## D3 Progetto

Immagine che contiene testo, schermata, Carattere, documento

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, documento

Descrizione generata automaticamente

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Il comando sudo systemctl start nessusd.service sul terminal di Kali mi permette di collegarmi al server di Nessus.

# Vulnerabilità

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Immagine che contiene schermata, testo, software, Software multimediale

Descrizione generata automaticamente

# NFS Export Share Information Disclosure

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

NFS = Network File System è un protocollo di sistema, che consente ai clienti di accedere a file e directory su una reta, questo vuol dire che sono accessibili da remoto. Se gli NFS non sono protetti correttamente c’è la possibilità che terze parti possano accedere a queste informazioni; modificandole o eventualmente divulgarle.

Creo una cartella da esportare alla macchina server mkdir /tmp/nfs  
Modifico i permessi agli NFS, permettendo a un solo indirizzo IP di poter accedere a quei file  
sudo nano /etc/exports  
Si apre un file, in cui all’interno modifico il path permettendo soltanto all’indirizzo IP di Kali di accedere agli NFS /path/to/exported/directory 192.168.50.100\*(rw,sync) e aggiungo anche il path della cartella con l’indirizzo IP di Kali.  
Salvo il file e aggiorno la configurazione NFS sudo exportfs -a, mentre con il comando showmount -e localhost controllo la condivisione.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

## VNC Server 'password' Password

Immagine che contiene testo, software, Software multimediale, schermata

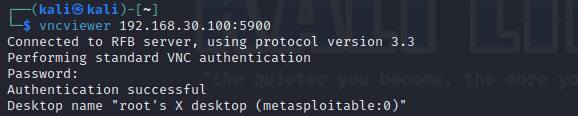
Descrizione generata automaticamente

VNC= Virtual Network Computing è un protocollo che consente a un utente di controllare un computer da remoto. Nessus mi consiglia di cambiare la password attuale con una più complessa.

Conoscendo l’ IP di Meta, tramite Kali scansiono le porte per trovare quella della VNC nmap -p 1-10000 192.168.30.100, così posso connettermi vncviewer 192.168.30.100 : 5900, e inserisco la password attuale.  
Il comando vncpasswd mi permette di cambiare la password.  
Apro un altro terminale da Kali, per verificare di aver cambiato la password correttamente, quindi riscrivo il comando vncviewer 192.168.30.100 : 5900 e inserisco la password scelta.

Immagine che contiene testo, schermata, schermo, software

Descrizione generata automaticamente



## Bind Shell Backdoor Detection

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Una Shell è in ascolto su una porta (la 1524) remota senza autenticazione. Questa può essere utilizzata da un attaccante che può collegarsi e inviare comandi. Nessus suggerisce di verificare se il sistema remoto è compromesso e di reinstallare il sistema se necessario.

Eseguo nmap -p 1524 -sV 192.168.30.100 per avere maggiori informazioni sulla porta e rilevare se ci sono servizi attivi, nc 192.168.30.100 1524 mi collego alla porta, mentre netstat -nltp vedo i processi attivi delle porte. Uso il comando kill -9 4419 per uccidere la shell attiva. Ma riavviando sistema, ritorna. Dal terminale di meta apro i file di testo dei servizi sudo vi /etc/services e della configurazione sudo vi /etc/inetd.conf e elimino la voce ingresslock che coincide con la porta 1524.

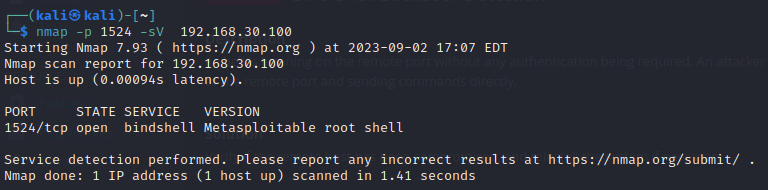




Immagine che contiene testo, schermata, menu

Descrizione generata automaticamente

Immagine che contiene testo, schermata, nero

Descrizione generata automaticamente

Immagine che contiene testo, schermata, menu, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, menu, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente



## 

## Rexecd Service Detection

Il servizio rexecd è progettato per consentire agli utenti di una rete di eseguire comandi in remoto su un sistema. Tuttavia, è importante notare che rexecd non fornisce un mezzo di autenticazione adeguato, il che significa che potrebbe essere abusato da un attaccante per eseguire comandi non autorizzati su un sistema di terze parti o per effettuare scansioni indesiderate su altre macchine.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente



Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

