

ESERCITAZIONE S5L5

Remediation

Attraverso la prima scansione delle vulnerabilità su Meta (192.168.1.102), ne abbiamo riscontrate 8 critiche, mentre con la seconda possiamo notare come siano diventate 6.

La prima vulnerabilità risolta è stata “Apache Tomcat AJP Connector Request Injection (Ghostcat)”. Essendo un servizio non utilizzato sulla macchina, invece di aggiornarlo, si è preferito disabilitare la porta “8009”, utilizzata dal servizio TomCat, inserendo un “!” all’inizio della sintassi.

```
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. -->
<!--
<Connector port="8082"
      maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
      enableLookups="false" acceptCount="100" connectionTimeout="20000"
```

Il file da modificare si trova all’interno del percorso `:/etc/tomcat5.5/server.xml`

La seconda vulnerabilità che è stata risolta è “VNC Server 'password' Password”. È stato sufficiente cambiare la password di default utilizzata per l’accesso alla vnc. Una volta trovato il file “passwd” all’interno del percorso `root/.vnc`, utilizzando il comando `vncpasswd` con i privilegi di root, si può impostare una password a propria scelta, così da modificare quella precedente.

```
[ Read 1 line ]

root@metasploitable:~/.vnc# ls .a
ls: cannot access .a: No such file or directory
root@metasploitable:~/.vnc# ls -a
.  metasploitable:0.log  metasploitable:1.log  passwd
.. metasploitable:0.pid  metasploitable:2.log  xstartup
root@metasploitable:~/.vnc# pwd
/root/.vnc
root@metasploitable:~/.vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~/.vnc# _
```