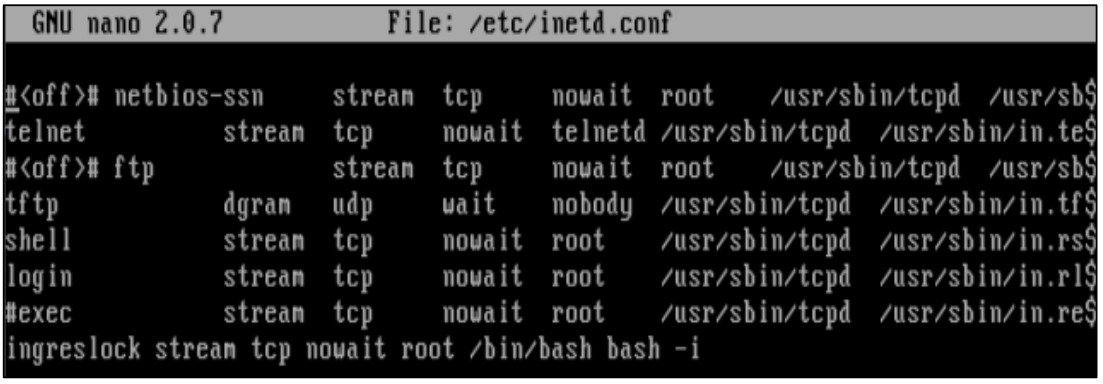
M3 - Progetto Finale - Remediation

Mitigazione Vulnerabilità 1: Porta 512/tcp (netkit-rsh rexecd)

Descrizione: il servizio rexecd (remote execution daemon) in esecuzione sulla porta 512/tcp permette l'esecuzione di comandi remoti senza un'adeguata autenticazione, rappresentando un serio rischio per la sicurezza del sistema.

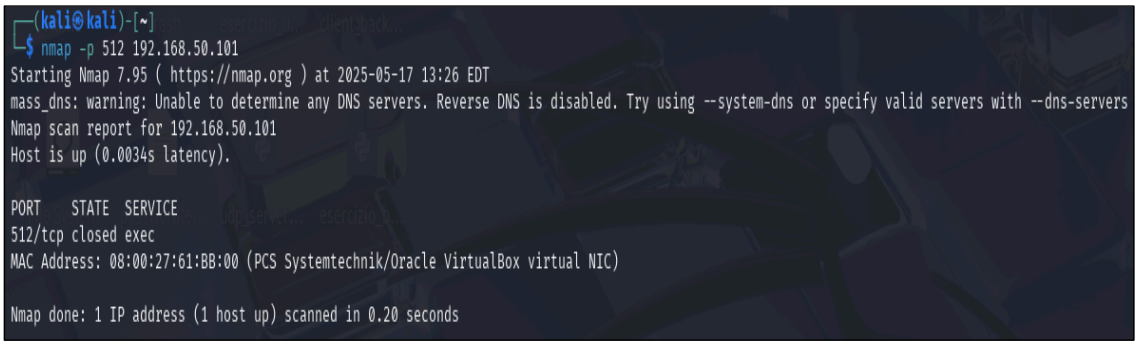
Azioni di Mitigazione intraprese

1. Disabilitazione tramite inetd.conf (Fase iniziale): il file di configurazione /etc/inetd.conf è stato modificato per disabilitare il servizio exec. La riga corrispondente a exec è stata commentata aggiungendo un # all'inizio, impedendo al demone inetd di avviare il servizio rexecd all'avvio del sistema o su richiesta.



2. Rimozione del pacchetto rsh-server (Soluzione definitiva): successivamente, il pacchetto rsh-server è stato completamente rimosso dal sistema. L'opzione —purge assicura che anche i file di configurazione associati al pacchetto vengano eliminati.

3. Verifica della Mitigazione: per confermare l'efficacia delle azioni intraprese, è stata eseguita una scansione Nmap specifica su porta 512 dal sistema Kali. Il risultato della scansione indica che la porta 512 ora risulta closed, a differenza di quanto rilevato nella scansione iniziale.

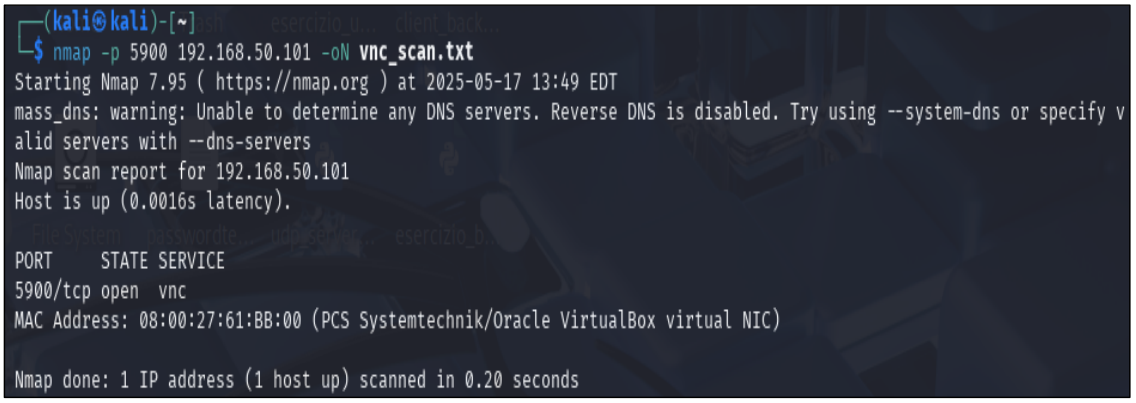


Mitigazione Vulnerabilità 2: Porta 5900/tcp (VNC)

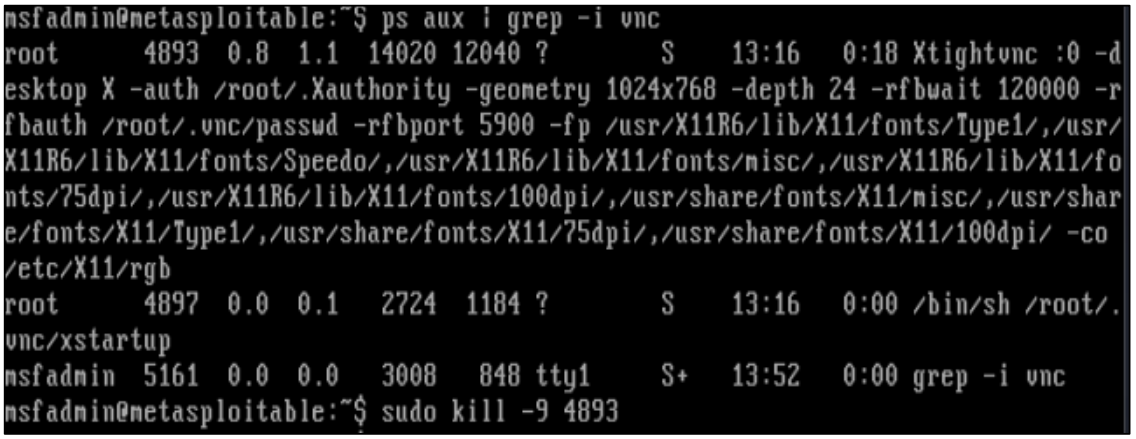
Descrizione: il servizio VNC (Virtual Network Computing) in esecuzione sulla porta 5900 utilizzava uno scambio di chiavi Diffie-Hellman, rendendo la connessione potenzialmente vulnerabile ad attacchi di tipo Man-in-the-Middle dove un attaccante potrebbe intercettare e decifrare la comunicazione.

Azioni di Mitigazione intraprese

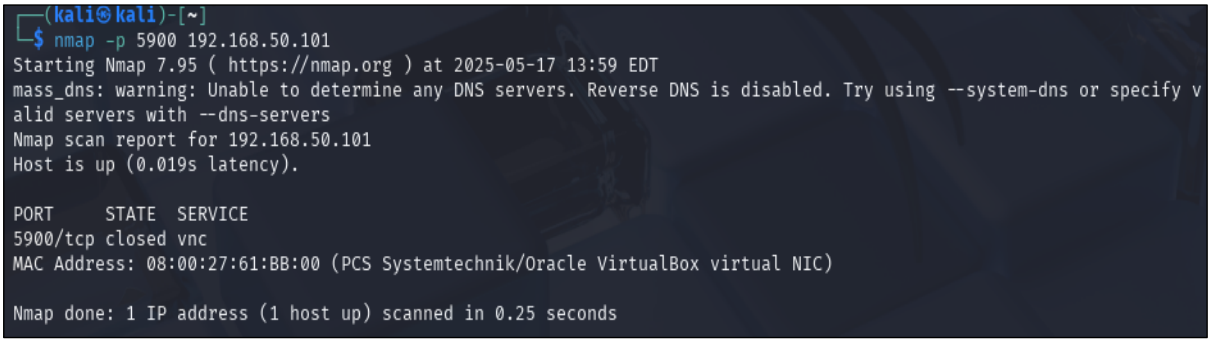
1. Scansione Nmap iniziale: una scansione effettuata con Nmap da Kali ha rilevato il servizio VNC in esecuzione sulla porta 5900.



2. Identificazione e terminazione del processo VNC: utilizzando il comando “ps aux | grep -i vnc”, è stato identificato il processo del server VNC in esecuzione. L’output ha rivelato il PID del processo, in questo caso 4893. Il processo VNC identificato è stato terminato tramite il comando “sudo kill -9 4893”. Questa azione ha interrotto l’esecuzione del server VNC.



3. Verifica Post-Mitigazione con Nmap: successivamente, è stata eseguita una nuova scansione Nmap da Kali per verificare lo stato della porta 5900 dopo la terminazione del processo VNC. Il risultato di questa scansione, indica che la porta 5900 ora risolta closed.



Mitigazione Vulnerabilità 3: Porta 6667/tcp (UnrealIRCd)

Descrizione: il server IRC UnrealIRCd, in esecuzione sulla porta 6667, è noto per diverse vulnerabilità nel corso del tempo, che potrebbero permettere ad attaccanti di eseguire codice arbitrario o causare denial-of-service.

Azioni di Mitigazione intraprese

1. Scansione Nmap: una scansione iniziale ha rilevato il servizio UnrealIRCd in esecuzione sulla porta 6667.

```
┌──(kali㉿kali)-[~]
└─$ nc -v 192.168.50.101 6667
192.168.50.101: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.50.101] 6667 (ircd) open
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
```

2. Identificazione dei file di UnrealIRCd: è stato utilizzato il comando "sudo find" per localizzare i file relativi a UnrealIRCd presenti sul sistema. Questo ha permesso di identificare il binario eseguibile /usr/bin/unrealircd e il file di configurazione /etc/unreal/unrealircd.conf.

```
msfadmin@metasploitable:~$ sudo find / -name "*unrealircd*" -type f -ls
344955 1364 -rwx------   1 root     root      1389596 May 20  2012 /usr/bin/unre
alircd
140913    4 --w----r-T   1 root     root         3884 May 20  2012 /etc/unreal/u
nrealircd.conf
```

3. Disabilitazione e terminazione del servizio: sono stati eseguiti i seguenti comandi per disabilitare e terminare il servizio.

```
msfadmin@metasploitable:~$ sudo chmod -x /usr/bin/unrealircd
msfadmin@metasploitable:~$ ps aux | grep UnrealIRCd
msfadmin  5018  0.0  0.0   3004   756 tty1     R+   11:47   0:00 grep UnrealIRCd
msfadmin@metasploitable:~$ sudo  lsof -i :6667
COMMAND    PID USER   FD   TYPE DEVICE SIZE NODE NAME
unrealirc 4945 root    2u  IPv4  12677       TCP *:ircd (LISTEN)
msfadmin@metasploitable:~$ sudo kill -9 4945
```

4. Verifica della Mitigazione: Successivamente, è stata eseguita una verifica dello stato della porta 6667, con la risposta connection refused. Non c'è più alcun servizio in ascolto sulla porta 6667, confermando l'efficacia delle azioni intraprese.

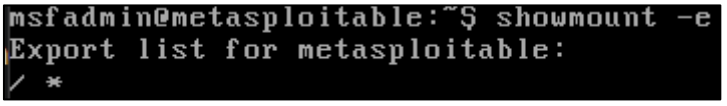
```
┌──(kali㉿kali)-[~]
└─$ nc -v 192.168.50.101 6667
192.168.50.101: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.50.101] 6667 (ircd) : Connection refused
```

Mitigazione Vulnerabilità 4: NFS (Network File System)

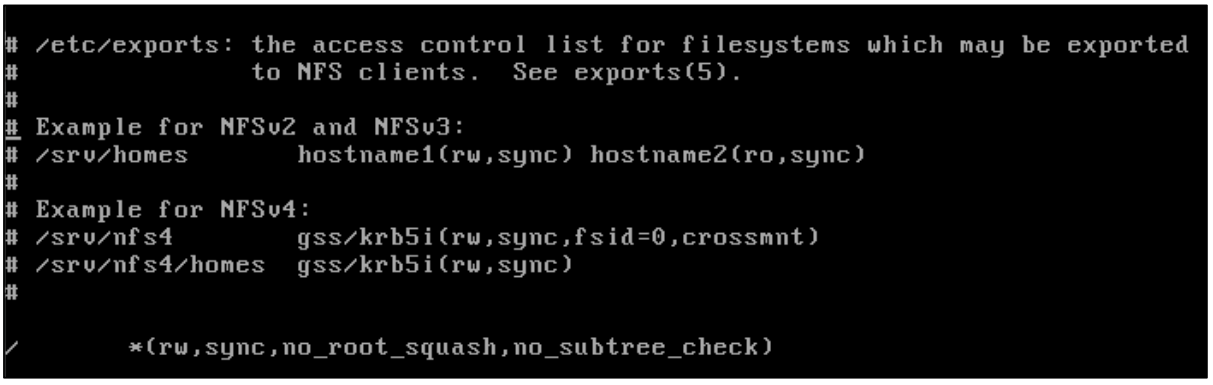
Descrizione: La configurazione iniziale del Network File System permetteva l'esportazione della directory radice (/) a qualsiasi host (*) con permessi di lettura/scrittura. Questa configurazione rappresentava un rischio significativo, in quanto un utente root su un client remoto avrebbe potuto ottenere privilegi di root sul server NFS.

Azioni di Mitigazione intraprese

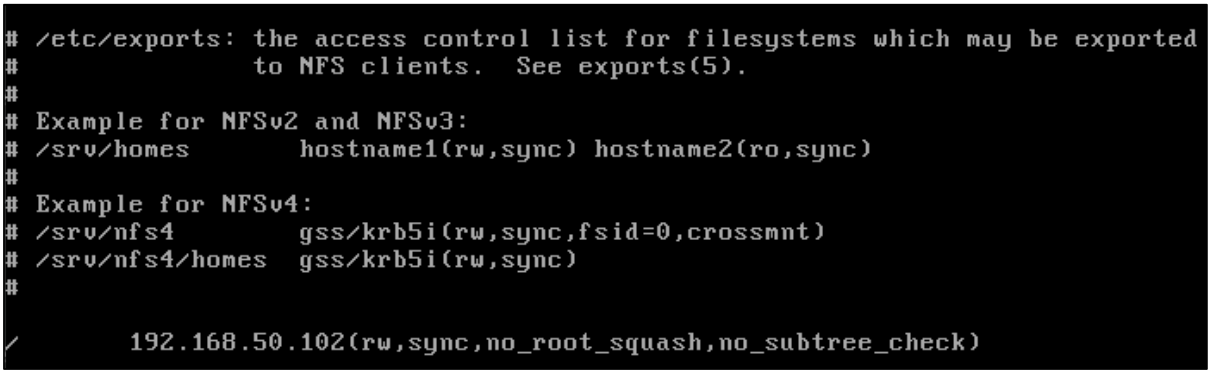
1. Verifica della configurazione iniziale: l'output del comando "showmount –e" evidenziava l'esportazione della directory radice (/) a tutti gli host (*).



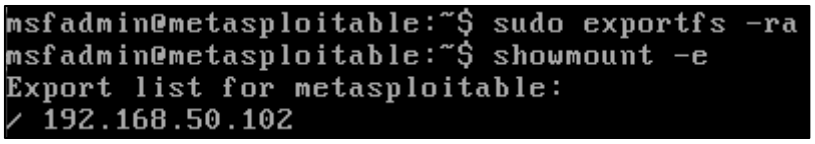
2. Analisi del file di configurazione iniziale: il prossimo screen mostra il contenuto del file /etc/exports prima delle modifiche. La riga "/* (rw,sync,no_root_squash,no_subtree_check)" confermava la configurazione permissiva che consentiva l'accesso in lettura/scrittura da qualsiasi host senza "squash" dell'utente root.



3. Modifica del file di configurazione: il file /etc/exports è stato modificato per limitare l'accesso all'host specifico "192.168.50.102".



4. Aggiornamento delle esportazioni NFS: dopo la modifica del file /etc/exports, è stato eseguito il comando “sudo exports -ra”. Questo comando rilegge il file di configurazione e aggiorna le tabelle delle esportazioni NFS senza richiedere il riavvio del servizio. Un successivo comando “showmount -e” ha confermato che la configurazione è stata aggiornata e ora la directory radice è esportata solo verso “192.168.50.102”.



Conclusioni

La fase di remediation si è concentrata sulla mitigazione di quattro vulnerabilità critiche e ad alto rischio identificate nella scansione iniziale: l'esecuzione di comandi remoti tramite rexecd (porta 512/tcp), la debolezza nello scambio di chiavi Diffie-Hellman nel servizio VNC (porta 5900/tcp), le potenziali vulnerabilità del server IRC UnrealIRCd (porta 6667/tcp) e la configurazione permissiva del Network File System (NFS).

Le azioni intraprese per affrontare queste vulnerabilità hanno incluso la rimozione del pacchetto rsh-server, la terminazione del processo VNC, la disabilitazione e la rimozione dei permessi di esecuzione per UnrealIRCd, e la restrizione degli accessi tramite la configurazione di NFS.

I risultati delle verifiche post-mitigazione, condotte tramite scansioni Nmap e analisi dei processi, hanno confermato l'efficacia delle misure adottate nel risolvere le specifiche vulnerabilità target. In particolare, i servizi vulnerabili non sono più attivi o sono stati configurati in modo più restrittivo.