VULNERABILITY ASSESSMENT

PROGETTO SETTIMANA 5 – IVAN GALATI

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Inizialmente avviamo una scansione delle vulnerabilità tramite Nessus, controlliamo le più critiche e andiamo a risolvere tre di esse. In questo caso scegliamo:

- VNC Server 'password' Password;

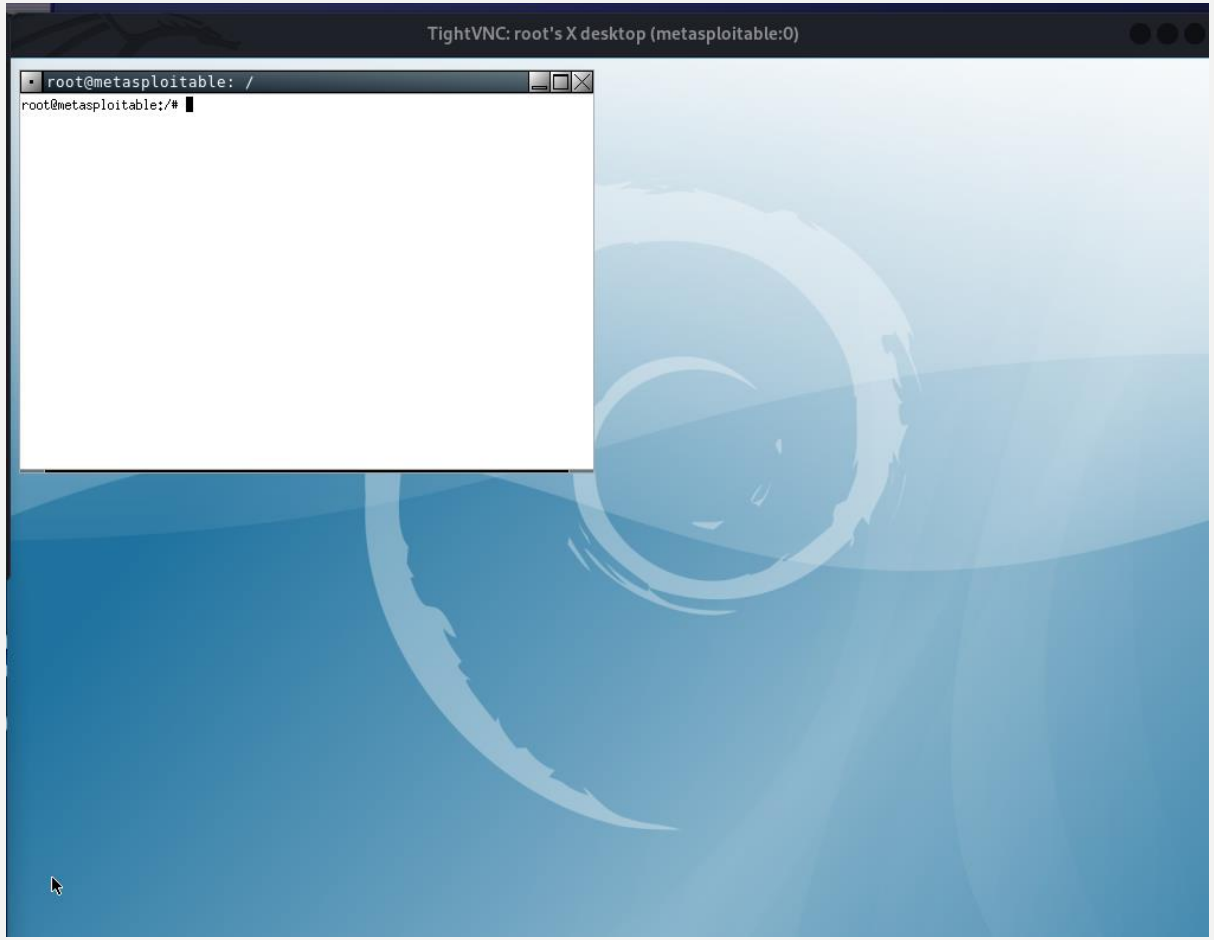
- NFS Exported Share Information Disclosure;

- Bind Shell Backdoor Detection.

1) VNC Server 'password' Password

Si riferisce al VNC (Virtual Network Control) che opera attraverso la porta 5900.
È un servizio di condivisione dello schermo creato per controllare in remoto un altro computer. Ciò significa che lo schermo, la tastiera e il mouse di un computer possono essere utilizzati in remoto da un altro dispositivo come se si fosse seduti proprio di fronte ad esso.
In questo caso Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e la password "password«[1].

1.



1) VNC Server 'password' Password

Soluzione:

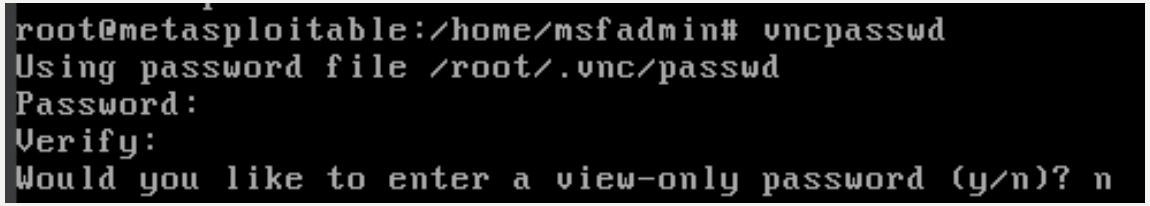
Accediamo quindi su Metasploitable e tramite il comando «vncpasswd»[1] andiamo ad impostare una nuova password per il servizio VNC.

Successivamente col comando «vncviewer ip_meta»[2] facciamo partire la comunicazione.

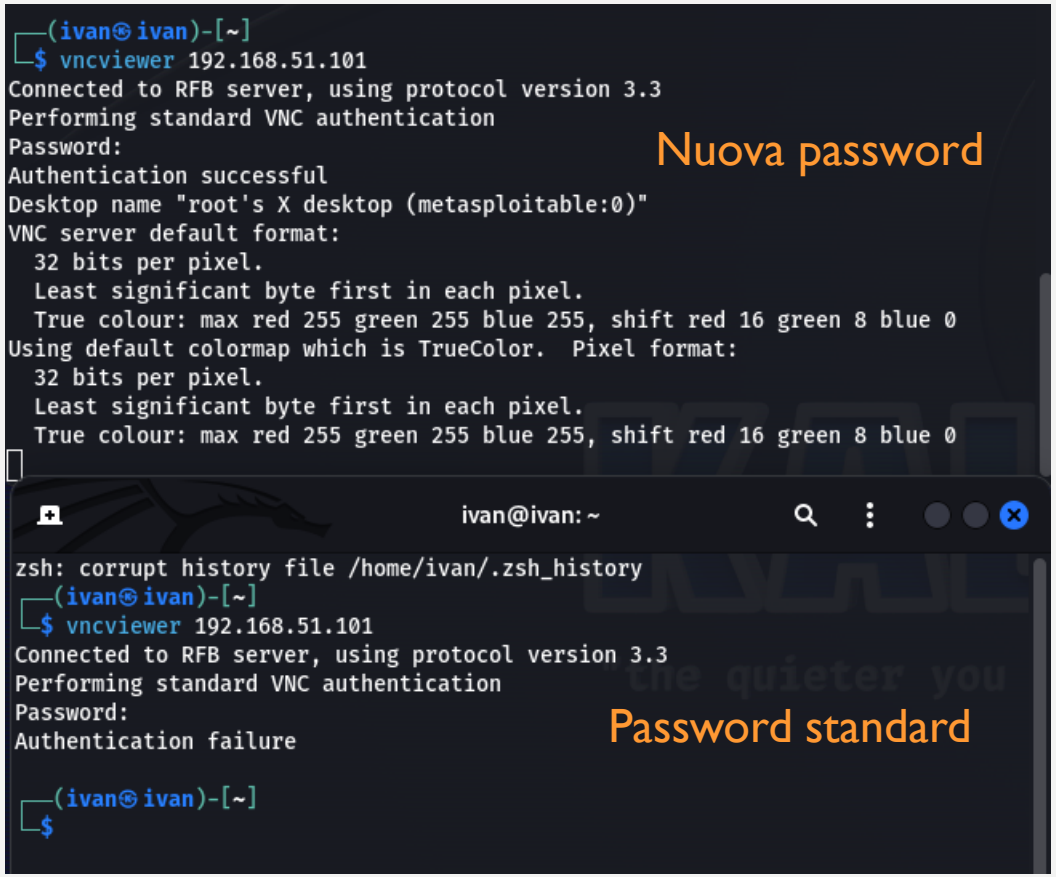
Possiamo notare che utilizzando 'password' ci dia un messaggio di errore 'Authentication Failure'.

Con la nuova password, invece, avvia la comunicazione permettendoci di comunicare con la macchina Metasploitable.

1.



2.



2) NFS Exported Share Information Disclosure

Si riferisce al protocollo NFS (Network File System) che agisce sulla porta 2049.
NFS consente ad un utente di accedere (quindi visualizzare, archiviare e aggiornare) in remoto a file e directory (tra i più importanti boot, librerie, root) su una rete di computer come se fossero archiviati localmente.
NFS è una tecnologia essenziale in ambienti aziendali in cui è necessario condividere file tra server e client.

2) NFS Exported Share Information Disclosure

Soluzione:

Andiamo ad ovviare al problema tramite l'utilizzo di due comandi:

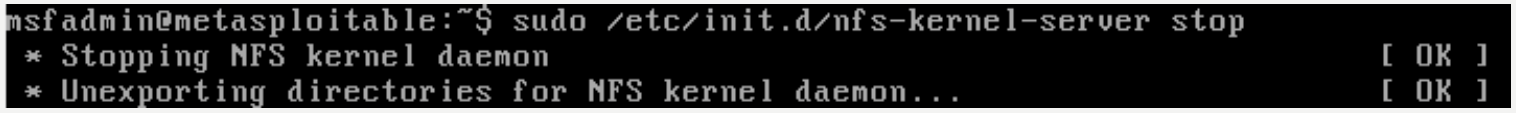
- «sudo /etc/init.d/nfs-kernel-server stop»[1]

Il nfs-kernel-server è il servizio principale per la condivisione dei file. Arrestando questo servizio, interrompiamo la possibilità di condividere.

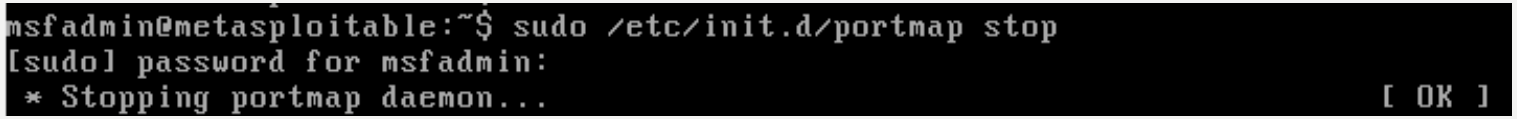
- «sudo /etc/init.d/portmap stop»[2]

Portmap è un servizio utilizzato con NFS (Network File System) per mappare i nomi dei servizi di rete alle relative porte su una macchina.

1.

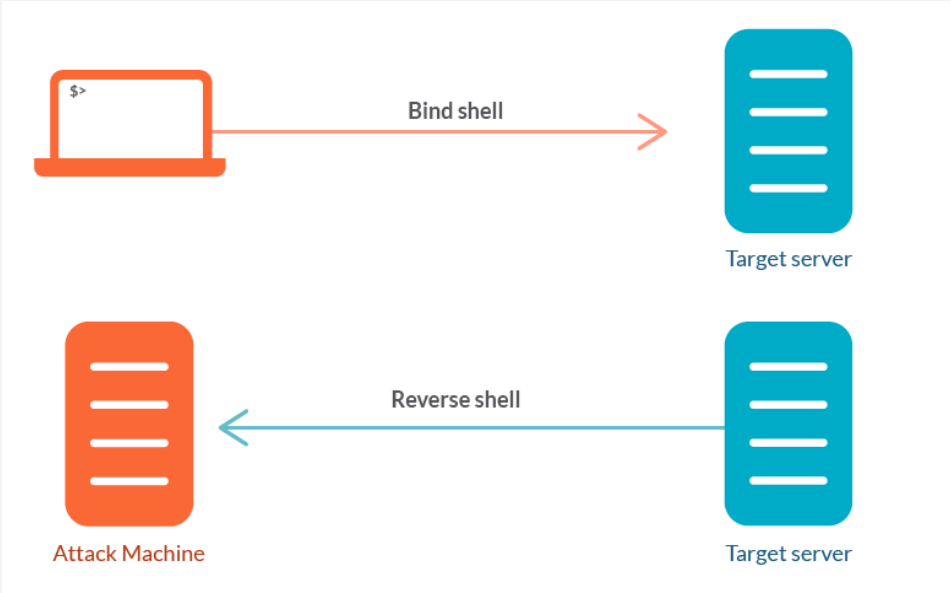


2.



3) Bind Shell Backdoor Detection

Si riferisce a una Shell che è associata alla porta 1524 (Metasploitable include un servizio Shell aperto sulla porta 1524).
Eseguirà tutto ciò che viene inviato a quella porta su Bash e risponderà con l'output.
Può essere utilizzata come strumento in fase di test per diagnosticare e risolvere problemi, ma può essere utilizzata da un black hat per connettersi ed eseguire comandi in remoto.
Nella Bind Shell, l'attaccante avvia la comunicazione col target.
È l'opposto della Reverse Shell, in cui è il target ad avviare la comunicazione con l'attaccante (utilizzata per aggirare i firewall dinamici).



3) Bind Shell Backdoor Detection

Soluzione:

Risolviamo la vulnerabilità andando a bloccare i pacchetti tcp indirizzati alla porta 1524 tramite il comando «iptables –A INPUT –p tcp –dport 1524 –j DROP»[1].

1.

```
root@metasploitable:/home/msfadmin# iptables -A INPUT -p tcp --dport 1524 -j DRO
P
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere            tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@metasploitable:/home/msfadmin#
```

Successivamente utilizziamo il comando «iptables –L» per visualizzare la lista di regole di iptables per verificare se sia impostato correttamente.

Infine eseguiamo una prova con Nmap sulla porta 1524 e notiamo come adesso abbia lo stato «Filtrata»[2].

2.

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 14:01 CEST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.
)
Host is up (0.00070s latency).

PORT     STATE    SERVICE
1524/tcp filtered ingreslock
MAC Address: 08:00:27:7C:EF:6E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

FINE