S5/L5

Traccia:

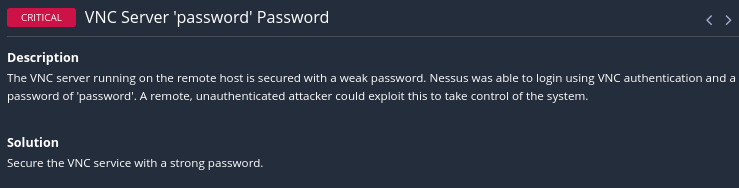
Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.

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.

Per prima cosa, effettuiamo la scansione su Nessus con l’IP di meta (192.168.50.101), come possiamo vedere escono delle vulnerabilità critiche:



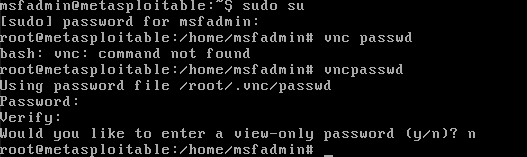
Proviamo ad analizzare e risolvere la vulnerabilità critica VNC server ‘password’ Password:



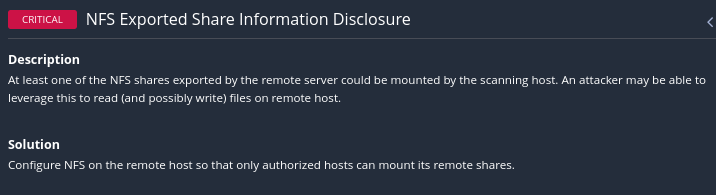
Il messaggio di Nessus indica che il server VNC (virtual network computing, è un sistema che consente ad un utente di controllare il computer da remoto attraverso una connessione) in esecuzione sull'host remoto è protetto con una password debole ("password") sulla porta 5900; Nessus è riuscito ad accedere utilizzando questa “password”. Questa è una situazione di sicurezza rischiosa, poiché una password debole può facilitare l'accesso non autorizzato al sistema.

La soluzione suggerita è di proteggere il servizio VNC con una password complessa.

Per cui andiamo sulla nostra metasploitable e inseriamo il comando “vncpasswd” ed inseriamo una password più sicura.



Adesso analizziamo la vulnerabilità critica NFS Exported Share information Disclosure:



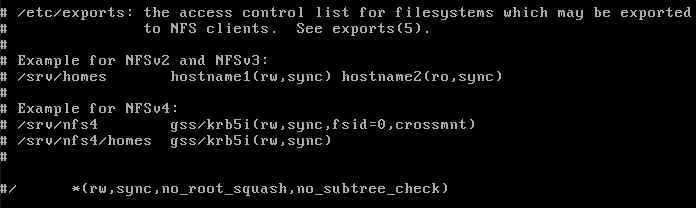
Il messaggio di Nessus indica che è stata rilevata una vulnerabilità legata alla configurazione di NFS (Network File System) sul server remoto. Questo può portare a un problema di sicurezza perché può consentire ad un utente malintenzionato di montare e accedere condivisioni NFS del server remoto senza autorizzazione. Ricordiamo che NFS è un protocollo di comunicazione utilizzato per la condivisione di file su una rete, così che gli utenti possano accedere a file remoti ma possano anche "montare" condivisioni NFS su un sistema locale, rendendo i file remoti disponibili come se fossero parte del filesystem locale. Per ridurre il rischio è necessario limitare l'accesso alle condivisioni NFS solo agli host autorizzati.

Andiamo su meta e scriviamo il comando :

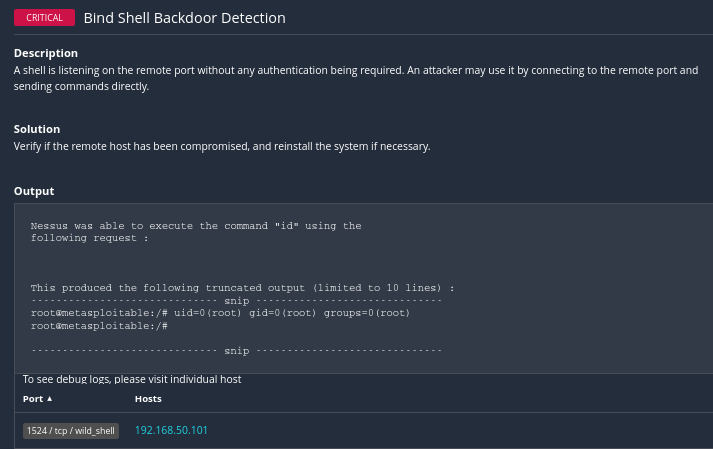
sudo nano /etc/exports, qui possiamo vedere le directory locali e nel nostro caso mettiamo a commento la riga:

#/\*(rw, sync, no\_root squah, no\_subtree\_check)

In questo modo la riga di comando verrà ignorata dal sistema. In particolare, ora non è più consentito l’accesso in lettura e scrittura (rw). Mentre con “no\_root\_squash” da un punto di vista di sicurezza, consentire l’accesso di root senza restrizioni può essere rischioso, poiché potrebbe consentire modifiche non autorizzate ai dati del server da parte dei client, per questo abbiamo messo a commento questa riga di comando.

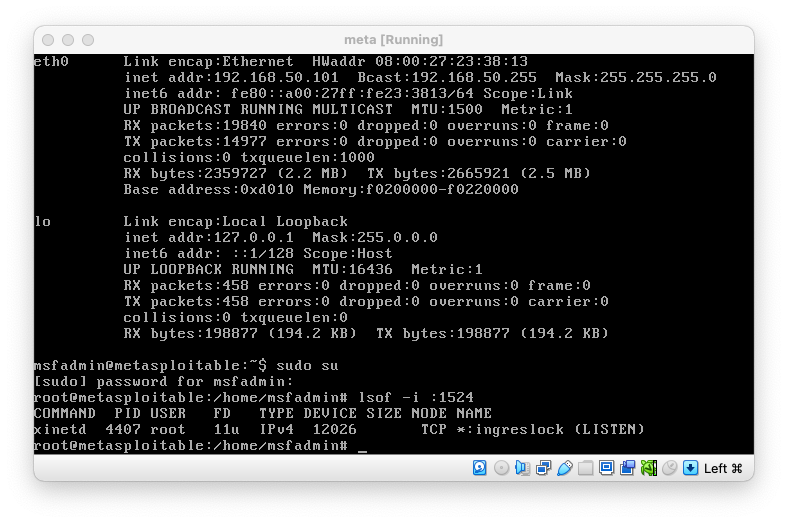


Vediamo un’altra vulnerabilità critica: Bind Shell Backdoor Detection



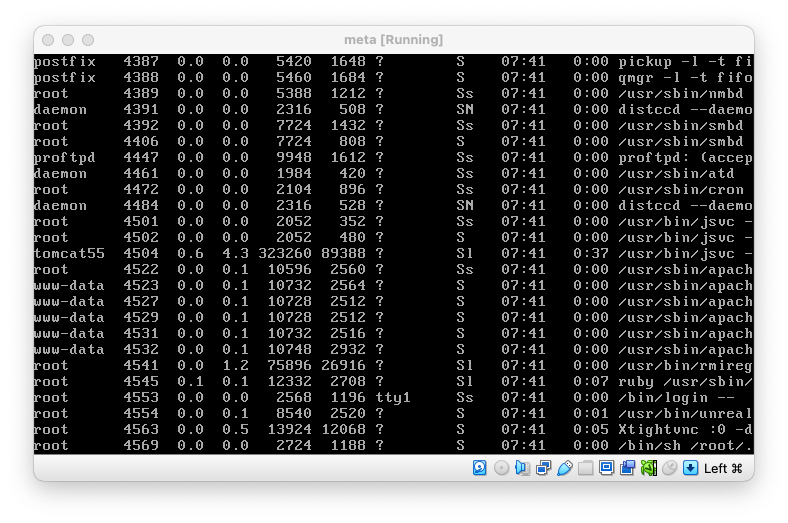
La descrizione suggerisce che una shell (interfaccia tra utente e sistema operativo) è in ascolto su una porta remota senza richiedere autenticazione. Questo rappresenta una vulnerabilità, poiché un utente malintenzionato potrebbe connettersi a questa porta: 1524 (port 1524, associata a comunicazioni di rete e a servizi che fanno parte di Ingres Database, un sistema di gestione di database relazionali) e inviare comandi direttamente, ottenendo un accesso non autorizzato al sistema.

Utilizziamo il comando “-isof -i:1524” il quale si indica i processi in ascolto su quella porta o processi che hanno stabilito connessioni attraverso essa.



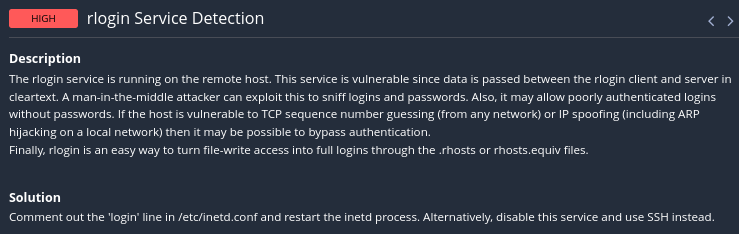
Se individuiamo un processo sospetto, possiamo utilizzare il comando kill seguito dall'PID del processo per terminarlo. Dopo aver inviato il segnale, utilizziamo il comando ”ps aux” per verificare se il processo è ancora in esecuzione. Ci viene mostrato un elenco di tutti i processi in esecuzione sul sistema ed andiamo a verificare se quello corrispondente al PID (in questo caso 4407) è ancora visibile o meno, non dovremmo vedere alcun risultato.





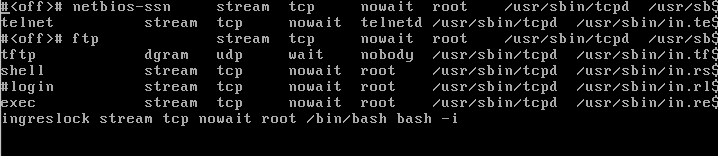


Vediamo infine una vulnerabilità di tipo “high”:



Il servizio “rlogin” è un protocollo di accesso remoto utilizzato per consentire ad un utente di accedere ed eseguire comandi ad un sistema remoto su una rete. Tuttavia il suo utilizzo è considerato non sicuro a causa della trasmissione non cifrata delle credenziali utente (nome utente e password).

La soluzione proposta suggerisce di commentare la riga “login” attraverso il comando: /etc/inetd.conf e riavviare il processo, oppure disabilitare il servizio e utilizzare SSH come alternativa più sicura. Noi abbiamo optato per la prima proposta:



Una volta completati tutti i comandi per cercare di risolvere le vulnerabilità, avvio una nuova scansione su Nessus sempre l’IP di meta e come possiamo vedere adesso non risultano esserci le vulnerabilità che vi erano nella prima scansione:

