Immagine che contiene testo, schermata, Carattere, documento

Descrizione generata automaticamente

Immagine che contiene testo, software, Software multimediale, schermata

Descrizione generata automaticamente

Dalla scansione effettuato alla macchina Metasploit risultano questo vulnerabilità critiche :

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

Da queste ho scelto queste vulnerabilità :

1. NFS Exported share information Disclosure :

La vulnerabilità "NFS Exported Share Information Disclosure" è considerata critica perché può esporre informazioni sensibili su un sistema, inclusi file e directory, attraverso il protocollo NFS (Network File System). L'NFS è un protocollo di condivisione file che consente a un sistema di montare in remoto filesystem da un altro sistema come se fossero locali.

Quando una condivisione NFS è configurata in modo non sicuro, potrebbe consentire a chiunque di ottenere accesso alle informazioni senza dover autenticarsi. Ecco perché questa vulnerabilità è significativa:

**Rivelazione di Informazioni Sensibili:** La vulnerabilità potrebbe permettere a un attaccante di elencare e recuperare informazioni su file e directory presenti nella condivisione NFS senza autenticazione. Questo può includere dati sensibili, configurazioni di sistema e altri file critici.

**Potenziale per l'Esecuzione di Comandi**: In alcuni casi, l'accesso non autorizzato tramite NFS potrebbe essere sfruttato per eseguire comandi arbitrari sul sistema remoto, portando a un compromesso della sicurezza.

**Violazione della Privacy e della Riservatezza**: Se la condivisione NFS contiene dati sensibili o riservati, la loro esposizione potrebbe violare la privacy e la riservatezza degli utenti o delle informazioni aziendali.

**Possibile Avvio di Attacchi a Catena**: L'accesso a informazioni sensibili potrebbe essere il primo passo per ulteriori attacchi, fornendo a un malintenzionato la conoscenza necessaria per pianificare e eseguire attacchi più mirati.

Risoluzione :

Sono andata dentro la macchina Metasploit ho scrito il comando :

sudo nano /etc/exports

che mi ha fatto entrare sul file exports , il quale non aveva nessuna regola che filtrava la lettura o scrittura , ho modificato le regole , salvato con Ctrl-X , dopo ho fatto restart .

/srv/homes 10.0.2.4(ro,sync)

hostname1(rw,sync) hostname2(ro,sync)

\*(rw,sync,no\_root\_squash,no\_subtree\_check)

sudo /etc/init.d/nfs-kernel-server restart

1. VNC server ‘password’

La vulnerabilità "VNC Server 'password' Password" indica che il server VNC (Virtual Network Computing) è configurato con una password debole o predefinita, che è spesso facilmente indovinabile. Questo tipo di vulnerabilità è critica e deve essere risolto per diverse ragioni:

Accesso Non Autorizzato: La presenza di una password debole o predefinita rende più facile per un attaccante indovinare o scoprire la password del server VNC. Ciò potrebbe consentire a un malintenzionato di ottenere accesso non autorizzato al desktop remoto e potenzialmente controllare il sistema.

Violazione della Riservatezza: Se il VNC server è utilizzato per accedere a un desktop contenente informazioni sensibili o riservate, una password debole potrebbe portare a una violazione della riservatezza. Un attaccante potrebbe visualizzare o acquisire dati sensibili dal desktop remoto.

Possibilità di Esecuzione di Comandi: Se un attaccante riesce ad ottenere l'accesso al desktop remoto, potrebbe avere la possibilità di eseguire comandi, installare malware o sfruttare altre vulnerabilità nel sistema.

Rischio di Attacchi di Forza Bruta: Una password debole o predefinita facilita gli attacchi di forza bruta, in cui un attaccante prova una serie di password fino a quando non trova quella corretta. Ciò aumenta il rischio di compromissione della password.

**Risoluzione :**

**Con il commando vncpasswd ci fa entrare nel server e poi scegliere se mettere in modalità solo view , mettendo un nuova password piu sicura**

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

1. Bind shell Backdoor Detection

La rilevazione di una bind shell backdoor è un problema critico di sicurezza che deve essere affrontato immediatamente. Ecco alcune ragioni per cui è importante risolvere questa vulnerabilità:

Accesso Non Autorizzato: Una bind shell backdoor apre una porta sul sistema che può essere utilizzata da un attaccante per ottenere accesso non autorizzato al sistema. Ciò significa che l'attaccante potrebbe ottenere controllo completo sul sistema compromesso.

Potenziale per Attacchi a Catena: La presenza di una bind shell fornisce all'attaccante un punto di ingresso per eseguire ulteriori attacchi sul sistema. Ad esempio, potrebbe essere usato come punto di partenza per l'installazione di malware, lo sfruttamento di altre vulnerabilità o il furto di dati sensibili.

Rischio per la Riservatezza dei Dati: Se un attaccante riesce a ottenere accesso tramite la bind shell, potrebbe esplorare il sistema alla ricerca di dati sensibili o informazioni aziendali riservate. Ciò rappresenta un grave rischio per la riservatezza dei dati.

Possibile Utilizzo in Attacchi Distribuiti: I sistemi compromessi possono essere sfruttati per partecipare a attacchi distribuiti come bot in una botnet. La presenza di una bind shell potrebbe essere sfruttata per controllare il sistema da remoto in un contesto più ampio.

Compromissione dell'Integrità del Sistema: Un attacco tramite bind shell potrebbe compromettere l'integrità del sistema, con possibilità di alterare file di sistema, configurazioni o persino installare backdoor persistenti.

Impatto sull'Affidabilità e la Disponibilità: Gli attacchi tramite bind shell possono avere un impatto sulla disponibilità e l'affidabilità del sistema, specialmente se l'attaccante effettua azioni dannose o intenzionalmente danneggia il sistema.

Risoluzione :

Dopo che il nessus ha indentificato il backdoor

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Andiamo con il commando :

sudo lsof -i :1524

ci fa vedere il PID della porta che e : 4530

sudo kill -9 4530

questo commando chiude la porta .

Immagine che contiene schermata, testo, software, Software multimediale

Descrizione generata automaticamentedopo questi risoluzione ho ripetuto lo scan e il risultato e ottimale .