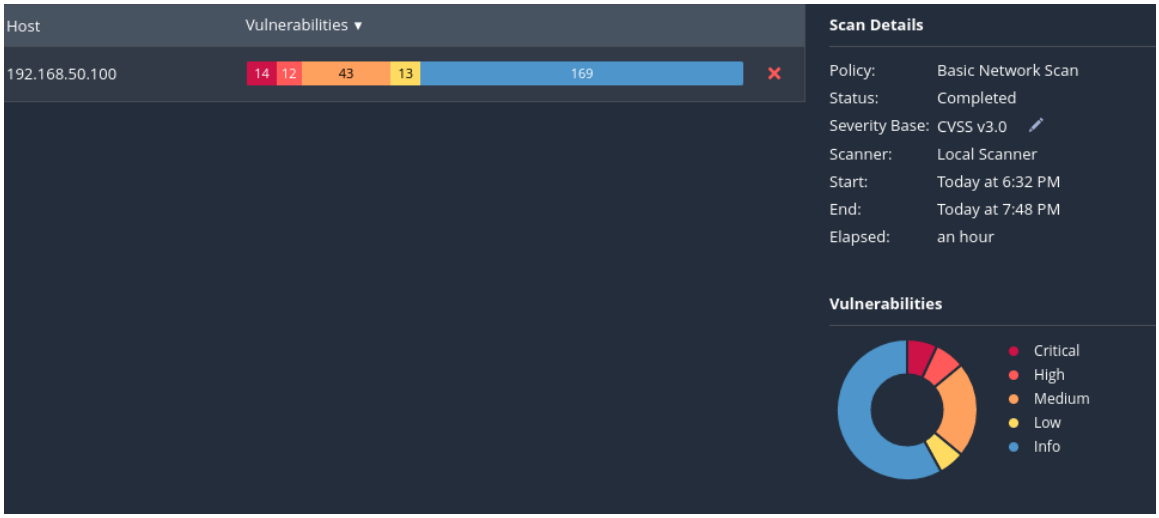
Report sull'Analisi delle Vulnerabilità



1. Introduzione

Questo report dettaglia le vulnerabilità identificate durante l'analisi condotta sul sistema Metasploitable. Il focus è posto sulle minacce critiche che richiedono attenzione immediata per prevenire possibili exploit.

2. Metodologia

L'analisi è stata effettuata utilizzando la piattaforma Nessus™, che ha eseguito una scansione completa, identificando vulnerabilità basate su pattern noti e configurazioni errate.

3. Elenco delle Vulnerabilità Critiche

- ID: 70728 - Esecuzione di Codice Remoto PHP-CGI

Descrizione: La versione di PHP installata permette l'esecuzione di codice arbitrario da remoto.

Soluzione: Aggiornamento a PHP versione 5.3.13 / 5.4.3 o successiva.

Rischio: Alto

Punteggio CVSS: 9.8

- ID: 32321 - Debolezza del Generatore di Numeri Casuali in Debian OpenSSH/OpenSSL

Descrizione: L'attaccante può ottenere la parte privata della chiave remota e decifrare le sessioni o configurare attacchi man-in-the-middle.

Soluzione: Rigenerare tutto il materiale crittografico sul host remoto.

Rischio: Critico

Punteggio CVSS: 10.0

4. Grafici della Pericolosità

(Inserire grafico qui: Mostrare la percentuale delle vulnerabilità classificate come critiche, alte, medie, e basse)

5. Impatto delle Vulnerabilità

Le vulnerabilità critiche identificate possono permettere agli attaccanti di compromettere completamente il sistema, con conseguente accesso non autorizzato a dati sensibili e potenziale interruzione delle operazioni.

6. Raccomandazioni per la Mitigazione

- Aggiornamento immediato del software vulnerabile.

- Implementazione di misure di sicurezza aggiuntive come firewall avanzati e sistemi di rilevamento delle intrusioni.

7. Conclusione

È imperativo prendere misure immediate per mitigare le vulnerabilità rilevate al fine di proteggere l'infrastruttura IT e mantenere la continuità operativa.

8. Appendice

Dettagli tecnici completi e output delle scansioni (per uso interno).