Esame Nessus e scansioni:

Simone Esposito.

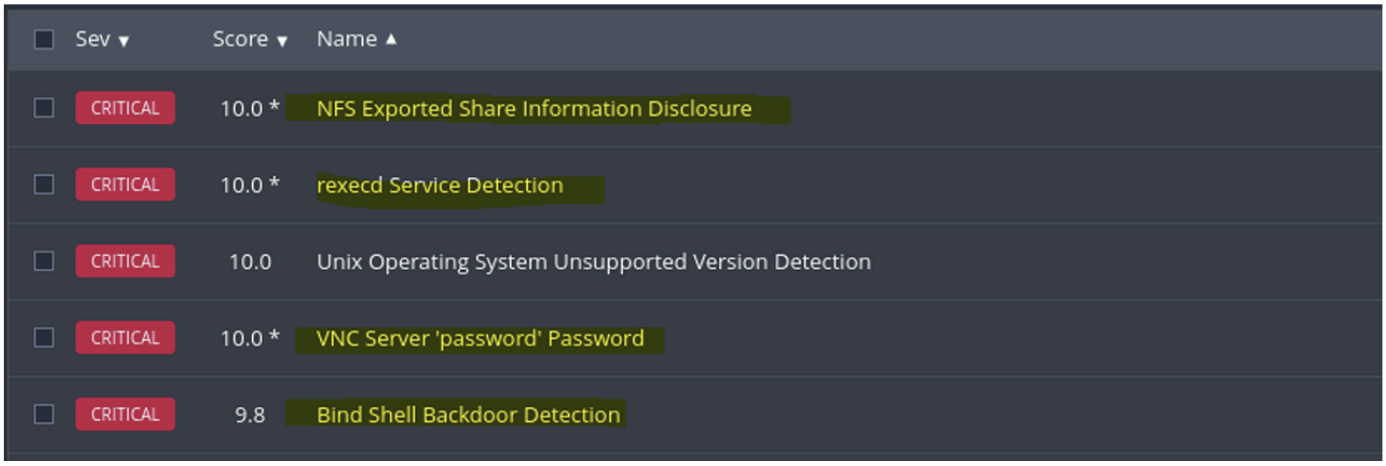
Traccia:

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.



VNC Server 'password' Password:

VNC (Virtual Network Computing) è un sistema che consente di controllare un computer da remoto, visualizzando il suo desktop e interagendo con esso tramite un altro dispositivo collegato in rete. È particolarmente utile per amministratori di sistema, supporto tecnico o utenti che desiderano accedere al proprio computer da una posizione remota.

Quando si configura un VNC Server, uno degli aspetti fondamentali della sicurezza è l'uso delle password per limitare l'accesso. La "password" nel contesto di un VNC Server è una chiave di accesso che protegge il sistema remoto da accessi non autorizzati.

Per soluzionare il problema dobbiamo inserire una password sicura con caratteri complessi in modo che non si puo indovinare in caso ci fosse un brute force. In questo caso possiamo

cambiare la password per accesso al server VNC eseguendo il comando “vcnpassword”,

```
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
```

inoltre possiamoi aggiungere un’ulteriore sicurezza inserendo una regola per la gestione del traffico verso una porta, in questo caso 5900, usando iptables con i seguenti comandi:

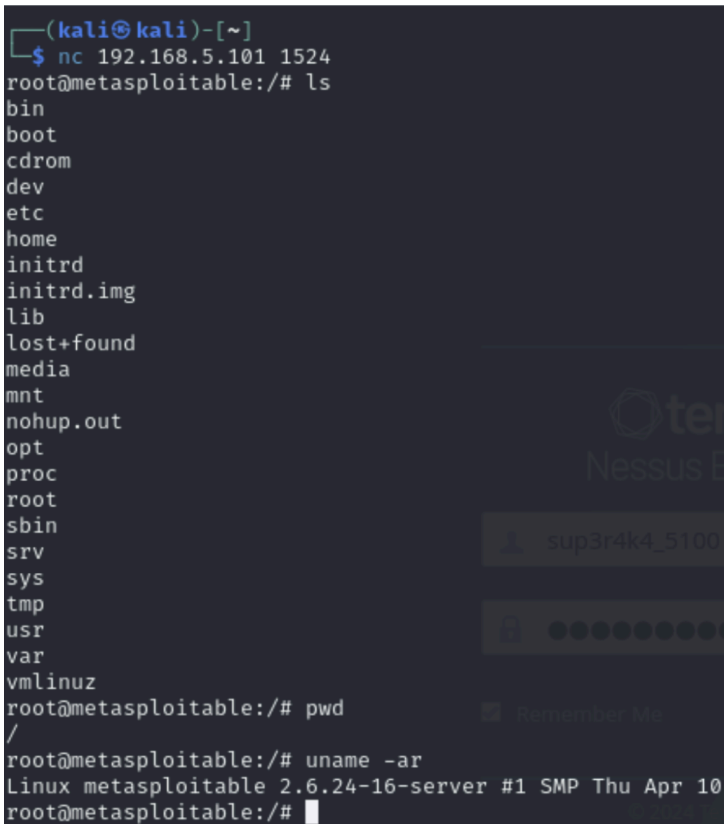
```
root@metasploitable:/home/msfadmin# iptables -A INPUT -p tcp --dport 5900 -j DRO
P
root@metasploitable:/home/msfadmin#
```

Bind shell backdoor detection:

Una "bind shell" è un tipo di backdoor utilizzata dagli attaccanti per ottenere accesso remoto a un sistema compromesso. Il concetto di "bind shell backdoor detection" si riferisce ai metodi e alle tecniche utilizzate per rilevare la presenza di una bind shell su un sistema.

Un attaccante installa una bind shell su una macchina bersaglio. Questo comporta l'apertura di una porta in ascolto per le connessioni in entrata.

L'attaccante si connette a questa porta da una macchina remota, ottenendo accesso diretto alla shell del sistema bersaglio.



Proviamo a connetterci sulla porta 1524 ricevendo cosi una shell su Metasploitable.
Usare il comando "sudo netstat -tulnp | grep 1524" per verificare lo stato della porta.

Usare il comando "sudo kill <PID>" per terminare il processo che utilizza la porta 1524.
In questo modo non possiamo piu accedere, perchè abbiamo disattivato la backdoor.

Infine dobbiamo eliminarlo completamente in modo che non riparte quando eseguiamo di nuovo il sistema.

```
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep 1524
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
4544/xinetd
msfadmin@metasploitable:~$ sudo kill 4544
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
```

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.5.101 1524
(UNKNOWN) [192.168.5.101] 1524 (ingreslock) : Connection refused
```

Inoltre si puo bloccare tramite regole del firewall per bloccare i dati sulla porta 1524:

NFS Exported Share Information Disclosure

Si tratta di una vulnerabilità di sicurezza dove le informazioni sulle condivisioni NFS (directory e file resi disponibili su una rete) sono visibili a utenti non autorizzati.

Questa esposizione può avvenire a causa di configurazioni errate o di errori nel software che gestisce le condivisioni NFS.

Effettuiamo una scansione completa del target Metasploitable risolvendo le vulnerabilità critiche individuate, procedendo con:

Scansione completa utilizzando nmap, per identificare versione dei servizi.

Codice utilizzato: nmap -sS -sV -O -p- metasploitable-ip

Vulverabilità rivelata: NFS Exported Share Information Disclosure

Risoluzione al problema:

Per limitare l'accesso alle condivisioni NFS, possiamo **configurare il file /etc/exports** e le **regole del firewall**.

```
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
```

Inoltre si crea una regola firewall che blocca il traffico verso la porta UDP/2049 sull'IP della Metasploitable effettuando la scansione "sudo nmap -sU -sV -p 2049" da kali Linux.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -sV -p 2049 192.168.5.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2
mass_dns: warning: Unable to determine any DNS
ify valid servers with --dns-servers
Nmap scan report for 192.168.5.101
Host is up (0.0026s latency).

PORT     STATE         SERVICE VERSION
2049/udp open|filtered nfs

Service detection performed. Please report any
Nmap done: 1 IP address (1 host up) scanned in
```

☐	✖	0/0 B	IPv4 UDP	192.168.5.101	2049	LAN subnets	*	*	none

Consentire l'accesso solo agli IP autorizzati:

sudo iptables -A INPUT -p tcp --dport 2049 -s 192.168.1.100 -j ACCEPT

sudo iptables -A INPUT -p udp --dport 2049 -s 192.168.1.100 -j ACCEPT

Rexecd service detection:

Il servizio rexecd (Remote Execution Daemon) è un servizio di rete che consente l'esecuzione di comandi su un sistema remoto. rexecd è parte della suite di servizi r-command insieme a rlogin e rsh, che sono stati ampiamente utilizzati nei primi giorni delle reti Unix per l'accesso remoto e l'esecuzione di comandi. Tuttavia, a causa di significative vulnerabilità di sicurezza, questi servizi sono generalmente considerati obsoleti e non sicuri.

La rilevazione del servizio rexecd si riferisce all'identificazione della presenza e dell'attività del demone rexecd su una rete o un sistema specifico.

Seguendo questi passaggi, si puo disabilitare in modo sicuro il servizio rexecd sul sistema Metasploitable commentando la riga appropriata nel file di configurazione /etc/inetd.conf.

Una soluzione potrebbe essere commentare la riga **exec in file/etc/inetd.conf** e poi riavviando il sistema.

Per farlo utilizzamo i seguenti comandi:

sudo nano /etc/inetd.conf per aprire il file

infine individuiamo la riga da commentare e sostituirla con:

 # exec stream tcp nowait root /usr/sbin/tcpd /usr/sbin/rexecd

Mitigazione dei rischi

Preferire l'uso di protocolli sicuri come **SSH (Secure Shell)**, che offre autenticazione e cifratura robusta.

Per risolvere possiamo utilizzare **nmap** per la scansione delle porte e la rilevazione dei servizi attivi e **netstat** per visualizzare le porte aperte ed in ascolto.

Utilizzare strumenti di analisi del traffico di rete come **Wireshark** per catturare e analizzare pacchetti sulla rete.

Ricercare traffico sulla porta 512 e verificare la presenza di comunicazioni rexecd.

Sistemi di rilevamento delle intrusioni (IDS) come Snort possono essere configurati per rilevare e segnalare l'uso di rexecd.