PREFAZIONE

Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni

Fasi dell'Esercizio:

Configurazione della Scansione:

1. Target: Metasploitable
2. Porte: Solo le porte comuni (es. 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389
3. Tipo di Scansione: Basic Network Scan: Configurazione predefinita per una scansione di rete.
   Advanced Scan: Configurabile in base alle tue esigenze specifiche. Esecuzione della Scansione:
4. Avvia la scansione configurata su Nessus.
5. Attendi il completamento della scansione e assicurati che tutte le porte specificate siano state analizzate.

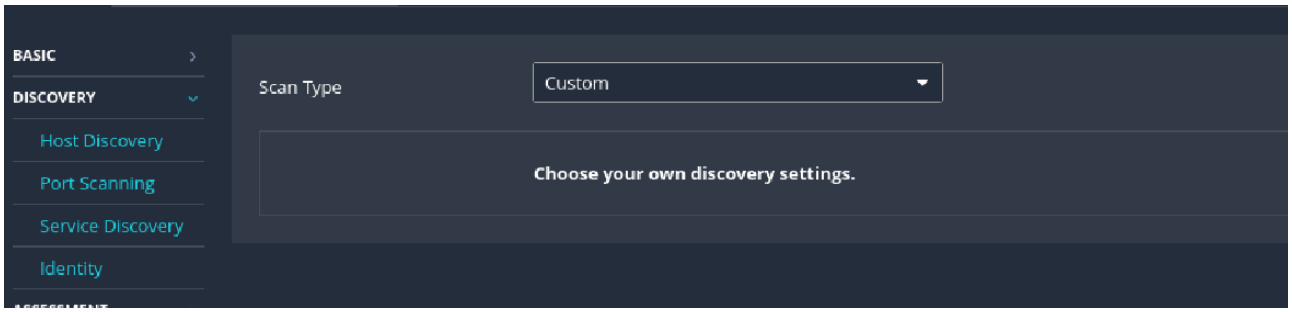
Obiettivi dell'Esercizio:
Pratica con Nessus:

- Imparare a configurare e avviare scansioni con Nessus.
- Capire come restringere le scansioni a porte specifiche. Familiarizzazione con le Vulnerabilità:
- Conoscere alcune delle vulnerabilità comuni che si possono incontrare.
- Imparare a interpretare i risultati dei report di Nessus.
- Sviluppare la capacità di approfondire e comprendere le vulnerabilità utilizzando risorse aggiuntive.

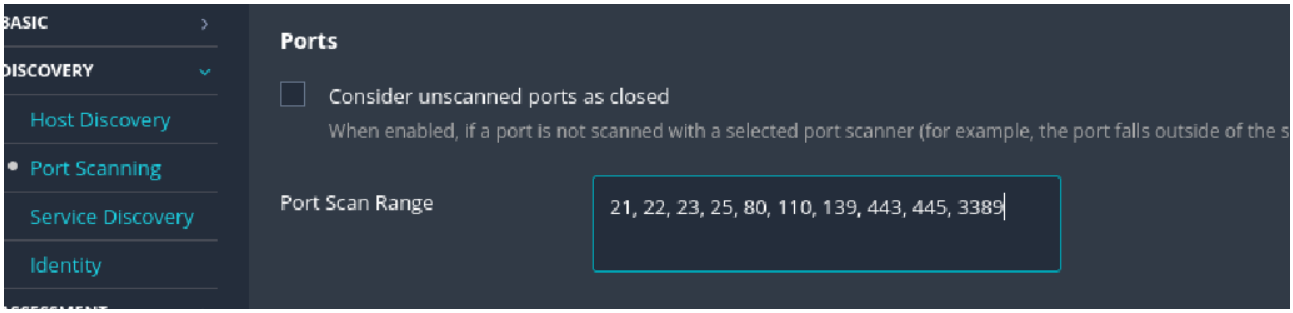
ESECUZIONE

Target: Metasploitable (Porta 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389)

Su Nessus creo una nuova scansione BASIC NETWORK SCAN "metasploitable port scan" e inserisco l'IP della Metasploitable da analizzare
Nella sezione DISCOVERY, come Scan Type inserisco "Custom"



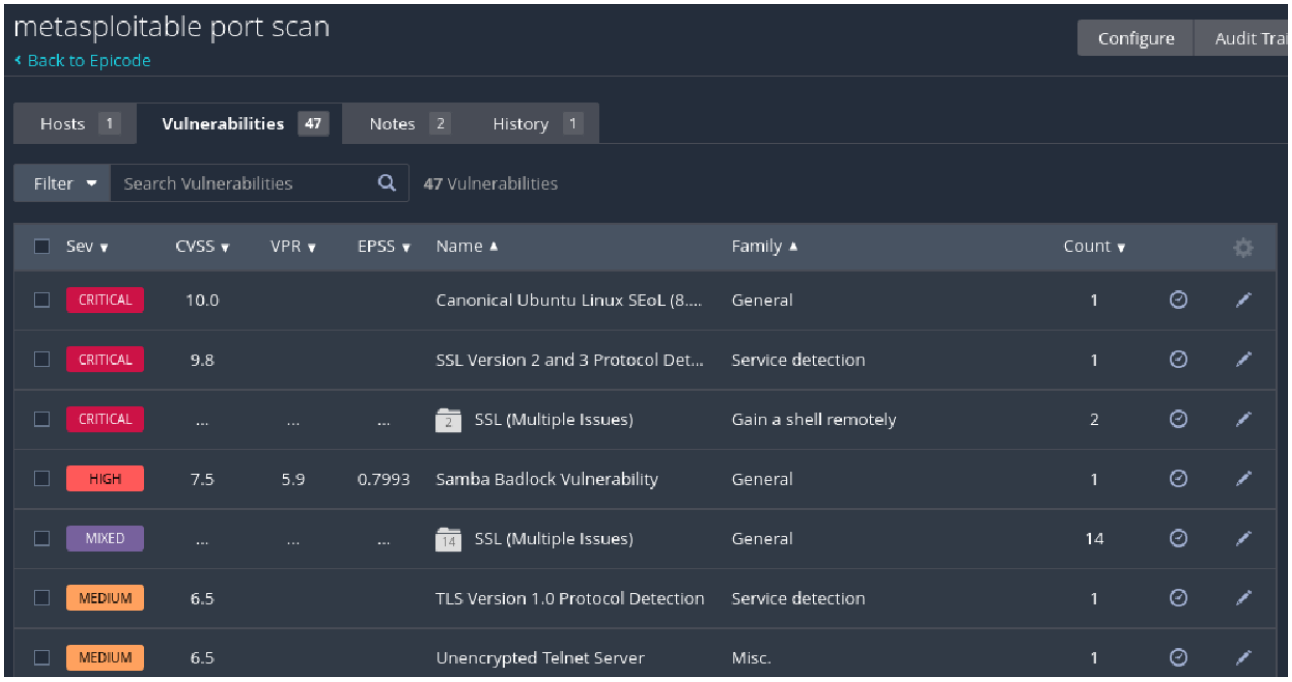
Attraverso Port Scanning inserisco le porte da analizzare



E abilito l'impostazione TCP per rilevare quali porte sono aperte
Salvo la configurazione e avvio la scansione.

Il risultato ottenuto specifica che all'interno delle Porte analizzate sono state trovate

N.47 Vulnerabilità



Le Vulnerabilità ritrovate vengono classificate in CRITICAL-HIGH-MIXED-MEDIUM- LOW E INFO

Nelle 47 Vulnerabilità, come da figura troviamo 3 di livello CRITICAL

1. Porta 80: la Vulnerabilità riguarda la versione obsoleta del Sistema Operativo nella Metasploitable (Ubuntu Linux 8.4)
   Soluzione: Effettuare un Upgrade del Sistema Operativo
2. Porta 25: SSL Version 2 and 3 Protocol Detection, trattasi di protocolli crittografici non sicuri e obsoleti. Un attaccante può sfruttare queste vulnerabilità per condurre attacchi **man-in-the-middle** o per **decifrare le comunicazioni** tra il servizio interessato e i client.
   Soluzione: Disabilitare SSL 2.0 e 3.0 e utilizzare al loro posto TLS 1.2 (o superiore)
3. Porta 22 e 25: Debian OpenSSH/OpenSSL – Debolezza del generatore di numeri casuali. La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della libreria OpenSSL.
   Un attaccante può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota oppure per impostare un attacco man-in-the-middle.
   Soluzione: Tutte le chiavi SSH, SSL e OpenVPN devono essere rigenerate

Livello HIGH troviamo 1 Vulnerabilità

1. Porta 445: Samba Vulnerabilità Badlock. La versione di Samba, server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è vulnerabile a un difetto noto come Badlock. Questo riguarda i protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD), dovuto a una negoziazione del livello di autenticazione non corretta sui canali Remote Procedure Call (RPC).Un attaccante man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa vulnerabilità per forzare un downgrade del livello di autenticazione.In questo caso l'attaccante potrebbeVisualizzare o modificare dati sensibili della sicurezza nel database di Active Directory (AD).
   - Visualizzare o modificare dati sensibili della sicurezza nel database di Active Directory (AD).
   - Disabilitare servizi critici.

   Soluzione: Effettuare un aggiornamento (Upgrade) a Samba, versione 4.2.11/4.3.8/4.4.2 o superiore

Livello MIXED, qui troviamo insieme Criticità di livello HIGH(1),MEDIUM(5),LOW(1) che riguardano la Porta 25:

1. Il problema principale è che il protocollo di sicurezza SSL (Secure Socket Layer) offre un cifrario di media sicurezza che causa Vulnerabilità.

Soluzione: Riconfigurare e utilizzare cifrari di forti in sicurezza e moderni

Vulnerabilità di Criticità MEDIUM sono 4:

1. Porta 25: TLS versione 1.0 obsoleto
   Soluzione:Disabilitare il supporto per il TLS1.0 e abilitare il supporto TLS 1.2 e 1.3
2. Porta 23: L'host sta lavorando su un server Telnet in un canale non criptato
   Soluzione: Disabilitare il servizio Telnet e usare lo SSH
3. Porta 25: L'host remoto supporta l'uso di cifrari SSL anonimi e non offre alcun meccanismo per verificare l'identità dell'host remoto e rende il servizio vulnerabile ad attacchi man-in-the-middle.

   Nota: questa vulnerabilità è notevolmente più facile da sfruttare se l'attaccante si trova sulla stessa rete fisica.
   Soluzione: Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrari deboli, in particolare i cifrari anonimi, e consentire esclusivamente cifrari sicuri che prevedano l'autenticazione tramite certificato.
4. Porta 25: L'host remoto supporta SSLv2 e potrebbe quindi essere affetto dalla vulnerabilità nota come DROWN (Decrypting RSA with Obsolete and Weakened eNcryption).
   Questa vulnerabilità è un attacco cross-protocol di tipo Bleichenbacher padding oracle, dovuto a un difetto nell'implementazione di Secure Sockets Layer versione 2 (SSLv2), che consente la decifratura del traffico TLS catturato.
   Soluzione: Disabilitare SSLv2 e le suite di cifratura a forza ridotta (export-grade).
   Assicurarsi che le chiavi private non vengano utilizzate in nessun software server che supporti connessioni SSLv2.

   Vulnerabilità MIXED 4 Criticità riscontrate

1. Porta 80: Il server web remoto supporta i metodi TRACE E/O TRACK
   Soluzione: Disabilitare i metodi Trace e Track

2. Porta 445: Sul server SMB remoto non è richiesta la firma dei messaggi.
   Un attaccante remoto non autenticato potrebbe sfruttare questa configurazione per eseguire attacchi man-in-the-middle contro il server SMB, intercettando o modificando il traffico.
   Soluzione: forzare la firma dei messaggi nella configurazione dell'host.
3. Porta 25: i protocolli SSLeTLS presentano vulnerabilità note.
   Soluzione: Attuare le soluzioni già evidenziate per SSL e TLS
4. Porta 25: Il servizio SMTP remoto presenta una vulnerabilità nell'implementazione di STARTTLS che potrebbe consentire a un attaccante remoto non autenticato di iniettare comandi durante la fase di protocollo in chiaro, i quali verrebbero poi eseguiti nella fase cifrata della comunicazione.

   Lo sfruttamento di questa vulnerabilità potrebbe permettere a un attaccante di intercettare le email della vittima o di rubare le credenziali SASL (Simple Authentication and Security Layer) associate.
   Soluzione: Contattare il fornitore del software per verificare la disponibilità di un aggiornamento o di una patch di sicurezza che risolva la vulnerabilità

   Vulnerabilità LOW

1. ICMP Timestamp Request: host remoto risponde alle richieste ICMP Timestamp. Questo consente a un attaccante remoto non autenticato di conoscere la data e l'ora impostate sulla macchina bersaglio, informazione che può essere utilizzata per aggirare meccanismi di autenticazione basati sul tempo.
   Soluzione: Filtrare le richieste ICMP Timestamp (tipo 13) e le risposte ICMP Timestamp (tipo 14), ad esempio tramite firewall o regole di rete.

Vulnerabilità MIXED

1. Porta 22: Algoritmi di Scambio delle Chiavi SSH Deboli Abilitati
   Soluzione: Contattare il fornitore del software o consultare la documentazione del prodotto per disabilitare gli algoritmi di scambio delle chiavi deboli e consentire esclusivamente algoritmi moderni e sicuri
2. Porta 22: Algoritmi MAC Deboli Abilitati su SSH.
   Soluzione: Contattare il fornitore del software o consultare la documentazione del prodotto per disabilitare gli algoritmi MAC MD5 e quelli a 96 bit, abilitando esclusivamente algoritmi MAC moderni e sicuri

Le altre Vulnerabilità NON SONO vere e proprie vulnerabilità, sono di livello INFO, cioè da monitorare