Consegna U2 S5/L3

Marco Falchi

Vulnerability Scanning mediante Nessus

Obiettivo

L'obiettivo di questo esercizio era eseguire una scansione delle vulnerabilità con Nessus sulla macchina virtuale **Metasploitable**. Identificare le vulnerabilità presenti, analizzarne i dettagli e riflettere sulle loro implicazioni per la sicurezza.

Configurazione della Rete

Ambiente configurato per la simulazione:

- **Macchine virtuali**:
    - **Kali Linux**: 192.168.50.100
    - **Metasploitable2**: 192.168.50.101

  Target della scansione: L'indirizzo della macchina vulnerabile, 192.168.50.101

Passaggi Eseguiti

Configurazione della Scansione

- **Tipo di scansione**: Basic Network Scan.
- **Target**: 192.168.50.101 con un focus sulle common port.

Esecuzione della Scansione

- La scansione "basic" ha impiegato circa **5 minuti** per completarsi.
- Risulato= **122 vulnerabilità rilevate**, distribuite così:
    - **Critical**: 9
    - **High**: 6
    - **Medium**: 19

- **Low**: 8
- **Info**: 80

Analisi del Report

Dai risultati della scansione Metasploitable, sono state identificate diverse principali vulnerabilità critiche e ad alto rischio che evidenziano le potenziali debolezze del sistema:

Vulnerabilità Critiche

1. **Apache Tomcat AJP Connector Request Injection (Ghostcat)**
   - **Porta:** TCP/8009
   - **Descrizione:** Una vulnerabilità nel connettore AJP di Apache Tomcat consente agli attaccanti di accedere a file arbitrari sul server o di eseguire codice arbitrario.
   - **Soluzione simulata:** Disabilitare il connettore AJP o configurarlo per accettare richieste solo da indirizzi IP fidati.
2. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**
   - **Porta:** TCP/22 (SSH)
   - **Descrizione:** Un difetto nel generatore di numeri casuali di OpenSSL su alcune versioni di Debian rende le chiavi crittografiche deboli e facilmente prevedibili.
   - **Soluzione simulata:** Rigenerare tutte le chiavi SSH e SSL e aggiornare OpenSSL.
3. **SSL Version 2 and 3 Protocol Detection**
   - **Porta:** TCP/25 (SMTP)
   - **Descrizione:** SSLv2 e SSLv3 sono protocolli deprecati con vulnerabilità note, come attacchi di tipo Man-in-the-Middle.
   - **Soluzione simulata:** Disabilitare SSLv2 e SSLv3, abilitando solo TLS 1.2 o versioni successive.
4. **VNC Server 'password' Password**
   - **Porta:** TCP/5900
   - **Descrizione:** Il server VNC utilizza una password debole o predefinita, consentendo accessi non autorizzati.
   - **Soluzione simulata:** Configurare una password sicura e abilitare l'autenticazione a due fattori.

Vulnerabilità di Alto Rischio

1. **Samba Badlock Vulnerability**
    - **Porta:** TCP/445 (SMB)
    - **Descrizione:** Una debolezza nei protocolli SAM e LSAD consente attacchi di tipo Man-in-the-Middle che possono compromettere dati sensibili.
    - **Soluzione simulata:** Aggiornare Samba alla versione 4.4.2 o successive.
2. **SSL Medium Strength Cipher Suites Supported (SWEET32)**
    - **Porta:** TCP/443 (HTTPS)
    - **Descrizione:** L'uso di cifrature di media forza, come 3DES, può esporre il sistema ad attacchi crittografici.
    - **Soluzione simulata:** Disabilitare le cifrature 3DES e configurare il server per utilizzare solo algoritmi di crittografia moderni.
3. **NFS Shares World Readable**
    - **Porta:** TCP/2049
    - **Descrizione:** Condivisioni NFS configurate in modo insicuro permettono l'accesso a file sensibili da parte di utenti non autorizzati.
    - **Soluzione simulata:** Limitare l'accesso NFS a host fidati e configurare i permessi di accesso correttamente.
4. **Telnet Server Detection**
    - **Porta:** TCP/23
    - **Descrizione:** Il server Telnet consente connessioni non crittografate, esponendo credenziali e dati a intercettazioni.
    - **Soluzione simulata:** Disabilitare Telnet e utilizzare SSH per le connessioni remote.

Raccomandazioni Generali

Aggiornare pacchetti e software vulnerabili nei sistemi reali: mantenere sempre aggiornati i servizi e applicare le patch di sicurezza fornite dai vendor.

Disabilitare protocolli e servizi non essenziali: ridurre la superficie di attacco eliminando funzionalità non necessarie.

Implementare crittografia moderna per SSL/TLS: garantire che solo protocolli sicuri (come TLS 1.2 o 1.3) siano abilitati.

Integrare regole di firewall più severe: configurare il firewall per limitare l'accesso alle porte e ai servizi vulnerabili solo a IP autorizzati.

Segmentare la rete: isolare i sistemi vulnerabili o di test in una VLAN dedicata per limitare i danni in caso di compromissione.

Nota personale

Metasploitable è progettata per essere vulnerabile.
Non ha senso quindi correggere le vulnerabilità identificate su questa macchina, perché il suo scopo principale è fungere da ambiente di pratica per la sicurezza informatica.

Tuttavia, comprendere le vulnerabilità è essenziale per applicare queste conoscenze a sistemi reali.