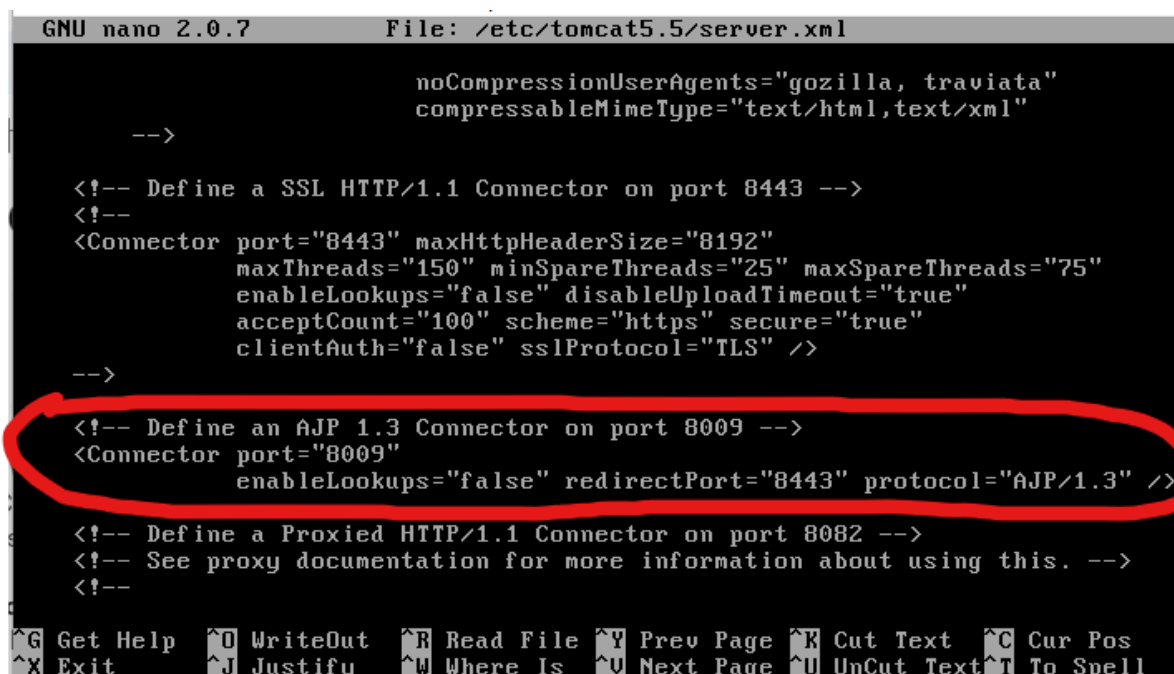
3) Apache Tomcat AJP Connector Request Injection (Ghostcat)

AJP è un **protocollo** di **comunicazione** progettato per **migliorare** le **prestazioni** della comunicazione **tra** un **server web** come Apache Tomcat **e** un **server web frontend** come Apache HTTP Server. Consente il **trasferimento efficiente** delle richieste **HTTP** tra il server web e il server di servlet.

Questo tipo di **vulnerabilità** **consente** a un attaccante di eseguire **attacchi** di injection di richieste **AJP** per **ottenere l'accesso non autorizzato ai file riservati** o per **eseguire codice malevolo sul server**.

SOLUZIONE: rimuovere dall'editor di testo l'intero blocco che definisce AJP

- 1) Comando **sudo nano /etc/tomcat5.5/server.xml** e rimuoviamo



```
GNU nano 2.0.7      File: /etc/tomcat5.5/server.xml

                                noCompressionUserAgents="gozilla, traviata"
                                compressableMimeType="text/html,text/xml"

-->

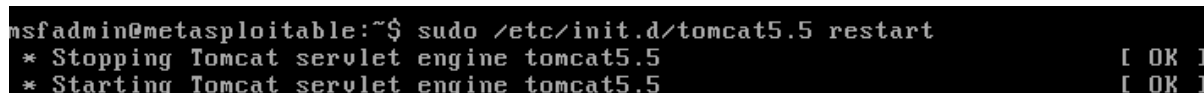
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" disableUploadTimeout="true"
          acceptCount="100" scheme="https" secure="true"
       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

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

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

^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
```

- 2) Riavvio server Tomcat con il comando: **sudo /etc/init.d/tomcat5.5 restart**



```
msfadmin@metasploitable:~$ sudo /etc/init.d/tomcat5.5 restart
* Stopping Tomcat servlet engine tomcat5.5      [ OK ]
* Starting Tomcat servlet engine tomcat5.5      [ OK ]
```

4) VNC Server password

Sulla macchina è presente un **servizio VNC** (virtual network computing), ovvero un **software** per **accesso/controllo remoto** che viene generalmente utilizzato per task amministrativi.

Un **utente** malintenzionato remoto e **non autenticato** potrebbe **sfruttare** questa situazione **per assumere il controllo del sistema**.

SOLUZIONE: Cambiamo la password con una difficile da indovinare con un bruteforce

1) Comando `vnc/passwd`

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$
```

5) Bind shell backdoor detection

Una backdoor è una **vulnerabilità** o un meccanismo nascosto all'interno di un **sistema informatico** che **consente l'accesso non autorizzato** o il **controllo remoto** da parte di un utente malintenzionato. Le backdoor possono essere deliberate, **inserite da un attaccante** durante lo sviluppo del software o introdotte accidentalmente come risultato di errori di programmazione. Una volta installata, una backdoor **può consentire** agli attaccanti di **bypassare** le normali **procedure** di **sicurezza** e ottenere **accesso** privilegiato al **sistema**. Le backdoor sono spesso **utilizzate** per **scopi dannosi**, come il **furto di dati sensibili**, il **monitoraggio delle attività degli utenti** o l'esecuzione di azioni dannose sul sistema compromesso.

SOLUZIONE: Chiudiamo la porta con un policy del Firewall

- 1) Con nmap scansioniamo la macchina per trovare la porta sulla quale si connette la backdoor

```
(kali@kali) ~$ sudo nmap 192.168.201.100 -p- -sV -O
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-08 08:17 EST
Nmap scan report for 192.168.201.100
Host is up (0.00052s latency).
Not shown: 65506 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?         Debian GNU/Linux 5.0.4 login (pro
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
3632/tcp  open  distccd        distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc            UnrealIRCd
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb            Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
47212/tcp open  status         1 (RPC #100024)
48678/tcp open  java-rmi       GNU Classpath grmiregistry
53270/tcp open  nlockmgr       1-4 (RPC #100021)
58483/tcp open  mountd         1-3 (RPC #100005)
MAC Address: 08:00:27:53:D2:9B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 176.76 seconds
```

- 2) Con netcat notiamo che è aperta

```
(kali㉿kali)-[~]  
$ nc 192.168.201.100 1524  
root@metasploitable:/#
```

- 3) La chiudiamo con una regola del firewall

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP  
msfadmin@metasploitable:~$
```

- 4) Verifichiamo che la porta sia chiusa con Netcat

```
(kali㉿kali)-[~]  
$ nc 192.168.201.100 1524  
_
```