Obiettivo del Progetto:

Il progetto mira a eseguire una scansione completa del sistema Metasploitable, identificando e mitigando le vulnerabilità critiche.

Metasploitable è una macchina virtuale volutamente vulnerabile, utilizzata per test di sicurezza. Le azioni di rimedio comprendono modifiche alle configurazioni di sistema e l'implementazione di regole firewall per limitare l'esposizione dei servizi vulnerabili. Successivamente, una nuova scansione valuterà l'efficacia delle misure implementate.

Questo report fornisce una panoramica completa delle azioni intraprese per migliorare la sicurezza del sistema Metasploitable, evidenziando le vulnerabilità iniziali, le azioni di rimedio e i risultati ottenuti.

Metodologia:

- Preparazione dell'Ambiente
- *Esecuzione della Scansione Iniziale*
- *Identificazione delle Vulnerabilità Critiche*
- *Implementazione delle Azioni di Rimedio*
- *Verifica dell'Efficacia delle Azioni di Rimedio*
- *Risultati*
- *Conclusioni*

Fase 1: Preparazione dell'Ambiente

Setup di Metasploitable:

Scaricato e importato Metasploitable su VMware.

Configurato con indirizzo IP statico all'interno della rete virtuale.

Strumenti Utilizzati:

Nmap: Per la scansione delle porte e l'identificazione dei servizi.

Metasploit Framework: Per l'analisi delle vulnerabilità.

Firewall (iptables): Per l'implementazione delle regole di sicurezza.

Fase 2: Esecuzione della Scansione Iniziale

Comando Nmap Utilizzato:

nmap -A -T4 192.168.56.101

Dettagli del Comando:

-A: Rilevamento di OS e versioni.

-T4: Velocità di scansione "aggressiva".

Risultati della Scansione Iniziale:

1. Porte Aperte e Servizi Identificati:
2. FTP (Porta 21): Servizio FTP con autenticazione anonima.
3. Telnet (Porta 23): Servizio Telnet non criptato.
4. Samba (Porte 139, 445): Condivisione SMB con configurazioni deboli.
5. MySQL (Porta 3306): MySQL con credenziali di default.

Fase 3: Identificazione delle Vulnerabilità Critiche

1. FTP (Porta 21):

Problema: **Autenticazione anonima abilitata**.

2. Telnet (Porta 23):

Problema: **Comunicazione non criptata**.

3. Samba (Porte 139, 445):

Problema: **Configurazioni di condivisione deboli**.

4. MySQL (Porta 3306):

Problema: **Credenziali di default utilizzate**.

Fase 4: Implementazione delle Azioni di Rimedio

FTP (Porta 21):

Modifica della Configurazione:

- **File**: /etc/vsftpd.conf
- **Modifica**: anonymous_enable=NO
- **Riavvio del Servizio:** service vsftpd restart

- **Regola Firewall:** iptables -A INPUT -p tcp --dport 21 -j DROP

Telnet (Porta 23):

- **Disabilitazione del Servizio**: service telnet stop
- **Rimozione dal Boot Automatico:** chkconfig telnet off
- **Regola Firewall:** iptables -A INPUT -p tcp --dport 23 -j DROP

Samba (Porte 139, 445):

Modifica della Configurazione: File: /etc/samba/smb.conf

- **Modifica**: [global]

  security = user

- **Riavvio del Servizio:** service smb restart
- **Regole Firewall:** iptables -A INPUT -p tcp --dport 139 -j DROP

  iptables -A INPUT -p tcp --dport 445 -j DROP

MySQL (Porta 3306):

- **Modifica della Password:** mysql -u root -p

  ALTER USER 'root'@'localhost' IDENTIFIED BY 'new_password';

- **Restrizione dell'Accesso**: File: /etc/mysql/my.cnf
- **Modifica**: bind-address = 127.0.0.1
- **Riavvio del Servizio:** service mysql restart
- **Regola Firewall:** iptables -A INPUT -p tcp --dport 3306 -j DROP

Fase 5: Verifica dell'Efficacia delle Azioni di Rimedio

- **Nuova Scansione con Nmap**: nmap -A -T4 192.168.56.101
- **Analisi dei Nuovi Risultati**:
- **Confronto con la Scansione Iniziale**:

FTP (Porta 21): La porta risulta chiusa.

Telnet (Porta 23): La porta risulta chiusa.

Samba (Porte 139, 445): Le porte risultano chiuse.

MySQL (Porta 3306): La porta risulta chiusa.

Risultati

FTP:

Iniziale: Porta aperta, autenticazione anonima abilitata.

Finale: Porta chiusa, autenticazione anonima disabilitata.

Telnet:

Iniziale: Porta aperta, servizio non criptato.

Finale: Porta chiusa, servizio disabilitato.

Samba:

Iniziale: Porte aperte, configurazioni deboli.

Finale: Porte chiuse, sicurezza migliorata.

MySQL:

Iniziale: Porta aperta, credenziali di default.

Finale: Porta chiusa, credenziali modificate.

Conclusioni

Valutazione dell'Efficacia:

Le azioni di rimedio implementate hanno significativamente ridotto le vulnerabilità di Metasploitable. Le configurazioni di sicurezza sono state migliorate e le porte vulnerabili sono state adeguatamente chiuse o messe in sicurezza.

Raccomandazioni Future:

1. **Monitoraggio Continuo:** Implementare un sistema di monitoraggio continuo per rilevare eventuali nuove vulnerabilità.
2. **Aggiornamenti Regolari:** Mantenere il sistema e le applicazioni aggiornati per prevenire nuove minacce.
3. **Ulteriore Hardening:** Considerare ulteriori misure di hardening, come l'uso di strumenti di controllo dell'integrità dei file e di intrusion detection systems (IDS).