Progetto epicode 27.10.2023

Vulnerability Scanner

Scopo del progetto

Utilizzare un Vulnerability Scanner (Nmap) per visualizzare le vulnerabilità critiche su una Macchina Virtuale con S.O. Metasploitable.

Dopo aver inviduato
3 vulnerabilità,
bisogna mitigarle

CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

```
root@metasploitable:/home/msfadmin# iptables -A INPUT -p tcp --dport 1524 -j DRO
P
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere            tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

1° vulnerabilità: Bindshell Backdoor Detection

La prima vulnerabilità riscontrata è una backdoor di tipo “bind” (da attaccante a target).
Per mitigare questo tipo di attacco è necessario mettere una regola su iptables (Firewall di Linux), dove si va a chiudere la connessione in entrata sulla porta 1524 (porta vulnerabile) poi controllo la lista delle regole con il comando iptables -L, come mostrato in figura

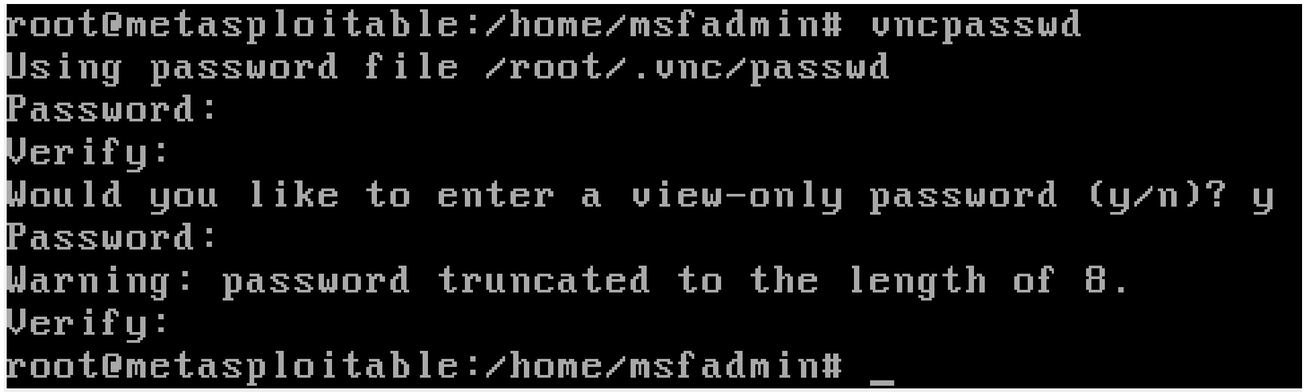
2° Vulnerabilità NFS Exported Share Information

Con questa vulnerabilità la condivisione NFS della nostra macchina Metasploitable è a rischio e persone o sistemi non autorizzati possono ottenere accesso ai nostri dati condivisi.
Andremo a mitigare questa vulnerabilità killando i demoni NFS kernel e portmap per evitare operazioni NFS tra server e client.

```
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server stop
 * Stopping NFS kernel daemon                                    [ OK ]
 * Unexporting directories for NFS kernel daemon...              [ OK ]
msfadmin@metasploitable:~$ sudo /etc/init.d/portmap stop
[sudo] password for msfadmin:
 * Stopping portmap daemon...                                    [ OK ]
```

3° Vulnerabilità Password Debole del VNC Server

Questa Vulnerabilità permette a chiunque di entrare da remoto nella nostra macchina Metasploitable, perchè la nostra password è debole (esempio potremo utilizzare un attacco brute force a dizionario per scoprire la password)
Per mitigare questa vulnerabilità andremo a cambiare all’interno della root di Meta la password del nostro VCN Server




Grazie