Analisi dei Report Nessus

1. Apache Tomcat AJP Connector Request Injection (Ghostcat)

- Descrizione: Una vulnerabilità che consente di leggere o includere file sfruttando il connettore AJP. In alcuni casi, potrebbe portare a un'esecuzione di codice remoto (RCE).

- Rischio: Critico

- Soluzione: Aggiornare Tomcat alle versioni 7.0.100, 8.5.51, 9.0.31 o superiori. Modificare la configurazione AJP per richiedere l'autorizzazione.

2. Bind Shell Backdoor Detection

- Descrizione: Presenza di una shell di backdoor sulla porta 1524 che potrebbe essere utilizzata da un attaccante.

- Rischio: Critico

- Soluzione: Verificare se il sistema è stato compromesso e reinstallare completamente il sistema, se necessario.

3. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

- Descrizione: Una debolezza nel generatore di numeri casuali che rende vulnerabili le chiavi SSH.

- Rischio: Critico

- Soluzione: Rigenerare tutte le chiavi SSH e materiali crittografici creati con le versioni affette di OpenSSL.

4. SSL Version 2 and 3 Protocol Detection

- Descrizione: I protocolli SSLv2 e SSLv3, affetti da diverse vulnerabilità, sono abilitati.

- Rischio: Critico

- Soluzione: Disabilitare SSLv2 e SSLv3 e utilizzare TLS 1.2 o versioni superiori.

5. VNC Server Weak Password

- Descrizione: Un server VNC con una password debole (`password`) consente l'accesso non autorizzato.

- Rischio: Critico

- Soluzione: Configurare una password robusta per il servizio VNC.

6. ISC BIND Service Downgrade / Reflected DoS

- Descrizione: Vulnabilità che consente il degrado del servizio o l'uso del server come riflettore per attacchi DoS.

- Rischio: Alto

- Soluzione: Aggiornare a una versione di ISC BIND non vulnerabile (es. 9.11.19 o successiva).

7. SMB Signing not Required

- Descrizione: Il servizio SMB non richiede la firma, rendendolo vulnerabile a man-in-the-middle (MITM).

- Rischio: Medio

- Soluzione: Forzare l'abilitazione della firma SMB nel sistema.

8. SSL/TLS Weak Cipher Suites

- Descrizione: Supporto di suite di cifratura deboli o medie (es. SWEET32).

- Rischio: Alto

- Soluzione: Riconfigurare il servizio per disabilitare le suite deboli e utilizzare solo cifre robuste.