

REPORT REMEDIATION ACTIONS

Nel report seguente andremo ad analizzare 4 delle **critics vulnerabilities** scansionate con il tool Nessus su macchina Metasploitable e mostreremo correttamente come rendere più sicuro un OS come Metasploitable che nasce come tool facilmente attaccabile in fase di test. Quelle che andremo ad analizzare sono rispettivamente:

- **UNIX Unsupported OS Version**
- **Bind Shell Backdoor Detection**
- **VNC Server Password**
- **NFS Exported Share Informations Disclosure**

Prima di passare ad analizzare le vulnerabilità che ho effettivamente risolto con delle remediation action vorrei includere che la traccia richiede anche la soluzione della vulnerabilità riferita a **rexecd Service Detection**.

Per cercare di risolverla ho avviato la scansione più volte sia in modalità basic che in modalità advanced attivando tutti i vari plugins di Nessun, ma mio malgrado sul sistema Metasploitable fornitoci non è stata trovata in alcun modo.

Ho formulato due ipotesi: la prima è che possa trattarsi di un falso positivo rilevato nella scansione l'altra è che la versione di Metasploitable fornitaci non la comprendeva .

UNIX Unsupported OS Version

Questa prima vulnerabilità in realtà non ha un remediation action possibile a meno che non si cambi direttamente l'OS e si passi a quello più aggiornato.

L'OS in questione è datato e non aggiornabile in quanto ha raggiunto come per molti altri OS ha raggiunto la cosiddetta "end of life" .

Per rimediare a questa vulnerabilità bisognerebbe semplicemente cambiare versione di Metasploitable e quindi cambiare direttamente tutto l'OS della VM installata.

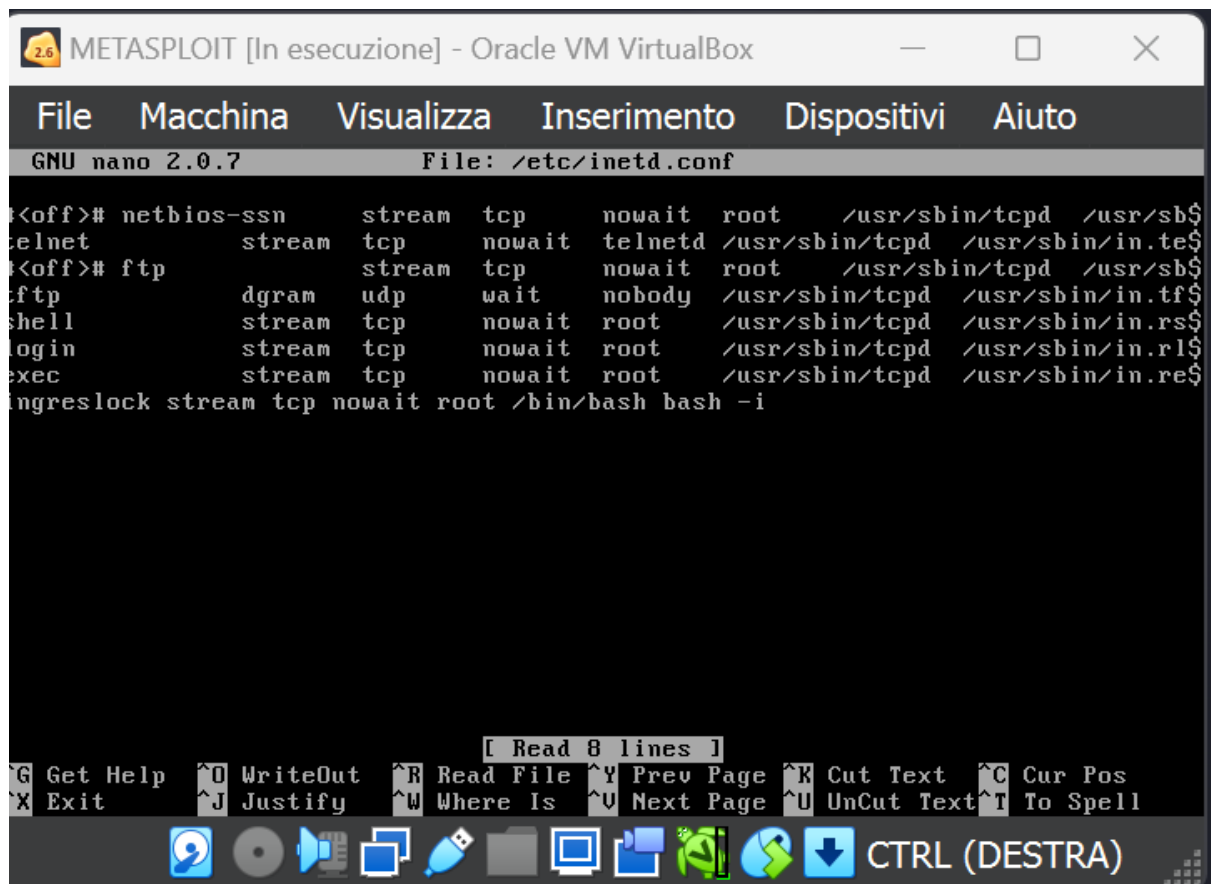
Bind Shell Backdoor Detection

Questa vulnerabilità descrive il caso nel quale una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione., in questo caso potenziale utente malintenzionato può utilizzare questa vulnerabilità collegandosi alla porta remota e inviando comandi direttamente in maniera remota.

Come possiamo vedere nella figura sotto nel percorso con l'editor di testo nano spostandosi sul file inetd.conf possiamo avere accesso al servizio ingreslock

La backdoor può essere rimossa ripristinando /etc/inetd.conf, rimuovendo qualsiasi file di configurazione e riavviando il processo inetd.

REPORT REMEDIATION ACTIONS



The screenshot shows a terminal window titled "METASPLOIT [In esecuzione] - Oracle VM VirtualBox". The window displays the GNU nano 2.0.7 text editor editing the file /etc/inetd.conf. The content of the file is as follows:

```
#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
telnet                  stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/inetd.$
#<off># ftp              stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
#<off># ftp              dgram   udp      wait    nobody   /usr/sbin/tcpd  /usr/sbin/inetd.$
shell                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
login                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
exec                   stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
xinetd                  stream  tcp      nowait  root    /bin/bash      bash -i
```

At the bottom of the terminal, there is a status bar with various keyboard shortcuts and a toolbar with icons for file operations. The status bar includes: [Read 8 lines], ^G Get Help, ^X Exit, ^O WriteOut, ^J Justify, ^R Read File, ^W Where Is, ^Y Prev Page, ^U Next Page, ^K Cut Text, ^U UnCut Text, ^C Cur Pos, and ^T To Spell. The toolbar includes icons for a file, a folder, a printer, a USB drive, a network icon, a power icon, and a download icon, followed by the text "CTRL (DESTRA)".

VNC Server Password

La funzione principale di VNC è quella di controllare un computer remoto (server) tramite un computer locale (client), in questo modo i contenuti desktop del VNC server saranno mostrati sul monitor locale. La sessione VNC non è vincolata al sistema operativo installato sul server o sul client.

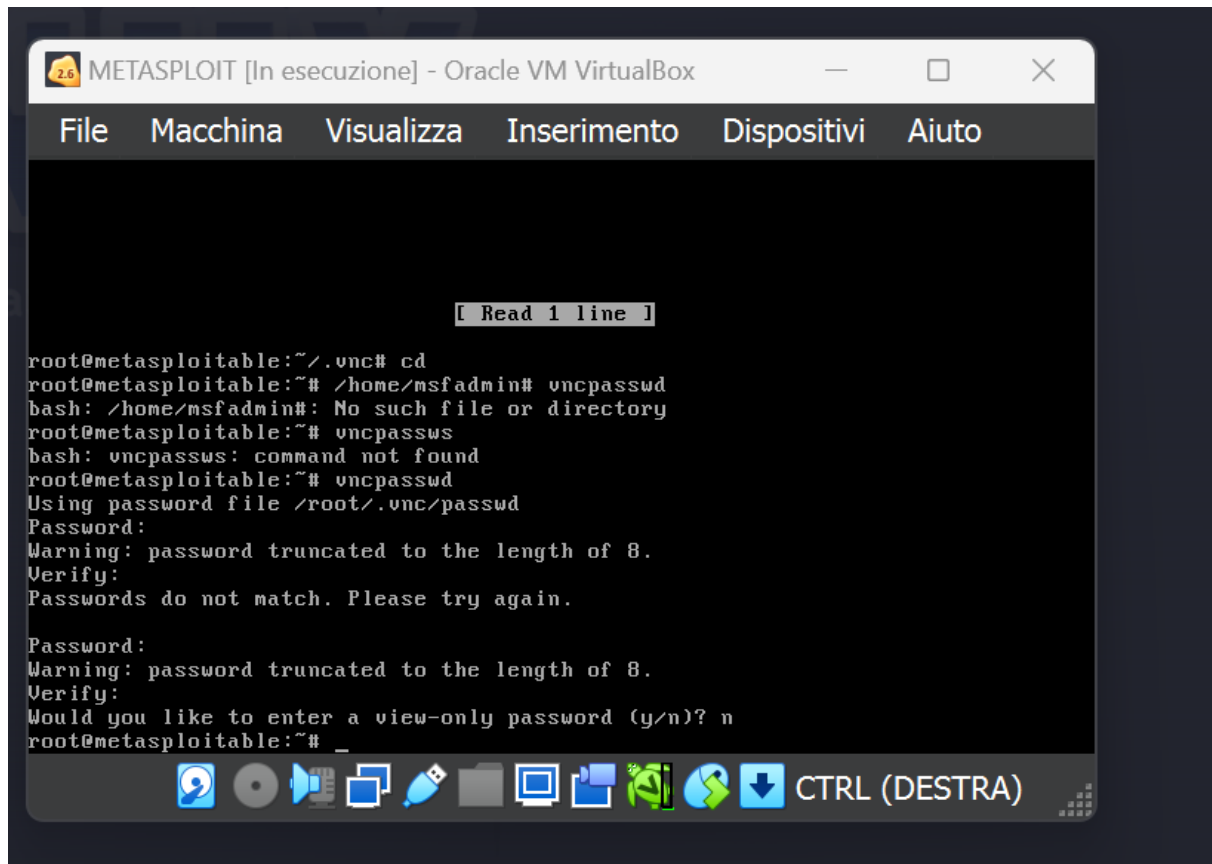
Sull'OS Metasploitable la password del servizio utilizzata è "password" quindi facilmente individuabile anche senza effettuare un brute force.

Nessus ci informa che bisognerebbe cambiare la password per rendere più sicuro il servizio, infatti cambieremo la password da "password" a "Milano1996!" che si appresta ad essere una password sicuramente più sicura in quanto composta da 11 cifre, lettere maiuscole, numeri e caratteri speciali"

Nella foto seguente vedremo come effettuare il cambio password per il servizio VNC.

Semplicemente avviamo il servizio con permessi di ROOT su Metasploitable avviando il comando "vncpasswd" e modifichiamo come desiderato la password del servizio come precedentemente già indicato.

REPORT REMEDIATION ACTIONS



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

[ Read 1 line ]

root@metasploitable:~/.vnc# cd
root@metasploitable:~# /home/msfadmin# vncpasswd
bash: /home/msfadmin#: No such file or directory
root@metasploitable:~# vncpassws
bash: vncpassws: command not found
root@metasploitable:~# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~# _
```

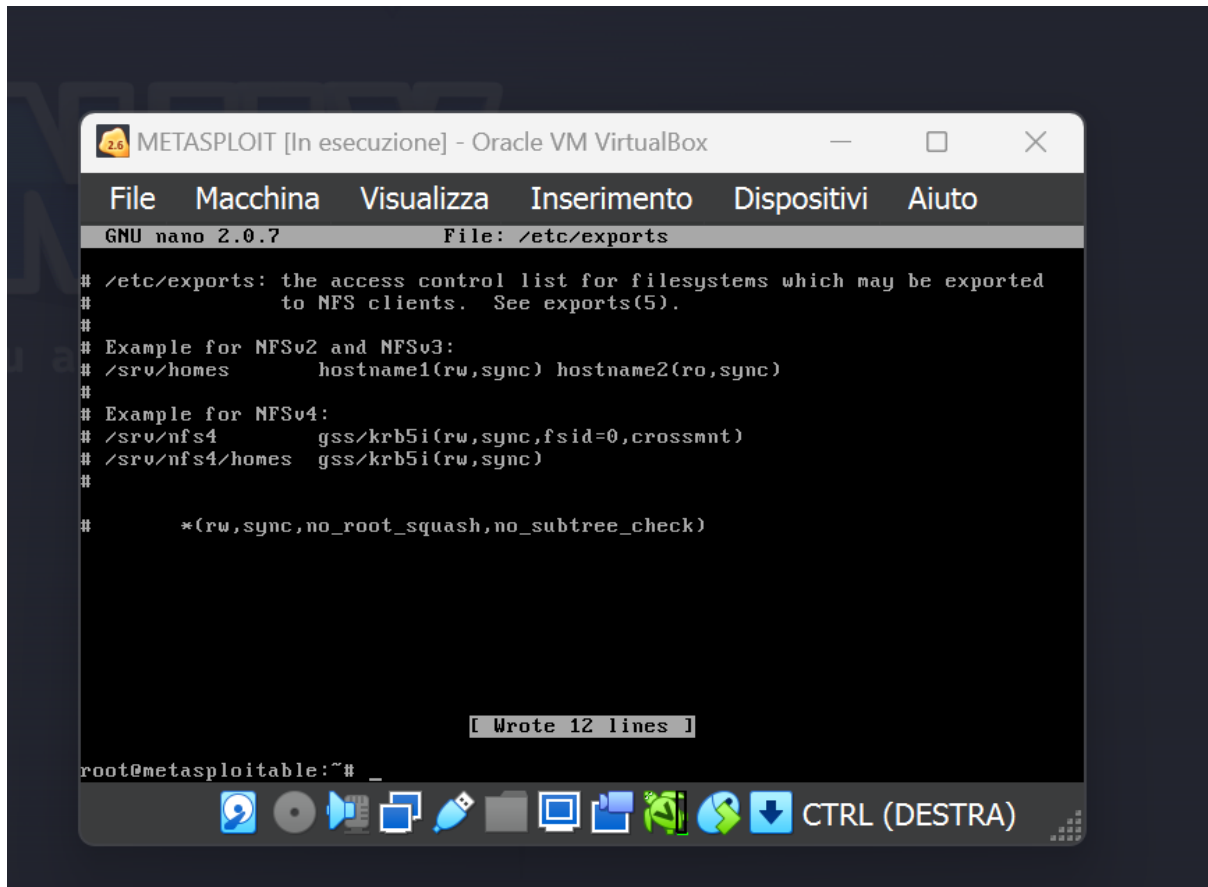
NFS Exported Share Informations Disclosure

L'NFS è un file system che consente a computer client di utilizzare la rete per accedere a directory condivise da server remoti come fossero disponibili in locale per cui se lo stesso è compromesso permette la lettura, la scrittura e la condivisione dei file presenti su un OS da un host remoto.

Per evitare che questo accada e quindi correggere la vulnerabilità dobbiamo con l'editor di testo nano modificare il file exports presente nella directory etc di Metasploitable.

Andremo quindi a commentare l'ultima riga del file in modo da non abilitare la condivisione in remoto.

REPORT REMEDIATION ACTIONS



The screenshot shows a terminal window titled "METASPLOIT [In esecuzione] - Oracle VM VirtualBox". The window contains a nano text editor editing the file `/etc/exports`. The content of the file is as follows:

```
# /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)
```

At the bottom of the terminal, a status bar indicates "[Wrote 12 lines]". The prompt shows the user is root on a machine named metasploitable.

CONCLUSIONI

Grazie a questa attività espletata utilizzando un potente strumento come Nessus Essential ho potuto constatare che un OS potrebbe contenere centinaia di vulnerabilità che andrebbero risolte il prima possibile, per evitare danni effettuati da malintenzionati sulla macchina stessa.

Non ho voluto utilizzare un firewall come soluzione per far sì che io potessi attraverso questa esercitazione apprendere il più possibile come risolvere una vulnerabilità senza bypassarla attraverso lo stesso.

Scovare le vulnerabilità e ridurle è stato particolarmente stimolante, e mi ha soprattutto permesso di mettere in atto tutto ciò che abbiamo analizzato assieme durante questa Unit.