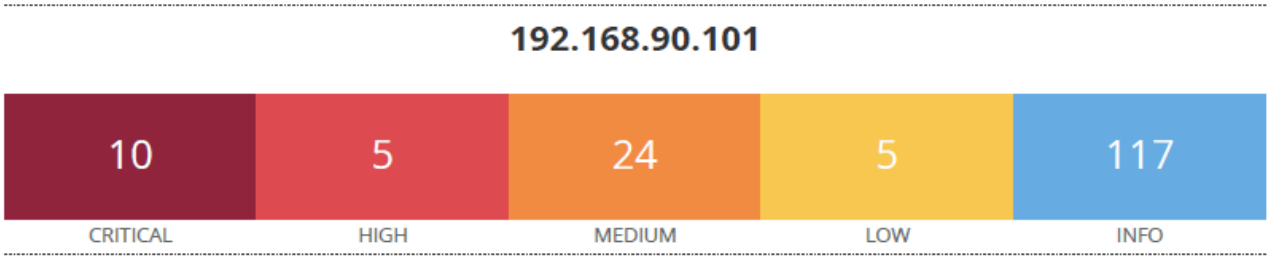
Scan_Metasploitable

Report generated by Nessus™ Thu, 24 Nov 2022 15:23:25 CET

Chiara Bortolotti

18/05/2024



VULNERABILITY ASSESSMENT – REPORT TECNICO

Informazioni sulla scansione

Inizio: 18/05/2024 14:53:49

Termine: 18/05/2024 15:23:25

Informazioni sull'host

Netbios Name: METASPLOITABLE

IP: 192.168.90.101

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

VULNERABILITA' DA CORREGGERE

61708 - VNC Server 'password' Password

Descrizione:

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di effettuare il login utilizzando l'autenticazione VNC e una password di tipo "password". Un attaccante remoto non autenticato potrebbe sfruttare questa situazione per prendere il controllo del sistema.

Soluzione:

Proteggere il servizio VNC con una password forte.

Fattore di Rischio: Critico

Plugin Output: tcp/5900/vnc

51988 - Bind Shell Backdoor Detection

Descrizione:

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla collegandosi alla porta remota e inviando direttamente i comandi.

Soluzione:

Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

Fattore di rischio: Critico

Plugin Output: tcp/1524/wild_shell

11356 - NFS Exported Share Information Disclosure

Descrizione:

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questa possibilità per leggere (ed eventualmente scrivere) i file sull'host remoto.

Soluzione:

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

Fattore di Rischio: Critico

Plugin Output: udp/2049/rpc-nfs

REMEDIATION ACTIONS

Metasploitable - W12D4

Chiara Bortolotti
CSPT0124

INTRODUZIONE

Nei passaggi successivi andremo a sanare alcune delle criticità che sabbiamo portato alla luce sulla vm Metasploitable, grazie all'utilizzo del tool Nessus.
Abbiamo iniziato facendo una scansione della VM impostando l'IP corrispondente, al termine dell'attività di remediation procederemo con una seconda scansione per verificare che le vulnerabilità prese in considerazione non siano più presenti.

INDICE VULNERABILITÀ SCELTE

01 61708 - VNC Server 'password' Password

02 51988 - Bind Shell Backdoor Detection

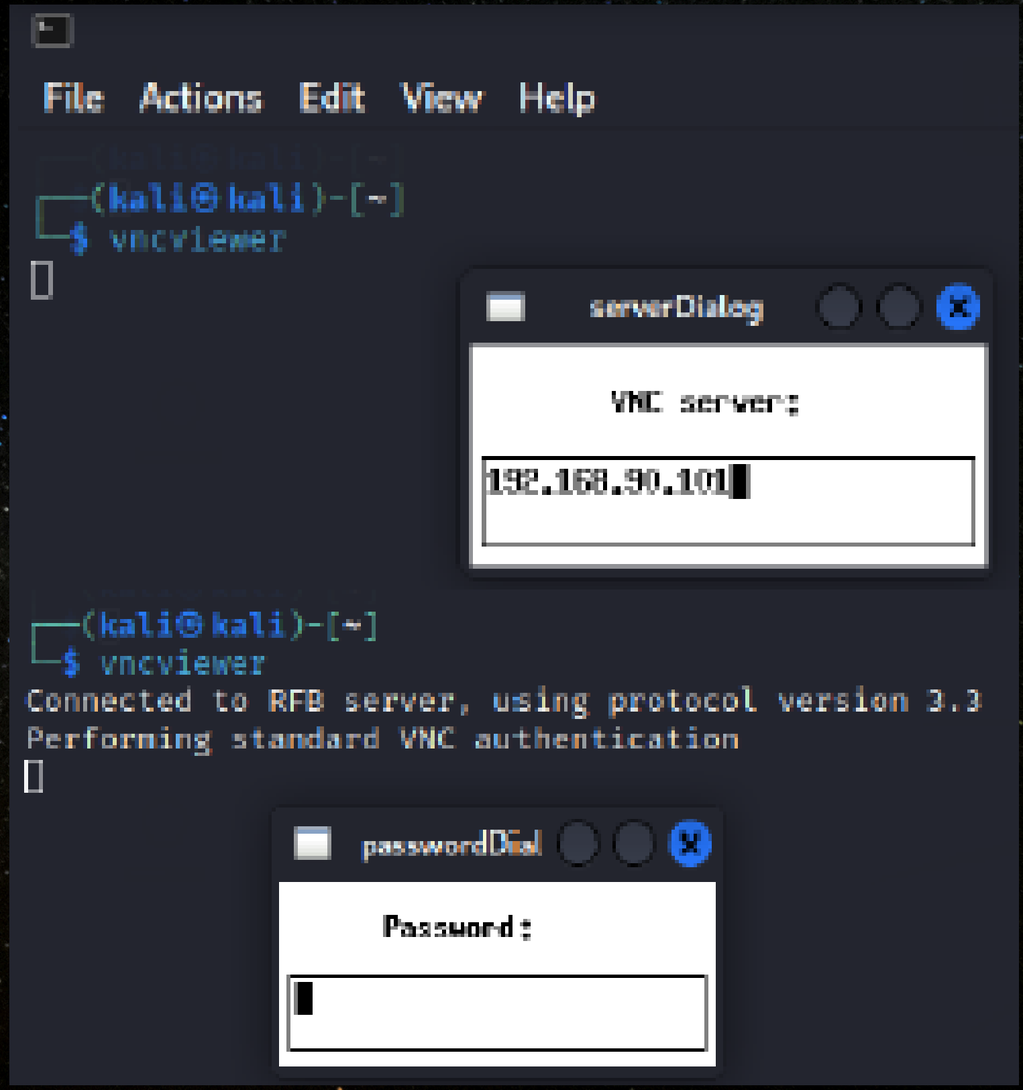
03 11356 - NFS Exported Share Information Disclosure

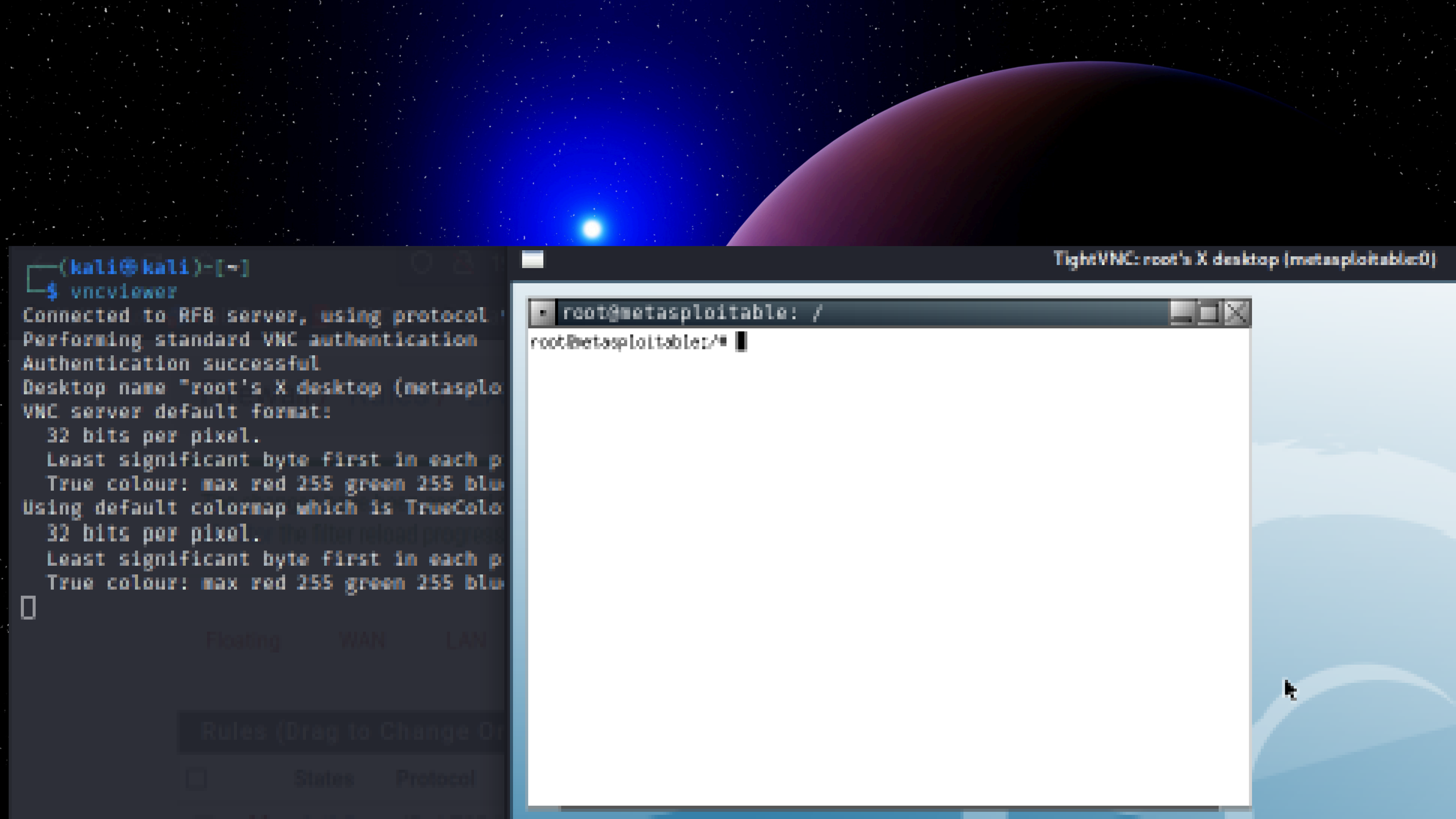
1. 61708

VNC Server 'password'
Password

REMEDIATION ACTION

Modifica della password di accesso a VNC Server.
Lo scopo è cambiare la credenziale “password” e lo facciamo tramite l'utilizzo di vncviewer all’host 192.168.90.101 dove abbiamo privilegi di root su Metasploitable




┌──(kali㉿kali)-[~]
└─$ vncviewer
Connected to RFB server, using protocol
Performing standard VNC authentication
Authentication successful
Desktop name "root's X desktop (metasplo
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each p
  True colour: max red 255 green 255 blu
Using default colormap which is TrueColo
  32 bits per pixel.
  Least significant byte first in each p
  True colour: max red 255 green 255 blu
TightVNC: root's X desktop (metasploitable0)
root@metasploitable: /
root@metasploitable:/#

Impostiamo una chiave sicura, formata da caratteri alfanumerici e caratteri speciali. Rispettiamo inoltre il numero massimo di 8 caratteri permessi da VNC.

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

Facendo un tentativo con la vecchia password ci restituisce una risposta negativa, perciò la modifica è andata a buon fine

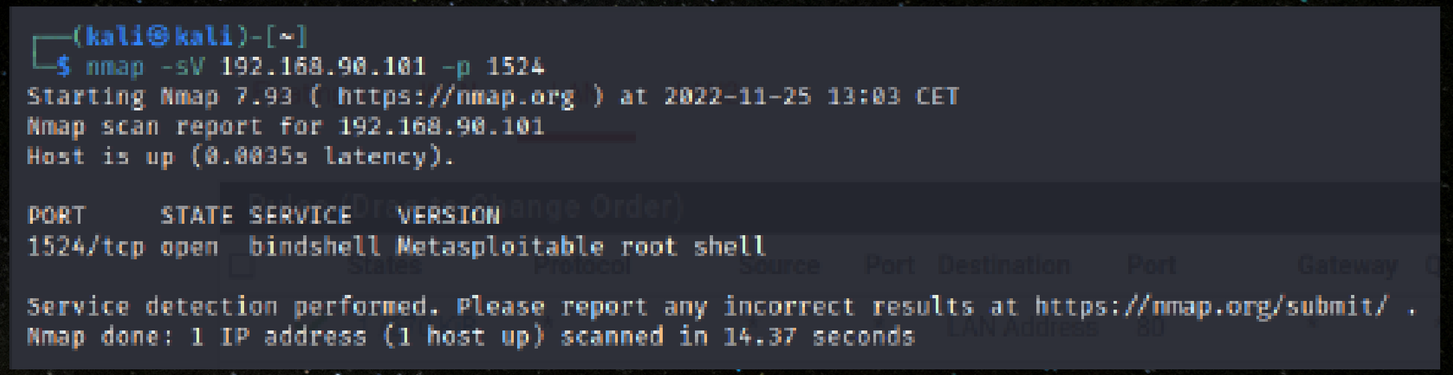
```
┌──(kali㉿kali)-[~]
└─$ vncviewer
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Authentication failure
```

2.51988

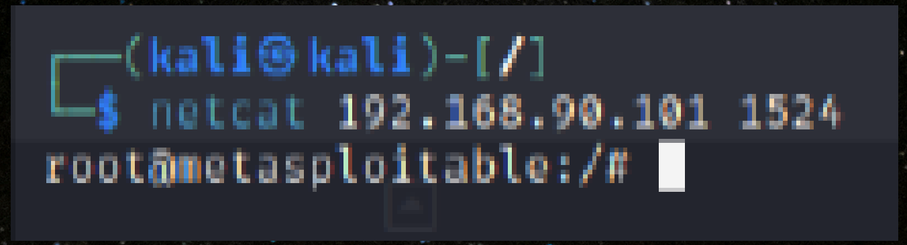
Bind Shell Backdoor Detection

REMEDIATION ACTION

Disabilitazione della shell in ascolto sulla porta 1524
Effettuo una scansione di version detection (nmap) per verificare lo stato della porta 1524 e il tipo di servizio in ascolto ad esso associato, ossia Metasploitable root shell.



Constatiamo che tramite Metasploitable root shell è facile accedere con privilegi di root all'host 192.168.90.101 tramite la porta 1524, utilizzando un tool simile a netcat:



Sarà necessario procedere con la disabilitazione della shell in ascolto in modo da andare ad evitare che in futuro possano essere ingaggiate delle connessioni. Accediamo dunque a inetd.conf, che corrisponde al file di configurazione dei servizi internet e procediamo a disabilitare la backdoor (commento la riga ingreslock stream tcp nowait root /bin/bash bash -i)

Faccio un nuovo tentativo con version detection possiamo evidenziare che la porta 1524 risulta chiusa rendendo impossibile stabilire una connessione con netcat, precedentemente ammessa.

```
┌──(kali㉿kali)-[/]
└─$ nmap -sV 192.168.90.101 -p 1524
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 14:14 CET
Nmap scan report for 192.168.90.101
Host is up (0.0014s 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 14.19 seconds
```

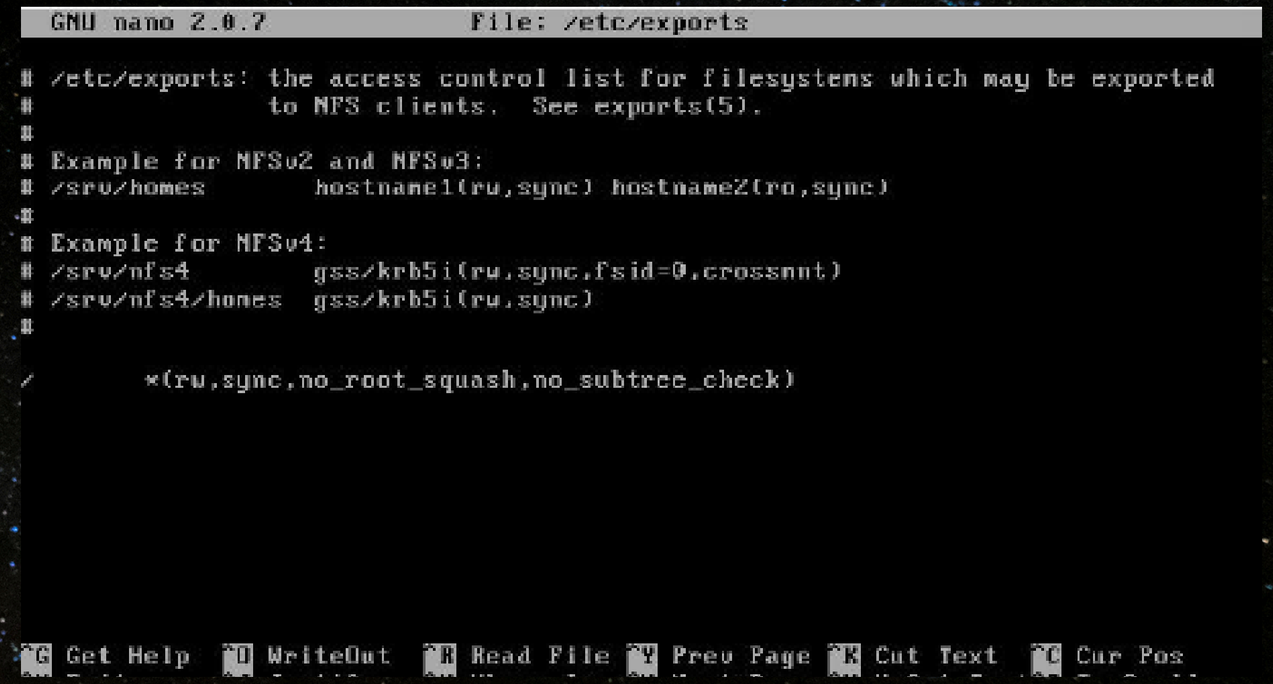
```
┌──(kali㉿kali)-[/]
└─$ netcat 192.168.90.101 1524
(UNKNOWN) [192.168.90.101] 1524 (ingreslock) : Connection refused
```

3. 11356

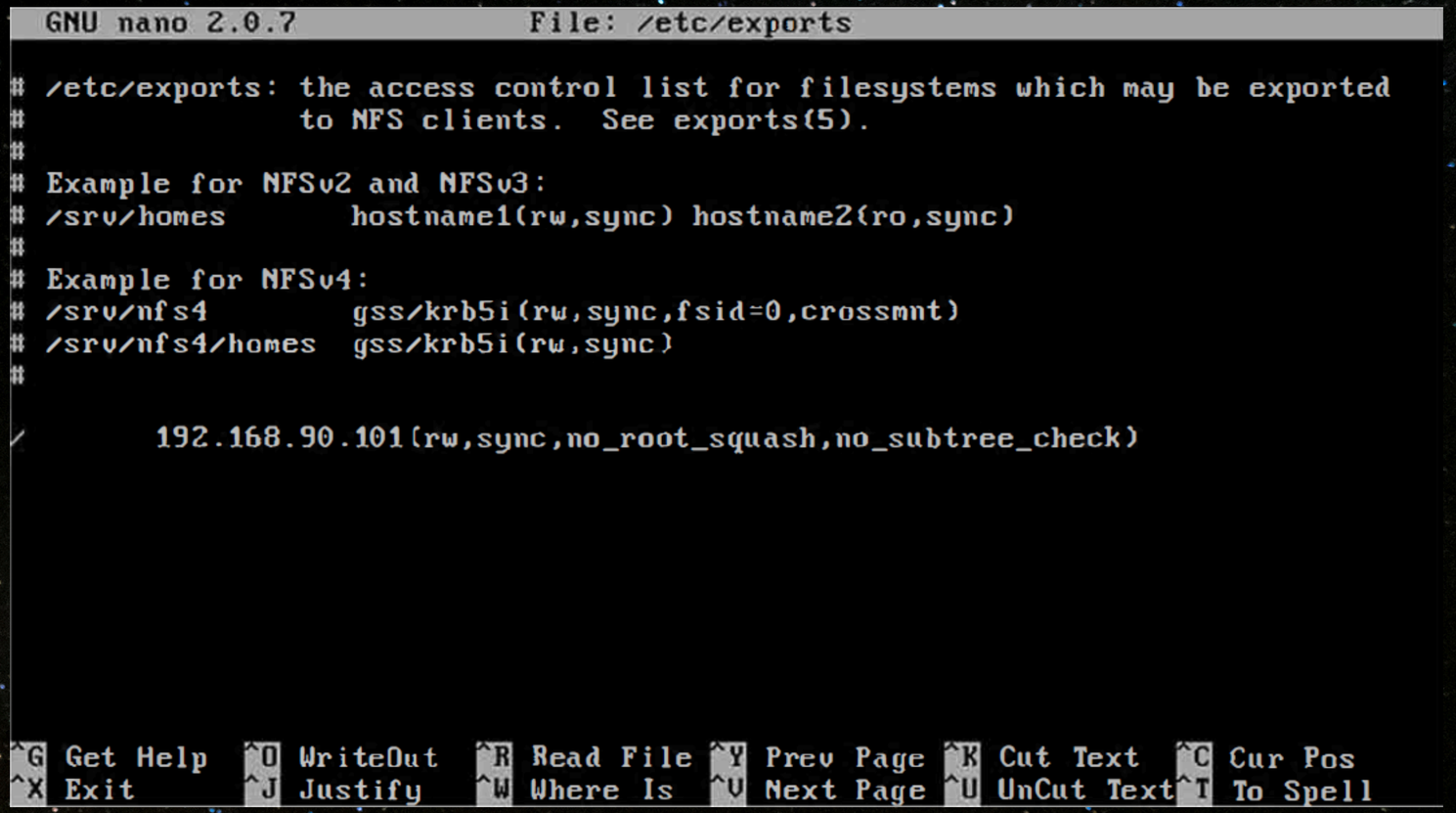
NFS Exported Share Information Disclosure

REMEDIATION ACTION

Impedire l’accesso e la condivisione di file con protocollo NFS ad utenti non autorizzati
Si dovrà procedere in modo da impedire l’accesso al servizio Network File System, così da evitare il rischio di eventuali attacchi. Iniziamo effettuando l'accesso con root privileges al file con percorso /etc/exports, procediamo all'eliminazione della wildcard e inseriamo l’indirizzo IP dell’host (192.168.90.101).



Evitiamo così che lettura, modifica e condivisione dei files possano essere effettuate da esterni.



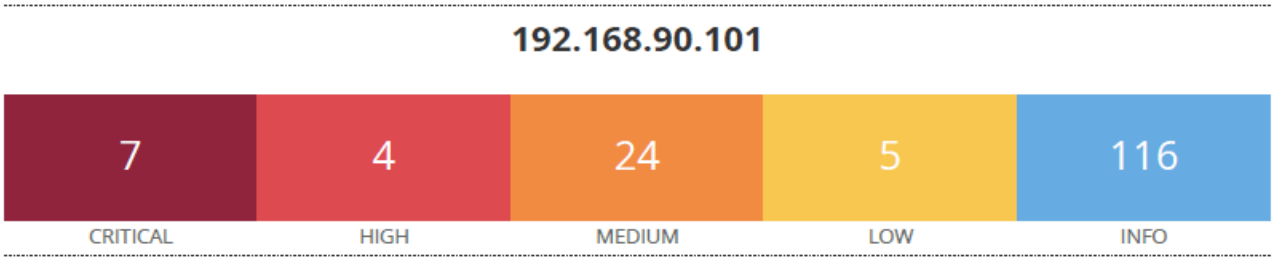
GRAZIE

Scan_new_Metasploitable

Report generated by Nessus™ Fri, 25 Nov 2022 14:49:28 CET

Chiara Bortolotti

18/05/2024



Informazioni sulla scansione

Inizio: 18/05/2024 16:20:01

Termine: 18/05/2024 16:49:28

Informazioni sull'host

Netbios Name: METASPLOITABLE

IP: 192.168.90.101

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

VULNERABILITA' CORRETTE:

1. **61708 - VNC Server 'password' Password**
2. **51988 - Bind Shell Backdoor Detection**
3. **11356 - NFS Exported Share Information Disclosure**