

EPICODE-CS0124

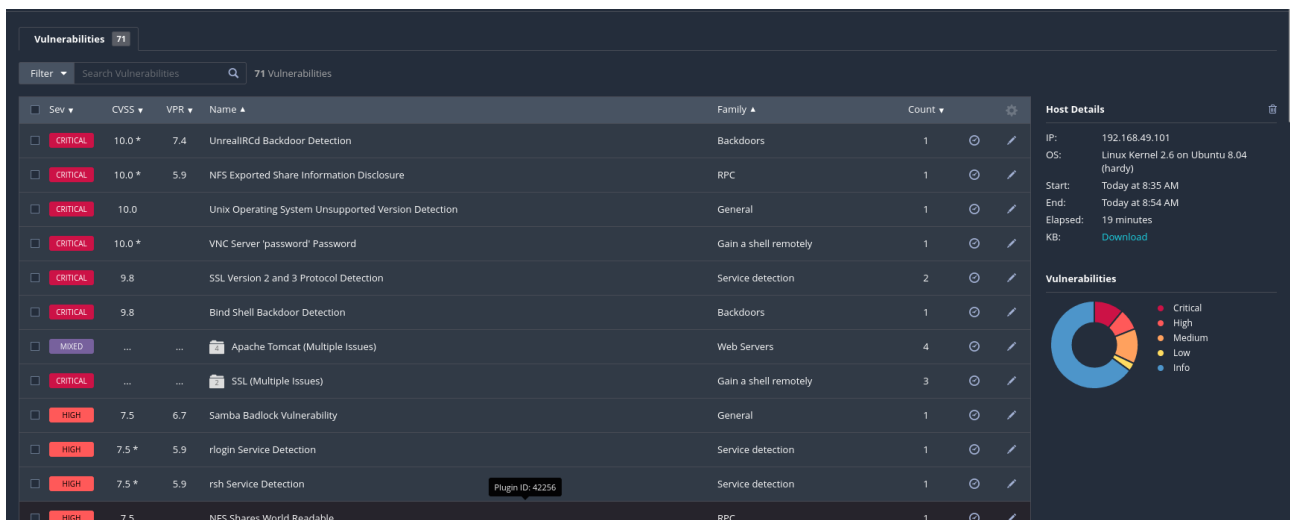
SETTIMANA 5 – PROGETTO FINALE

REPORT FINALE

La traccia del compito richiede di effettuare uno scan sul target Metasploitable, scegliere massimo 4 vulnerabilita' e successivamente cercare di migliorarle attraverso delle azioni di rimedio.

Al fine di effettuare uno scan completo di Metasploitable abbiamo utilizzato il software Nessus precedentemente installato su kali linux.

Dallo scan si evince che su Meta sono presenti diverse vulnerabilita' , evidenziando quelle critiche(High risk) in rosso;



Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
HIGH	7.5 *	5.9	rlogin Service Detection	Service detection	1
HIGH	7.5 *	5.9	rsh Service Detection	Service detection	1
HIGH	7.5		NFS Shares World Readable	RPC	1

Host Details

IP: 192.168.49.101
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 8:35 AM
End: Today at 8:54 AM
Elapsed: 19 minutes
KB: [Download](#)

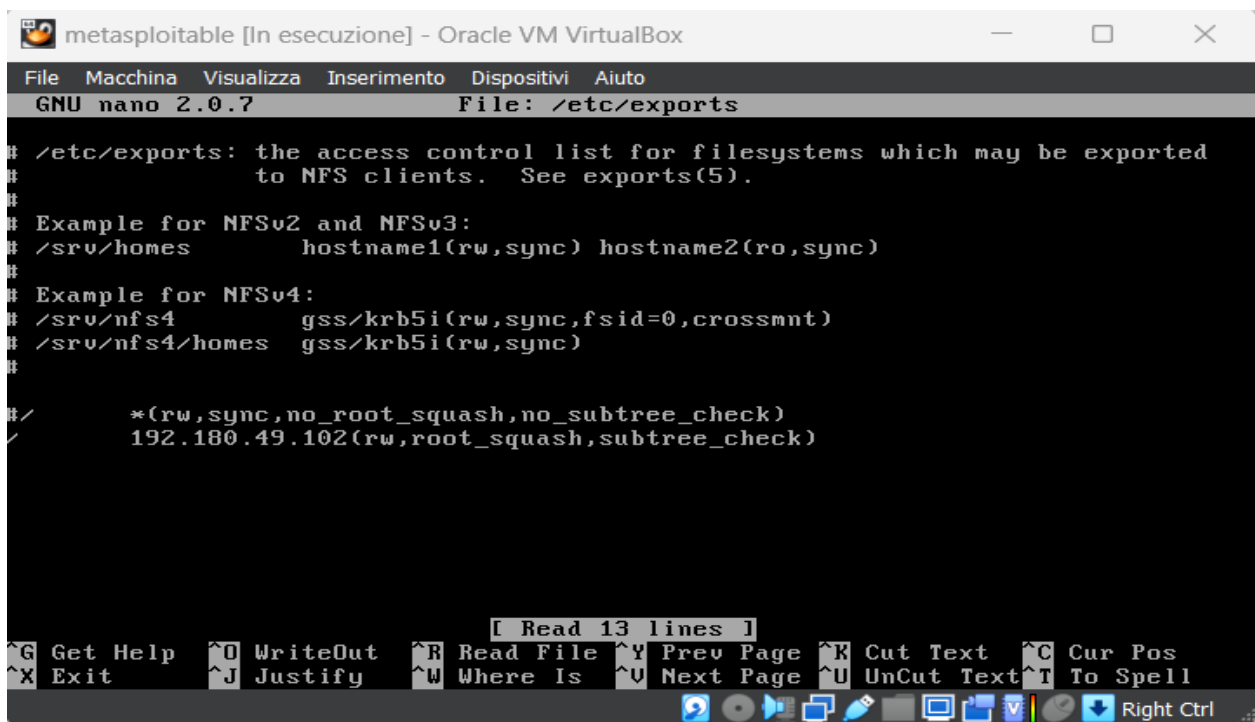
Vulnerabilities

Pie chart showing the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Una volta che abbiamo rilevato il quadro generale e acquisito la base di informazioni che ci interessano si passa all'azione su macchina Meta.

La prima vulnerabilita' di cui ci siamo occupati e' stata la NFS Exported Share information Disclosure .

Attraverso questa vulnerabilita' tutti gli host hanno accesso al protocollo NFS che serve per accedere a cartelle condivise da server remoti. Attraverso il comando `sudo nano /etc/exports/` abbiamo modificato il numero di host che si possono connettere mantenendo un host aperto con accesso al protocollo e mitigando i rischi da attacchi futuri.



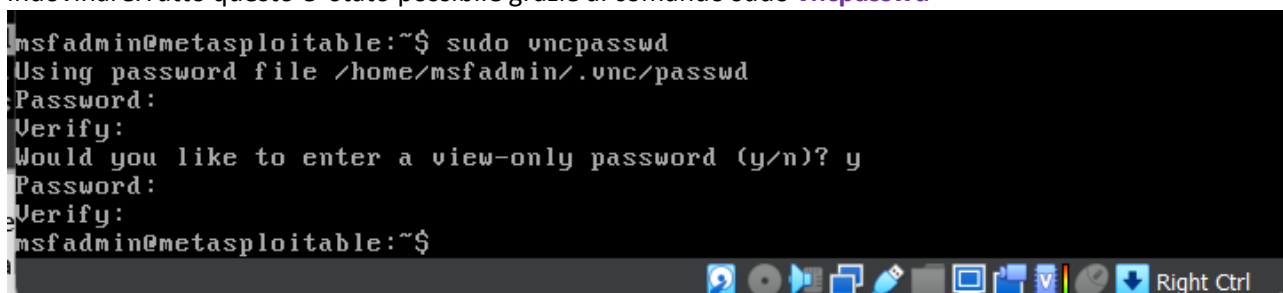
```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/exports

# /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)
# 192.168.49.102(rw,root_squash,subtree_check)

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

[ Read 13 lines ]
Right Ctrl
```

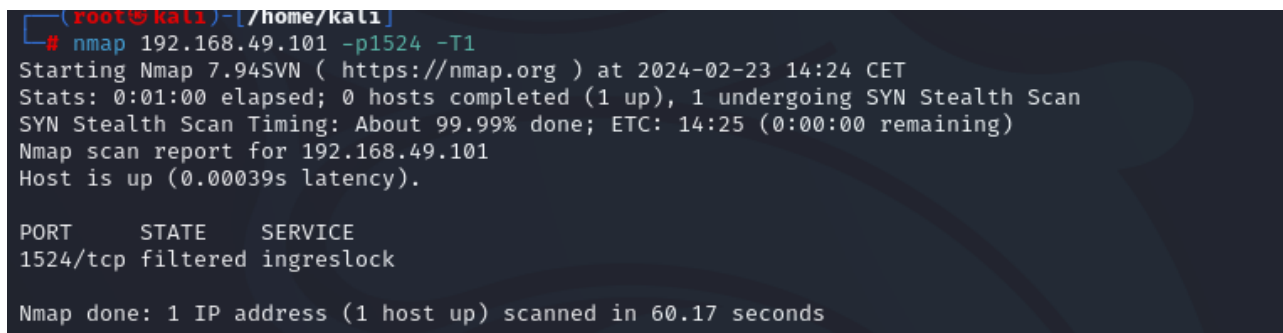
La seconda vulnerabilit  che abbiamo scelto di modificare   stata l'inserimento di una nuova password per connettersi al Virtual Network Computing, dal momento che quella in uso era obsoleta. Siamo andati quindi a modificare la password attuale e l'abbiamo sostituita con una password piu' efficace e meno facile da indovinare. Tutto questo   stato possibile grazie al comando `sudo vncpasswd`



```
msfadmin@metasploitable:~$ sudo vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$
```

L'ultima grande vulnerabilit  che abbiamo rilevato   stata la backdoor sulla porta **tcp 1524**. Al fine di evitare possibili attacchi hacker da parte di esterni siamo intervenuti prima accedendo alla lista delle regole di input tramite il comando `sudo iptables -L --line-numbers` e inserendo una regola di chiusura della porta di riferimento tramite comando `sudo iptables -A INPUT -p tcp --dport 1524 -j DROP`.

Eseguendo una scansione nmap da kali possiamo quindi confermare che la porta sia chiusa.



```
(root@kali) - [ /home/kali ]
# nmap 192.168.49.101 -p1524 -T1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 14:24 CET
Stats: 0:01:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 14:25 (0:00:00 remaining)
Nmap scan report for 192.168.49.101
Host is up (0.00039s latency).

PORT      STATE      SERVICE
1524/tcp  filtered  ingreslock

Nmap done: 1 IP address (1 host up) scanned in 60.17 seconds
```

CONCLUSIONE

A questo punto avviamo uno scan per verificare che tutte le vulnerabilita' che abbiamo preso come target siano state assolve, e possiamo vedere che a fronte delle 71 iniziali adesso ne risultano 67, quindi possiamo dedurre che il lavoro che abbiamo svolto e' andato a buon fine.

