

# Report di Sicurezza sui Servizi NFS, VNC, Bind Shell e AJP

## Introduzione

Misure correttive su servizi critici quali NFS, VNC, Bind Shell e AJP. Di seguito, riporto le azioni intraprese e i risultati ottenuti.

## NFS (Network File System)

**Descrizione del Servizio:** Il Network File System (NFS) è un protocollo che consente a un utente su un client di accedere ai file tramite una rete come se fossero in locale. NFS è comunemente utilizzato per condividere file tra server e client Unix/Linux.

**Problema Riscontrato:** Il servizio NFS era configurato con permessi eccessivamente permissivi, consentendo accessi non autorizzati ai file condivisi.

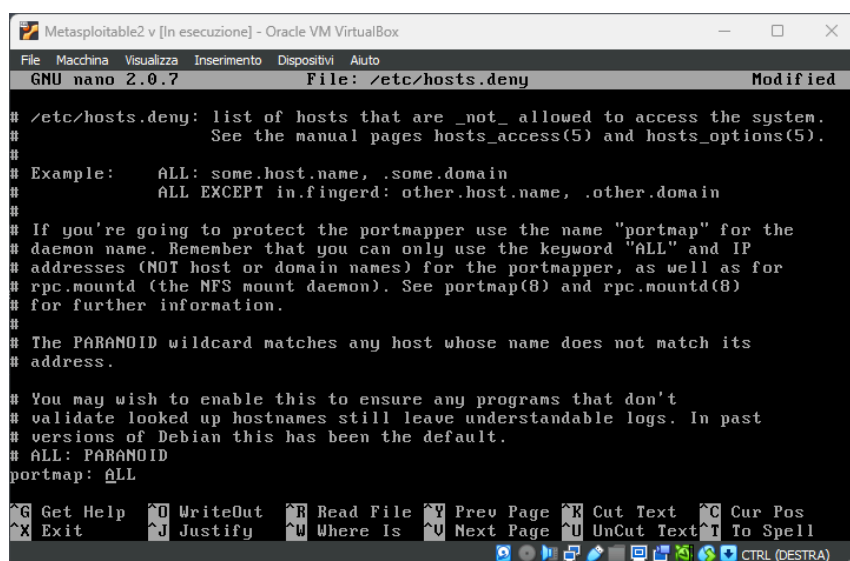
**Azione Correttiva:** Ho modificato i file di configurazione per restringere i permessi di accesso alle condivisioni NFS.

### Comandi Eseguiti:

#### 1.Modifica di `/etc/hosts.deny`:

```
sudo nano /etc/hosts.deny
```

```
portmap: ALL
```



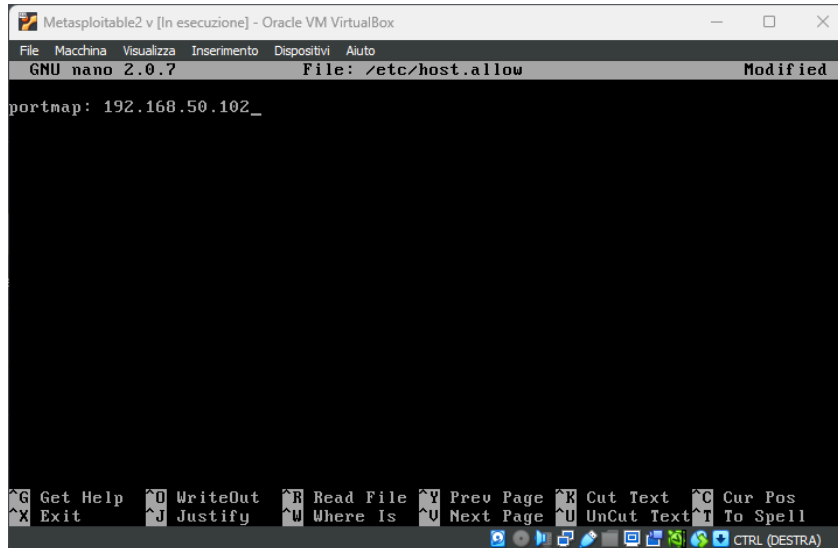
```
Metasploitable2 v [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/hosts.deny Modified
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# 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
^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^X Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

## 2.Modifica di `/etc/hosts.allow`:

```
sudo nano /etc/hosts.allow
```

```
portmap: 192.168.50.102
```

**Risultato:** Dopo aver applicato le modifiche, l'accesso alle condivisioni NFS è ora limitato solo agli IP autorizzati, migliorando la sicurezza.



# VNC (Virtual Network Computing)

**Descrizione del Servizio:** Il Virtual Network Computing (VNC) è un sistema di condivisione del desktop grafico che utilizza il protocollo Remote Frame Buffer (RFB) per controllare un altro computer da remoto.

**Problema Riscontrato:** La scansione di sicurezza ha rilevato che il server VNC era configurato con una password debole e senza crittografia, esponendo il sistema a potenziali accessi non autorizzati.

**Azione Correttiva:** Ho impostato una nuova password robusta per il server VNC e configurato il file di configurazione per utilizzare l'autenticazione e la crittografia.

## Comandi Eseguiti:

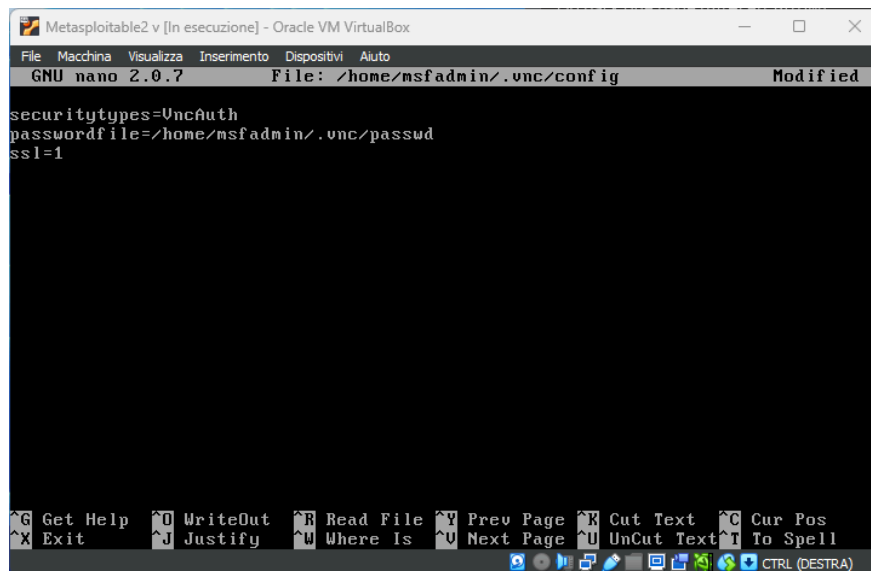
### Impostazione della password per VNC:

```
vncpasswd
```

## 1.Creazione del file di configurazione `/home/msfadmin/.vnc/config`:

```
sudo nano /home/msfadmin/.vnc/config
```

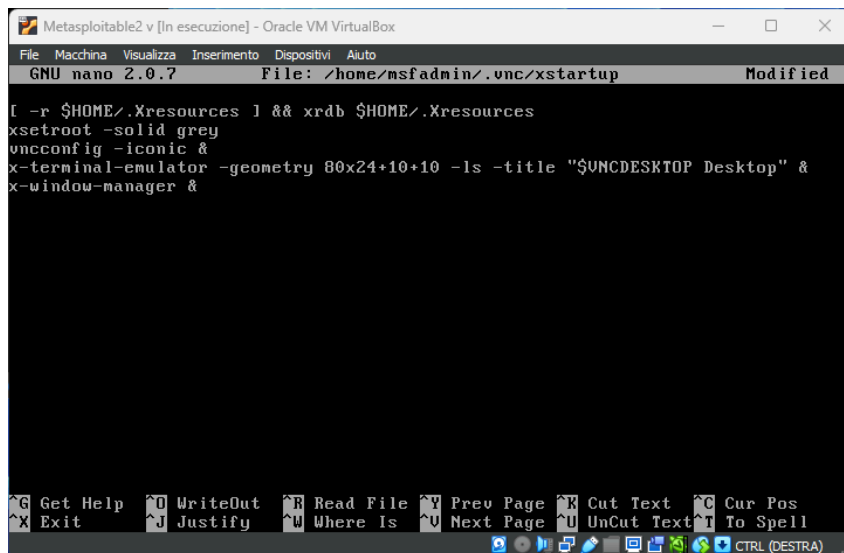
```
securitytypes=VncAuth  
passwordfile=/home/msfadmin/.vnc/passwd  
ssl=1
```



## 2.Modifica del file `xstartup`:

```
sudo nano /home/msfadmin/.vnc/xstartup
```

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



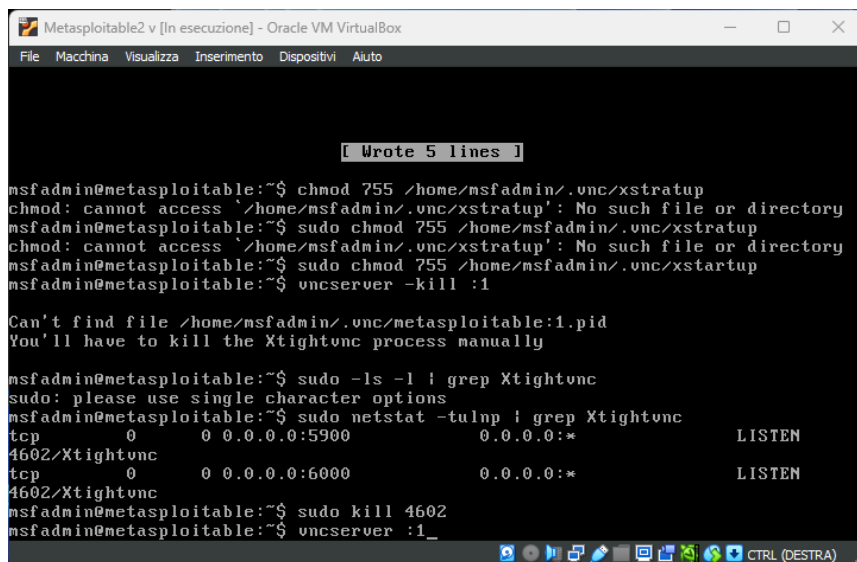
```
Metasploitable2 v [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /home/msfadmin/.vnc/xstartup Modified

[ -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 &

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)
```

### 3.Rendo eseguibile il file **xstartup**:

**chmod 755 /home/msfadmin/.vnc/xstartup**



```
Metasploitable2 v [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

[ Wrote 5 lines ]

msfadmin@metasploitable:~$ chmod 755 /home/msfadmin/.vnc/xstartup
chmod: cannot access '/home/msfadmin/.vnc/xstartup': No such file or directory
msfadmin@metasploitable:~$ sudo chmod 755 /home/msfadmin/.vnc/xstartup
chmod: cannot access '/home/msfadmin/.vnc/xstartup': No such file or directory
msfadmin@metasploitable:~$ sudo chmod 755 /home/msfadmin/.vnc/xstartup
msfadmin@metasploitable:~$ vncserver -kill :1

Can't find file /home/msfadmin/.vnc/metasploitable:1.pid
You'll have to kill the Xtightvnc process manually

msfadmin@metasploitable:~$ sudo -ls -l | grep Xtightvnc
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
4602/Xtightvnc
tcp        0      0 0.0.0.0:6000          0.0.0.0:*            LISTEN
4602/Xtightvnc
msfadmin@metasploitable:~$ sudo kill 4602
msfadmin@metasploitable:~$ vncserver :1_
```

### 4.Riavvio del server VNC:

**sudo netstat -tulnp | grep Xtightvnc**

**sudo kill 4602**

**vncserver :1**

**Risultato:** Dopo aver applicato queste modifiche, il server VNC è ora protetto con una password robusta e utilizza la crittografia, migliorando la sicurezza delle connessioni remote.

# Bind Shell

**Descrizione del Problema:** Durante la scansione, è stata rilevata una backdoor di tipo bind shell che permetteva l'accesso remoto non autorizzato al sistema.

**Azione Correttiva:** Ho identificato e terminato il processo della bind shell e ho eliminato la backdoor dal sistema.

**Comandi Eseguiti:**

**Identificazione del processo bind shell sulla porta 1524 (porta trovata sul report csv):**

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

	A	B	C	D	E	F	G	H	I	J
121	51891		None	192.168.50.101	tcp	25-SSL Session Resume Supported	The remote host allows resuming SSL sessions.	This script performs reconnaissance on a cache. n/a		
122	51988	10.0	Critical	192.168.50.101	tcp	1524 Bind Shell Backdoor Detection	The remote host may have been compromised.	A shell is being used post and system if necessary. Verify if the remote system if necessary.		
123	52611	CVE-2011-0411	4.0	Medium	192.168.50.101	tcp	25-SMTP Service STARTTLS Plaintext Command Injection	The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.	The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.	
124	52611	CVE-2011-1430	4.0	Medium	192.168.50.101	tcp	25-SMTP Service STARTTLS Plaintext Command Injection	The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.	The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.	
125	52611	CVE-2011-1431	4.0	Medium	192.168.50.101	tcp	25-SMTP Service STARTTLS Plaintext Command Injection	The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.	The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.	

**Visualizzazione del processo:**

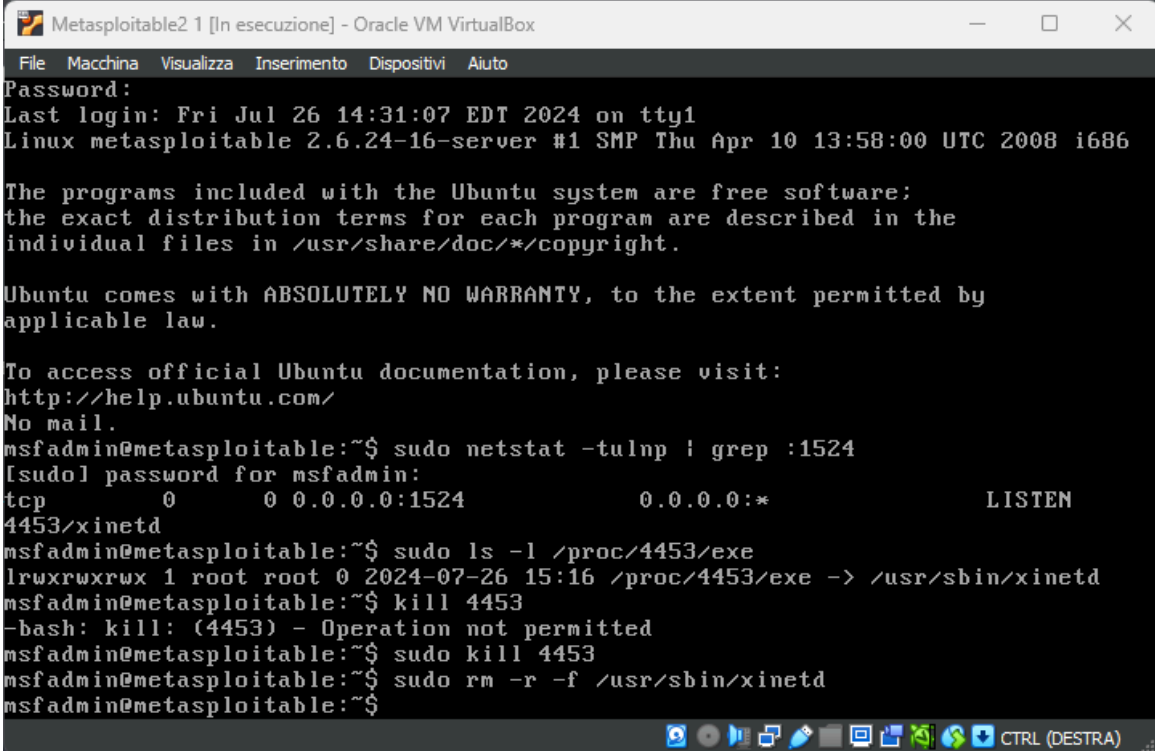
```
sudo ls -l /proc/4453/exe
```

**1. Terminazione del processo bind shell:**

```
sudo kill 4453
```

## 2.Rimozione della backdoor:

```
sudo rm -r -f /usr/sbin/xinetd
```



```
Metasploitable2 1 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
Password:
Last login: Fri Jul 26 14:31:07 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
4453/xinetd
msfadmin@metasploitable:~$ sudo ls -l /proc/4453/exe
lrwxrwxrwx 1 root root 0 2024-07-26 15:16 /proc/4453/exe -> /usr/sbin/xinetd
msfadmin@metasploitable:~$ kill 4453
-bash: kill: (4453) - Operation not permitted
msfadmin@metasploitable:~$ sudo kill 4453
msfadmin@metasploitable:~$ sudo rm -r -f /usr/sbin/xinetd
msfadmin@metasploitable:~$
```

**Risultato:** Il processo della bind shell è stato terminato e la backdoor è stata rimossa dal sistema, eliminando il vettore di attacco.

# AJP (Apache JServ Protocol)

**Descrizione del Servizio:** L'Apache JServ Protocol (AJP) è un protocollo binario che consente il collegamento tra un server web (come Apache) e un application server (come Tomcat).

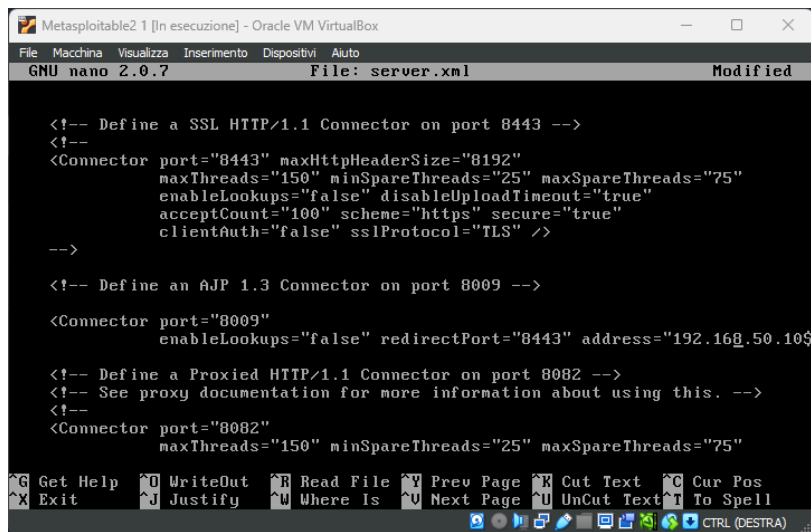
**Problema Riscontrato:** Il servizio AJP era configurato per accettare connessioni da qualsiasi indirizzo IP, esponendo il sistema a potenziali attacchi.

**Azione Correttiva:** Ho modificato la configurazione del connettore AJP in Tomcat per limitare l'accesso solo agli indirizzi IP di fiducia.

## Comandi Eseguiti:

1.Modifica del file di configurazione di Tomcat `/etc/tomcat/server.xml`:

sudo nano /etc/tomcat/server.xml

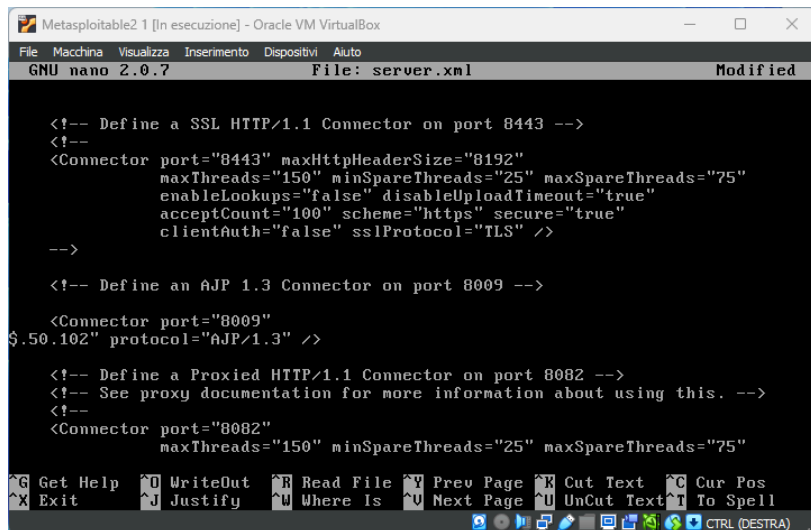


```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192"
  maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
  enableLookups="false" disableUploadTimeout="true"
  acceptCount="100" scheme="https" secure="true"
  clientAuth="false" sslProtocol="TLS"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

<!-- Define an AJP 1.3 Connector on port 8009 -->

<Connector port="8009"
  enableLookups="false" redirectPort="8443" address="192.168.50.105"
  protocol="AJP/1.3" />

<!-- Define a Proxied 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" proxy="http://127.0.0.1:8080"
  scheme="http" secure="false" />
-->
```



```
<!-- 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="192.168.50.102"
  protocol="AJP/1.3" />

<!-- Define a Proxied 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" proxy="http://127.0.0.1:8080"
  scheme="http" secure="false" />
-->
```

Modifica del connettore AJP:

```
<Connector port="8009" protocol="AJP/1.3" address="192.168.50.102"
protocol="AJP/1.3" />
```

## 2.Riavvio del servizio Tomcat:

sudo systemctl restart tomcat

**Risultato:** Dopo aver applicato queste modifiche, l'accesso al servizio AJP è ora limitato agli indirizzi IP autorizzati, migliorando la sicurezza.