

18.05.2025



VULNERABILITY ASSESSMENT

REMEDIATION VULNERABILITY
FABIO MUNGIOVÌ

REMEDIATION VULNERABILITY

METASPLOITABLE 2

INDICE

SOMMARIO.....	2
ESECUZIONE	3
1 - Apache Tomcat AJP Connector Request Injection.....	3
2 - SSL Version 2 and 3 Protocol Detection	4
3 -NFS Shares World Readable	5
4 - Bind Shell Backdoor Detection	6
5 - VNC Server 'password' Password	7

SOMMARIO

Nel seguente report verranno analizzate e risolte alcune vulnerabilità riscontrate nella scansione iniziale del sistema Metasploitable.

Nello specifico verranno risolte le seguenti vulnerabilità:

1	NOME	CVSS
	Apache Tomcat AJP Connector Request Injection (Ghostcat) Port tcp/8009/ajp13 Synopsis È presente un connettore AJP vulnerabile in ascolto sull'host remoto.	CRIT 9.8

2	NOME	CVSS
	SSL Version 2 and 3 Protocol Detection Port tcp/5432/postgresql tcp/25/smtp Synopsis Il servizio remoto crittografa il traffico utilizzando un protocollo con punti deboli noti.	CRIT 9.8

3	NOME	CVSS
	Bind Shell Backdoor Detection Port tcp/1524/wild_shell Synopsis Shell di comando in ascolto sulla porta senza autenticazione.	CRIT 9.8

4	NOME	CVSS
	NFS Shares World Readable Port tcp/2049/rpc-nfs Synopsis Il server NFS remoto esporta condivisioni leggibili da tutti.	HIGH 7.5

5	NOME	CVSS
	VNC Server 'password' Password Port tcp/5900/vnc Synopsis Un server VNC in esecuzione sull'host remoto è protetto da una password debole.	CRIT 10

ESECUZIONE

1 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

È presente un connettore AJP vulnerabile in ascolto sull'host remoto.

Il protocollo AJP esposto è insicuro, poiché trasmette dati in chiaro, il che implica che chiunque possa intercettare queste comunicazioni all'interno di una rete non protetta.

La soluzione migliore nella nostra situazione è quindi disabilitare AJP del tutto in Tomcat, dato che eventualmente può essere sostituito da protocolli come HTTP o HTTPS che risultano protocolli più robusti.

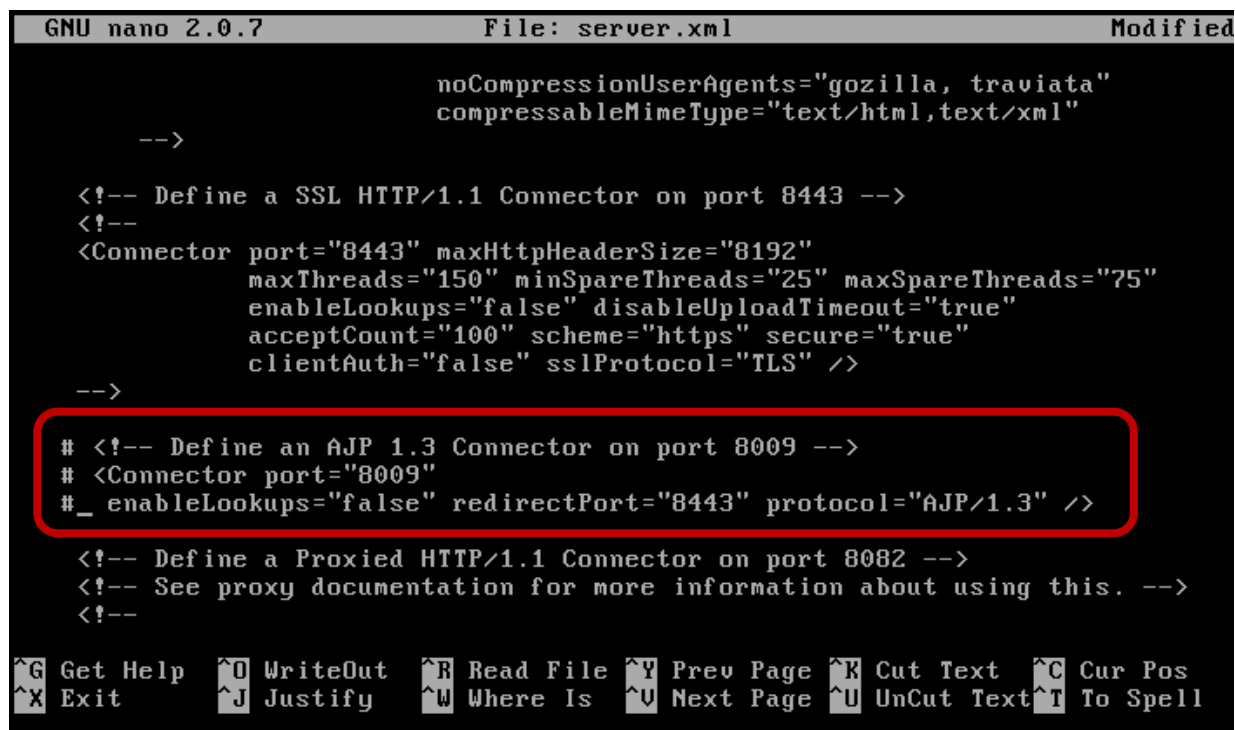
Per disabilitare AJP bisogna aprire il file di configurazione di Tomcat, *server.xml* all'indirizzo:

```
$ /etc/tomcat5.5
```

```
msfadmin@metasploitable:/$ cd /etc/tomcat5.5/  
msfadmin@metasploitable:/etc/tomcat5.5$ sudo nano server.xml
```

Una volta aperto il file, commentare (#) le righe che abilitano il servizio, così come da immagine.

In questo modo il servizio verrà disabilitato.



```
GNU nano 2.0.7      File: server.xml      Modified  
  
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  ^V Next Page  ^U UnCut Text ^T To Spell
```

2 - SSL Version 2 and 3 Protocol Detection

I servizi SSL 2.0 e/o SSL 3.0 sono versioni di SSL affette da diversi difetti crittografici noti, facilmente sfruttabili da un attaccante esterno.

La migliore soluzione è di disabilitarli.

È possibile disabilitare questi servizi andando a modificare il file di configurazione *ssl.conf*, all'indirizzo:

```
$ /etc/apache2/mods-available
```

```
msfadmin@metasploitable:/etc/apache2/mods-available$ sudo nano ssl.conf
```

Una volta aperto il file di configurazione, rimuovere il commento (#) dalla riga contenente il seguente comando:

```
SSLProtocol all -SSLv2 -SSLv3
```

In questo modo disabiteremo questi servizi lasciando abilitato TLSv1, che risulta più sicuro.

```
GNU nano 2.0.7      File: ssl.conf      Modified

#SSLSessionCache      dbm:/var/run/apache2/ssl_scache
SSLSessionCache      shmcb:/var/run/apache2/ssl_scache(512000)
SSLSessionCacheTimeout 300

# Semaphore:
# Configure the path to the mutual exclusion semaphore the
# SSL engine uses internally for inter-process synchronization.
SSLMutex file:/var/run/apache2/ssl_mutex

-
# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
# enable only secure ciphers:
#SSLCipherSuite HIGH:MEDIUM:!ADH

# enable only secure protocols: SSLv3 and TLSv1, but not SSLv2
SSLProtocol all -SSLv2 -SSLv3

</IfModule>

^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
```

3 -NFS Shares World Readable

Il server NFS è esposto senza limitare l'accesso (in base al nome host, all'IP o all'intervallo IP).

Per correggere questa vulnerabilità, senza disabilitarla del tutto, bisogna indicare, nel file di configurazione del servizio, un IP o più a cui concedere l'accesso.

Il file di configurazione *exports* è rintracciabile all'interno della directory */etc*

Nella prima immagine si può notare come, nel file di configurazione, tramite l'asterisco, la condivisione della root directory (/) sia condivisa ad ogni IP in ascolto sulla porta.

```
GNU nano 2.0.7      File: 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)
```

Andiamo quindi a sostituire l'asterisco con uno o più IP a cui vogliamo consentire l'accesso.

Possiamo eventualmente anche cambiare la directory condivisa se si volesse restringere la condivisione solo a determinati file.

```
GNU nano 2.0.7      File: exports      Modified

# /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)
#
/ 192.168.50.100_(rw,sync,no_root_squash,no_subtree_check)
```

4 - Bind Shell Backdoor Detection

Una shell è in ascolto sulla porta 1524 senza che sia richiesta alcuna autenticazione.

Un utente malintenzionato può utilizzarlo connettendosi alla porta remota e inviando direttamente comandi.

La soluzione migliore per mitigare questo problema è bloccare ogni accesso alla porta tramite una regola firewall.

Il sistema Ubuntu, su cui è bastato Metasploitable, possiede un firewall interno, *ufw*, configurabile con semplici comandi elencati di seguito:

- `ufw enable`

Abilita il firewall, anche al riavvio del sistema.

- `ufw default allow`

Imposta il firewall in modo da permettere ogni connessione.

Il firewall *ufw*, di default, blocca tutte le porte del sistema, disabilitando quindi ogni servizio.

Abilitandole tutte andremo a chiudere poi solo le porte target della mitigazione.

- `ufw deny 1524`

Aggiunge la regola che nega l'accesso da qualsiasi sorgente alla porta indicata.

- `ufw status`

Comando che permette di verificare l'attivazione del firewall e delle regole impostate.

```
msfadmin@metasploitable:~$ sudo ufw enable
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
msfadmin@metasploitable:~$ sudo ufw deny 1524
Rule added
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded

To Action From
--
1524:tcp DENY Anywhere
1524:udp DENY Anywhere

msfadmin@metasploitable:~$ _
```

In questo modo la regola di firewall è attiva, escludendo la possibilità di connessione esterna alla shell della porta 1524.

5 - VNC Server 'password' Password

Il server VNC in esecuzione è protetto da una password debole. ("password")

Per risolvere questa vulnerabilità è necessario andare a settare una password più efficace per il servizio VNC.

Per cambiare la password del servizio, digitare a comando:

```
$ vncpasswd
```

Quindi inserire una password differente.

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password: _
```