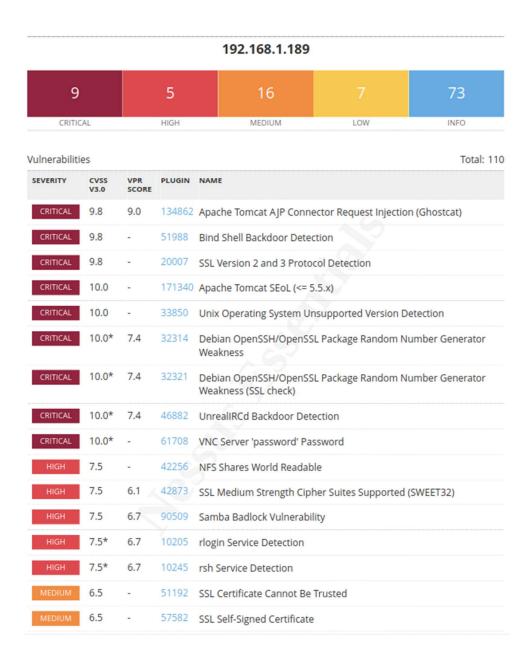
PRATICA S5L4 - Giorgio Trovesi

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:



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.

