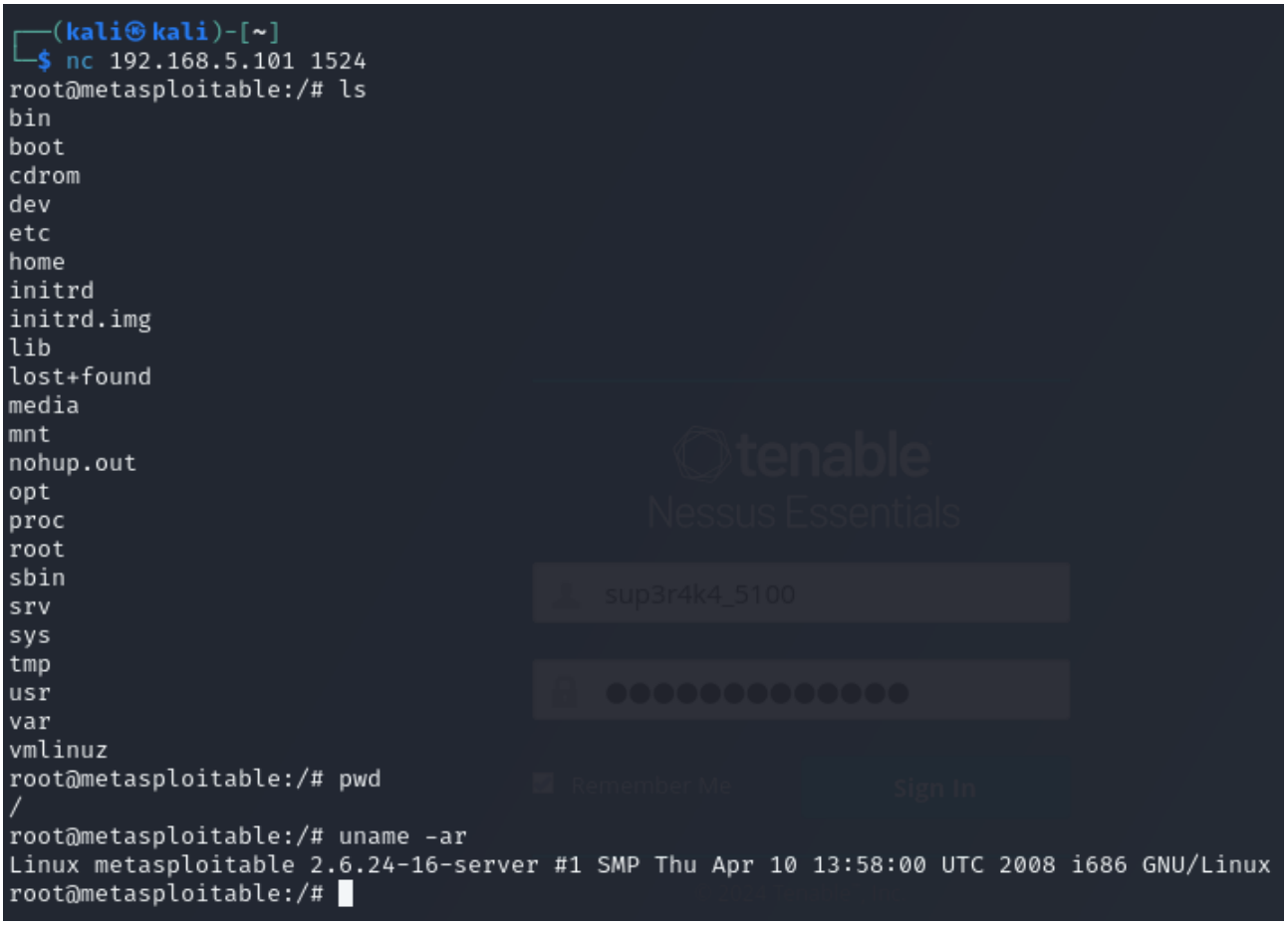
REPORT DI NESSUS: SCANSIONE METASPLOITABLE

Consegna U2-S5-L5

Esame di vulnerabilità critiche presenti sulla macchina Metasploitable e remediation actions per la loro risoluzione.

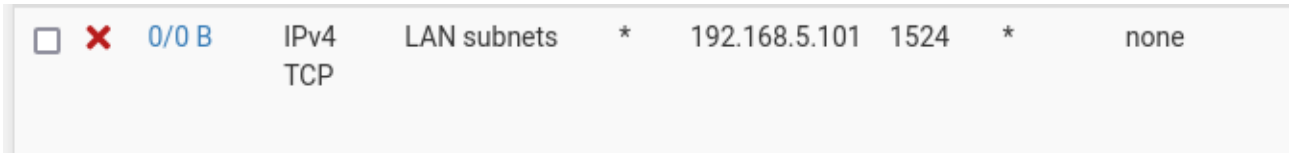
- **Bind Shell Backdoor Detection (Falla non più rilevata da Nessus)**
  È presente sulla macchina host una shell in ascolto sulla porta tcp/1524 senza alcun controllo dell'autenticazione. Qualsiasi malintenzionato potrebbe eseguire ogni genere di comando senza aver bisogno di autorizzazioni e di conseguenza compromettere l'intera macchina.

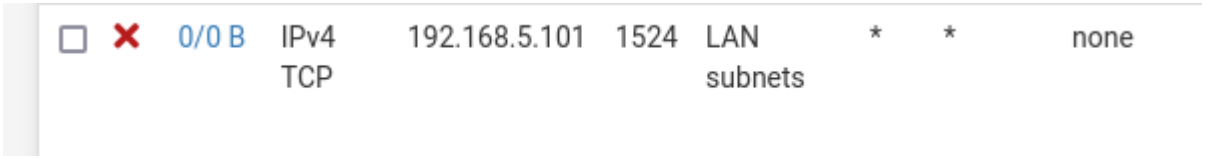


Dall'immagine si può vedere come ci si può facilmente connettere alla macchina Metasploitable utilizzando il tool di Kali "Netcat". Da notare i privilegi di root attivi (#).

Possibile soluzione alla falla:

- Si potrebbe impostare un paio di regole sul firewall per limitare e bloccare il traffico sulla porta 1524 della macchina Metasploitable.






```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.5.101 1524
(UNKNOWN) [192.168.5.101] 1524 (ingreslock) : Connection timed out
```

- Eventualmente si potrebbe disabilitare l'avvio del servizio in ascolto sulla porta tcp/1524 si Matasploitable. Usando il comando "lsof -i :1524" nella Metasploitable si può risalire al nome del servizio (xinetd) ed al PID del servizio in esecuzione. Col comando "sudo /etc/init.d/xinetd stop" si mette in pausa il servizio fino al prossimo riavvio. Provando dalla Kali con netcat (nc 192.168.5.101 1524) a connettersi alla porta 1524 il tentativo fallisce. Quindi editando con "sudo nano /etc/init.d/xinet" il file di configurazione, ed eliminando lo switch (--start) e riavviando la machina, ci si accorge che il servizio xinetd in ascolto sulla porta 1524 non è più attivo. La connessione con netcat da Kali fallisce.

```
msfadmin@metasploitable:~$ sudo lsof -i :1524
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd  4518 root   12u  IPv4  12096       TCP *:ingreslock (LISTEN)
msfadmin@metasploitable:~$ _
```

```
msfadmin@metasploitable:~$ sudo /etc/init.d/xinetd stop
 * Stopping internet superserver xinetd                              [ OK ]
```

```
case "$1" in
    start)
        checkportmap
        log_daemon_msg "Starting internet superserver" "$NAME"
        start-stop-daemon --start --quiet --background --exec "$DAEMON" -- \
            -pidfile "$PIDFILE" $XINETD_OPTS
        log_end_msg $?
        ;;
```

```
case "$1" in
    start)
        checkportmap
        log_daemon_msg "Starting internet superserver" "$NAME"
        start-stop-daemon --quiet --background --exec "$DAEMON" -- \
            -pidfile "$PIDFILE" $XINETD_OPTS
        log_end_msg $?
        ;;
```

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.5.101 1524
(UNKNOWN) [192.168.5.101] 1524 (ingreslock) : Connection refused
```

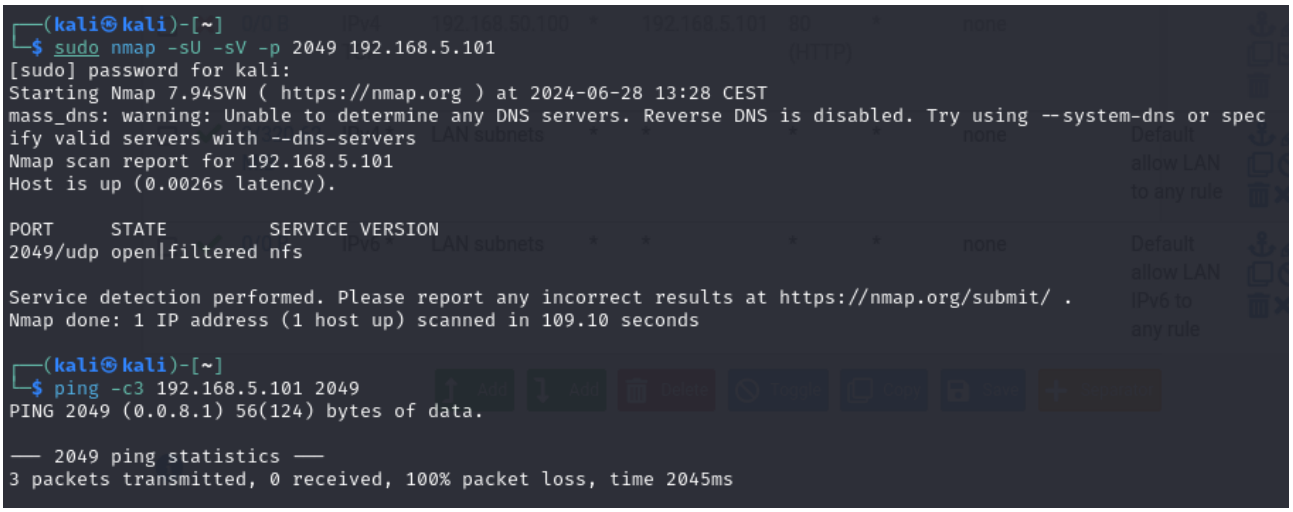
- **NFS Exported Share Information Disclosure**
  La falla permette l'accesso ai file sul server condivisi tramite NFS.
  L'NFS (Network File System) è un file system che consente a computer client di utilizzare la rete per accedere a directory condivise da server remoti come fossero disponibili in locale. Un attaccante potrebbe leggere e probabilmente anche modificare dei file presenti sulla macchina. Il servizio è attivo sulla porta udp/2049.

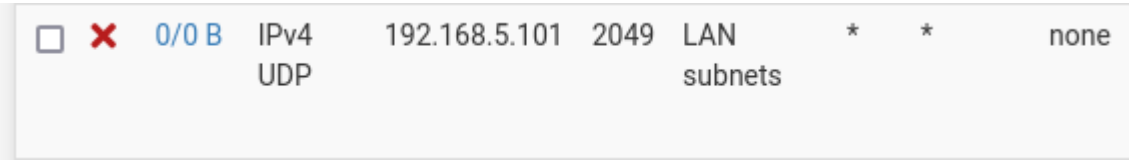
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 2049 192.168.5.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 13:20 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or spec
ify valid servers with --dns-servers
Nmap scan report for 192.168.5.101
Host is up (0.0041s latency).

PORT     STATE SERVICE VERSION
2049/tcp open  nfs     2-4 (RPC #100003)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.34 seconds
```

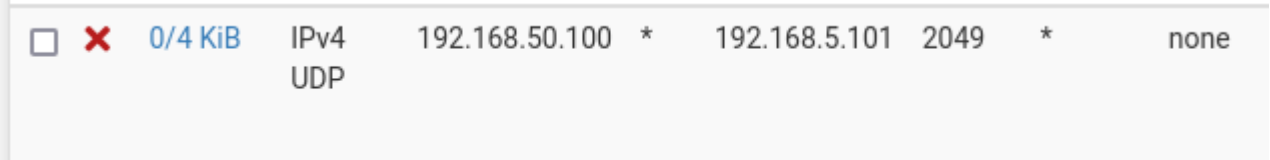
Scansione tramite nmap sulla porta udp/2049 all'IP della Metasploitable.

Possibile soluzione alla falla:

- Si può optare per creare una regola di firewall che blocchi il traffico da e verso la porta udp/2049 all'IP della Metasploitable. Effettuando la scansione con "sudo nmap -sU -sV -p 2049 192.168.5.101" dal terminale della Kali la porta adesso risulta filtrata e non si ottiene risposta neanche eseguendo il comando "ping". Lo switch "-sU" effettua una connessione col protocollo UDP, mentre "-sV" ci serve per verificare i servizi attivi sulla suddetta porta.







- (BONUS) si potrebbe optare per l'installazione e configurazione di Kerberos per NFS.

  https://www.baeldung.com/linux/nfs-security-over-internet

- Il punto 3.1. Installare e configurare Kerberos per NFS

Per abilitare NFSv4 con Kerberos sul nostro server NFS, **iniziamo installando e configurando il pacchetto Kerberos** *krb5-user* **con** *apt*:

```
$ sudo apt install krb5-user
```

Dopo l'installazione di Kerberos, utilizziamo l'utilità *kadmin* per creare una chiave per il server NFS con un amministratore principale:

```
$ sudo kadmin -p baeldung/admin -q "addprinc -randkey nfs/j-nfs-server.vms"
```

L'utility *kadmin* fornisce il controllo sul database Kerberos. Qui, **usiamo *kadmin* per creare voci *di keytab* per il server e il client NFS**. Un *keytab* è un file che contiene coppie di principi Kerberos e le relative chiavi di crittografia, che autenticheranno il server e il client NFS durante la struttura di connessione.

In questo esempio, ***baeldung* e *admin* rappresentano il nome principale di Kerberos e i privilegi associati**. Un principio è un'identità unica all'interno di un regno di Kerberos, che rappresenta un utente, un servizio o un host. Possiamo sostituirlo con il nostro principio preferito e il suo privilegio associato.

Per capire meglio questo, esaminiamo le opzioni nel comando *kadmin*:

- *-p* = specifica il nome principale da utilizzare per le operazioni amministrative
- *-q* = esegue un singolo comando (*addprinc -randkey nfs/j-nfs-servervms*) e poi esce dall'utility *kadmin*
- *addprinc* = aggiunge un principio al database Kerberos
- *-randkey* = genera una chiave casuale per il principale
- *nfs/j-nfs-servervms* = *nfs* rappresenta il servizio o l'host per il quale stiamo creando il principale, e *j-nfs-servervms* è il nome specifico del server o dell'host NFS

In breve, il comando sopra genera una chiave casuale per il principio *nfs/j-nfs-servervms*. Quindi, estraiamo la chiave creata nel *keytab locale*:

```
$ sudo kadmin -p baeldung/admin -q "ktadd nfs/j-nfs-server.vms"
Authenticating as principal baeldung/admin with password.
Password for baeldung/admin@VMS:
Entry for principal nfs/j-nfs-server.vms with kvno 2, encryption type aes256-cts-hmac-sha1-96 added to keytab
FILE:/etc/krb5.keytab.
Entry for principal nfs/j-nfs-server.vms with kvno 2, encryption type aes128-cts-hmac-sha1-96 added to keytab
FILE:/etc/krb5.keytab.
```

Simile alla nostra precedente interazione, ***ktadd nfs/j-nfs-servervms* istruisce *kadmin* ad aggiungere una voce *di keytab* per il principio *nfs/j-nfs-servervms***. Quindi, autentica il principale ed estrae la chiave. Come possiamo vedere, la voce *keytab* include tipi di crittografia come *aes256-cts-hmac-sha1-96* e *aes128-cts-hmac-sha1-96*, fornendo un'autenticazione sicura per l'accesso alle condivisioni NFS.

3, punto del file Verificare la configurazione di Kerberos per NFS

Dopo aver creato la voce *keytab* per il server NFS, possiamo utilizzare il comando *klist* per verificarne l'estrazione di successo nel *keytab* locale. Il flag *-k* visualizza il contenuto del file *keytab* e le relative informazioni associate:

```
$ sudo klist -k
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------------
   2 nfs/j-nfs-server.vms@VMS
   2 nfs/j-nfs-server.vms@VMS
```

Il nostro output mostra il nome *chiave* e le voci principali con i numeri di versione chiave associati (*KVNO*). Queste informazioni confermano che la chiave è stata estratta con successo nel file *keytab*.

3.3. Installare e configurare il server NFS con Kerberos

Ora, procediamo a installare il nostro pacchetto server NFS *nfs-kernel-server*:

```
$ sudo apt install nfs-kernel-server
```

Una volta terminata l'installazione, i servizi NFS relativi a Kerberos si avvieranno automaticamente a causa della presenza di *file /etc/krb5.keytab*.

Quindi popoliamo le *esportazioni /etc/export* per limitare le esportazioni all'autenticazione Kerberos. Ad esempio, possiamo esportare */storage* usando *krb5p*:

```
/storage *(rw,sync,no_subtree_check,sec:krb5p)
```

Questo popola ed esporta */storage* utilizzando *krb5p* per limitare l'accesso all'esportazione al processo di autenticazione Kerberos.

Infine, **utilizziamo il comando *exportfs* per aggiornare le esportazioni per garantire che il server NFS sia a conoscenza della configurazione aggiornata:**

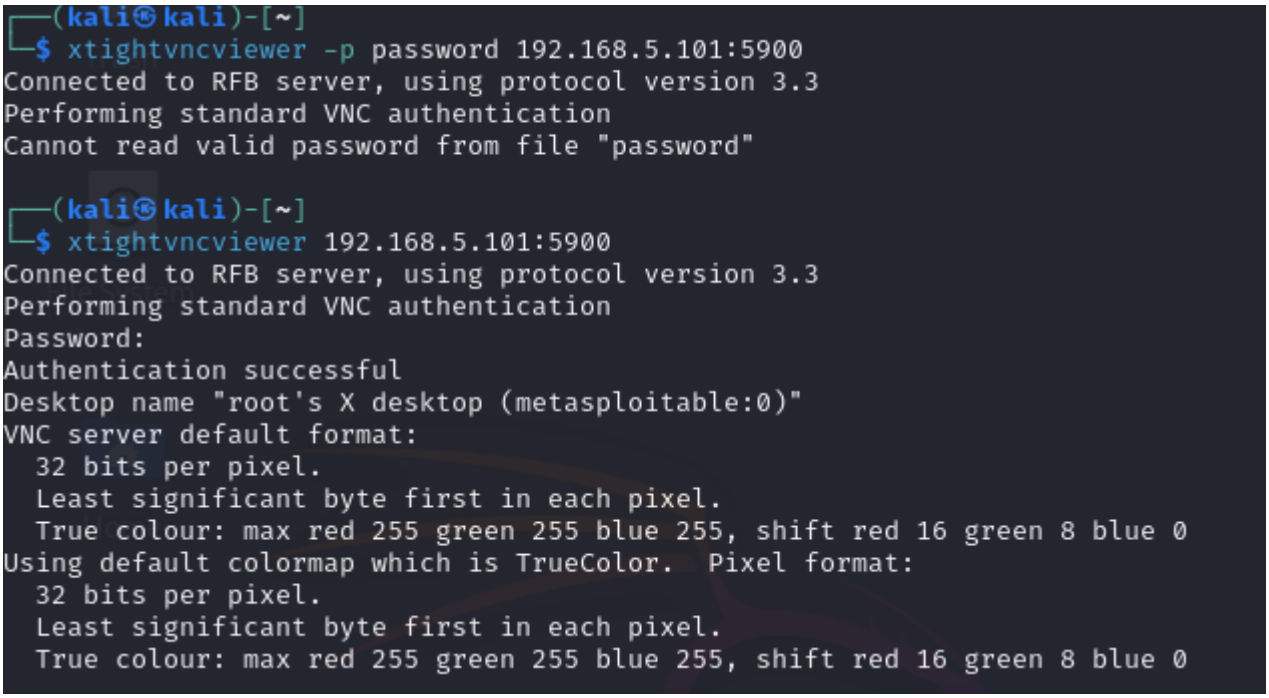
```
$ sudo exportfs -rav
exporting *:/storage
```

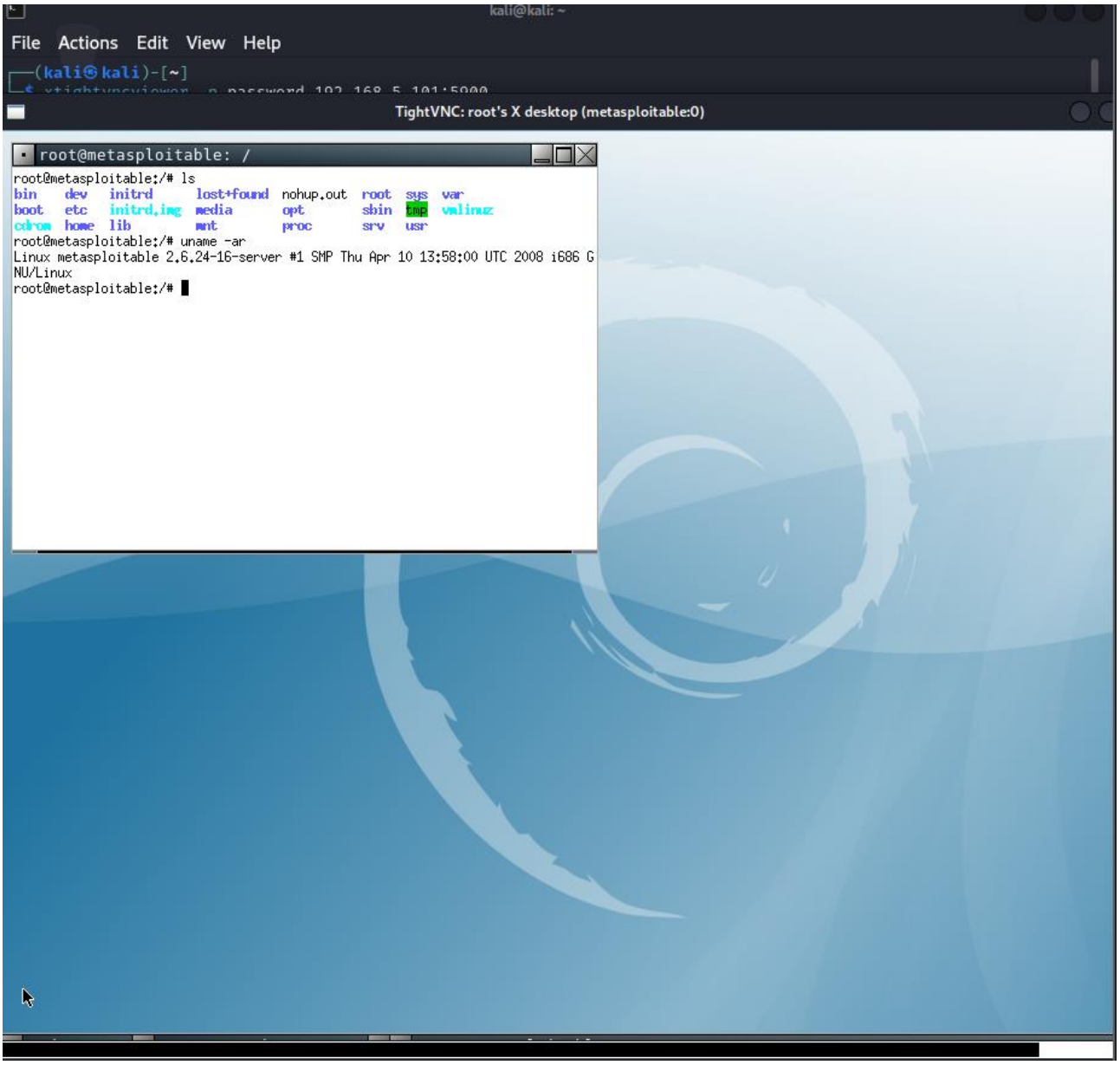
Qui, l'opzione *-r* aggiorna la tabella delle esportazioni, *-a* garantisce che tutte le voci in */etc/exports* vengano elaborate, mentre *-v* consente un output verboso, fornendo ulteriori dettagli di esportazione.

Ogni volta che modifichiamo il file */etc/exports* per aggiornare le directory condivise o le loro configurazioni, dobbiamo aggiornare le esportazioni affinché le modifiche abbiano effetto. Ciò garantisce che il server NFS sia a conoscenza delle esportazioni aggiornate e le metta a disposizione dei clienti.

È importante configurare attentamente il file */etc/exports* e comprendere le implicazioni delle modifiche prima di aggiornare le esportazioni, poiché **configurazioni errate possono portare a problemi di accesso o vulnerabilità di sicurezza**.

- **VNC Server 'password' Password (Falla non più rilevata da Nessus)**
  È presente un server VNC su porta tcp/5900 protetto da una password troppo debole. Un attaccante potrebbe avere acceso remoto alla macchina facilmente.





Possibile soluzione alla falla:
Al posto di ‘password’ usare una password molto lunga e con tipi di carattere differenti.

```
msfadmin@metasploitable:~$ sudo su
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# exit
msfadmin@metasploitable:~$
```

```
┌──(kali㉿kali)-[~]
└─$ xtightvncviewer 192.168.5.101:5900
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure
```

- **UnrealIRCd Backdoor Detection**
  Il server remoto IRC contiene una backdoor che permette ad un attaccante di eseguire del codice malevolo sulla macchina Metasploitable in modo arbitrario.
  Il server è in ascolto sulla porta tcp/6667.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.5.101 6667
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 17:49 CEST
Nmap scan report for 192.168.5.101
Host is up (0.012s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open     smtp        Postfix smtpd
53/tcp   open     domain      ISC BIND 9.4.2
80/tcp   open     http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open     rpcbind     2 (RPC #100000)
139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1099/tcp open     java-rmi    GNU Classpath grmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs         2-4 (RPC #100003)
2121/tcp open     ftp         ProFTPD 1.3.1
3306/tcp open     mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open     postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc         VNC (protocol 3.3)
6000/tcp open     X11         (access denied)
6667/tcp open     irc         UnrealIRCd
8009/tcp open     ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Linux, Unix; CPE: cpe:/o:linux:li
nux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (1 host up) scanned in 20.71 seconds
```

Possibile soluzione alla falla:

tenendo conto del fatto che sia impossibile aggiornare il pacchetto sul sistema, si può creare una regola su PFSense per arginare il rischio di intrusione.

☐	✗	0/0 B	IPv4 TCP	192.168.5.101	6667	LAN subnets	*	*	none

☐	✖	0/600 B	IPv4 TCP	LAN subnets	*	192.168.5.101	6667	*	none

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.5.101 6667
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 17:54 CEST
Nmap scan report for 192.168.5.101
Host is up (0.043s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open     smtp        Postfix smtpd
53/tcp   open     domain      ISC BIND 9.4.2
80/tcp   open     http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open     rpcbind     2 (RPC #100000)
139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1099/tcp open     java-rmi    GNU Classpath grmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs         2-4 (RPC #100003)
2121/tcp open     ftp         ProFTPD 1.3.1
3306/tcp open     mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open     postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc         VNC (protocol 3.3)
6000/tcp open     X11         (access denied)
6667/tcp filtered irc
8009/tcp open     ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host:  metasploitable.localdomain; OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (1 host up) scanned in 20.68 seconds
```