

# Remediation Action Meta

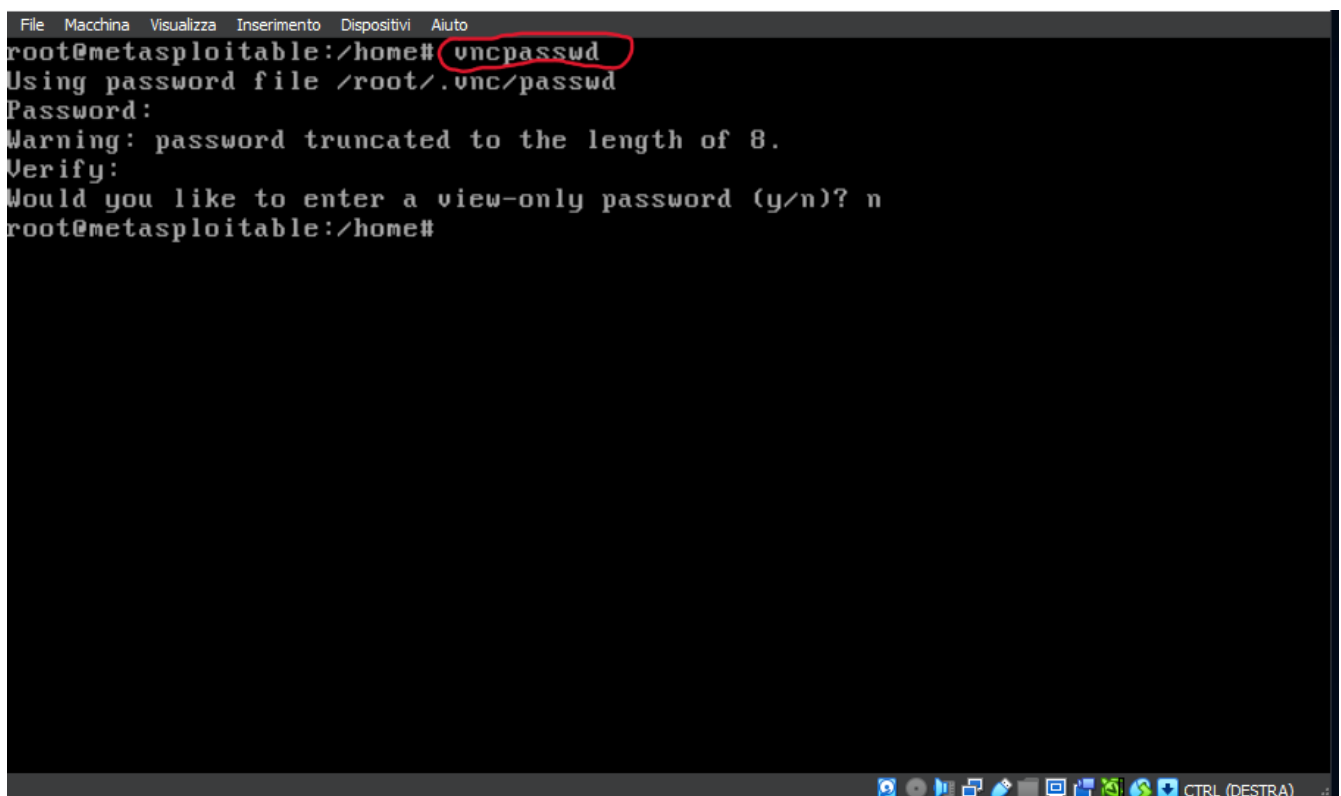
## Vulnerabilità

- 1 VNC server password
- 2 NSF exported Share Information Disclosure
- 3 BInd Shell Backdoor Detection (porta 1524)
- 4 Debian OpenSSL Package Random Number Generator Weakness

1VNC (Virtual Network Computing) Il VNC ha lo scopo di controllare un pc da remoto e di conseguenza visualizzare tutti i dati presenti su di esso.

Per aggirare tale vulnerabilità bisogna cambiare la password (password), in una decisamente più complessa composta da caratteri speciali/lettere/numeri ecc..

Per implementare quest'ultima bisogna eseguire il comando "sudo su" per poi eseguire un'ulteriore comando "vncpasswd" e in seguito inserire la nuova (password) "#51FCURrBpXuw"



```
File Macchina Visualizza Inserimento Dispositivi Aiuto
root@metasploitable:/home# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home#
```

## 2 NFS (porta 2049)

NFS è un protocollo che consente di accedere e condividere file di varia entità, difatti se le informazioni/file/directory non sono adeguatamente protette, sarebbero vulnerabili ad attacchi hacker di vario genere che potrebbero rubare dati sensibili quali nomi/indirizzi, dati aziendali ecc..

Tale vulnerabilità si risolve (agira) dando i permessi di root al file /etc/exports e aggiungendo il commento # come da foto

```
GNU nano 2.0.7      File: /etc/exports      Modified
# /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          192.168.50.0/24(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes    192.168.50.0/24(rw,sync)
#
#/*(rw,sync,no_root_squash,no_subtree_check)
```

GNU nano 2.0.7 File: /etc/exports Modified

^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

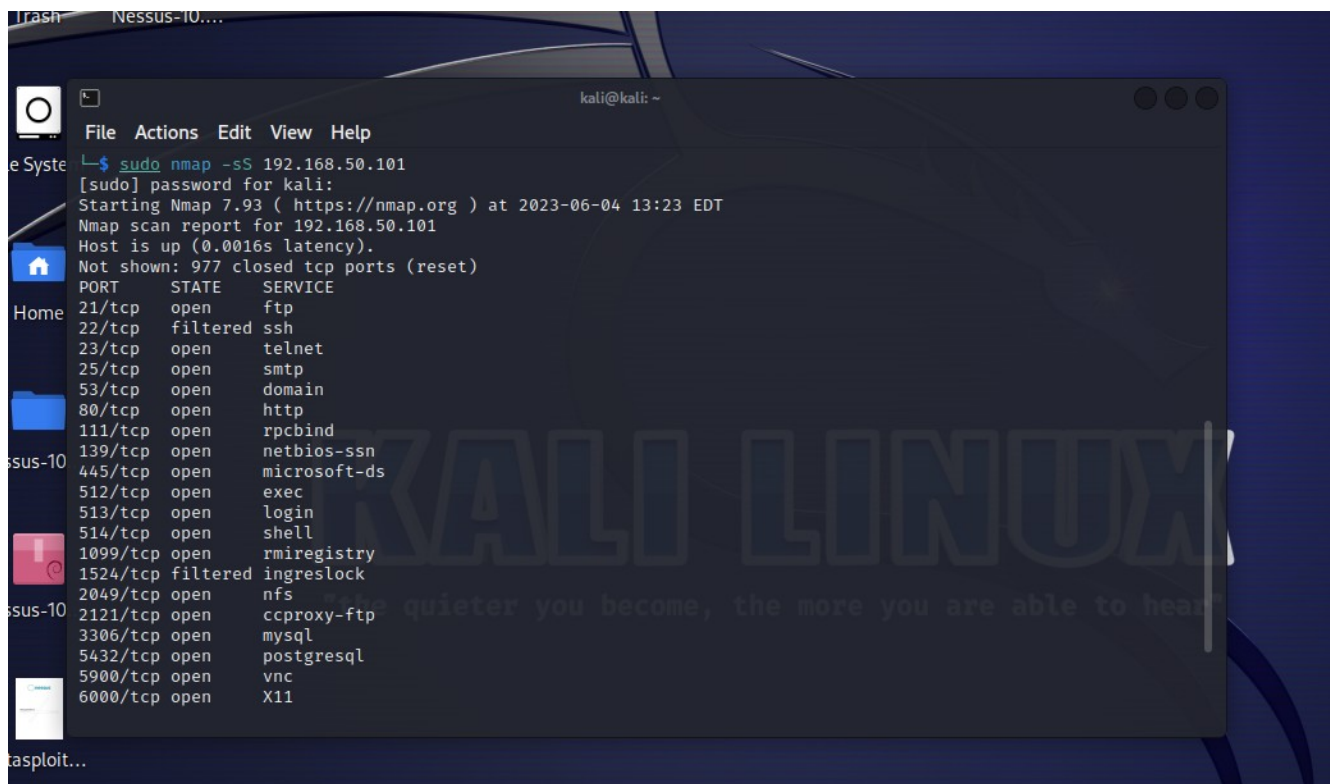
### 3 Bind Shell Backdoor Detection (porta 1524)

Backdoor di tipo bind shell. Quest'ultima è un tipo di attacco informatico che aggira i sistemi di protezione, che consente di accedere ad un qualunque dispositivo che può essere un pc, un cellulare ecc...

La soluzione a questa vulnerabilità è stata aggiungere una linea di comando quale:

`""iptables -I INPUT -p tcp -s 192.168.50.101 -dport 1524 -j DROP""` così facendo blocchiamo il traffico sulla porta 1524.

```
--source      -s [!] address[/mask]
               source specification
--destination -d [!] address[/mask]
               destination specification
--in-interface -i [!] input name[+]
               network interface name ([+] for wildcard)
--jump        -j target
               target for rule (may load target extension)
--goto        -g chain
               jump to chain with no return
--match       -m match
               extended match (may load extension)
--numeric     -n
               numeric output of addresses and ports
--out-interface -o [!] output name[+]
               network interface name ([+] for wildcard)
--table       -t table
               table to manipulate (default: 'filter')
--verbose     -v
               verbose mode
--line-numbers
               print line numbers when listing
--exact       -x
               expand numbers (display exact values)
[!] --fragment -f
               match second or further fragments only
--modprobe=<command>
               try to insert modules using this command
--set-counters PKTS BYTES
               set the counter during insert/append
[!] --version  -V
               print package version.
root@metasploitable:/home/msfadmin# iptables -I INPUT -p tcp -s 192.168.50.101 -dport 1524 -j DROP
```



The screenshot shows a Kali Linux desktop with a dark theme. A terminal window is open, displaying the results of an Nmap scan. The terminal title is 'kali@kali: ~'. The command executed is 'sudo nmap -sS 192.168.50.101'. The output shows the scan was successful, identifying several open ports and their corresponding services. A large 'KALI LINUX' watermark is visible in the background of the terminal window.

```
File Actions Edit View Help
└─$ sudo nmap -sS 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 13:23 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    filtered ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
```





