Floriana Feminò

25/11/2022

REMEDIATION ACTIONS

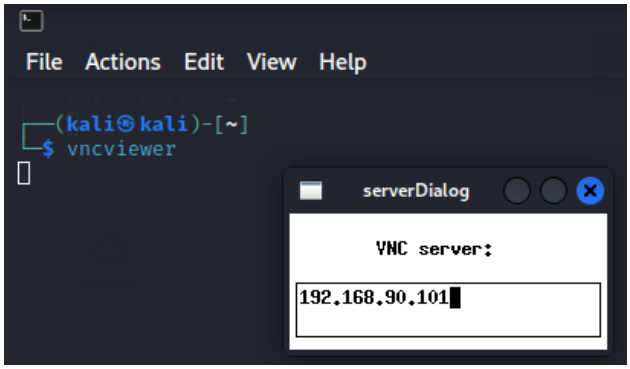
1. **61708 - VNC Server 'password' Password**
2. **51988 - Bind Shell Backdoor Detection**
3. **11356 - NFS Exported Share Information Disclosure**

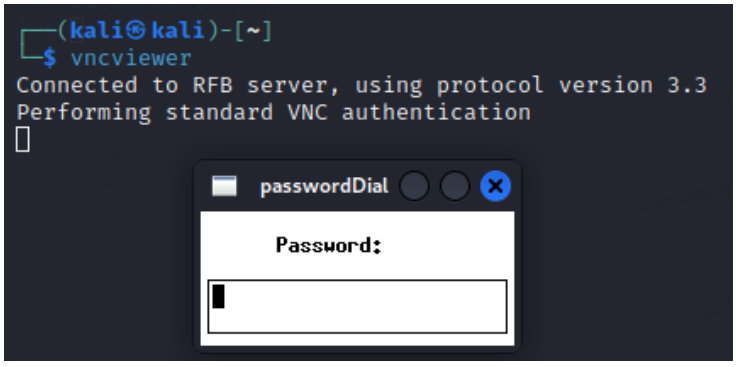
---

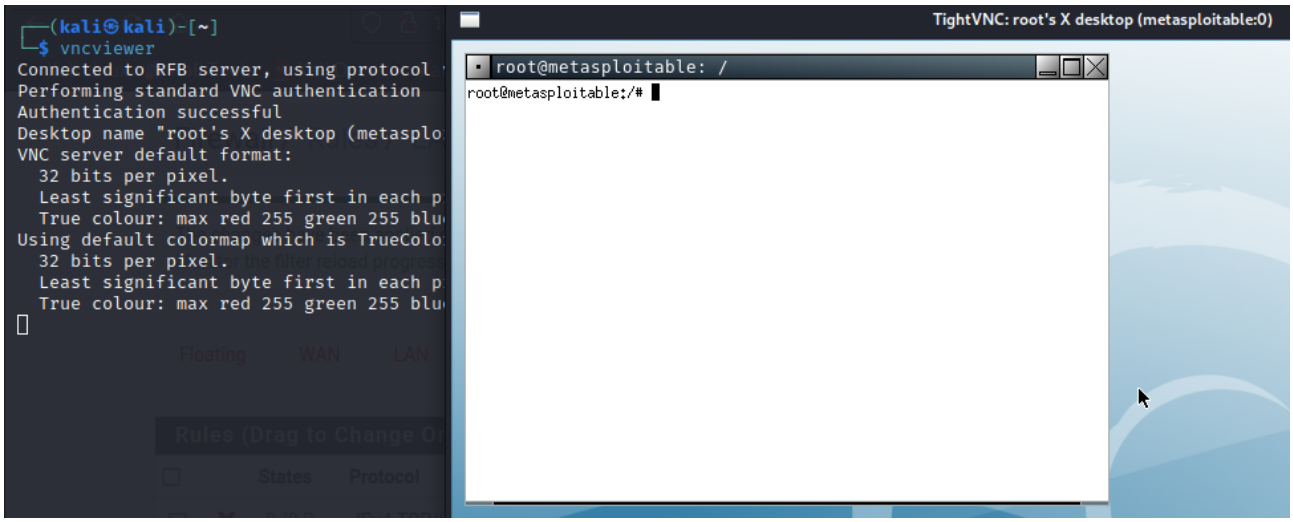
1. 61708 - VNC Server 'password' Password

Remediation action: modifica della password di accesso a VNC Server

La password da modificare è “password”. Utilizzando questa semplicissima chiave, allo stato attuale possiamo accedere molto facilmente tramite **vncviewer** all’host 192.168.90.101 ed avere controllo completo (privilegi di root) sulla macchina Metasploitable:







Andiamo dunque ad impostare una password sicura, che includa caratteri alfanumerici e caratteri speciali. Il limite massimo di caratteri consentiti per la chiave di accesso a VNC è di 8, quindi in questo caso ho scelto come chiave **Ak0/=1g-**

```
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#
```

Una volta apportata la modifica, la verifica di mancato accesso al servizio con la vecchia password ha esito positivo:

```
┌──(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

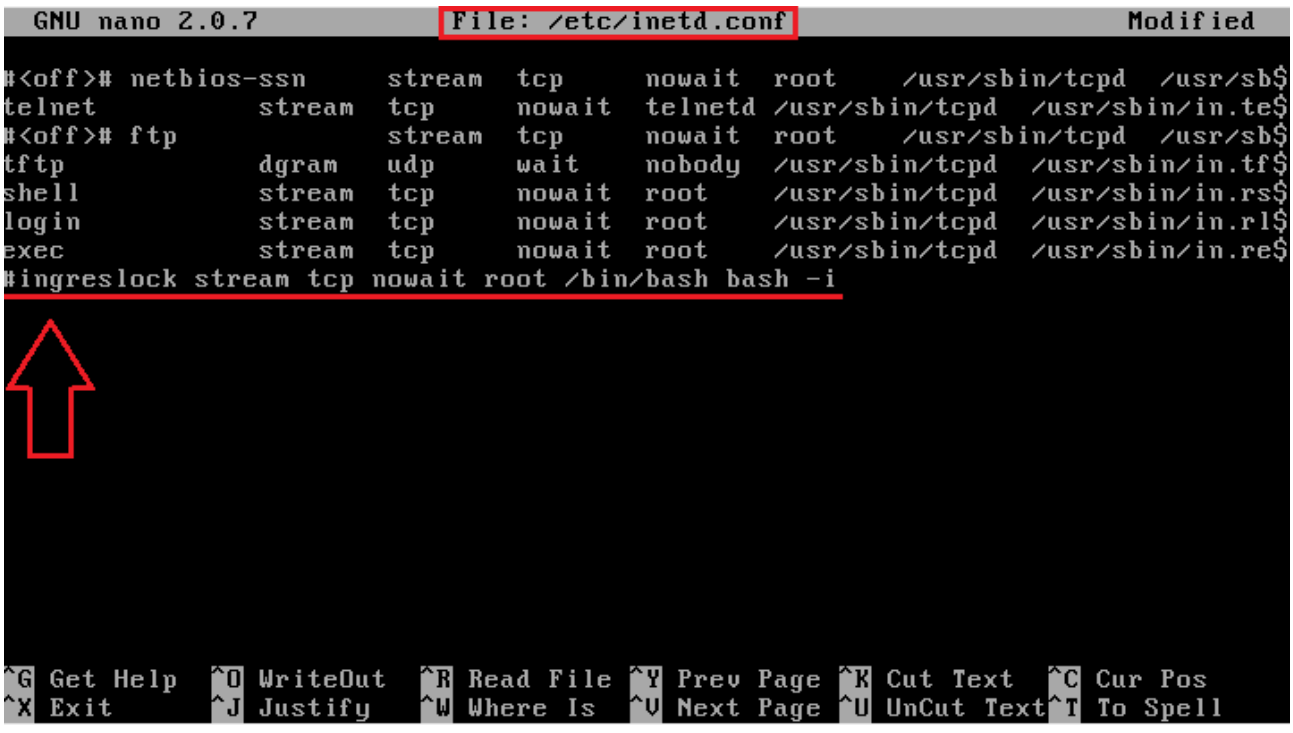
Come si può vedere nella figura sottostante, ho verificato tramite una scansione di tipo version detection di nmap lo stato della porta 1524 e il tipo di servizio in ascolto ad esso associato, ossia Metasploitable root shell.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.90.101 -p 1524
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 13:03 CET
Nmap scan report for 192.168.90.101
Host is up (0.0035s latency).

PORT     STATE SERVICE    VERSION
1524/tcp open  bindshell Metasploitable root shell

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.37 seconds
```

Ciò significa che, allo stato attuale, è possibile accedere facilmente e con privilegi di root all'host 192.168.90.101 tramite la porta 1524, utilizzando un servizio come netcat:

```
┌──(kali㉿kali)-[/]
└─$ netcat 192.168.90.101 1524
root@metasploitable:/#
```

Si rende dunque necessario disabilitare la shell in ascolto per bloccare eventuali future connessioni. Per far ciò, accediamo al file di configurazione dei servizi internet (**inetd.conf**) e disabilitiamo la backdoor commentando la riga **ingreslock stream tcp nowait root /bin/bash bash -i**



Successivamente, ho verificato la nuova impostazione ripetendo i test iniziali, entrambi con esito negativo: la porta 1524 risulta ora **chiusa** e non è più possibile stabilire una connessione con netcat.

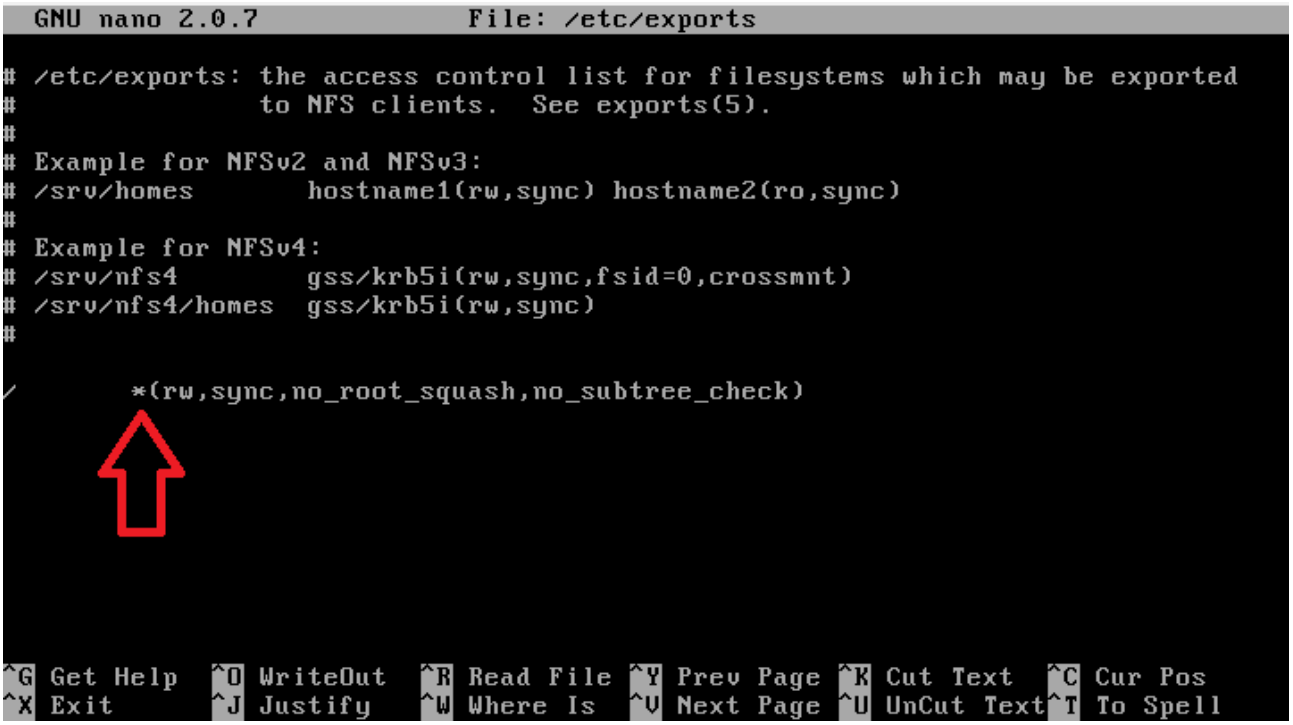
```
┌──(kali㉿kali)-[/]
└─$ nmap -sV 192.168.90.101 -p 1524
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 14:14 CET
Nmap scan report for 192.168.90.101
Host is up (0.0014s latency).

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
```

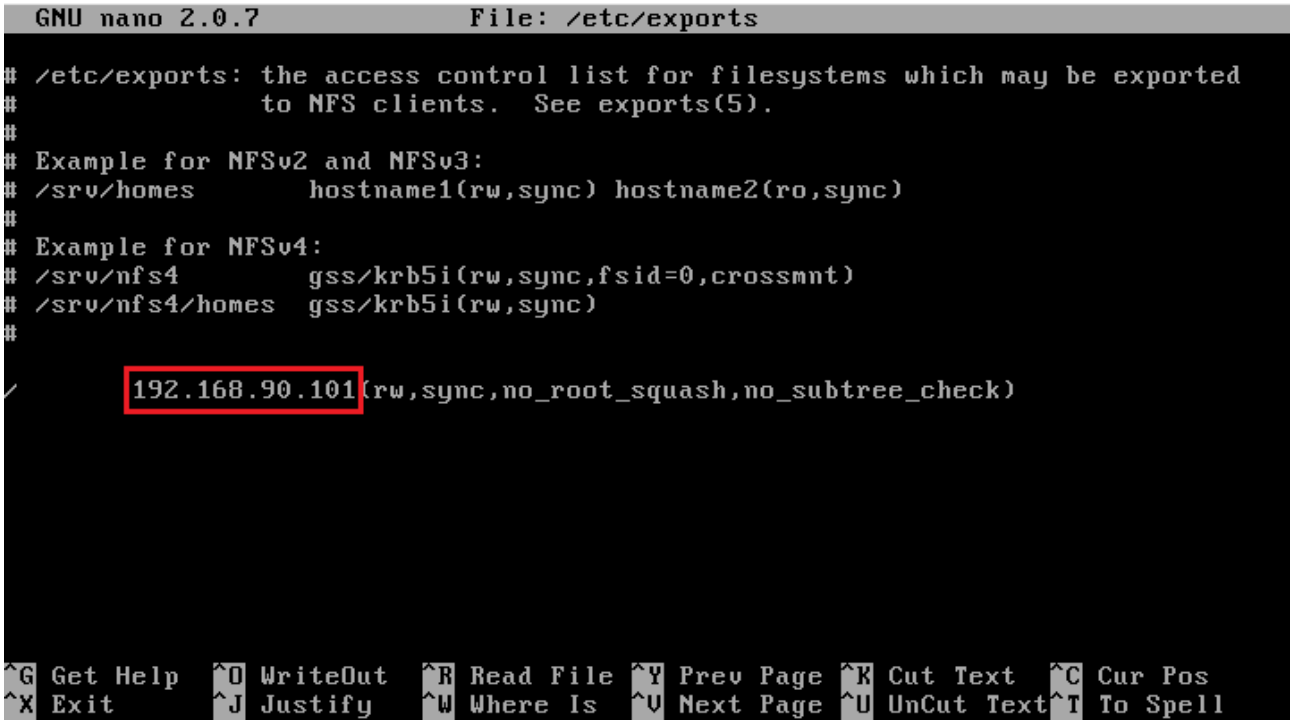
```
┌──(kali㉿kali)-[/]
└─$ netcat 192.168.90.101 1524
(UNKNOWN) [192.168.90.101] 1524 (ingreslock) : Connection refused
```

3. 11356 - NFS Exported Share Information Disclosure

Remediation action: impedire l'accesso e la condivisione di file con protocollo NFS ad utenti non autorizzati

Impediamo l'accesso al servizio NFS (*Network File System*) a utenti malintenzionati, accedendo con privilegi di root al file **exports** situato nella directory **/etc/** e sostituendo la wildcard presente all'ultima riga con l'indirizzo IP dell'host (192.168.90.101). In questo modo, la lettura, la modifica e la condivisione dei files sono bloccate per utenti esterni.




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)
#
/ 192.168.90.101(rw,sync,no_root_squash,no_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