Esercizio S5L4 di Ciaschini Giorgio del 22/02/2024

Per l'esercizio di oggi siamo andati ad esaminare tutte le vulnerabilità che sono presenti sulla macchina Metasploitable attraverso l'utilizzo di Nessus Essential che a fine scansione rilascia un report delle vulnerabilità con diversi valori di criticità. Di seguito un screen-shot del risultato.

192.168.49.101

10	5	21		110
CRITICAL	HIGH	MEDIUM	LOW	INFO
Host Information				
Netbios Name:	METASPLOITABLE			
P:	192.168.49.101			

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Come possiamo vedere abbiamo trovato 10 vulnerabilità critiche, 5 alte, 21 medie, 7 basse. Grazie al report abbiamo una lista di possibili soluzioni alle vulnerabilità presenti. Ad esempio in questo caso ci viene consigliato di aggiornare le configurazioni di "AJP" e il Tomcat server da 7.0.100 a 8.5.51, |9.0.31 o più.