PROGETTO NESSUS

Il mio obiettivo è condurre una scansione completa su Metasploitable, con il Vulnerability scanner “Nessus” ,al fine di identificare da 2 a 4 vulnerabilità di alto o alto impatto. Dopo questa fase di identificazione, intendo implementare azioni di rimedio mirate.
Queste azioni possono includere la configurazione di regole firewall per mitigare le esposizioni dei servizi vulnerabili.
Tuttavia, per dimostrare l'efficacia delle azioni di rimedio, mi concentrerò su una vulnerabilità specifica.
Infine, ripeterò la scansione sul target e confronterò i risultati con quelli ottenuti inizialmente.

Dopo aver completato la prima scansione, Nessus ha identificato le seguenti vulnerabilità sulla macchina Metasploitable:

- 9 critical
- 6 high
- 18 medium
- 7 low

1.**VNC Server 'password' Password**

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito a effettuare l'accesso tramite l'autenticazione VNC(controllo remoto di un host attraverso la rete) utilizzando la password 'password'.
Un attaccante remoto non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema.

Quindi Nessus ci consiglia di sostituire la password corrente con una più robusta.

1. Come primo passaggio ho usato il codice **“sudo su”** per ottenere l'accesso all’ account utente con privilegi di superutente ;
2. **“ls -a”** per controllare i file all’interno della directory ,inclusi quelli nascosti;
3. Entriamo nella directory “.vnc” che all’interno avrà il file passwd
4. una volta entrati si potrà inserire la nuova password ;

2. **NFS Exported Share Information Disclosure**

NFS sta per "Network File System" ed è un protocollo di condivisione di file e una tecnologia di rete che consente a computer in una rete di accedere e condividere file e directory tra loro

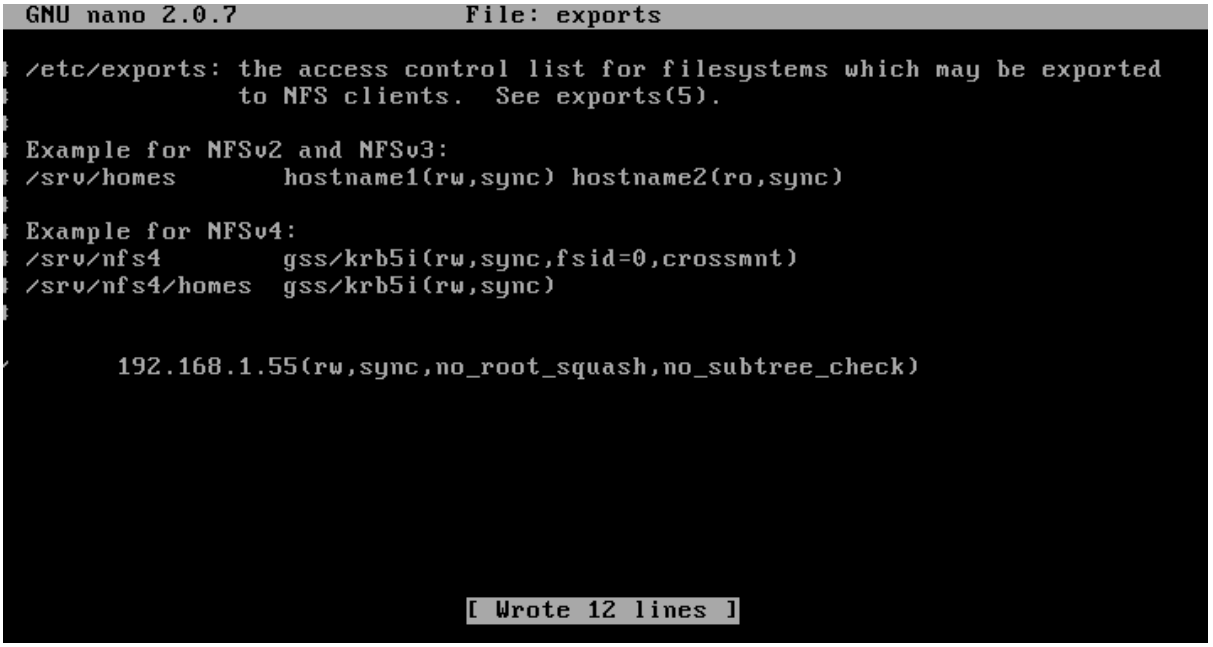
Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.

Andiamo a configurare l’accesso al sistemo kali

```
root@metasploitable:/etc# cd ..
root@metasploitable:/# sudo su
root@metasploitable:/# cd /
root@metasploitable:/# cd etc
root@metasploitable:/etc#
```

```
dpkg                    mailname            sudoers
e2fsck.conf             manpath.config      su-to-rootrc
emacs                   mediaprm            sysctl.conf
environment             menu                syslog.conf
esound                  menu-methods        terminfo
event.d                 mime.types          timezone
exports                 mke2fs.conf         tomcat5.5
fdmount.conf            modprobe.d          ucf.conf
firefox-3.0             modules             udev
fonts                   motd                ufw
fstab                   motd.tail           unreal
ftpchroot               mtab                updatedb.conf
ftpusers                mysql               update-manager
fuse.conf               nanorc              vim
gai.conf                network             vsftpd.conf
gconf                   networks            w3m
gdm                     nsswitch.conf       wgetrc
groff                   opt                 wpa_supplicant
group                   pam.conf            X11
group-                  pam.d               xinetd.conf
grub.d                  pango               xinetd.d
gshadow                 passwd              zsh_command_not_found
gshadow-                passwd-
gssapi_mech.conf        pcmcia
root@metasploitable:/etc# _
```

entreremo con il comando **sudo nano exports**



dando cosi i permessi d ‘accesso solo al sistema kali

3.**Bind Shell Backdoor Detection**

Ci avvisa che c'è un problema di sicurezza in cui una shell (un'interfaccia da linea di comando) è in esecuzione su una porta remota del sistema, e questa shell non richiede alcuna autenticazione o password per accedervi. Questo scenario è estremamente rischioso, poiché un potenziale attaccante può connettersi a questa porta e ottenere accesso diretto al sistema, consentendogli di eseguire comandi o operazioni non autorizzate.

Soluzione
Isolare il sistema.
Controllare se il sistema è corrotto
La reinstallazione del sistema è spesso l'opzione più sicura per garantire che il sistema sia di nuovo sotto controllo e non soggetto a ulteriori compromissioni

In questa situazione, ho optato per la chiusura forzata della porta, sebbene avremmo potuto configurare una regola direttamente nel firewall per filtrarla.

```
msfadmin@metasploitable:/$ sudo netstat -tulnp | grep 1524
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
4415/xinetd
msfadmin@metasploitable:/$ sudo kill 4415
msfadmin@metasploitable:/$ _
```

Il comando **sudo netstat -tulnp | grep 1524** è utilizzato per individuare tutte le connessioni di rete che sono in modalità "ascolto" (listening) sul sistema e che utilizzano la porta numerata 1524. Questo comando estrae le informazioni correlate a tali connessioni, inclusi i processi specifici che stanno ascoltando su questa porta. L'obiettivo principale è identificare i servizi o le applicazioni che utilizzano la porta 1524 sulla macchina.

- -t: Visualizza le connessioni TCP.
- -u: Visualizza le connessioni UDP.
- -l: Mostra solo le connessioni in ascolto (listening), ossia quelle su cui il sistema è in attesa di connessioni in ingresso.
- -n: Visualizza gli indirizzi IP e le porte numerate invece di cercare di risolverli in nomi.
- -p: Mostra il processo (PID) associato a ciascuna connessione

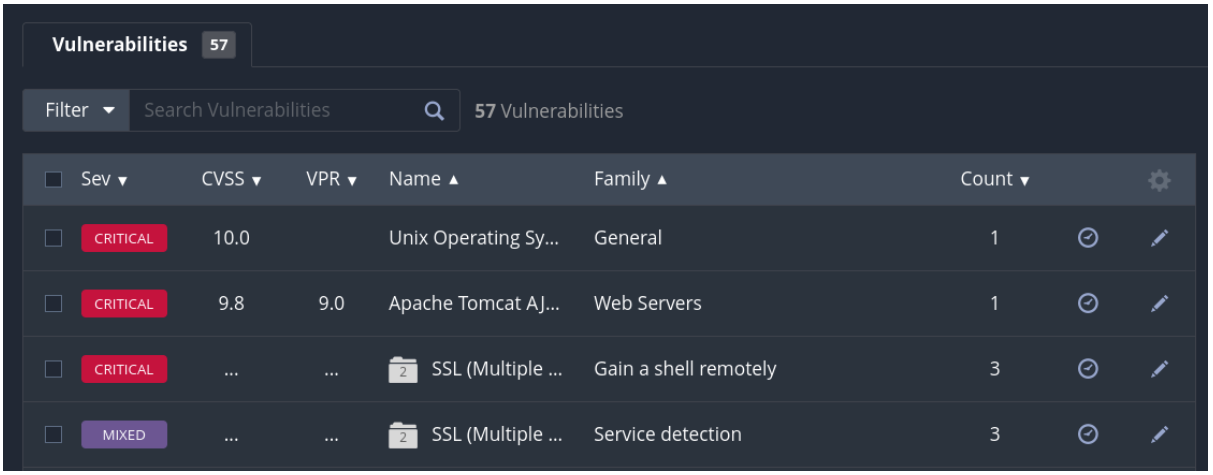
Nello stesso modo chiuderemo anche :

4. UnrealIRCd Backdoor Detection

```
root@metasploitable:/# sudo netstat -tulnp | grep 6667
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN
4553/unrealircd
root@metasploitable:/# sudo kill 4553
root@metasploitable:/#
```

Inizio

Fine


Vulnerabilities 57
Filter
Search Vulnerabilities
57 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
CRITICAL
10.0
Unix Operating Sy...
General
1
CRITICAL
9.8
9.0
Apache Tomcat AJ...
Web Servers
1
CRITICAL
...
...
2
SSL (Multiple ...
Gain a shell remotely
3
MIXED
...
...
2
SSL (Multiple ...
Service detection
3