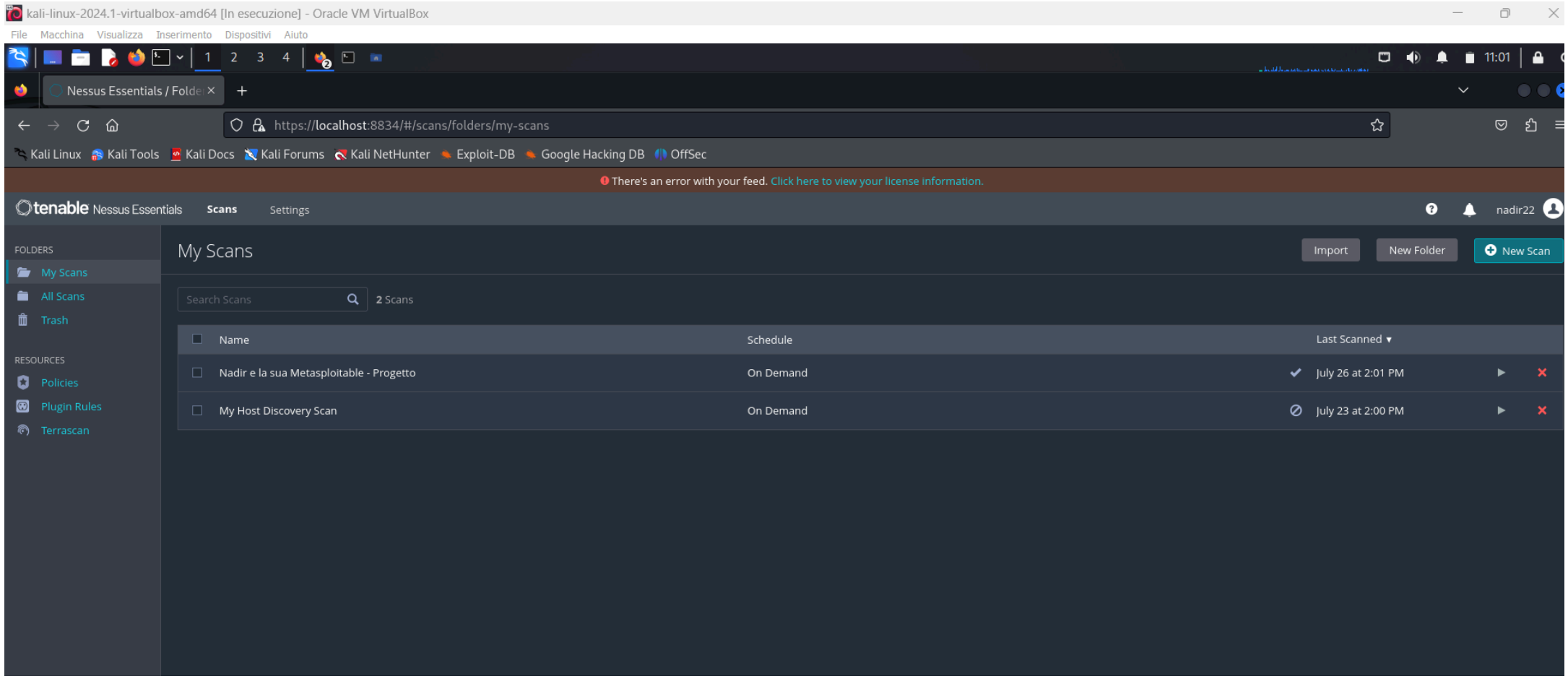



# ESEGUIAMO LA SCANSIONE…

Nadir e la sua Metasploitable - Progetto

‹ Back to My Scans

Configure | Audit Trail | Launch ▾ | Report | Export

**Hosts** 1 | Vulnerabilities 70 | Remediations 7 | History 2

Filter ▾ | Search Hosts | 1 Host

| Host | Vulnerabilities ▾ |
|---|---|
| 192.168.50.101 | 56 / 6 / 22 / 8 / 125 |

**Scan Details**

| | |
|---|---|
| Policy: | Basic Network Scan |
| Status: | Completed |
| Severity Base: | CVSS v3.0 |
| Scanner: | Local Scanner |
| Start: | July 26 at 1:38 PM |
| End: | July 26 at 2:01 PM |
| Elapsed: | 23 minutes |

**Vulnerabilities**

- Critical
- High
- Medium
- Low
- Info

# Remediation 1 - Backdoor con Bindshell alla porta 1524

BIND SHELL BACKDOOR (come segnala lo screenshot in basso, alla porta 1524 c'è una shell)

Nadir e la sua Metasploitable - Progetto / Plugin #51988

Configure | Audit Trail | Launch | Report | Export

Back to Vulnerabilities

Hosts 1 | Vulnerabilities 70 | Remediations 7 | History 2

CRITICAL Bind Shell Backdoor Detection

**Description**

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

**Solution**

Verify if the remote host has been compromised, and reinstall the system if necessary.

**Output**

```
Nessus was able to execute the command "id" using the
following request :


This produced the following truncated output (limited to 10 lines) :
----------------------------- snip -----------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

----------------------------- snip -----------------------------
```

To see debug logs, please visit individual host

| Port ▲ | Hosts |
|---|---|
| 1524 / tcp / wild_shell | 192.168.50.101 |

**Plugin Details**

| | |
|---|---|
| Severity: | Critical |
| ID: | 51988 |
| Version: | 1.10 |
| Type: | remote |
| Family: | Backdoors |
| Published: | February 15, 2011 |
| Modified: | April 11, 2022 |

**Risk Information**

Risk Factor: Critical

**CVSS v3.0 Base Score 9.8**

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Infatti ho provato a connettermici da KALI con NETCAT e utilizzarla

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

1 2 3 4

kali@kali: ~

File Actions Edit View Help

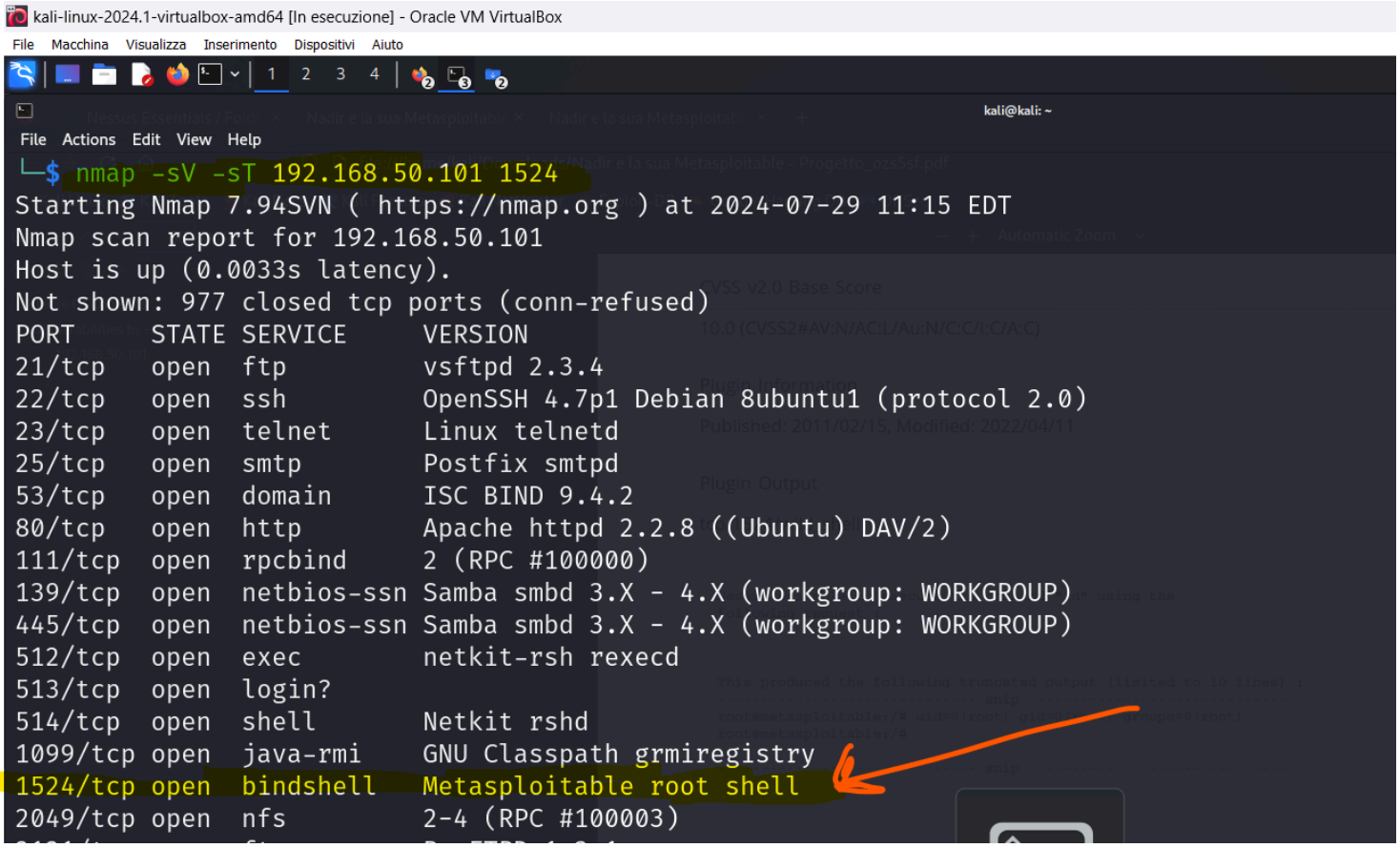
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.101 1524
root@metasploitable:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:72:ce:37
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe72:ce37/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:202 errors:0 dropped:0 overruns:0 frame:0
          TX packets:90 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12954 (12.6 KB)  TX bytes:8999 (8.7 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:151 errors:0 dropped:0 overruns:0 frame:0
          TX packets:151 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:41767 (40.7 KB)  TX bytes:41767 (40.7 KB)

root@metasploitable:/#
```

Il TOOL dice di verificare se la macchina è stata compromessa e di reinstallarla da capo eventualmente. Noi sappiamo che Metasploitable è compromessa di sua natura, quindi ci limiteremo a cancellare la backdoor

Facendo una ricerca -sV su nmap ho identificato il servizio bindshell e lo debbo killare dalla macchina metasploitable




Con netstat chiedo il PID del servizio che va su quella porta e faccio il KILL

netstat -tulpn | grep :1524

```
msfadmin@metasploitable:~$ sudo netstat -tulpn | grep :1524
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
4501/xinetd
msfadmin@metasploitable:~$ kill 4501
-bash: kill: (4501) - Operation not permitted
msfadmin@metasploitable:~$ sudo kill 4501
msfadmin@metasploitable:~$
```

Riprovo la connessione con NETCAT

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

1 2 3 4

kali@kali: ~

File Actions Edit View Help

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.101 1524
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection refused
```

# Remediation 2 - Server VNC per controllo remoto con password ‘password’ alla porta 5900

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.101 -p 5900
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-30 09:38 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).

PORT     STATE SERVICE
5900/tcp open  vnc

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

┌──(kali㉿kali)-[~]
└─$
```

```
msfadmin@metasploitable:~$ kill 4501
-bash: kill: (4501) - Operation not permitted
msfadmin@metasploitable:~$ sudo kill 4501
msfadmin@metasploitable:~$ kill 4501
-bash: kill: (4501) - No such process
msfadmin@metasploitable:~$ netstat -tulnp | grep 5900
(No info could be read for "-p": geteuid()=1000 but you should be root.)
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN
-
msfadmin@metasploitable:~$ sudo netstat -tulpn | grep 5900
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN
4656/Xtightvnc
msfadmin@metasploitable:~$
```

Qui il PID è 4656

Secondo le mie ricerche il comando da Meta per cambiare la password di Vnc è vncpasswd

```
Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Mon Jul 29 12:14:26 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ 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:~$
```

INSERISCO: EpicodeNadir44 COME PASSWORD

Riavvio Xtightvnc

```
msfadmin@metasploitable:~$ kill tightvncserver
-bash: kill: tightvncserver: arguments must be process or job IDs
msfadmin@metasploitable:~$ sudo netstat -tulpn | grep tightvncserver
msfadmin@metasploitable:~$ sudo service xinetd restart
sudo: service: command not found
msfadmin@metasploitable:~$ sudo kill Xtightvnc
ERROR: garbage process ID "Xtightvnc".
Usage:
  kill pid ...              Send SIGTERM to every process listed.
  kill signal pid ...       Send a signal to every process listed.
  kill -s signal pid ...    Send a signal to every process listed.
  kill -l                   List all signal names.
  kill -L                   List all signal names in a nice table.
  kill -l signal            Convert between signal numbers and names.
msfadmin@metasploitable:~$ sudo killall Xtightvnc
msfadmin@metasploitable:~$ sudo killall tightvncserver
tightvncserver: no process killed
msfadmin@metasploitable:~$ tightvncserver :1

New 'X' desktop is metasploitable:1

Starting applications specified in /home/msfadmin/.vnc/xstartup
Log file is /home/msfadmin/.vnc/metasploitable:1.log

msfadmin@metasploitable:~$
```

Riavvio la scansione e fra le Critiche non compaiono più le mie 2 vulnerabilità

BASICAuno / 192.168.50.101

‹ Back to Hosts

**Vulnerabilities** 39

Filter ▾ Search Vulnerabilities 🔍 **39** Vulnerabilities

| Sev ▾ | CVSS ▾ | VPR ▾ | Name ▲ | Family ▲ | Count ▾ |
|---|---|---|---|---|---|
| CRITICAL | 10.0 | | Apache Log4Shell RCE detection via callback correlation (Direct Check RPCBIND) | RPC | 10 |
| CRITICAL | 10.0 | | Apache Log4Shell RCE detection via callback correlation (Direct Check SMB) | Gain a shell remotely | 2 |
| CRITICAL | 10.0 | | Apache Log4Shell RCE detection via callback correlation (Direct Check DNS) | DNS | 1 |
| CRITICAL | 10.0 * | | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness | Gain a shell remotely | 1 |
| CRITICAL | 10.0 * | | NFS Exported Share Information Disclosure | RPC | 1 |
| CRITICAL | 10.0 | | SIP Script Remote Command Execution via log4shell | General | 1 |
| CRITICAL | ... | ... | 4 Apache Log4j (Multiple Issues) | Misc. | 6 |
| HIGH | 7.5 | | Samba Badlock Vulnerability | General | 1 |

# Remediation 3 - NFS disclosure

Il file manager NFS può essere modificato da utenti esterni con il comando ‘mount’ senza problemi, dobbiamo impedirlo.

Dalle ricerche effettuate, in metasploitable il file /etc/exports è quello che contiene le regole di condivsione, quindi lo dobbiamo modificare con nano

PRIMA lo visualizzo con ‘cat’

```
29/07/24 16:07:16 Copyright (C) 1999 AT&T Laboratories Cambridge.
29/07/24 16:07:16 Copyright (C) 2000-2002 Constantin Kaplinsky.
29/07/24 16:07:16 All Rights Reserved.
29/07/24 16:07:16 See http://www.uk.research.att.com/vnc for information on VNC
29/07/24 16:07:16 See http://www.tightvnc.com for TightVNC-specific information
29/07/24 16:07:16 Desktop name 'x11' (:0)
29/07/24 16:07:16 Protocol version supported 3.3
29/07/24 16:07:16 Listening for VNC connections on TCP port 5900

Fatal server error:
Couldn't add screen
msfadmin@metasploitable:~$ cat /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)
#

/       *(rw,sync,no_root_squash,no_subtree_check)
msfadmin@metasploitable:~$ _
```

Come vediamo l’ultima riga dà il permesso a * tutti di leggere sincronizzare…. In più il permesso è impostato su “/” quindi la cartella base. Quindi dobbiamo fare in modo che sia consentito solo a qualcuno, nello specifico decidiamo che sia l’host metasploitable, quindi 192.168.50.101

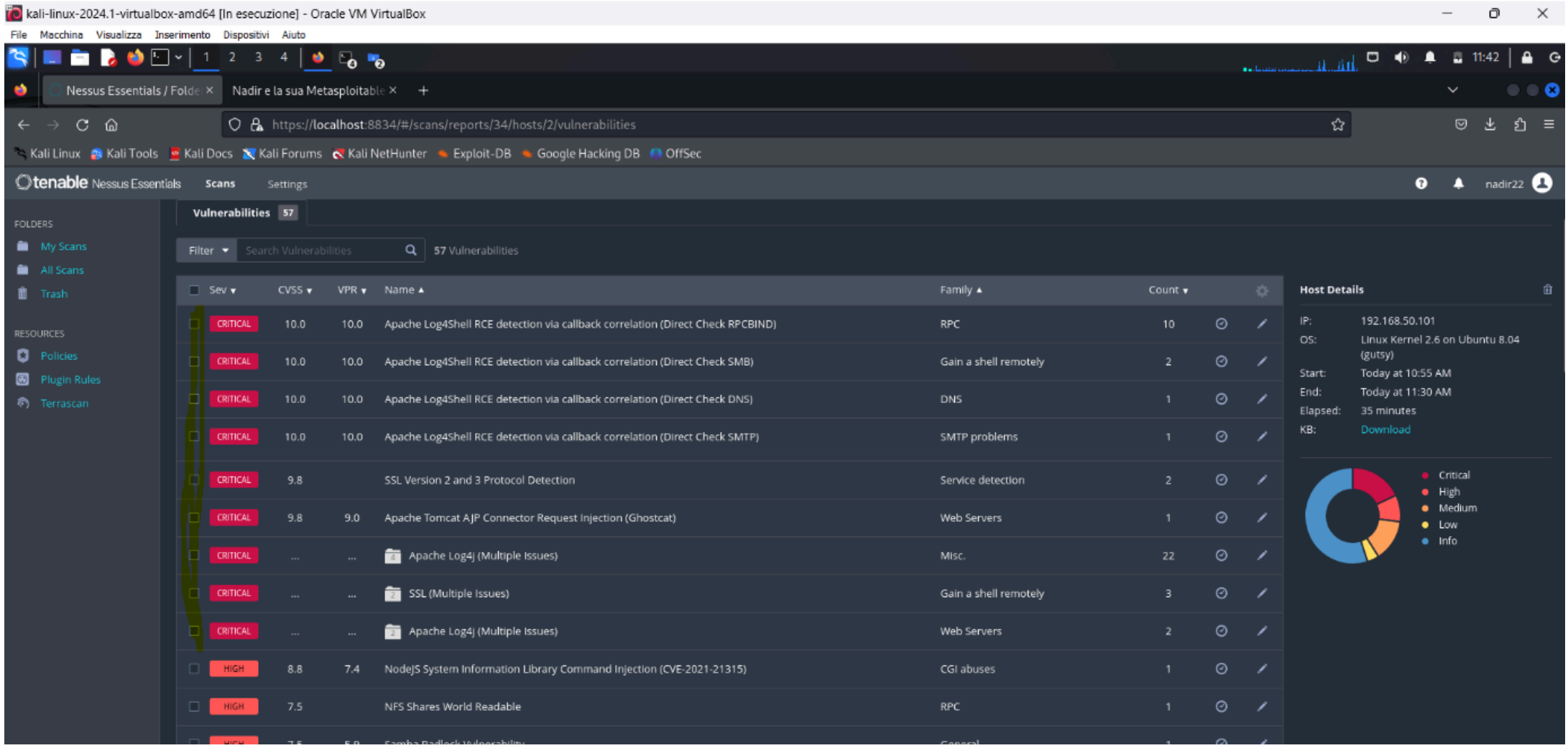
```
msfadmin@metasploitable:~$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#

/       192.168.50.101(rw,sync,no_root_squash,no_subtree_check)

msfadmin@metasploitable:~$ showmount -e 192.168.50.104
msfadmin@metasploitable:~$ showmount -e 192.168.50.101
Export list for 192.168.50.101:
/ *
msfadmin@metasploitable:~$
```

Ecco, modificata la riga con 192.168.50.101

Infine devo riprovare a fare la scansione delle vulnerabilità per vedere se è tutto a posto




LE vulnerabilità non compaiono più