Ricerca delle vulnerabilità tramite Nessus

**Introduzione**

Come richiesto dalla traccia è stata condotta una dettagliata analisi di vulnerabilità sulla macchina virtuale Metasploitable, specificatamente all'indirizzo IP 192.168.1.3. Per questa analisi, è stato impiegato Nessus, uno degli strumenti di scansione di vulnerabilità più diffusi e affidabili nel campo della sicurezza informatica. Nessus aiuta gli analisti a identificare le vulnerabilità esistenti in un sistema, fornendo dettagliate relazioni che elencano e classificano i potenziali rischi in base alla loro gravità.

L'obiettivo principale di questa attività è stato quello di scoprire, valutare e mitigare efficacemente le vulnerabilità presenti nel sistema target, facendo leva sulla capacità di Nessus di eseguire scansioni profonde e accurate.

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

Report di Risoluzione delle Vulnerabilità

**Vulnerabilità Affrontate:**

1. CRITICAL 9.8 9.0 134862 Apache Tomcat A JP Connector Request Injection (Ghostcat)

2. CRITICAL 10.0 - 171340 Apache Tomcat SEoL (<= 5.5.x)

3. NFS Exported Share Information Disclosure

Passaggi Eseguiti per la Risoluzione:

**1. Apache Tomcat A JP Connector Request Injection (Ghostcat):**

- Analisi della Vulnerabilità: La vulnerabilità Ghostcat è stata identificata come una potenziale minaccia alla sicurezza del server Apache Tomcat. Questa vulnerabilità consente a un attaccante di eseguire un attacco di iniezione di richieste sul connettore AJP di Tomcat.

- Soluzione Implementata: Per risolvere questa vulnerabilità, è stata eseguita l'aggiornamento di Apache Tomcat alla versione più recente disponibile, che includeva le correzioni di sicurezza per affrontare la vulnerabilità Ghostcat

**2. Apache Tomcat SEoL (<= 5.5.x):**

- Analisi della Vulnerabilità: La vulnerabilità SEoL in Apache Tomcat (versioni <= 5.5.x) è stata identificata come una minaccia potenziale alla sicurezza del server Tomcat. Questa vulnerabilità può consentire a un attaccante di eseguire attacchi di tipo denial-of-service (DoS) contro il server Tomcat.

- Soluzione Implementata: Per mitigare questa vulnerabilità, è stata eseguita l'installazione dell'ultima versione disponibile di Apache Tomcat, che includeva le correzioni di sicurezza per affrontare la vulnerabilità SEoL.

**3. NFS Exported Share Information Disclosure:**

- Analisi della Vulnerabilità: La vulnerabilità **"NFS Exported Share Information Disclosure"** è stata identificata come una minaccia potenziale alla sicurezza del sistema. Questa vulnerabilità può consentire a un attaccante di ottenere informazioni sensibili sulle condivisioni NFS esportate dal server, compromettendo la riservatezza dei dati.

- Soluzione Implementata: Per affrontare questa vulnerabilità, sono state esaminate e valutate le condivisioni NFS esistenti sul sistema Metasploitable. Le condivisioni non essenziali sono state rimosse o disabilitate modificando il file di configurazione NFS “/etc/exports”.

- Utilizzando un editor di testo come “nano”, sono state rimosse o commentate le linee nel file “/etc/exports” relative alle condivisioni NFS non necessarie.

- Ad esempio, se vi è una linea nel file “/etc/exports” che definisce una condivisione NFS non necessaria, questa è stata commentata aggiungendo il carattere “#” all'inizio della linea o rimuovendola completamente.

- Verifica dell'Implementazione: Dopo aver apportato le modifiche al file “/etc/exports”, il servizio NFS è stato riavviato per applicare le modifiche utilizzando il comando:

“sudo service nfs-kernel-server restart”

**Immagine che contiene testo, elettronica, schermata, software

Descrizione generata automaticamente**

**Risultati della Scansione:**

Dopo aver completato i passaggi sopra descritti e aver risolto le tre vulnerabilità critiche identificate nella prima scansione, è stata eseguita una seconda scansione di sicurezza utilizzando Nessus. I risultati della seconda scansione hanno dimostrato che tutte e 3 le vulnerabilità riscontrate nella prima scansione sono state risolte con successo.

**Immagine che contiene testo, schermata, numero, Carattere

Descrizione generata automaticamente**

**Conclusioni:**

Attraverso l'implementazione delle correzioni di sicurezza descritte sopra, il sistema Metasploitable è stato rafforzato e reso più sicuro. L'eliminazione delle vulnerabilità critiche precedentemente identificate ha ridotto significativamente il rischio di compromissione della sicurezza e ha contribuito a proteggere il sistema da potenziali attacchi.