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.

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.