RAPPORTO HTTP E VALUTAZIONE DI SICUREZZA

Tipologia di Test: Verifica delle operazioni HTTP.
Esito Complessivo: Tutte le richieste completate con successo.

Dettagli dei Test:

- **Richiesta GET:**
  - Status Code: 200 (OK).
  - Risultato: Risposta ricevuta correttamente.
- **Richiesta POST:**
  - Status Code: 200 (OK).
  - Risultato: Dati inviati e accettati correttamente.
- **Richiesta PUT:**
  - Status Code: 201 (Created).
  - Risultato: Risorsa creata con successo.
- **Richiesta DELETE:**
  - Status Code: 204 (No Content).
  - Risultato: Risorsa eliminata con successo.

Consigli per la Sicurezza

1. **Validazione delle Richieste:**
   - Verifica che solo client autorizzati possano eseguire operazioni come POST, PUT e DELETE.
   - Implementa un sistema di autenticazione e autorizzazione (es. OAuth 2.0).
2. **Protezione dei Dati:**
   - Assicurati che il traffico HTTP sia crittografato (usare HTTPS).
   - Evita di accettare payload non sicuri per richieste POST e PUT; valida i dati in ingresso.
3. **Log delle Attività:**
   - Registra tutte le richieste ricevute e i relativi codici di risposta per analisi e tracciabilità.
4. **Rate Limiting:**
   - Limita il numero di richieste per IP per prevenire attacchi DoS.
5. **Verifica del Contenuto:**
   - Per DELETE, verifica che le richieste siano provenienti da utenti autorizzati per evitare eliminazioni non intenzionali.

RAPPORTO DI SICUREZZA PER LA SCANSIONE PORTE

Indirizzo IP Scansionato: 192.168.50.101 (Server-Metasploitable2)
Range di Porte Analizzate: 1-100

Porte Aperte:

- **21 (FTP)**: Utilizzata per il trasferimento di file. Rischi: accessi non autorizzati.
- **22 (SSH)**: Accesso remoto sicuro. Rischi: brute force.
- **23 (Telnet)**: Protocollo non sicuro. Rischio elevato di intercettazione.
- **25 (SMTP)**: Utilizzato per l'invio email. Rischio di abuso per spam.
- **53 (Domain)**: DNS server. Potenziale vulnerabilità a cache poisoning.
- **80 (HTTP)**: Servizio web non crittografato. Rischio di intercettazione dei dati.

Porte Filtrate: Nessuna.
Porte Chiuse: 94.

Consigli sulla Sicurezza:

1. **FTP (porta 21)**: Configurare FTPS o disabilitare il servizio se non necessario.
2. **SSH (porta 22)**: Limitare accessi per IP, usare chiavi RSA, disabilitare login con password.
3. **Telnet (porta 23)**: Sostituire con SSH o disabilitare.
4. **SMTP (porta 25)**: Implementare autenticazione e limiti anti-spam.
5. **DNS (porta 53)**: Monitorare per attività sospette.
6. **HTTP (porta 80)**: Implementare HTTPS per crittografare il traffico.

Generale: Limitare accesso alle porte aperte tramite firewall e usare sistemi di rilevamento delle intrusioni (IDS). Monitorare log regolarmente per rilevare attività anomale.