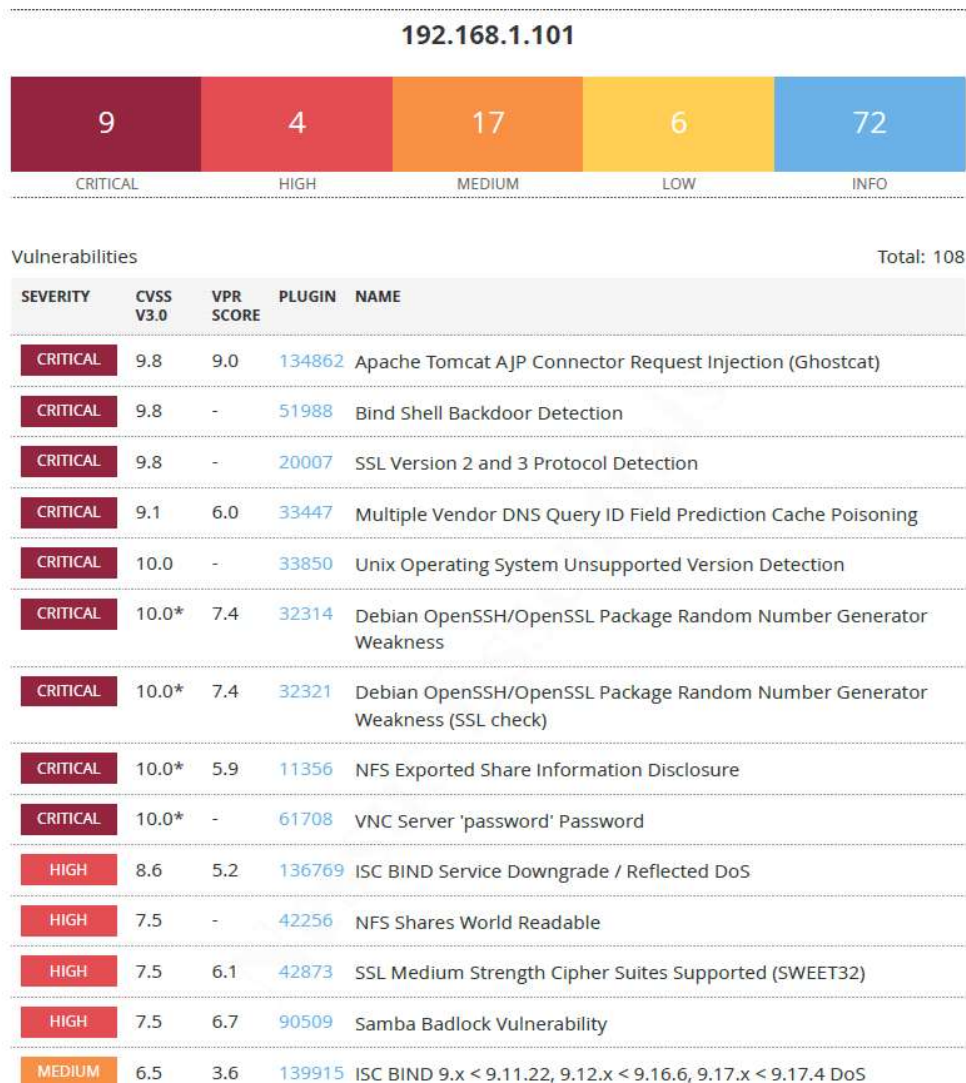


ProgettoW5L5-Scansione e rimedio

L'esercizio di oggi prevede di effettuare una scansione completa con Nessus sul target Metasploitable, andare a prendere delle vulnerabilità critiche e implementare delle azioni di rimedio.

Facendo la prima scansione il risultato è questo:



Possiamo notare che abbiamo 9 vulnerabilità critiche e altre meno critiche, per un totale di 108 potenziali vulnerabilità.

1. La prima vulnerabilità che andiamo ad analizzare e sistemare è la **Bind Shell Backdoor Detection**.

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può usarlo da collegandosi alla porta

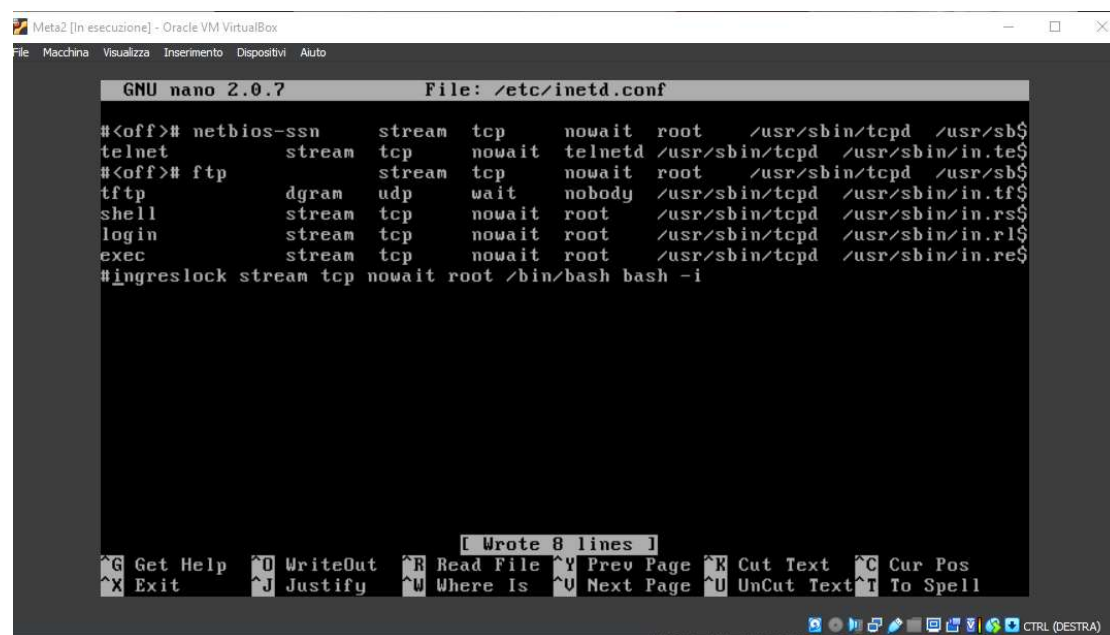
remota e inviando comandi direttamente. In una bind shell, la shell in ascolto è sul sistema bersaglio e l'attaccante si connette ad essa. Ciò significa che il programma di shell sul sistema bersaglio ascolta su una determinata porta, in attesa di una connessione in entrata dall'attaccante.

Attraverso lo scan si vede che la porta interessata è la n.1524 ma non sapendo il servizio attivo su di essa ho effettuato una scansione con nmap sulla porta.

```
nmap done: 0 IP addresses (0 hosts up) scanned in 20.037 seconds
root@metasploitable:/home/msfadmin# nmap 192.168.50.101 -p1524

Starting Nmap 4.53 ( http://insecure.org ) at 2023-10-27 05:48 EDT
Interesting ports on 192.168.50.101:
PORT      STATE SERVICE
1524/tcp  open  ingreslock
```

Una volta visto il servizio attivo sulla porta ho utilizzato il comando <sudo nano /etc/inetd.conf> che mi ha aperto il file di configurazione dei servizi di rete forniti da 'inetd', andando a commentare l'ultima riga del codice ho bloccato il servizio che rendeva possibile l'entrata della backdoor.



```
Meta2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

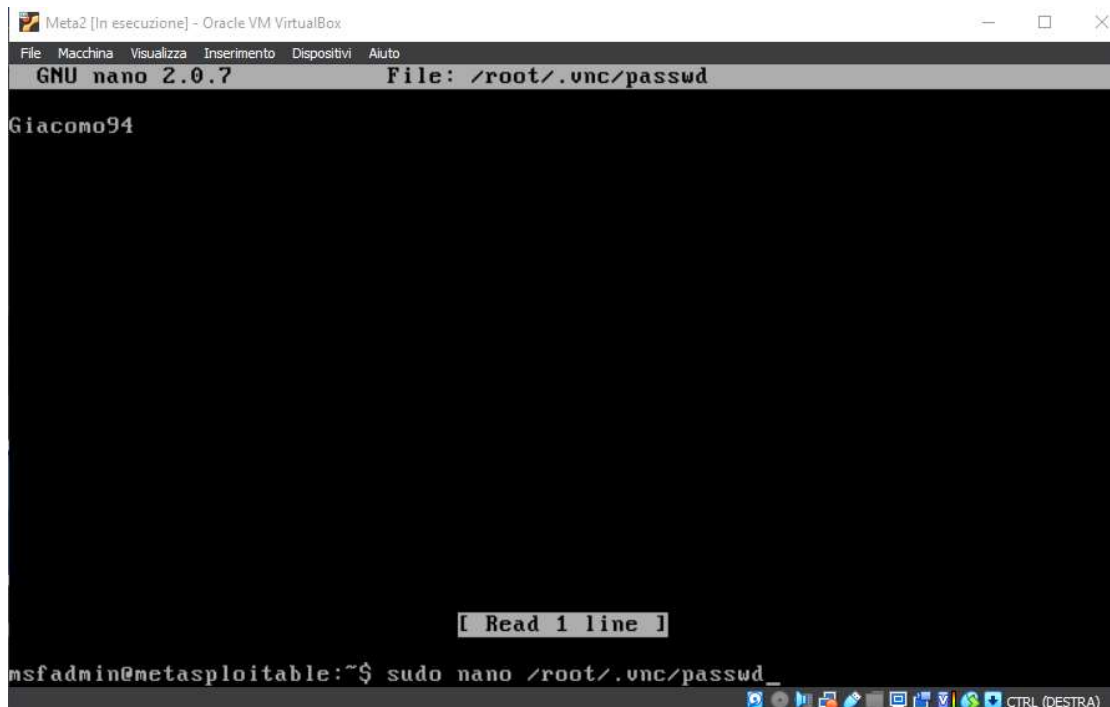
GNU nano 2.0.7 File: /etc/inetd.conf

#<off># netbios-ssn  stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.
telnet      stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te
#<off># ftp        stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin
tftp        dgram  udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tf
shell       stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs
login       stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl
exec        stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re
#ingreslock stream  tcp    nowait  root    /bin/bash bash -i

[ Wrote 8 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^V Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

2. La seconda vulnerabilità critica che sono andato ad analizzare è VNC Server 'password' Password

Questa vulnerabilità mi dice che un server VNC in esecuzione sull'host remoto è protetto con una password debole, quindi sono andato a cambiare la password con una più complessa utilizzando il comando <sudo nano /root/.vnc/passwd>.



```
Meta2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7                               File: /root/.vnc/passwd
Giacono94

[ Read 1 line ]
msfadmin@metasploitable:~$ sudo nano /root/.vnc/passwd_
CTRL (DESTRA)
```

3. La terza vulnerabilità critica che ho analizzato è **NFS Exported Share Information Disclosure**

Questa vulnerabilità avviene perchè almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione dato che è possibile accedere sull'host da remoto senza nessun problema. Un'attaccante potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.

Utilizzando il comando `<sudo nano /etc/exports>` ho aperto il file di testo per configurare le condivisioni NFS esportate da un server NFS. Come si vede nell'ultima riga di comando chiunque poteva entrare e aveva i poteri di root, poteva cambiare directory liberamente, leggere e scrivere su qualsiasi file. Quindi un malintenzionato avrebbe preso il possesso della macchina in breve tempo.

Andando a commentare con '#' l'ultima riga del codice leviamo tutti i privilegi a chiunque utilizzerà il servizio NFS.

Nel secondo screen il codice per riavviare il servizio NFS.

```

Meta2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Auto

GNU nano 2.0.7 File: /etc/exports

# /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)
#
#/*(rw,sync,no_root_squash,no_subtree_check)

[ Wrote 12 lines ]

msfadmin@metasploitable:~$ sudo nano /etc/exports

```

```

msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server start
[sudo] password for msfadmin:
* Exporting directories for NFS kernel daemon... [ OK ]
* Starting NFS kernel daemon [ OK ]
msfadmin@metasploitable:~$

```

Qui sotto allego uno screen di una scansione effettuata dopo la sistemazione di queste vulnerabilità e come possiamo vedere sono arrivato ad avere 5 vulnerabilità critiche e 3 alte.

