**PROGETTO S5-L5**

Traccia:

Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio. N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità. Per dimostrare l’efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

STEP 1

Mi assicuro innanzitutto di aver configurato correttamente le schede di rete sia di Kali sia di Metasploitable impostando una rete interna. Per verificare che le due macchine stiano comunicando tra loro vado ad effettuare un ping.

Immagine che contiene testo, schermata, Carattere, bianco e nero

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente

STEP 2

Avvio Nessus utilizzando il comando in figura:

Immagine che contiene testo, schermata, Carattere, Software multimediale

Descrizione generata automaticamente

Adesso vado ad effettuare una nuova scansione impostando come target l’indirizzo IP di Metasploitable. Nella sezione “Plugins” posso eventualmente andare a selezionare o deselezionare le vulnerabilità interessate. Avvio la scansione:

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Terminata la scansione posso osservare le varie vulnerabilità individuate e contrassegnate da colori diversi a seconda della criticità.

Immagine che contiene testo, schermata, Carattere, linea

Descrizione generata automaticamente

Immagine che contiene testo, software, Software multimediale, Software per la grafica

Descrizione generata automaticamente

In questo caso prendo in esame alcune vulnerabilità “Critical”.

STEP 3

Vado a esaminare le seguenti vulnerabilità:

VULNERABILITA’ “NFS Exported Share Information Disclosure”.

Questa vulnerabilità riguarda i sistemi che utilizzano il NFS (Network File System), un protocollo che consente a diversi sistemi operativi di condividere risorse di file su una rete. Più precisamente NFS consente a un sistema di archiviazione remoto (server) di esportare o condividere directory e file, consentendo ad altri sistemi (client) di accedervi come se fossero archiviati localmente. Naturalmente queste condivisioni possono essere configurate con vari livelli di autorizzazione e accesso. Avendo trovato questa vulnerabilità, posso dedurre che il server NFS sia configurato in modo non sicuro. Questo consentirebbe a eventuali utenti non autorizzati di accedere ai file esportati. Correggere questa vulnerabilità è molto importante poiché l'esposizione non autorizzata di eventuali informazioni sensibili può compromettere la riservatezza dei dati e portare a gravi conseguenze.

Inizio utilizzando il comando “sudo nano /etc/exports” sul terminale di Metasploitable, che elenca tutte le condivisioni NFS attualmente configurate sul server:

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Nel file di configurazione trovo diversi parametri:

1. \*: indica l'indirizzo IP o il nome del client a cui si applica la configurazione, in questo caso a tutti i client che possono quindi accedere alla condivisione.
2. rw: "read-write" (lettura-scrittura), consente ai client di leggere e scrivere file sulla condivisione NFS.
3. sync: specifica come il server NFS gestisce la scrittura dei dati sulla condivisione NFS. Con questa opzione, il server NFS conferma la scrittura dei dati solo dopo averli scritti sul disco, garantendo un comportamento sincrono e riducendo il rischio di perdita di dati in caso di errore del sistema.
4. no\_root\_squash: quando questa opzione viene utilizzata, il server NFS consente all'utente root di eseguire operazioni privilegiate come se fosse locale, senza ridurre i privilegi come di solito fa con l'utente root remoto (root squashing).
5. no\_subtree\_check: disabilita il controllo delle autorizzazioni per le sottodirectory.

*Remediation Action*

Disattivo questa configurazione semplicemente commentando la riga:

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Vulnerabilità “VNC Server ‘password’ Password”

Analizzo adesso la vulnerabilità “VNC Server ‘password’ Password”. Questa vulnerabilità implica che il server VNC (Virtual Network Computing) sia stato configurato con una password di accesso predefinita o debole. Questo significa che chiunque conosca la password predefinita o sia in grado di indovinarla potrebbe ottenere l'accesso non autorizzato al sistema VNC.

*Remediation Action*

Per risolvere questa problematica accedo al root di Metasploitable e utilizzo il comando “vncpasswd”. Questo mi consentirà di inserire una password più sicura. Scelgo infine di non inserire una password di sola lettura.

Immagine che contiene testo, schermata, Carattere, nero

Descrizione generata automaticamente

Adesso posso provare ad accedere al server VNC di Metasploitable da terminale su Kali, per verificare che il procedimento abbia avuto successo. Assicurandomi prima del fatto che il pacchetto “vncviewer” risulti installato su Kali Linux, vado a utilizzare il comando “vncviewer 192.168.50.101” per accedere al server. Nel momento in cui mi verrà chiesto di inserire la password, provo prima a inserire quella precedente:

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

L’autenticazione è fallita. Provo a inserire la nuova password:

Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente

Immagine che contiene testo, computer, schermata, software

Descrizione generata automaticamente

Ho ottenuto l’accesso a Metasploitable, quindi la password è stata sostituita con successo.

Vulnerabilità “Bind Shell Backdoor Detection”

Prendo in esame la vulnerabilità “Bind Shell Backdoor Detection”. Questa vulnerabilità si riferisce alla presenza di una backdoor (Bind Shell) su un sistema. Una backdoor è un tipo di malware o software dannoso che consente agli attaccanti di ottenere un accesso non autorizzato e di controllare un sistema remoto. Precisamente “Bind Shell” è un tipo di backdoor che apre una porta di rete sul sistema e ascolta le connessioni in entrata su quella porta. Quando viene stabilita una connessione con la porta, l'attaccante può dunque ottenere un accesso remoto al sistema. Di solito, la configurazione predefinita di Metasploitable include un servizio Bind Shell sulla porta 1524, che quindi andremo a controllare. Per bloccarla utilizziamo il firewall UFW (Uncomplicated Firewall) su Metasploitable. UFW è uno strumento di gestione del firewall che semplifica notevolmente la configurazione e l'amministrazione delle regole del firewall stesso.

*Remediation Action*

Accedo al root di Metasploitable e vado a utilizzare il comando “ufw deny 1524”. Questo comando andrà a impostare una regola nel firewall che servirà a bloccare il traffico in ingresso sulla porta 1524. Come possiamo vedere se in seguito utilizzerò il comando “ufw status”, vedrò che qualsiasi tentativo di connessione in entrata sulla porta 1524 (TCP e UDP) sarà respinto dal firewall e non avrò quindi il permesso di raggiungere Metasploitable.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

STEP 4

Eseguo infine una nuova scansione del target Metasploitable su Nessus per verificare che tra le vulnerabilità “Critical” rimaste non ci siano più quelle che ho risolto:

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente