PRATICA S5L4 – Giorgio Trovesi

Traccia: effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni. Al completamento della scansione prendere in esame le prime 4 vulnerabilità critiche e commentarle.

Dopo aver effettuato la scansione abbiamo esportato il report delle vulnerabilità trovate sulla macchina Metasploitable, a seguire possiamo osservarne un estratto:

192.168.1.189

9	5	16	7	73
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 110

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	6.7	10205	rlogin Service Detection
HIGH	7.5*	6.7	10245	rsh Service Detection
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate

1) **134862 – APACHE TOMCAT AJP CONNECTOR REQUEST INJECTION (GHOSTCAT):**
   E' stata rilevata una vulnerabilità nel connettore AJP, un attaccante potrebbe sfruttare questo exploit per le leggere i file delle applicazioni web sul server. Nel caso in cui il server consenta il caricamento di file il malintenzionato potrebbe caricare codice JSP dannoso e ottenere l'esecuzione in modalità remota.
   SOLUZIONE: Aggiornare la configurazione AJP e/o richiedere l'autorizzazione per aggiornare il server Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successivi.

2) **51988 – BLIND SHELL BACKDOOR DETECTION:**
   Un utente malintenzionato può utilizzarla per collegarsi da remoto e inviare direttamente i comandi.
   SOLUZIONE: Verificare se l'host è compromesso e reinstallare il sistema se necessario.

3) **20007 – SSL VERSION 2 AND 3 PROTOCOL DETECTION:**
   Il servizio remoto accetta connessioni crittografate utilizzando SSL2.0 e/o SSL 3.0.
   Un attaccante potrebbe sfruttare queste falle per condurre attacchi "man-in-the-middle" o per decrittografare le comunicazioni tra il servizio interessato e il client.
   SOLUZIONE: Disabilitare SSL 2.0/3.0 e utilizzare TLS 1.2 o una versione più recente.

4) **171340 – APACHE TOMCAT SEOL (<=5.5X):**
   La versione del server è inferiore alla 5.5.x pertanto non è più gestita dal fornitore, ciò implica una mancanza di supporto post-vendita; il venditore non rilascerà più nuovi aggiornamenti di sicurezza a riguardo e pertanto potrebbero esserci delle vulnerabilità.
   SOLUZIONE: Aggiornare la versione di Apache Tomcat alla versione corrente supportata.