Relazione Scansione Metasploitable2 da Nessus

La scansione effettuata con **Nessus** sull'host **Metasploitable2**: `192.168.50.152` ha rilevato diverse vulnerabilità critiche. Di seguito riportato i principali problemi riscontrati

1. **Codice Errore (Critical, 10.0): CVE-2008-0166**
   Questo è un grave problema nel pacchetto **OpenSSL** su sistemi **Debian** e **Ubuntu**. L'errore riguarda il generatore di numeri casuali, che rende le chiavi SSH prevedibili.
   Un attaccante potrebbe decifrare facilmente le sessioni SSH o eseguire attacchi *"man-in-the-middle"*, intercettando il traffico.

2. **Codice Errore (Critical**, **9.8): Supporto di SSL Versioni 2 e 3**
   Il sistema consente connessioni cifrate tramite versioni obsolete di **SSL (2.0 e 3.0)**, che presentano vulnerabilità note, tra cui problemi di padding con cifrari CBC e falle nella negoziazione delle sessioni.

3. **Cifrari SSL Deboli (High, Attacco SWEET32 - CVE-2016-2183, 7.5)**
   Il sistema supporta cifrari di media sicurezza, che lo rendono vulnerabile all'attacco **SWEET32**. Un attaccante, se connesso alla stessa rete, potrebbe riuscire a decifrare informazioni sensibili.
4. **Vulnerabilità "Badlock" in Samba (CVE-2016-2118, 7.5)**
   Vulnerabilità nel server Samba che permette ad un attaccante di eseguire attacchi *"man-in-the-middle"*, intercettando e manipolando il traffico nei protocolli di autenticazione.

La scansione è stata fatta secondo le istruzioni della traccia sulle **porte 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389.** Tuttavia le porte **110,443,3389** non risultano visibili nel report in quanto porte chiuse. Ragion per cui sono state esaminate tramite terminale su Kali Linux.