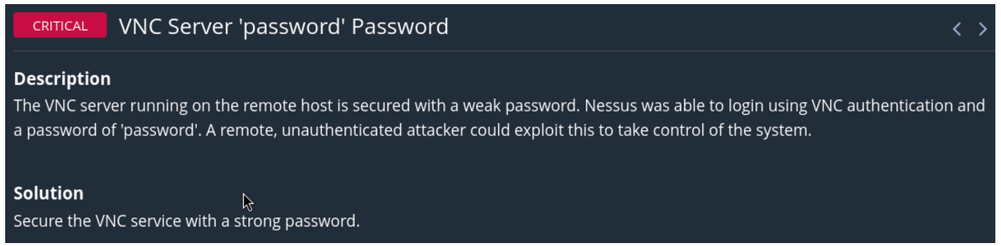
Scansione e risoluzione criticità

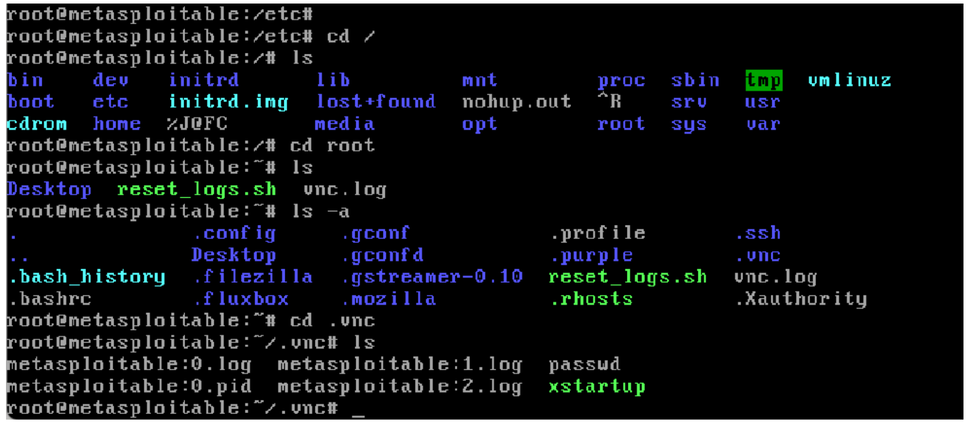
Utilizzando Nessus individuare criticità e risolverle.

Vincenzo Colletta 27/10/2023

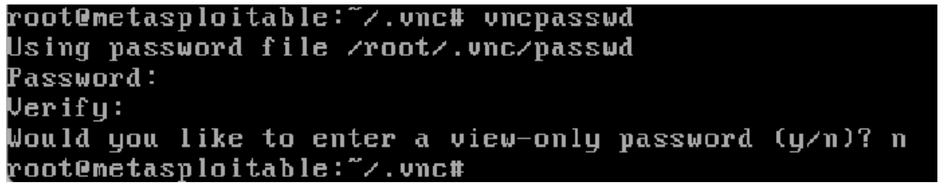
Prima criticità: Credenziali deboli



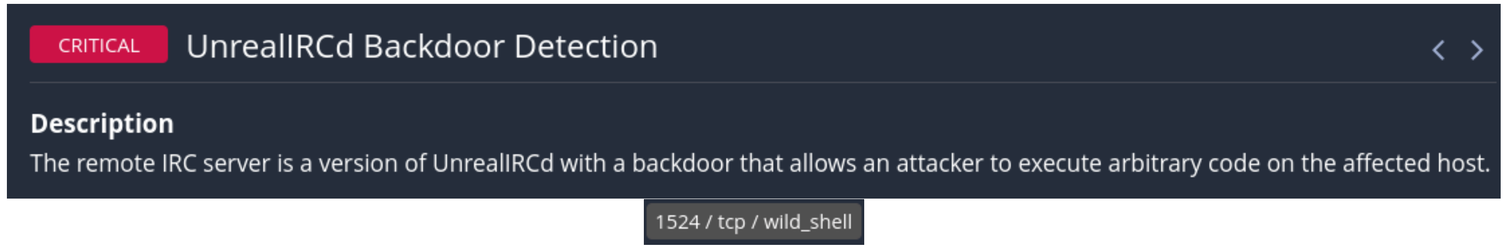
Nessus in questo caso è stato in grado di rilevare che la nostra password è debole, riuscendo a decifrarla. Per ovviare a questa vulnerabilità ci basterà andare a modificare la password, utilizzandone una più robusta. Questo primo passo ci aiuterà a rendere la nostra macchina più sicura.

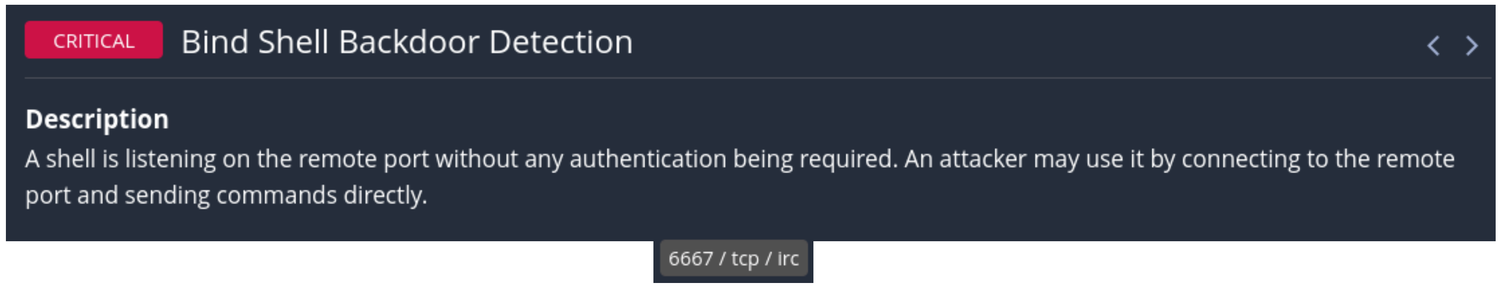


Per andare a modificare la password, tramite terminale di meta, dobbiamo andare a modificare il documento nella quale sono descritte le credenziali di accesso.
Il percorso che dobbiamo fare è partire dal root, muoverci nella cartella root, poi digitiamo il comando "*ls -a*" per visualizzare i file e le directory nascoste, poi a questo punto andiamo su .vcn, e all'interno della directory avviamo il comando "*vncpasswd*", il terminale ci chiederà di inserire le nuove credenziali e di verificarne la correttezza, una volta fatto ciò, confermiamo e la nostra password sarà modificata.



Seconda Criticità: Backdoors





La seconda criticità che rileviamo è la presenza di due backdoor differenti, aperte e accessibili a tutti. Una backdoor come sappiamo è una porta di accesso, che non richiede autorizzazioni, bypassando il sistema di autenticazione. Nessus ci informa anche del numero della porta aperta, sulle quali andremo a lavorare, per rendere più sicuro il nostro ambiente di rete.

Per regolamentare l'accesso alle nostre porte, ci sono almeno due soluzioni: chiuderla, o applicare delle regole specifiche sul firewall.

Chiusura delle porte

```
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:/$ _
```

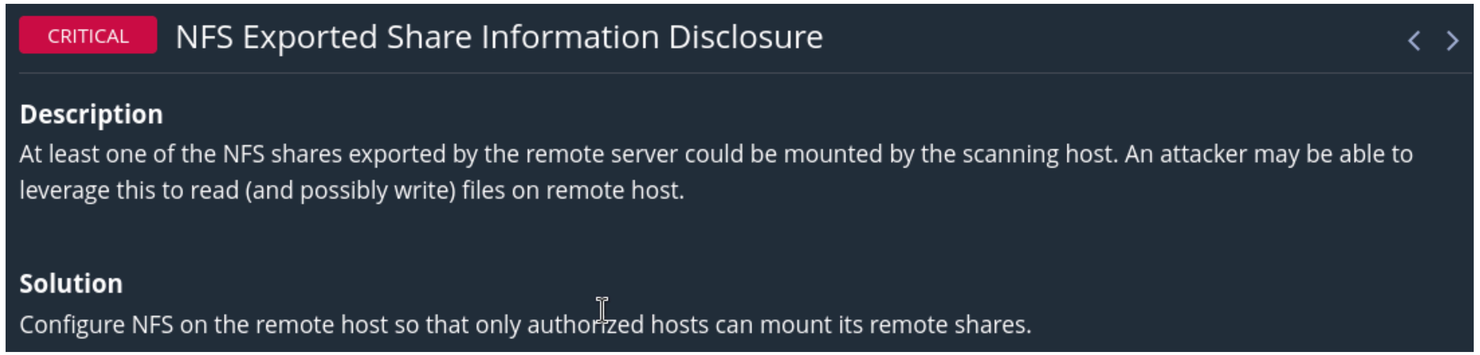
```
root@metasploitable:/# netstat -tulnp | grep 6667
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN
4792/unrealircd
root@metasploitable:/# sudo kill 4792
root@metasploitable:/# _
```

Per chiudere le porte apriamo il terminale di meta e andiamo a digitare:
*“sudo netstat -tulnp | grep *numero_porta*”*
Questo comando viene utilizzato per visualizzare le informazioni sulle connessioni di rete e i servizi in ascolto sulla porta selezionata. L'output sarà una lista di informazioni sulle connessioni di rete e i servizi in ascolto sulla porta 1524 o 6667, se ce ne sono. In questo caso vediamo che ci sono dei servizi attivi sulle porte. Con il comando successivo, andiamo a interrompere i servizi attivi su quelle porte, chiudendo appunto le porte stesse. In basso vediamo la scansione effettuata con nmap, che ci mostra lo stato delle porte.

```
┌──(fox㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.1.16 -p 1524
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 13:43 BST
Nmap scan report for kali.station (192.168.1.16)
Host is up (0.00052s latency).

PORT     STATE  SERVICE    VERSION
1524/tcp closed ingreslock

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

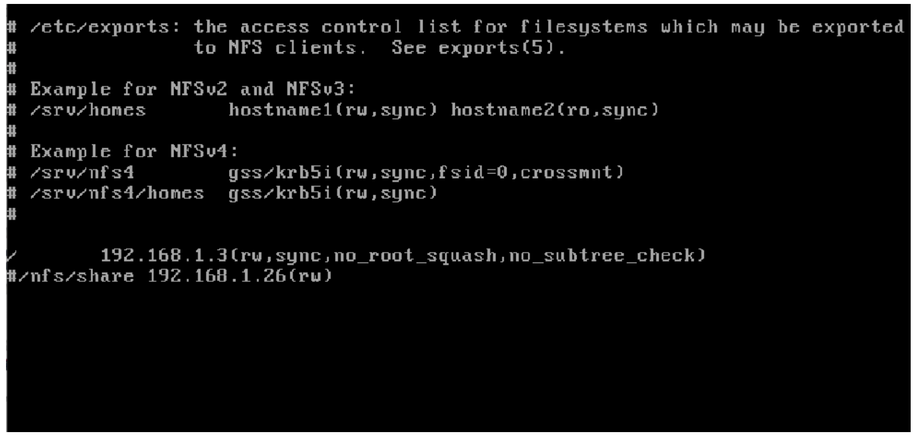
```
┌──(fox㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.1.16 -p 6667
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 13:48 BST
Nmap scan report for kali.station (192.168.1.16)
Host is up (0.0011s latency).

PORT     STATE  SERVICE VERSION
6667/tcp closed irc

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

┌──(fox㉿kali)-[~/Desktop]
└─$
```

Configurazione del servizio NFS

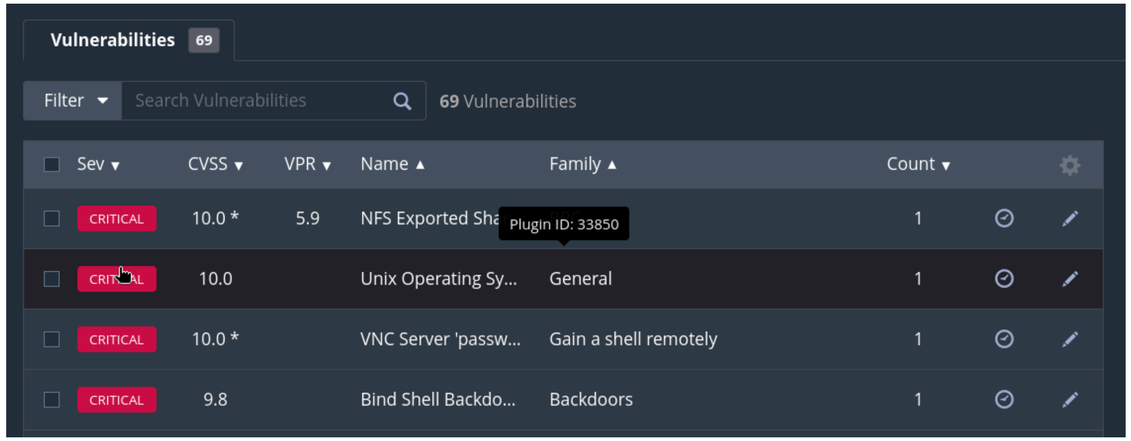


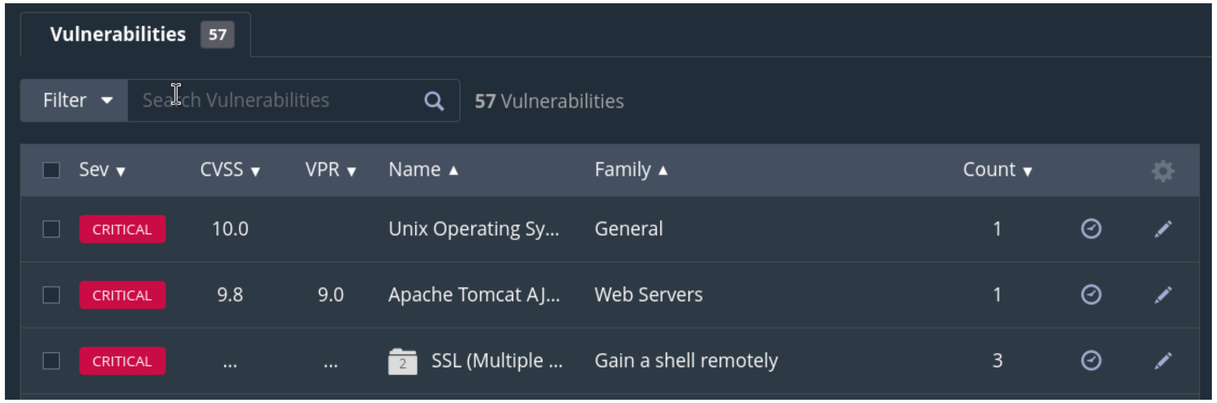
Per andare a modificare le configuarzioni andiamo a modificare il file “export” che si trova all’interno della cartella “/etc” in questo caso apriamo l’editor di testo e andiamo a modificare il parametro che regola l’accessibilità agli host. In altre parole, prima era una condivisione pubblica aperta a tutti gli host nella rete, ma una volta modificata come nella figura sotto, solamente l’IP selezionato avrà l’accesso al servizio.

L'errore "NFS Exported share information disclosure” in Nessus indica che il tool di scansione ha rilevato un problema o una potenziale vulnerabilità relativa alle condivisioni NFS (Network File System) su un sistema. NFS è un protocollo utilizzato per condividere file e risorse su una rete, e la scansione potrebbe aver rilevato problemi legati a come le condivisioni NFS sono configurate o protette. Quindi sta a noi andare a modificare i file di configurazione per stabilirne i parametri.



Come possiamo evincere da questi screen, e con i report in allegato, siamo riusciti a ridurre il numero di criticità.





Fin.

Vincenzo Colletta 27/10/2023