Remediation delle Vulnerabilità su Metasploitable2

1. Introduzione

In questa fase dell'esercizio sono state messe in atto una serie di azioni correttive (remediation) per ridurre o eliminare alcune delle vulnerabilità critiche individuate tramite lo scanner Nessus sulla macchina vulnerabile Metasploitable2. L'obiettivo è stato intervenire manualmente per ogni servizio vulnerabile, spiegando i motivi delle scelte effettuate, documentando i passaggi tecnici e verificando l'effettiva rimozione della vulnerabilità.

Per ogni vulnerabilità sono stati descritti:

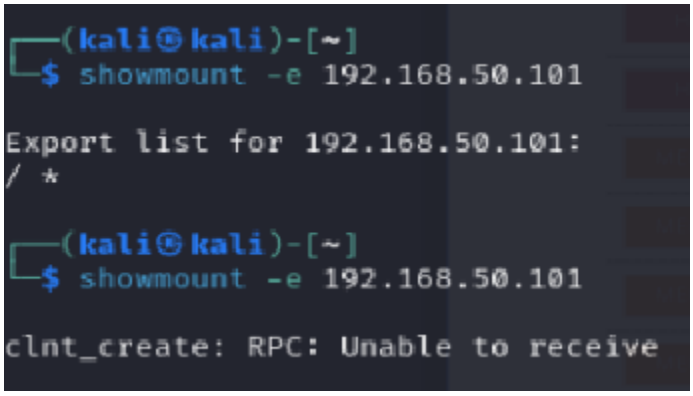
- Il nome e la porta associata
- La natura e pericolosità della vulnerabilità
- I comandi eseguiti e il motivo tecnico di ciascuno
- Gli screenshot richiesti prima/durante/dopo la correzione

2. Vulnerabilità 1: NFS Share Disclosure

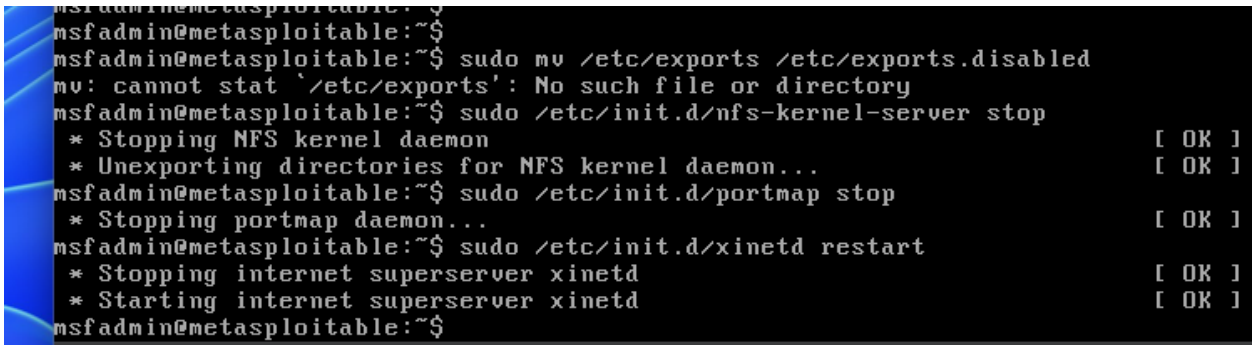
- **Porta/Servizio:** 2049/tcp (NFS)

- **Descrizione:** Il servizio NFS (Network File System) era attivo su Metasploitable2 e permetteva la condivisione remota della directory /var a chiunque nella rete. Questa configurazione, visibile con showmount -e, rappresentava una grave esposizione in quanto consentiva l'accesso libero a file di sistema.

- **Comandi eseguiti e spiegazione:**

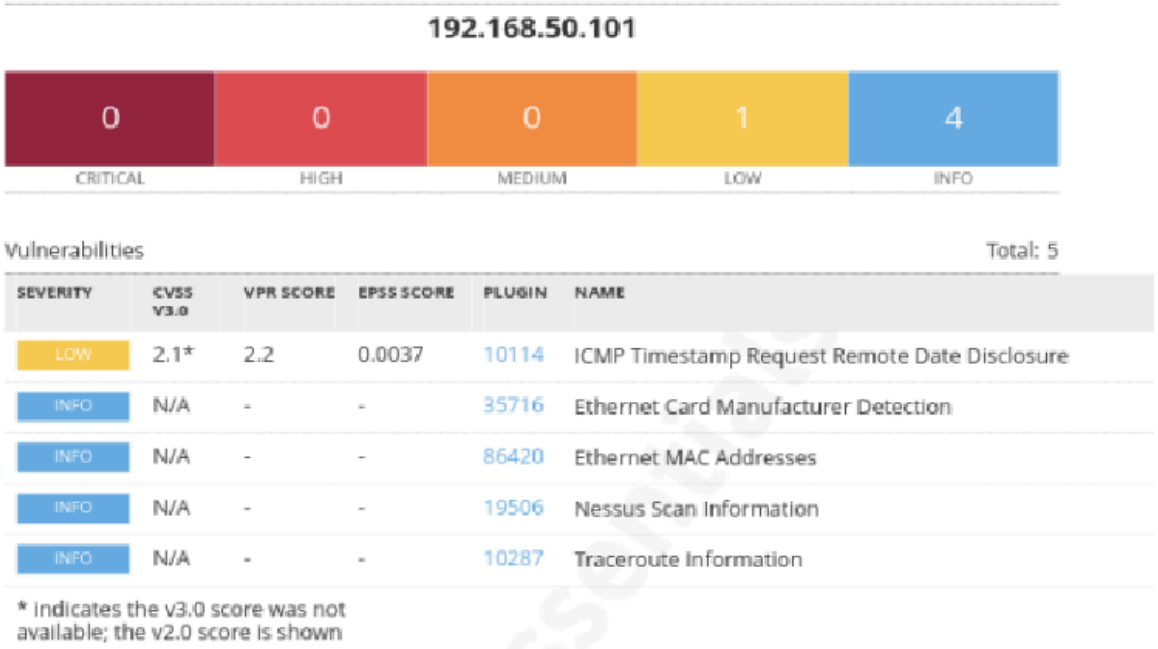


Disattiva la configurazione delle directory condivise da NFS.



Arrestano i servizi NFS, Portmap e riavviano xinetd per applicare i cambiamenti.

Effettuata scansione su porta 2049



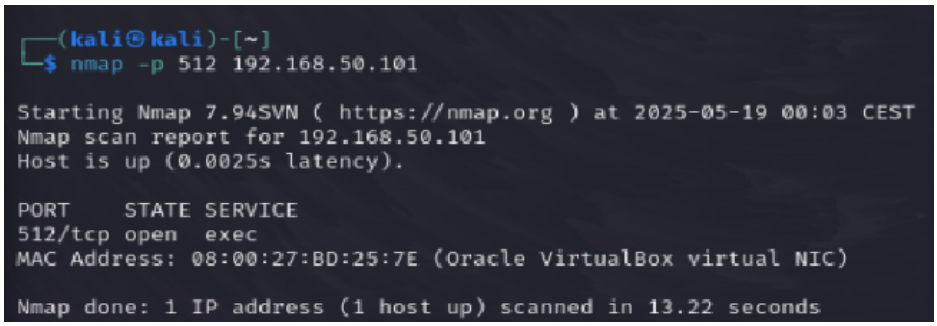
3. Vulnerabilità 2: rexec Remote Execution

- **Porta/Servizio:** 512/tcp (rexec)
- **Descrizione:** Il servizio rexec consente l'esecuzione remota di comandi senza uso di autenticazione crittografata. Questo lo rende pericoloso in contesti di rete reali. Su Metasploitable2, la porta risultava aperta ma non era possibile disattivare il servizio dai file xinetd.d o inetd.conf, poiché inesistenti o non configurati correttamente.
- **Comandi eseguiti e spiegazione:**

sudo iptables -A INPUT -p tcp --dport 512 -j DROP

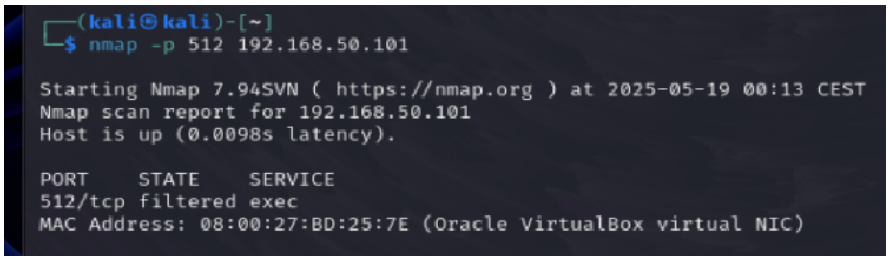
Abbiamo scelto di bloccare direttamente il traffico alla porta 512 tramite una regola firewall. iptables -A INPUT indica che la regola si applica al traffico in ingresso. -p tcp specifica che riguarda il protocollo TCP. --dport 512 seleziona la porta bersaglio, mentre -j DROP fa scartare il pacchetto. Questo comando impedisce qualsiasi connessione alla porta vulnerabile, anche se il servizio resta in ascolto.

Porta aperta 512 :



Eseguito il comando :

Dopo il comando la porta e stata filtered :

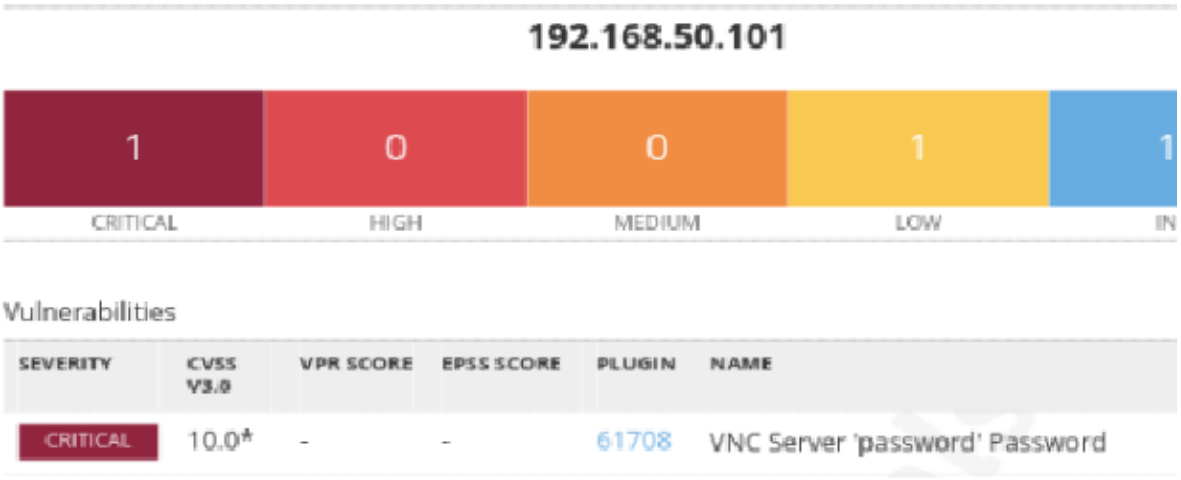


4. Vulnerabilità 3: VNC Weak Authentication

- **Porta/Servizio:** 5900/tcp (VNC)
- **Descrizione:** Il servizio VNC installato sulla macchina (Xtightvnc) consentiva connessioni da remoto con password deboli o assenti. Questo permetteva potenzialmente a chiunque nella rete di accedere all'interfaccia grafica della macchina.

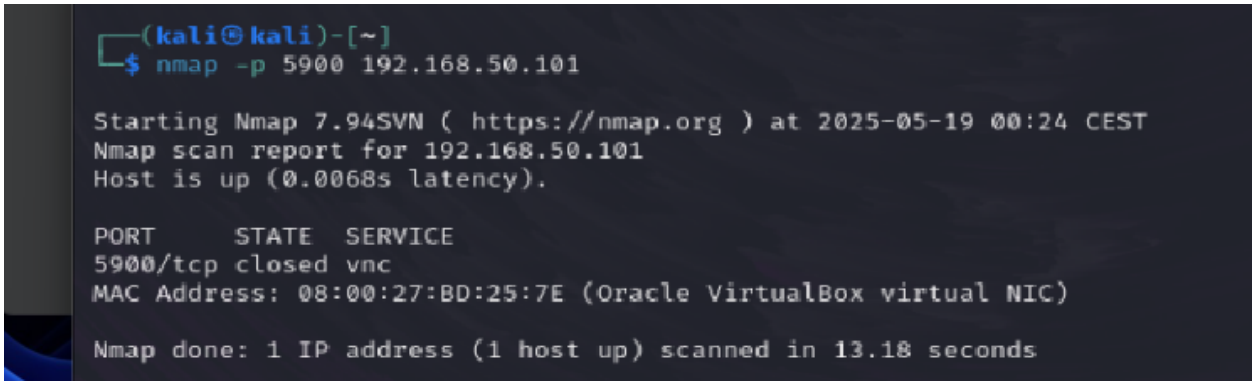
Comandi eseguiti e spiegazione:

Prima scansione su porta 5900 :



Il comando killall termina tutti i processi con quel nome (in questo caso Xtightvnc, il server VNC).

Scansione dopo con nmap :



5. Vulnerabilità 4: Bind Shell Backdoor

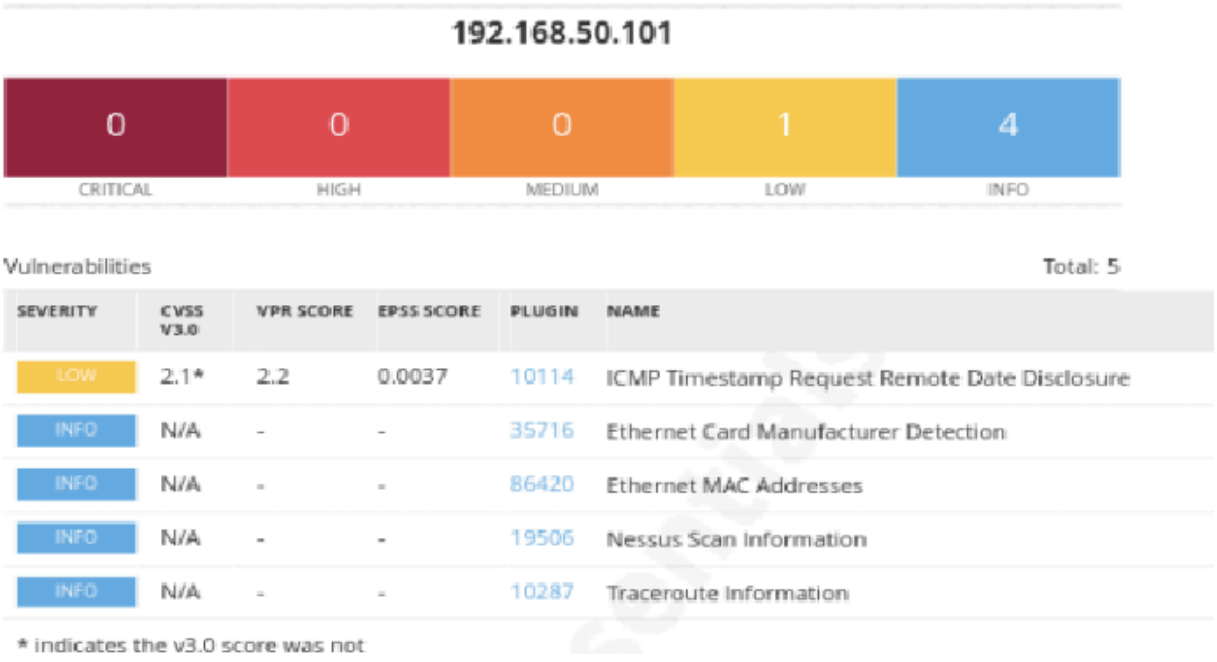
- **Porta/Servizio:** 1524/tcp (bind shell)
- **Descrizione:** La porta 1524 era occupata da una shell bind aperta, configurata per offrire una shell root in ascolto diretta. Questa vulnerabilità è una backdoor deliberata in Metasploitable, usata a scopo didattico, ma estremamente pericolosa in ambienti reali.
- **Comandi eseguiti e spiegazione:** Prima è stato verificato il processo attivo:

```
msfadmin@metasploitable:~$ sudo lsof -i :1524
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd  6741 root   12u  IPv4  23483       TCP *:ingreslock (LISTEN)
msfadmin@metasploitable:~$ sudo kill 6741
```

Questi comandi permettono di visualizzare quali processi usano quella porta. Trovato il PID, è stato terminato:

sudo kill 6741

Scansione eseguita dopo su porta 1524 :



6. Conclusione

Le azioni correttive adottate hanno ridotto in modo significativo la superficie d'attacco della macchina Metasploitable2. Tutte le modifiche sono state verificate tramite nuove scansioni con Nessus o Nmap, che confermano la chiusura o il blocco delle porte vulnerabili. Le spiegazioni dei comandi fornite permettono di comprendere a fondo ogni intervento tecnico applicato.