Task 04/12/24: Vulnerability Scanning

Traccia

Obiettivo:

Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

Istruzioni:

1. Configurazione della Scansione:
Target: Metasploitable
Porte: Solo le porte comuni (es. 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389
Tipo di Scansione (scegline una):
Basic Network Scan: Configurazione predefinita per una scansione di rete.
Advanced Scan: Configurabile in base alle tue esigenze specifiche.

2. Esecuzione della Scansione:
Avvia la scansione configurata su Nessus.
Attendi il completamento della scansione e assicurati che tutte le porte specificate siano state analizzate.

3. Analisi del Report:
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.

Task 04/12/24: Vulnerability Scanning

Analisi del Report di Nessus

Risultati Principali

Dalla scansione della macchina Metasploitable (IP: 192.168.50.101), Nessus ha identificato numerose vulnerabilità. Per ogni categoria di rischio (Critical, High, Medium, Low), vengono elencate le 5 vulnerabilità più significative identificate nel report, insieme a una **descrizione approfondita**, **porte coinvolte** e **possibile soluzione**.

Vulnerabilità Critiche

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Descrizione Approfondita: Ghostcat consente agli attaccanti di accedere ai file dell'applicazione web e potenzialmente eseguire codice remoto caricando file JSP. Questo attacco sfrutta una configurazione errata nel connettore AJP di Apache Tomcat.

Porta: `8009`

Soluzione: Aggiornare Tomcat alla versione più recente e configurare correttamente l'AJP connector.

UnrealIRCd Backdoor Detection

Descrizione Approfondita: La versione compromessa di UnrealIRCd consente agli attaccanti di eseguire codice arbitrario con privilegi root. Questo backdoor è stato introdotto in una versione compromessa del software distribuita pubblicamente.

Porta: `6667`

Soluzione: Scaricare una versione sicura di UnrealIRCd e verificare gli hash del file.

OpenSSH/OpenSSL Weak Random Number Generator

Descrizione Approfondita: Le chiavi SSH/SSL generate su Debian/Ubuntu affetti da questa vulnerabilità sono facilmente decifrabili. Questo bug ha avuto un impatto significativo sulla sicurezza globale.

Porta: `22`

Soluzione: Rigenerare tutte le chiavi crittografiche e aggiornare OpenSSL.

VNC Server 'password' Password

Descrizione Approfondita: L'uso di password predefinite deboli (es. "password") espone il server a compromissioni facili. Gli attaccanti possono ottenere il controllo completo del sistema.

Porta: `5900`

Soluzione: Cambiare la password con una forte e complessa.

SSL Version 2 and 3 Protocol Detection

Descrizione Approfondita: SSLv2/SSLv3 contiene falle crittografiche che permettono attacchi come POODLE. Sono protocolli obsoleti non più considerati sicuri per la comunicazione.

Porta: Vari (es. `25`, `5432`).

Soluzione: Disabilitare SSLv2/SSLv3 e usare TLS 1.2 o superiore.

Vulnerabilità Alte

rlogin Service Detection

Descrizione Approfondita: Il servizio rlogin trasmette dati (compresi username e password) in chiaro. È vulnerabile a sniffing e spoofing, rendendo possibili attacchi di tipo man-in-the-middle.

Porta: `513`

Soluzione: Disabilitare il servizio e utilizzare SSH.

rsh Service Detection

Descrizione Approfondita: Come rlogin, rsh trasmette dati non crittografati. Permette inoltre accessi non autenticati con configurazioni errate.

Porta: `514`

Soluzione: Disabilitare il servizio in `/etc/inetd.conf`.

Apache Tomcat Default Files

Descrizione Approfondita: I file di default su Apache Tomcat possono essere utilizzati dagli attaccanti per raccogliere informazioni sul server e trovare ulteriori vulnerabilità.

Porta: `8180`

Soluzione: Rimuovere tutti i file di esempio e configurare correttamente il server.

Bind Shell Backdoor Detection

Descrizione Approfondita: Un backdoor consente l'esecuzione remota di comandi senza autenticazione.

Porta: `1524`

Soluzione: Verificare la compromissione e reinstallare il sistema.

Samba Badlock Vulnerability

Descrizione Approfondita: Vulnerabilità nel protocollo SMB che consente attacchi man-in-the-middle.

Porta: `445`

Soluzione: Aggiornare Samba a una versione sicura.

Vulnerabilità Medie

NFS Shares World Readable

Descrizione Approfondita: Le condivisioni NFS senza restrizioni di accesso espongono i dati sensibili a utenti non autorizzati.

Porta: `2049`

Soluzione: Configurare restrizioni di accesso per IP o hostname.

HTTP TRACE / TRACK Methods Allowed

Descrizione Approfondita: Questi metodi di debug HTTP possono essere sfruttati per attacchi di tipo Cross-Site Tracing (XST).

Porta: `80`

Soluzione: Disabilitare i metodi TRACE/TRACK nel file di configurazione.

DNS Cache Snooping

Descrizione Approfondita: Un attaccante può determinare quali domini sono stati risolti recentemente, esponendo pattern di utilizzo o informazioni sensibili.

Porta: `53`

Soluzione: Configurare il DNS per rifiutare le query cache non autorizzate.

SMB Signing Not Required

Descrizione Approfondita: La firma SMB non obbligatoria espone il sistema ad attacchi man-in-the-middle.

Porta: `445`

Soluzione: Abilitare la firma SMB obbligatoria nelle configurazioni del server.

SSL Medium Strength Cipher Suites Supported

Descrizione Approfondita: Crittografia di forza media (es. 3DES) può essere compromessa da attaccanti avanzati.

Porta: Vari (es. `25`, `5432`).

Soluzione: Disabilitare le suite di crittografia di forza media e utilizzare algoritmi più robusti.

Vulnerabilità Basse

SSL Anonymous Cipher Suites Supported

Descrizione Approfondita: I cipher SSL anonimi non autenticano il server, consentendo attacchi man-in-the-middle.

Porta: Vari.

Soluzione: Configurare il server per non accettare cipher anonimi.

SSL Certificate Cannot Be Trusted

Descrizione Approfondita: Certificati autofirmati o scaduti rendono difficile verificare l'autenticità del server.

Porta: Vari (es. `25`).

Soluzione: Acquistare e configurare un certificato SSL valido.

HTTP Directory Listing Enabled

Descrizione Approfondita: La lista delle directory HTTP può esporre file sensibili agli attaccanti.

Porta: `80`.

Soluzione: Disabilitare la lista delle directory nel file di configurazione del web server.

SSH Weak Algorithms Supported

Descrizione Approfondita: Supporto per algoritmi SSH deboli facilita attacchi contro le connessioni SSH.

Porta: 22.

Soluzione: Configurare SSH per utilizzare solo algoritmi sicuri.

FTP Anonymous Login

Descrizione Approfondita: L'accesso FTP anonimo espone il server a utilizzi non autorizzati.

Porta: 21.

Soluzione: Disabilitare l'accesso anonimo per il servizio FTP.