W12D4

Scansione finale

Informazioni generali

- Progetto: VA sulla Metasploitable 2
- Ip target: 192.168.51.100
- Data: 18/05-20/05
- Autore del report: Fabio Falato

Sommario

Vulnerabilità mitigate

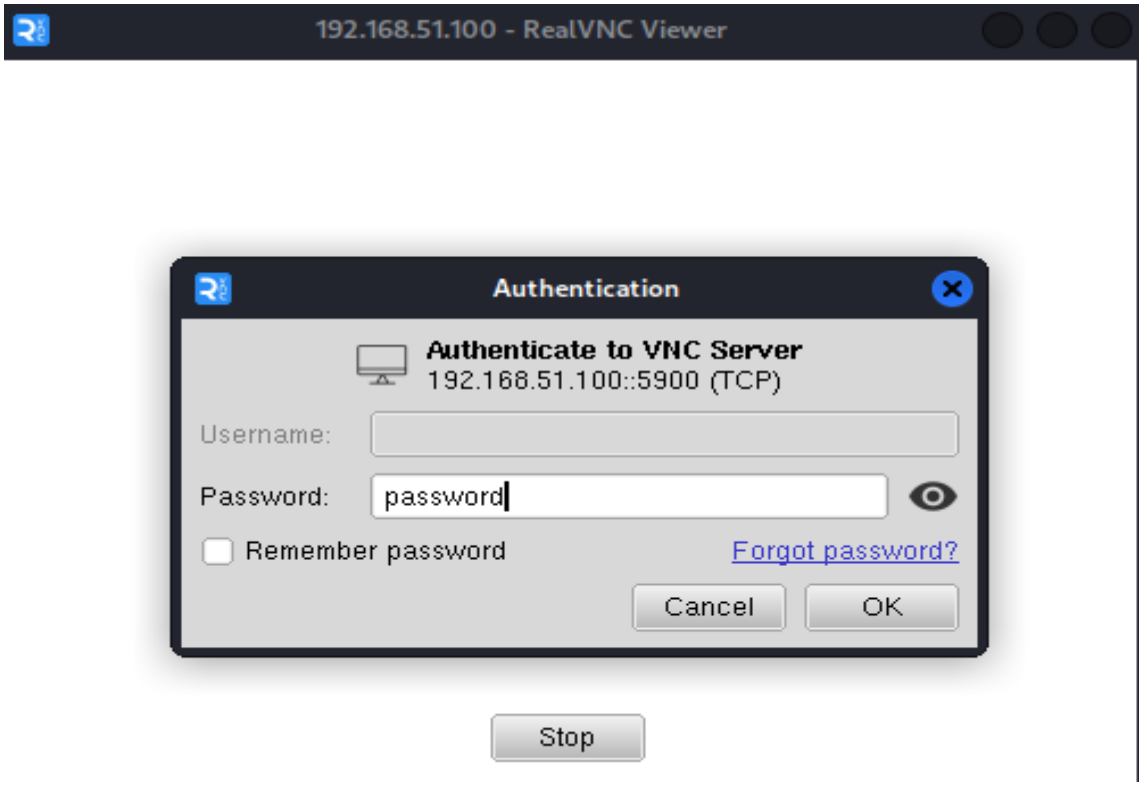
VNC Server 'password' Password

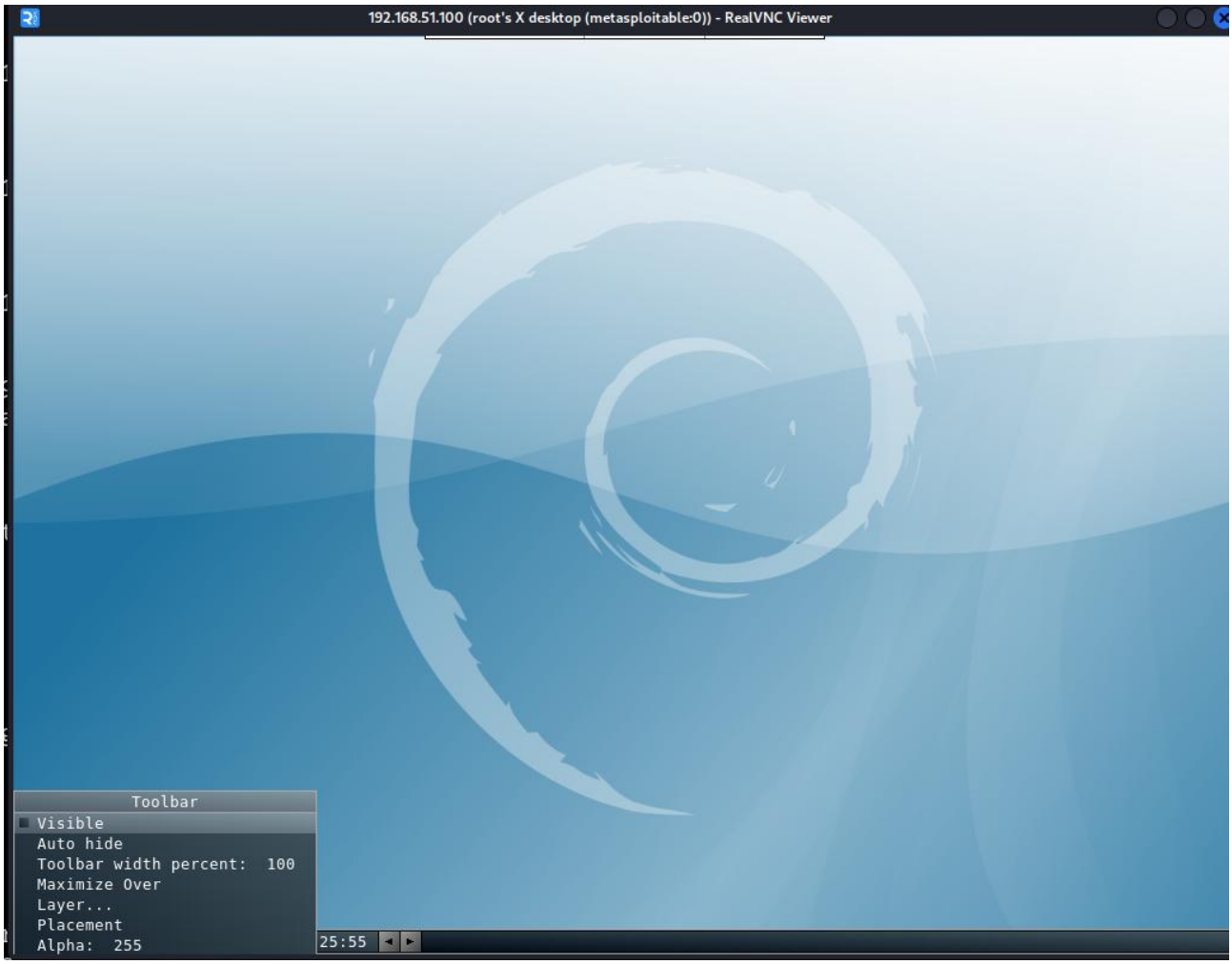
La macchina target espone la porta 5900 associata al servizio VNC mantenendo una password molto comune ovvero la parola “password”

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nmap 192.168.51.100 -sV -sS -p 5900
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 18:48 CEST
Nmap scan report for 192.168.51.100
Host is up (0.00083s latency).

PORT     STATE SERVICE VERSION
5900/tcp open  vnc     VNC (protocol 3.3)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

POC

Tentiamo un accesso VNC sulla macchina target inserendo la password standard identificata durante la fase di assesment dal Sw Nessus





L’accesso avviene regolarmente

Remediation

Per mantenere attivo il servizio VNC in sicurezza è sufficiente impostare una nuova password personalizzata inserendo numeri lettere e caratteri speciali

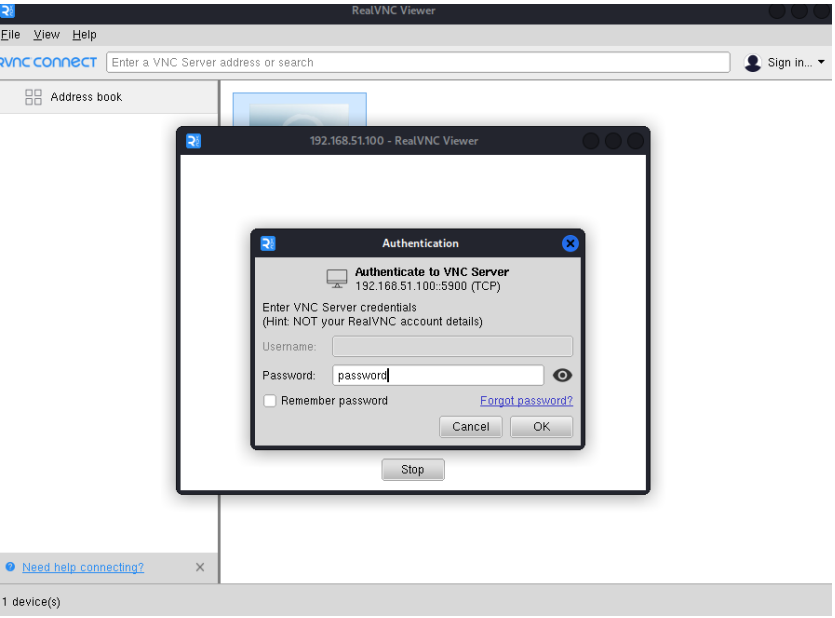
```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

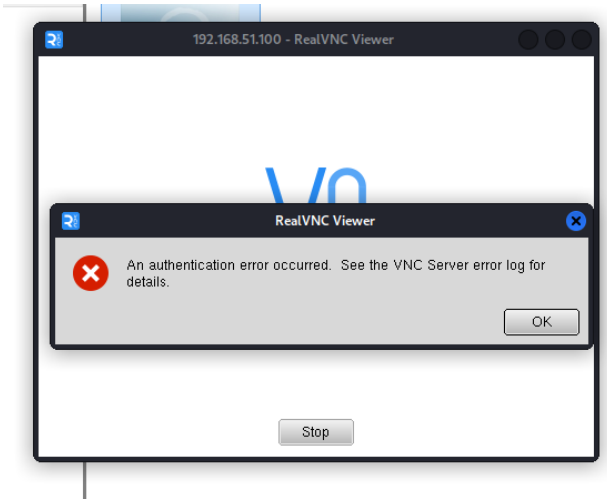
```
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# sudo vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin# _
```

Come rappresentato negli screenshot superiori andiamo ad impostare una password per il servizio Vnc, è importante modificare le credenziali di accesso per entrambi gli utenti della macchina msfadmin e root .

Infine sarà sufficiente un riavvio per modificare le password.

Test finale



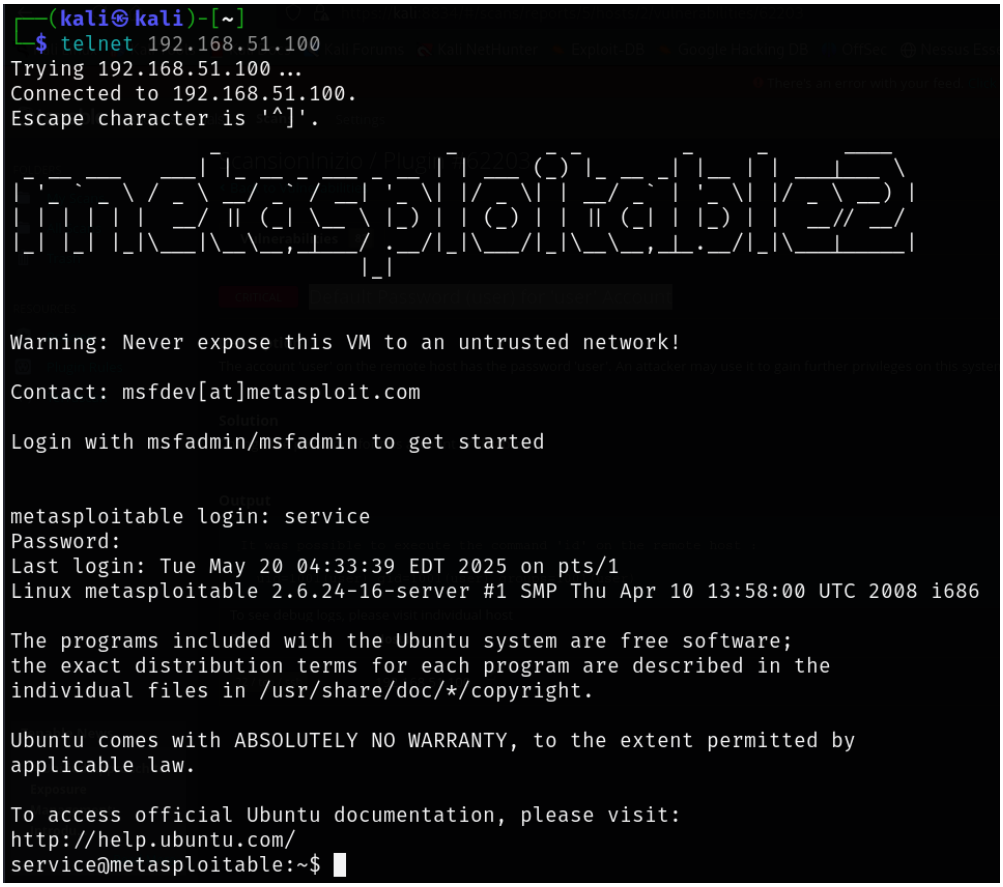


Default Password 'service' for 'service' Account / Default Password (user) for 'user' Account

ho deciso di accoppiare queste due vulnerabilità in un unico punto per la loro similarità; infatti, per entrambe si tratta nuovamente di una password di default lasciata negli account ***service*** e ***user***

POC

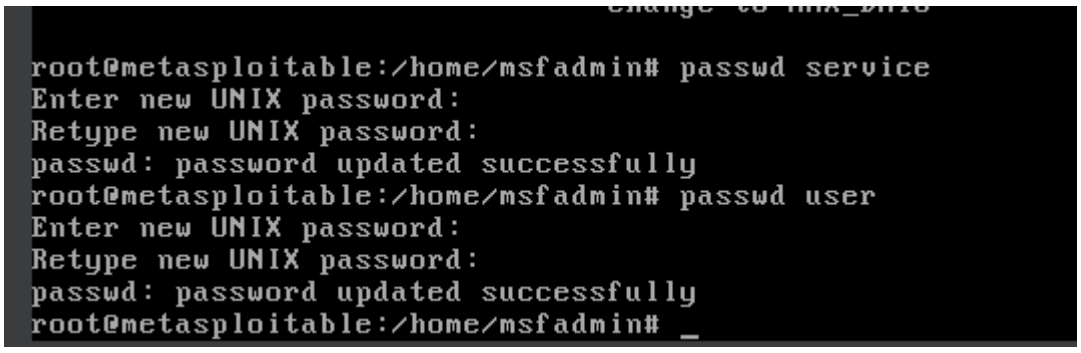
Anche se la vulnerabilità viene riscontrata sulla porta 22 è valida per tutto l'account qui viene eseguito un accesso su porta 23 con le credenziali trovate dal VA User ***service*** passw: ***service***



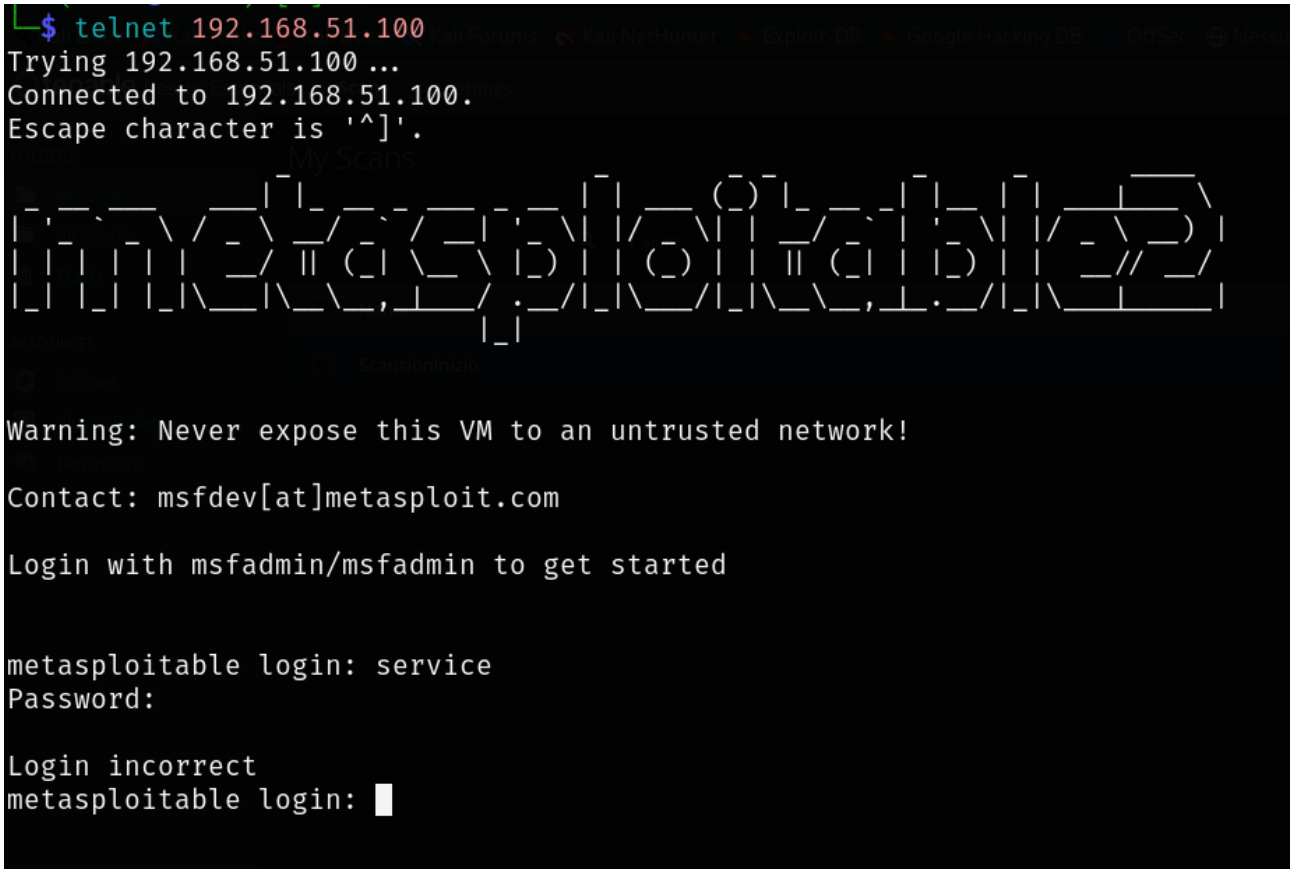
Remediation

La base della fix è come per l'anomalia precedente l'impostazione di una nuova password seguendo moderne policy di sicurezza

Come da screenshot, con l'account di root andiamo a modificare le password su entrambi gli account con il comando passwd



Test finale



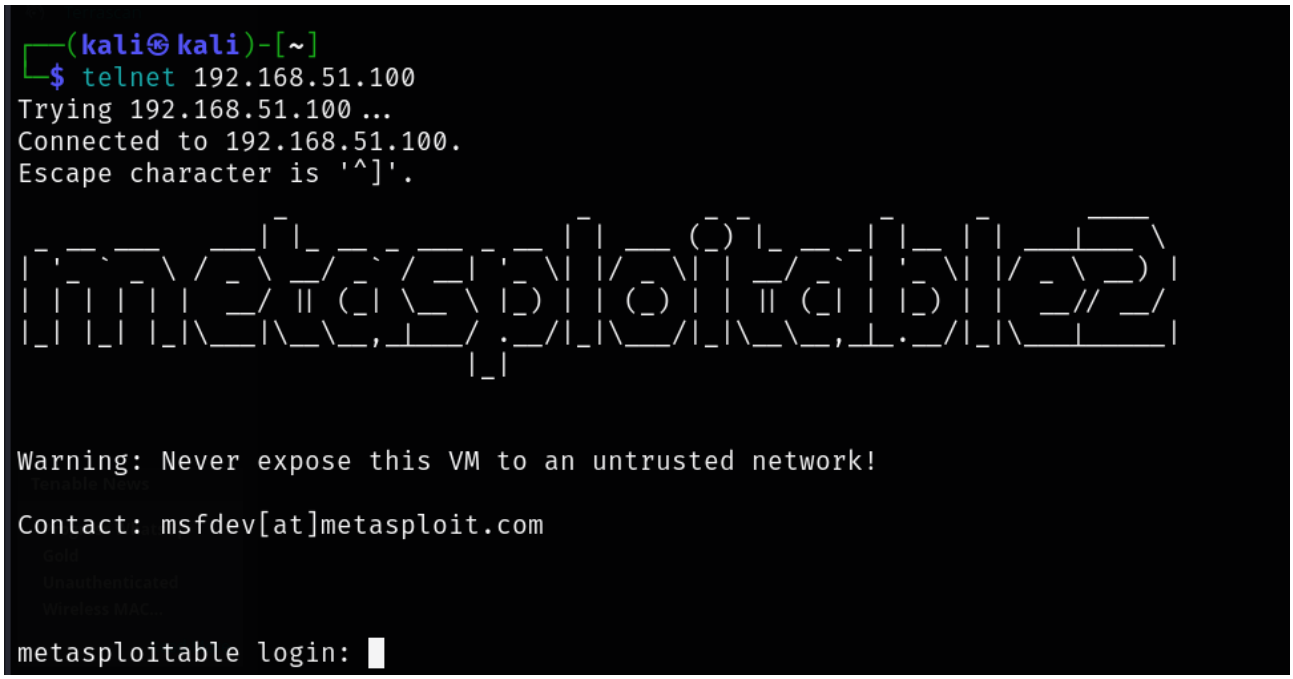
La modifica ha risolto le criticità di accesso sui due account, da notare come però il banner di login comunque esponga in chiaro user e password del account ***msfadmin***

Correzione banner di login

Per modificare il banner andiamo a modificare il file di configurazione /etc/issue.net

Test del banner

Andiamo a testare nuovamente l'accesso in telnet ed effettivamente questa volta nel banner di login non è più presente nessuna informazione che aiuterebbe un eventuale attaccante



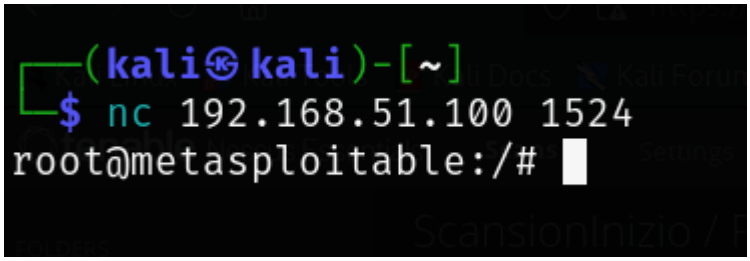
Bind Shell Backdoor Detection

Questa vulnerabilità è estremante grave in quanto espone una shell sulla porta 1524 con i privilegi amministrativi.

POC

Provo a fare accesso con netcat sul target 192.168.51.100 alla porta 1524.

L'accesso avviene facilmente senza che venga richiesta alcuna password



Remediation

Soluzione 1

Identifichiamo il processo che espone la porta 1524.

```
root@metasploitable:/home/msfadmin# netstat -tulp | grep -i "shell"
tcp        0      0 *:shell                 *:*                     LISTEN
4515/xinetd
root@metasploitable:/home/msfadmin# lsof -i :1524
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd  4515 root   12u  IPv4  12175       TCP *:ingreslock (LISTEN)
root@metasploitable:/home/msfadmin#
```

Il servizio è **XINTED**, purtroppo non possiamo andare semplicemente a rimuovere il servizio o a fermarlo perché in tal modo andremo a fermare successivamente tutti gli altri servizi di accesso remoto come ssh e telnet.

```
┌──(kali㉿kali)-[~]
└─$ netcat 192.168.51.100 1524
(UNKNOWN) [192.168.51.100] 1524 (ingreslock) : Connection refused

┌──(kali㉿kali)-[~]
└─$ telnet 192.168.51.100
Trying 192.168.51.100 ...
telnet: Unable to connect to remote host: Connection refused

┌──(kali㉿kali)-[~]
```

Questa sarebbe la soluzione migliore se non avessimo bisogno di servizi di shell remota

Soluzione 2

Andiamo a bloccare con il firewall iptables

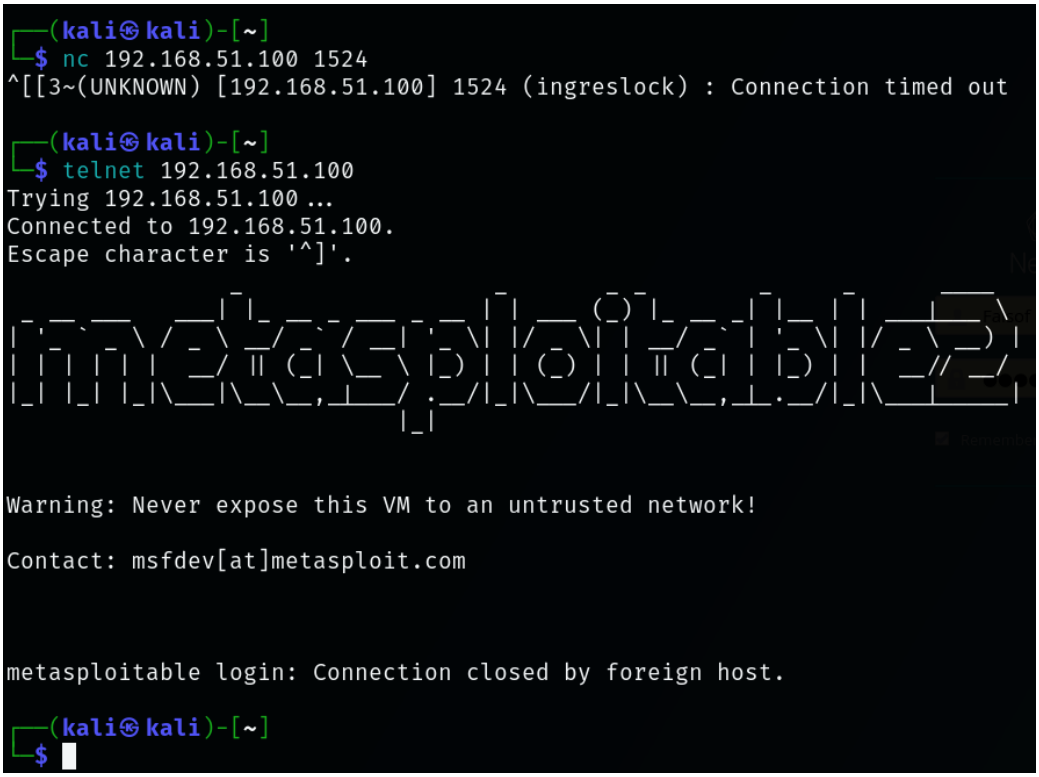
Il comando è

iptables -A INPUT -p tcp --dport 1524 -j DROP

```
iptables-restore  iptables-xml
root@metasploitable:/home/msfadmin# iptables -A INPUT -p tcp --dport 1524 -j DRO
P
root@metasploitable:/home/msfadmin# _
```

Test finale

Con questa soluzione abbiamo la possibilità di tenere in piedi accesso ssh/telnet ma bloccare l'accesso senza password delle shell



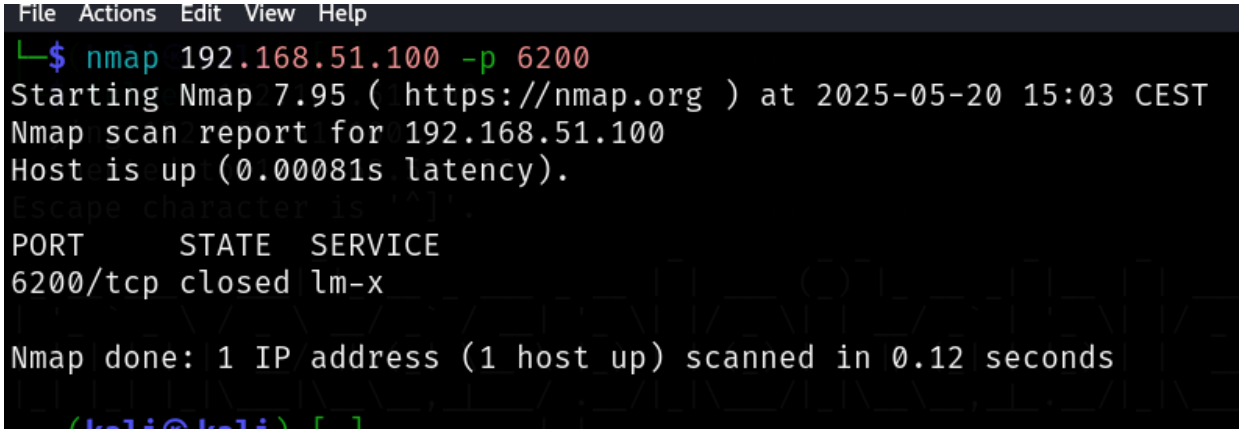
vsftpd Smiley Face Backdoor

In sostanza è stata inserita una backdoor che permette di accedere ad una shall con privilegi di root.

La backdoor si attiva se si inserisce uno user + smile :) , la backdoor permette di fa apparire una shell root sulla porta TCP 6200, senza autenticazione

POC

1. monitoriamo la porta 6200



2. Ci connettiamo in FTP inserendo uno username con lo smile :)

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.51.100
Connected to 192.168.51.100.
220 (vsFTPd 2.3.4)
Name (192.168.51.100:kali): user:)
331 Please specify the password.
Password:

421 Service not available, remote server timed out. Connection closed.
ftp: Login failed
ftp> exit
```

3. Ora la porta 6200 è attiva

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.51.100 -p 6200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 15:08 CEST
Nmap scan report for 192.168.51.100
Host is up (0.00049s latency).

PORT     STATE SERVICE
6200/tcp open  lm-x

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

4. Exploitation proviamo a connetterci alla porta 6200 con netcat, vediamo subito che il cursore rimane appeso in attesa di istruzioni proviamo un semplicissimo ls

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.51.100 6200

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Remediation

La soluzione ideale sarebbe quella di andare a disinstallare e reinstallare ftp, purtroppo la macchina al momento non ha accesso ad Internet, dunque non sarebbe possibile a meno che non si voglia rinunciare al servizio FTP.

Purtroppo anche questa volta l'unica opzione praticabile è quella di impostare una regola firewall che vada a bloccare la porta della backdoor

iptables -A INPUT -p tcp --dport 6200 -j DROP

```
root@metasploitable:/home/msfadmin# iptables -A INPUT -p tcp --dport 6200 -j DROP
root@metasploitable:/home/msfadmin#
```

Test finale

Ritentiamo nuovamente la connessione sulla porta 6200 ma questa volta non va a buon fine come è possibile vedere la porta ora è filtrata

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.51.100 -p 6200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 16:05 CEST
Nmap scan report for 192.168.51.100
Host is up (0.00086s latency).

PORT     STATE    SERVICE
6200/tcp filtered lm-x

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
┌──(kali㉿kali)-[~]
└─$ nc 192.168.51.100 6200
ls
(UNKNOWN) [192.168.51.100] 6200 (?) : Connection timed out
```

Scansione finale

Di seguito il report delle scansioni rilevata dalla macchina a seguito di un VA successivo alle mitigation riportate.

Chiaramente le condizioni di nessus sono le medesime e anche le impostazioni del firewall Pfsense

Persiste:

Titolo	**Canonical Ubuntu Linux SEoL (8.04.x)**
Descrizione	Secondo la versione indicata, Canonical Ubuntu Linux è la 8.04.x. Di conseguenza, non è più supportata dal fornitore. La mancanza di supporto implica che non verranno rilasciate nuove patch di sicurezza per il prodotto. Di conseguenza, potrebbe contenere vulnerabilità di sicurezza.
Gravità	Critica

Titolo	**Samba Badlock Vulnerability**
Descrizione	La versione di Samba sull'host remoto è vulnerabile alla falla **Badlock**, che consente a un attaccante di intercettare le comunicazioni e ottenere accesso non autorizzato a dati sensibili o servizi critici tramite un abbassamento del livello di autenticazione
Gravità	Alta

Titolo	**NFS Shares World Readable**
Descrizione	Il server NFS remoto condivide una o più risorse senza limitare l'accesso, permettendo potenzialmente a chiunque di connettersi.
Gravità	Alta

Titolo	**Samba 3.0.0 'SamrChangePassword' RCE**
Descrizione	La versione di Samba sull'host remoto presenta una vulnerabilità che permette l'esecuzione di codice da remoto, sfruttabile da un attaccante autenticato tramite input non validati in specifiche chiamate RPC, specialmente con l'opzione 'username map script' attivata.
Gravità	Media

Titolo	**Web Server Generic XSS**
Descrizione	Il server web remoto non filtra correttamente le richieste contenenti JavaScript maligno, permettendo a un attaccante di eseguire codice arbitrario nel browser degli utenti sfruttando questa vulnerabilità.
Gravità	Media

Titolo	**Browsable Web Directories**
Descrizione	Diversi plugin di Nessus hanno rilevato che sul server web sono presenti directory accessibili e navigabili pubblicamente.
Gravità	Media

Titolo	**Backup Files Disclosure**

Descrizione	Aggiungendo suffissi come .old, .bak, ~ ai nomi di alcuni file sull'host remoto, è possibile accedere ai loro contenuti, rischiando la divulgazione di informazioni sensibili.
Gravità	Media

Titolo	**Web Application Potentially Vulnerable to Clickjacking**
Descrizione	Il server web remoto non imposta gli header di risposta **X-Frame-Options** né **Content-Security-Policy (frame-ancestors)**, esponendo il sito a possibili attacchi di clickjacking. Questi attacchi permettono a un malintenzionato di indurre un utente a cliccare su elementi diversi da quelli percepiti, causando operazioni fraudolente o dannose. Gli header X-Frame-Options e CSP sono attualmente le misure più affidabili per prevenire questo tipo di attacchi, anche se non le uniche.
Gravità	Media

Differenze

Sono presenti ancora molte delle criticità segnalate dal primo VA, comunque dalle 6 critiche iniziali ne rimane solamente una che è risolvibile solamente aggiornando il S.o con una versione più moderna che riceve regolarmente patch di sicurezza.

Tra le alte ne rimangono solo 2 mentre le medie restano invariate.

Conclusioni finali

La macchina rimane ancora molto debole anche se le principali vulnerabilità sono state in parte mitigate procedendo con ulteriore lavoro e magari avendo a disposizione accesso sicuro verso internet, non sarebbe comunque possibile garantire una macchina sicura al 100% a causa della versione del S.o