### ****Relazione sull’Esercizio di Vulnerability Scanning****

#### ****Target****: Macchina Metasploitable (IP: 192.168.50.101)

#### ****Strumento Utilizzato****: Nessus

### ****2. Configurazione della Scansione****

* **Target**: 192.168.50.101
* **Porte Analizzate**:
  + 21 (FTP), 22 (SSH), 23 (Telnet), 25 (SMTP), 80 (HTTP), 110 (POP3), 139 (NetBIOS), 443 (HTTPS), 445 (SMB), 3389 (RDP).
* **Tipi di Scansione Effettuati**:
  + **Basic Network Scan**: Configurazione standard per un’analisi generale.
  + **Advanced Scan**: Configurazione personalizzata per approfondire specifiche vulnerabilità.

### ****3. Panoramica dei Risultati della Scansione****

| **Gravità** | **Numero di Vulnerabilità** |
| --- | --- |
| Critiche | 9 |
| Alte | 7 |
| Medie | 25 |
| Basse | 6 |
| Informative | 134 |

#### ****Distribuzione delle Famiglie di Vulnerabilità****

* **Access Control e Autenticazione**: Password deboli e configurazioni predefinite.
* **Reti e Servizi Obsoleti**: Versioni non aggiornate di software critici.
* **Problemi di Cifratura**: Uso di cifrari deboli o protocolli obsoleti (SSL 2.0/3.0).
* **Backdoor e Accessi Non Autorizzati**: Porte aperte con servizi malevoli (es. porta 1524).

### ****4. Dettaglio delle Vulnerabilità Critiche****

#### 4.1. ****Backdoor Rilevata (Bind Shell)****

* **Porta Coinvolta**: 1524
* **Descrizione**: Una backdoor consente l’accesso remoto non autorizzato alla macchina.
* **Impatto**: Accesso completo al sistema da parte di un attaccante remoto.
* **Soluzione**: Analisi e rimozione del software malevolo; reinstallazione del sistema se necessario.

#### 4.2. ****VNC Protetto da Password Debole****

* **Porta Coinvolta**: 5900
* **Descrizione**: L’utilizzo di una password predefinita rende vulnerabile il servizio VNC.
* **Impatto**: Accesso remoto al desktop del sistema.
* **Soluzione**: Configurare una password robusta e attivare restrizioni di accesso.

#### 4.3. ****Versione Obsoleta di Apache Tomcat****

* **Porta Coinvolta**: 8180
* **Descrizione**: Uso di Tomcat 5.5.x, non più supportato dal 2012.
* **Impatto**: Vulnerabilità non patchate che consentono attacchi di tipo RCE.
* **Soluzione**: Aggiornare a una versione supportata e configurare accessi sicuri.

#### 4.4. ****Cifrari Deboli su SSL/TLS (SWEET32)****

* **Descrizione**: Uso di cifrari insicuri per SSL/TLS che espongono a attacchi di tipo brute force.
* **Impatto**: Dati sensibili trasmessi attraverso connessioni insicure.
* **Soluzione**: Aggiornare il protocollo a TLS 1.2 o superiore e disabilitare SSL 2.0/3.0.

#### 4.5. ****Weak Keys - Debian OpenSSL Randomness Issue****

* **Descrizione**: Generazione di chiavi crittografiche deboli su Debian compromette connessioni SSH e SSL.
* **Impatto**: Possibile intercettazione del traffico o accesso non autorizzato.
* **Soluzione**: Rigenerare le chiavi crittografiche e aggiornare OpenSSL.

### ****5. Raccomandazioni per la Mitigazione****

**Aggiornamenti e Patch**:

* + Aggiornare tutti i software vulnerabili, inclusi Tomcat, OpenSSH, e servizi critici come SMB.

**Controlli di Sicurezza**:

* + Eliminare backdoor (porta 1524) e verificare l’integrità del sistema.
  + Configurare restrizioni su porte non necessarie e limitare l’accesso remoto.

**Miglioramenti alla Cifratura**:

* + Implementare configurazioni sicure per SSL/TLS e rimuovere cifrari deboli.

**Hardening del Sistema**:

* + Utilizzare password robuste per servizi come VNC e SSH.
  + Eseguire una scansione periodica per individuare nuove vulnerabilità.

### ****6. Analisi dei Dati Integrativi dallo Screenshot****

Grazie allo screenshot fornito, sono stati evidenziati i seguenti aspetti:

* **134 Vulnerabilità Informative**: Molte vulnerabilità possono essere considerate a basso impatto, ma rappresentano punti di ingresso per potenziali attacchi.
* **Famiglie Maggiormente Rappresentate**: La maggior parte delle vulnerabilità deriva da configurazioni errate o software obsoleti.
* **Grafico di Distribuzione**: I dati visivi del grafico aiutano a comprendere l’urgenza delle priorità.

### ****7. Conclusioni****

Questa analisi ha mostrato una combinazione di vulnerabilità critiche e di media gravità, che espongono la macchina Metasploitable a rischi significativi. La priorità dovrebbe essere data alla rimozione delle backdoor, all’aggiornamento dei software e alla configurazione sicura dei servizi esposti. L’utilizzo di Nessus ha permesso di identificare in modo sistematico e chiaro le problematiche di sicurezza, fornendo una solida base per azioni correttive.