RELAZIONE S5L3

Durante questo esercizio è stato utilizzato lo strumento **Nessus** per effettuare una scansione di sicurezza su un host target configurato su una macchina virtuale Metasploitable con indirizzo IP statico. L'obiettivo principale era identificare e analizzare le vulnerabilità presenti sull'host, concentrandosi sulle problematiche di maggiore gravità, al fine di proporre soluzioni concrete per la loro mitigazione.

La scansione iniziale si è concentrata sulle porte richieste dall'esercizio. Successivamente, per ottenere una panoramica più dettagliata, sono state incluse anche altre porte comuni trovate aperte sull'host target. L'analisi si è quindi focalizzata su tre vulnerabilità particolarmente critiche.

Configurazione della scansione:

- La scansione è stata impostata per verificare inizialmente le seguenti porte: 21 (FTP), 22 (SSH), 23 (Telnet), 25 (SMTP), 80 (HTTP), 110 (POP3), 139 (NetBIOS), 443 (HTTPS), 445 (SMB), 3389 (RDP).
- Successivamente, sono state aggiunte altre porte comuni rilevate sull'host per ampliare l'analisi:
  53 (DNS), 111 (RPC), 2049 (NFS), 3306 (MySQL), 5432 (PostgreSQL), 8080 (HTTP alternativo), 8180 (HTTP alternativo), 5900 (VNC), 6667 (IRC).

Strumento utilizzato:

- **Nessus**, uno strumento professionale per la scansione delle vulnerabilità, è stato configurato per eseguire una scansione approfondita su tutte le porte specificate e per identificare eventuali vulnerabilità conosciute sull'host.

Criteri di selezione:

- Delle 168 vulnerabilità rilevate, sono state analizzate in dettaglio tre problematiche tra le più gravi, selezionate in base alla loro criticità e al potenziale impatto sulla sicurezza del sistema.

Statistiche della scansione:

- **Totale vulnerabilità rilevate:** 168.
- **Categorie di rischio:**
  - Critiche: 26.
  - Alte: 61.
  - Medie: 73.
  - Basse: 8.

Vulnerabilità analizzate in dettaglio:
Tra le vulnerabilità critiche, sono state selezionate per un'analisi approfondita le seguenti:

- **Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow.**
- **Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows.**
- **PHP Unsupported Version Detection.**

Analisi delle vulnerabilità

1. **Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow**
   - **Descrizione:** Questa vulnerabilità consente a un attaccante remoto di causare un heap overflow sfruttando una gestione impropria della memoria nella libreria APR.
   - **Impatto:** Potenziale esecuzione di codice arbitrario e Denial of Service (DoS).
   - **Mitigazione:** Aggiornare Apache alla versione 2.2.13 o successiva.
2. **Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows**
   - **Descrizione:** Problemi di buffer overflow nei meccanismi RPC di Samba, che possono essere sfruttati per eseguire codice arbitrario con i privilegi del servizio.
   - **Impatto:** Remote Code Execution (RCE) e Denial of Service (DoS).
   - **Mitigazione:** Aggiornare Samba alla versione 3.6.4 o successive, o limitare l'accesso remoto al servizio.
3. **PHP Unsupported Version Detection**
   - **Descrizione:** Il sistema utilizza una versione non più supportata di PHP, esponendolo a vulnerabilità conosciute.
   - **Impatto:** Rischio elevato di exploit per Remote Code Execution (RCE) o furto di dati.
   - **Mitigazione:** Aggiornare PHP a una versione supportata, come PHP 8.x, e garantire la compatibilità delle applicazioni.

Conclusione

La scansione ha evidenziato una serie di vulnerabilità critiche che potrebbero compromettere seriamente la sicurezza del sistema. Ovviamente è corretto specificare che la macchina metasploitable è pensata proprio per fare test e per essere vulnerabile e facilmente penetrabile. Il focus su tre vulnerabilità di alto rischio ha permesso di identificare i problemi principali e di proporre soluzioni pratiche, tra cui aggiornamenti software e configurazioni di sicurezza migliorate.

L'analisi delle porte aggiuntive ha fornito ulteriori informazioni sul livello di esposizione del sistema, confermando l'importanza di eseguire scansioni regolari e aggiornare costantemente i servizi in uso.

Raccomandazioni

1. **Aggiornamenti software:**
   - Aggiornare tutti i servizi vulnerabili alle versioni più recenti supportate.
2. **Hardening del sistema:**
   - Limitare l'accesso alle porte critiche e configurare firewall per bloccare connessioni non autorizzate.
3. **Monitoraggio continuo:**

    - Implementare un sistema di monitoraggio e rilevamento delle intrusioni (IDS/IPS) per identificare attività sospette.
4. **Manutenzione regolare:**
    - Eseguire scansioni periodiche con Nessus per mantenere il sistema sicuro.