Progetto S5-L5

Studente: Simone Mininni

Obiettivo: Fase di scansione della rete o di un sistema con l'ausilio di un vulnerability scanner alla ricerca di vulnerabilità conosciute, e successivamente applicare le remediation action sulle vulnerabilità critiche e high.

Software utilizzato per la scansione è Nessus, mentre il target della scansione è la macchina Metasploitable.

Analizziamo i risultati prodotti dalla scansione iniziale:

Possiamo notare che sono state trovate diverse vulnerabilità di cui 22 critiche, 7 high, 18 medium, 7 low…

Sicuramente i risultati critici meritano la priorità assoluta e sono quelli su cui cercheremo di trovare e applicare una soluzione.

Link report Nessus iniziale:
https://github.com/simonemin/S5-Progetto/blob/main/scansioneInizio.pdf

Ai fini del progetto andrò a rimediare a quattro situazioni critiche/high.

1) Vulnerabilità critica: Vnc server password

Vnc server , applicazioni software che permettono il controllo da remoto di una macchina. Si nota l' utilizzo di una password debole, facilmente trovabile con un attacco brute force.

Soluzione: sostituire con una password mediamente complessa.

sudo su
vncpasswd

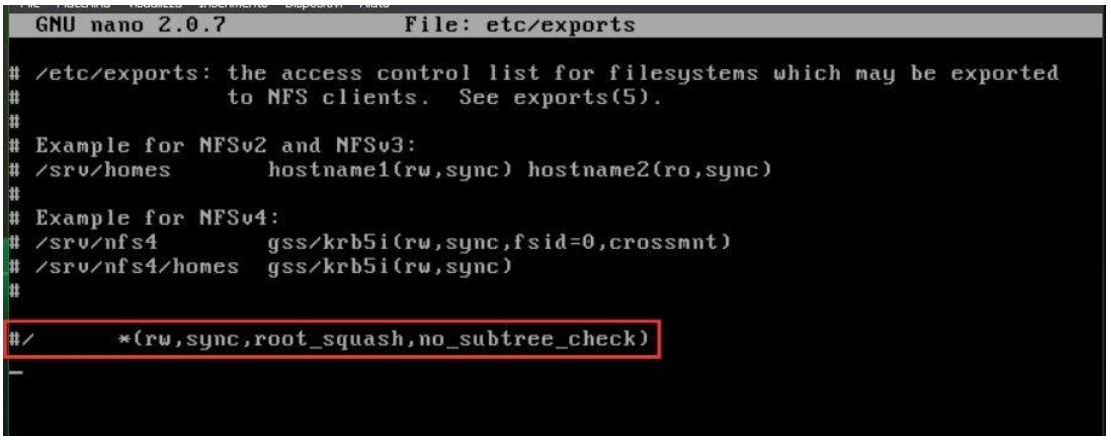
Passaggi per cambiare la password sulla metasploitable con i privilegi root.

2) Vulnerabilità critica: NFS

NFS (Network File Sharing) è un protocollo che permette di condividere file system(directories e files) sulla rete.
In questo caso vi è una criticità importante poichè un malintenzionato(client linux) potrebbe montare il file system e ispezionare tranquillamente directories file e magari anche manipolarli.

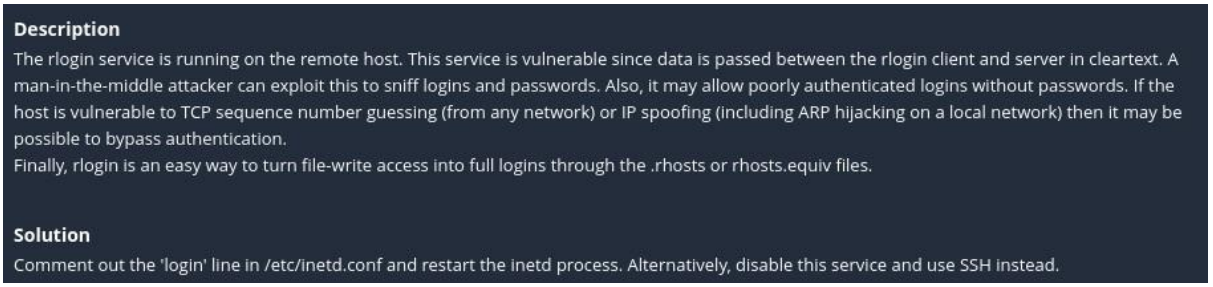
Bisogna quindi impostare NFS in modo che possa essere accessibile solo da client autorizzati.

Nel nostro caso andiamo a manipolare il file di configurazione (/etc/exports) ed a commentare la riga di condivisione della directory, in modo che nfs non condivida nessun filesystem sulla rete.

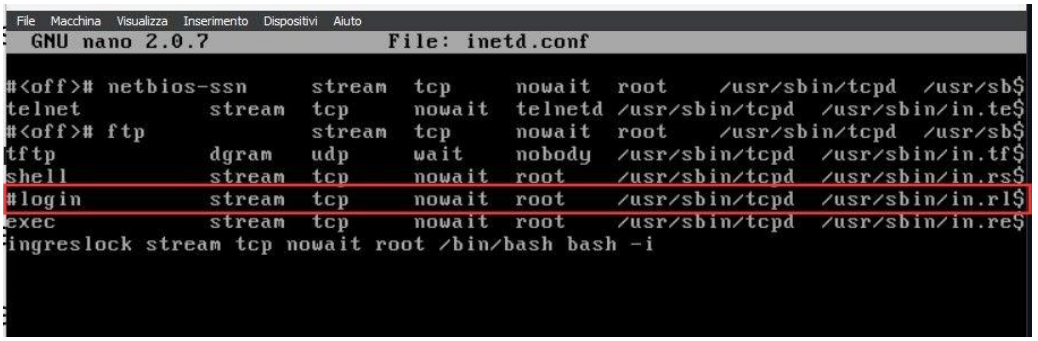


In questo modo andiamo a risolvere le due vulnerabilità.

3)Vulnerabilità high: rlogin service detection

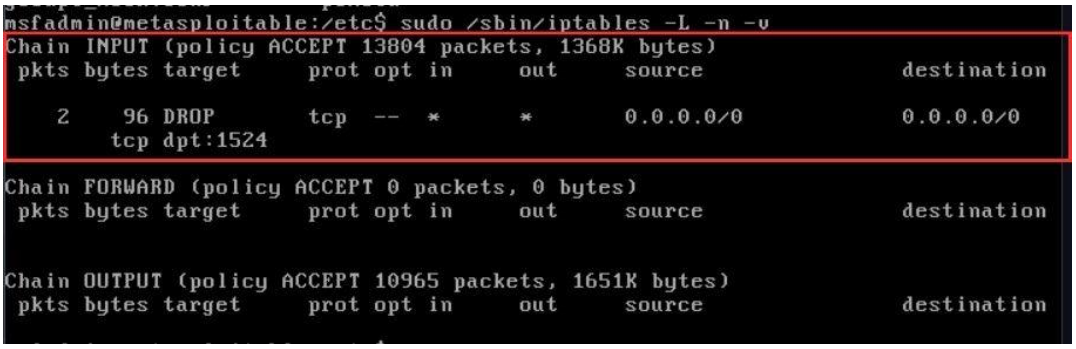


Dal report di Nessus si evince che è possibile risolvere facilmente il problema commentando la riga di login nel file /etc/inetd.conf.



4) Vulnerabilità critica: Bind Shell Backdoor Detection

Bind shell backdoor permette all' attaccante di connettersi alla macchina vittima bypassando i sistemi di autenticazione e quindi prendere il controllo della stessa.
Soluzione: ho impostato una rule sul firewall iptables in modo tale da rigettare tutto il traffico in entrata sulla porta '1524' dove è in ascolto il servizio della backdoor.
comando da shell:
'sudo /sbin/iptables -A INPUT -p tcp –dport 1524 -j DROP'



Risultati scansione post remediation actions

Rispetto al report iniziale si nota quattro criticità in meno.
Link report finale:
https://github.com/simonemin/S5-Progetto/blob/main/scansioneFine.pdf