VULNERABILITY ASSESTMENT REPORT

by Marina Flocco

index

introduction 01

detected vulnerabilities 02

examinated vulnerabilities 03

remediation 04

post-remediation scansion 05

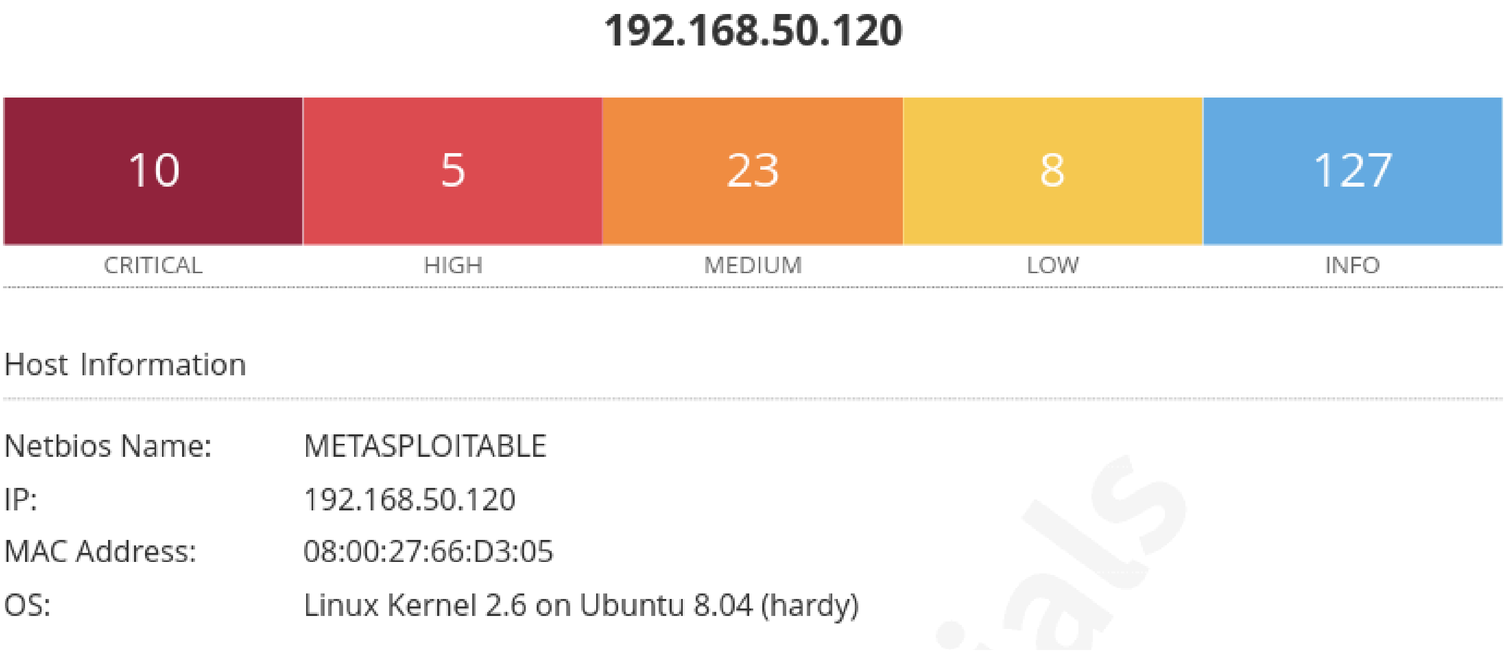
conclusion 06

1. Introduction

The purpose of the following document is to assest the vulnerabilities on the Metasploitable machine, and to put up a remediation plan for the most critical issues.

2. detected vulnerabilities

2. detected vulnerabilities



192.168.50.120

CRITICAL	HIGH	MEDIUM	LOW	INFO
10	5	23	8	127

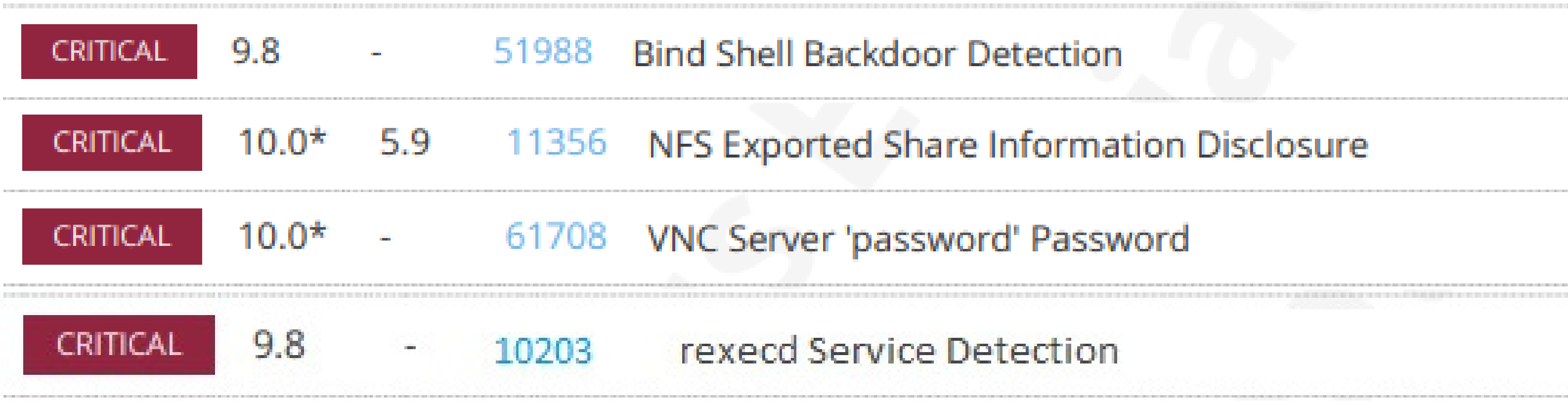
Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.120
MAC Address:	08:00:27:66:D3:05
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

3. Examinated Vulnerabilities

3. Examinated Vulnerabilities

vulnerabilities:



CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
CRITICAL	9.8	-	10203	rexecd Service Detection

51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

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.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (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 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

Plugin Output

tcp/1524/wild_shell

11356 - NFS Exported Share Information Disclosure

Synopsis

It is possible to access NFS shares on the remote host.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Risk Factor

Critical

VPR Score

5.9

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

Exploitable With

Metasploit (true)

Plugin Information

Published: 2003/03/12, Modified: 2023/08/30

Plugin Output

udp/2049/rpc-nfs

61708 - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

tcp/5900/vnc

```
Nessus logged in using a password of "password".
```

10203 rexecd Service Detection

Synopsis

The rexecd service is running on the remote host.

Description

The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely.

However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.

Solution

Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (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 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

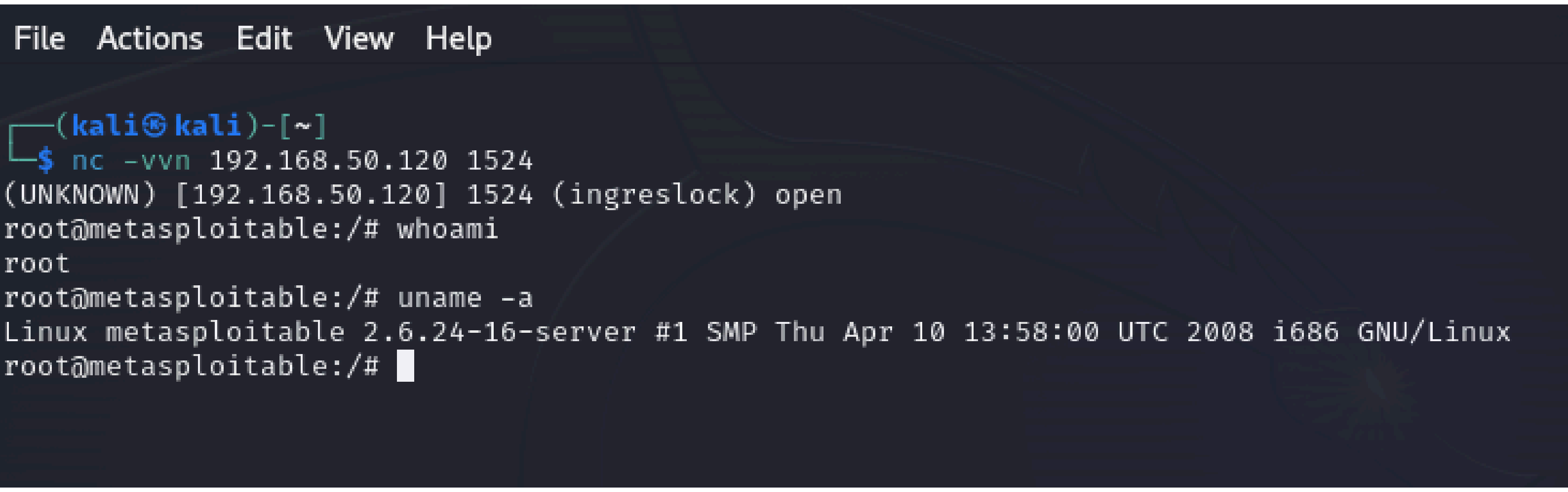
4. remediation

51988 - Bind Shell Backdoor Detection (port 1524)

check port 1524 status:

- nc 192.168.50.120 1524
- whoami
- uname -a

When trying to use netcat to connect to the suspect port 1524, we can confirm that a shell let's us see inside the machine's root user.



```
┌──(kali㉿kali)-[~]
└─$ nc -vvn 192.168.50.120 1524
(UNKNOWN) [192.168.50.120] 1524 (ingreslock) open
root@metasploitable:/# whoami
root
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# 
```

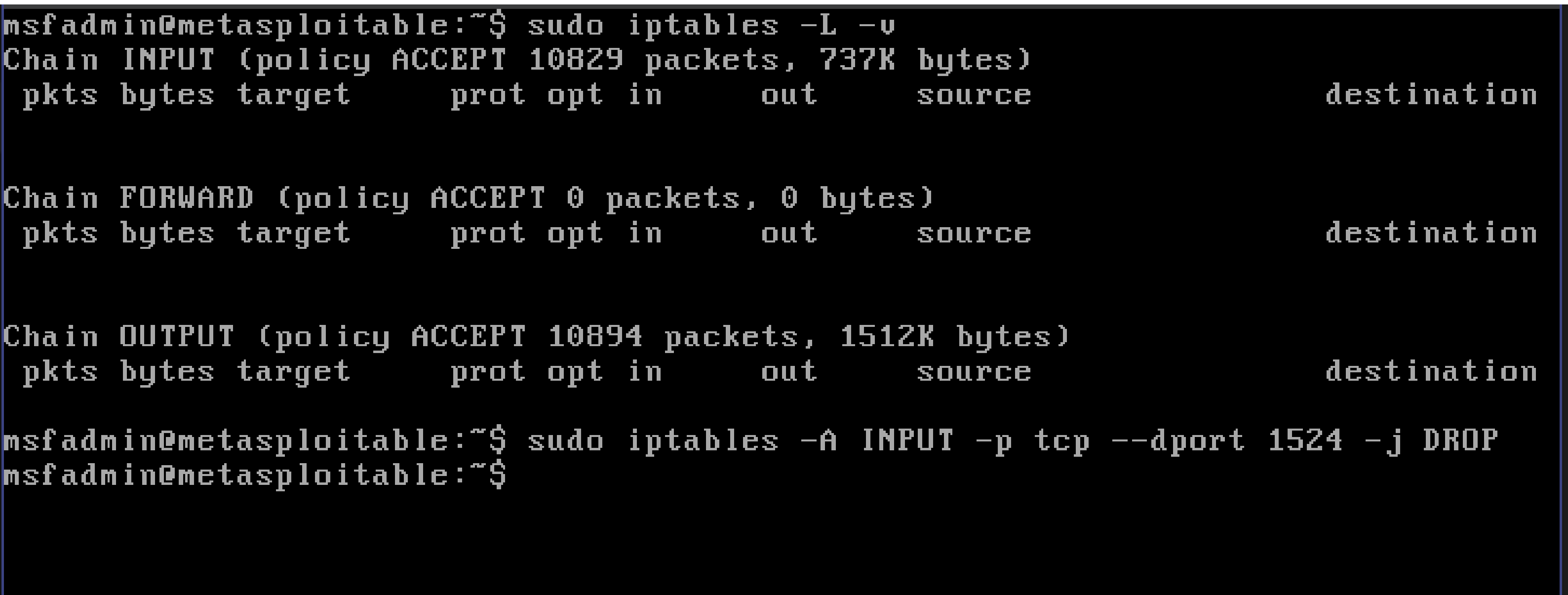
We use nmap to confirm again the open port:

- nmap -sS 192.168.50.120
- 1524/tcp/ open ingreslock

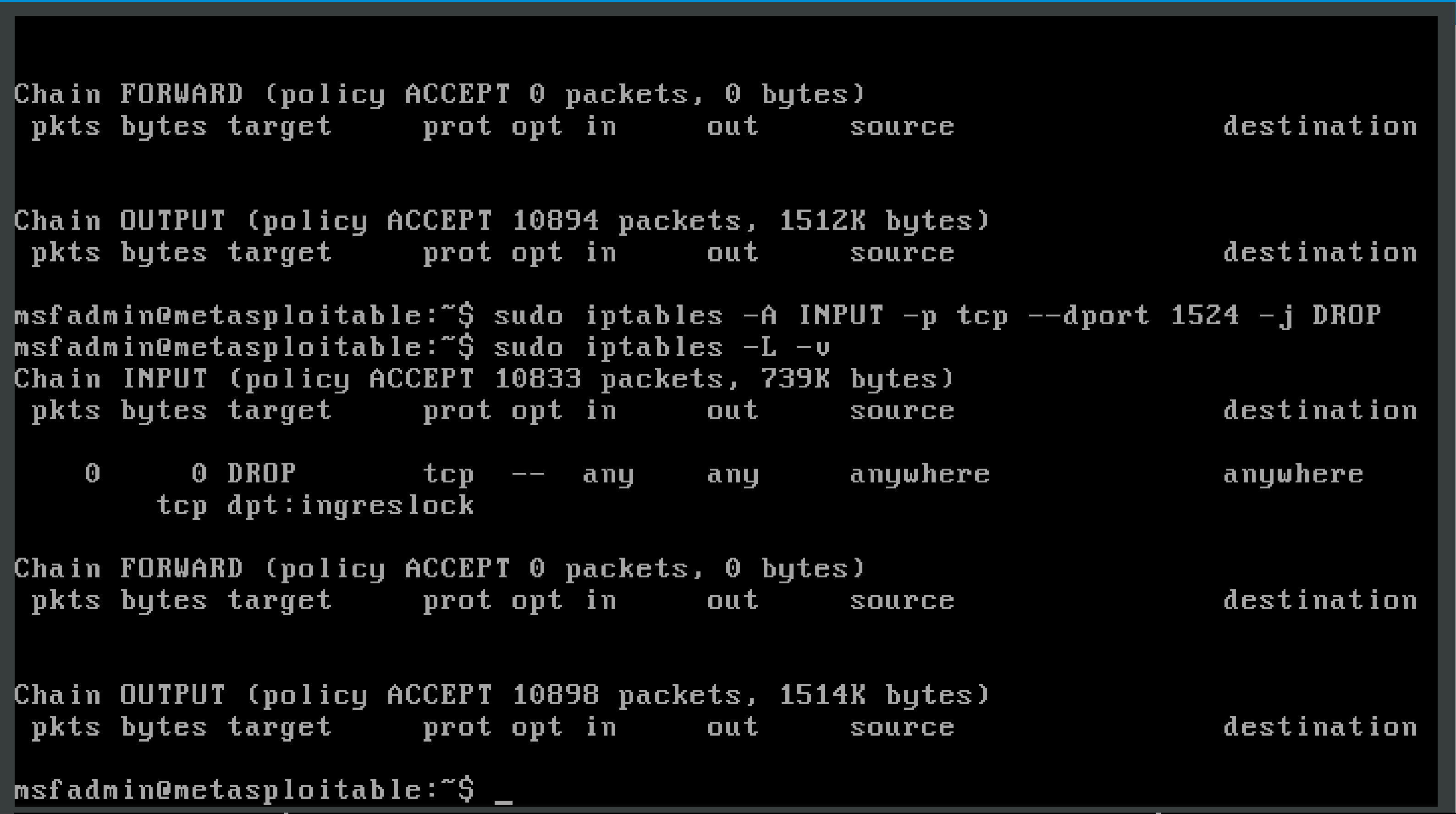
We insert a firewall rule that will block the access to the 1524 port:

- sudo iptables -L (FA VISIONARE LA LISTA DELLE REGOLE FIREWALL)
- sudo iptables -A INPUT -p tcp --dport 1524 -j DROP (CI FA INSERIRE LA REGOLA FIREWALL CHE FARA FALLIRE IL TENTATIVO DI CONNESSIONE CON "DROP")
- sudo iptables-save (SALVIAMO LA REGOLA)

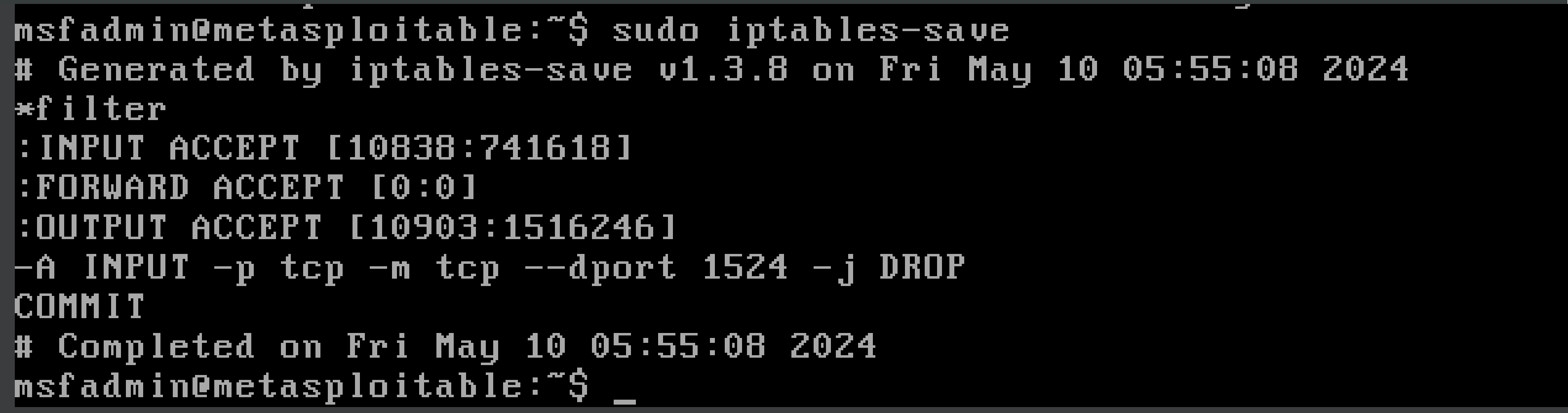
We check if the backdoor is still available trying to connect again to the port using netcat, but connection fails:
nc -v 192.168.50.120



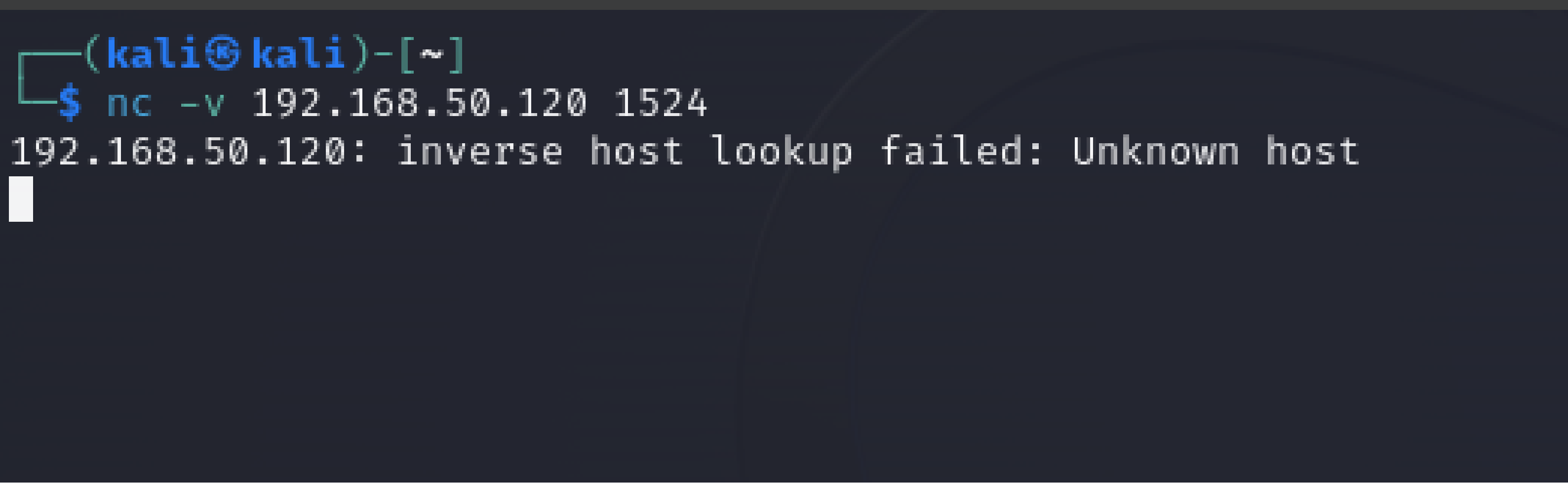
```
msfadmin@metasploitable:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 10829 packets, 737K bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 10894 packets, 1512K bytes)
 pkts bytes target     prot opt in     out     source               destination

msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
msfadmin@metasploitable:~$
```



```
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 10894 packets, 1512K bytes)
 pkts bytes target     prot opt in     out     source               destination

msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
msfadmin@metasploitable:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 10833 packets, 739K bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 DROP       tcp  --  any    any     anywhere             anywhere
        tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 10898 packets, 1514K bytes)
 pkts bytes target     prot opt in     out     source               destination

msfadmin@metasploitable:~$ _
```



```
msfadmin@metasploitable:~$ sudo iptables-save
# Generated by iptables-save v1.3.8 on Fri May 10 05:55:08 2024
*filter
:INPUT ACCEPT [10838:741618]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [10903:1516246]
-A INPUT -p tcp -m tcp --dport 1524 -j DROP
COMMIT
# Completed on Fri May 10 05:55:08 2024
msfadmin@metasploitable:~$ _
```



```
┌──(kali㉿kali)-[~]
└─$ nc -v 192.168.50.120 1524
192.168.50.120: inverse host lookup failed: Unknown host
```

11356 - NFS Exported Share Information Disclosure

Machine: Metasploitable

We check with nmap if the open port showed inside Nessus is true:
nmap 192.168.50.120 -p 2049
2049/tcp open nfs

It is suspected that an attacker may be able to leverage the port to read (and possibly write) files on remote host. We check the permissions.

- cat /etc/exports

ISSUES:

- rw permissions on root (/)
- no_root_squash

- cat /etc/hosts.allow

ISSUES:

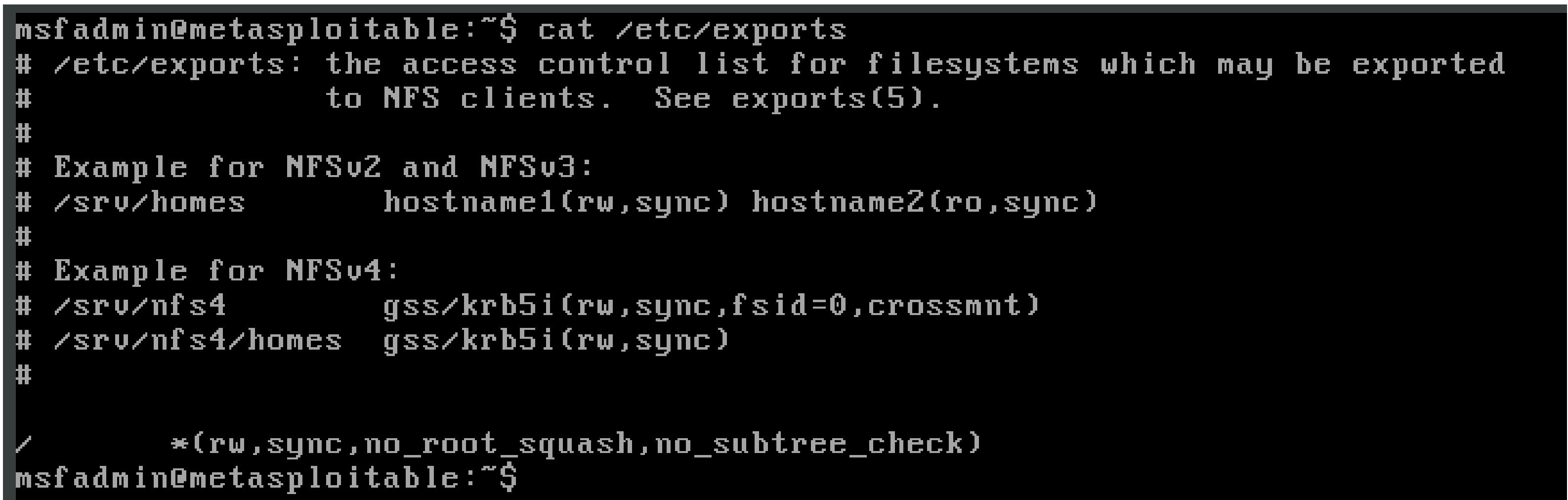
ALL:ALL

ACTIONS TAKEN

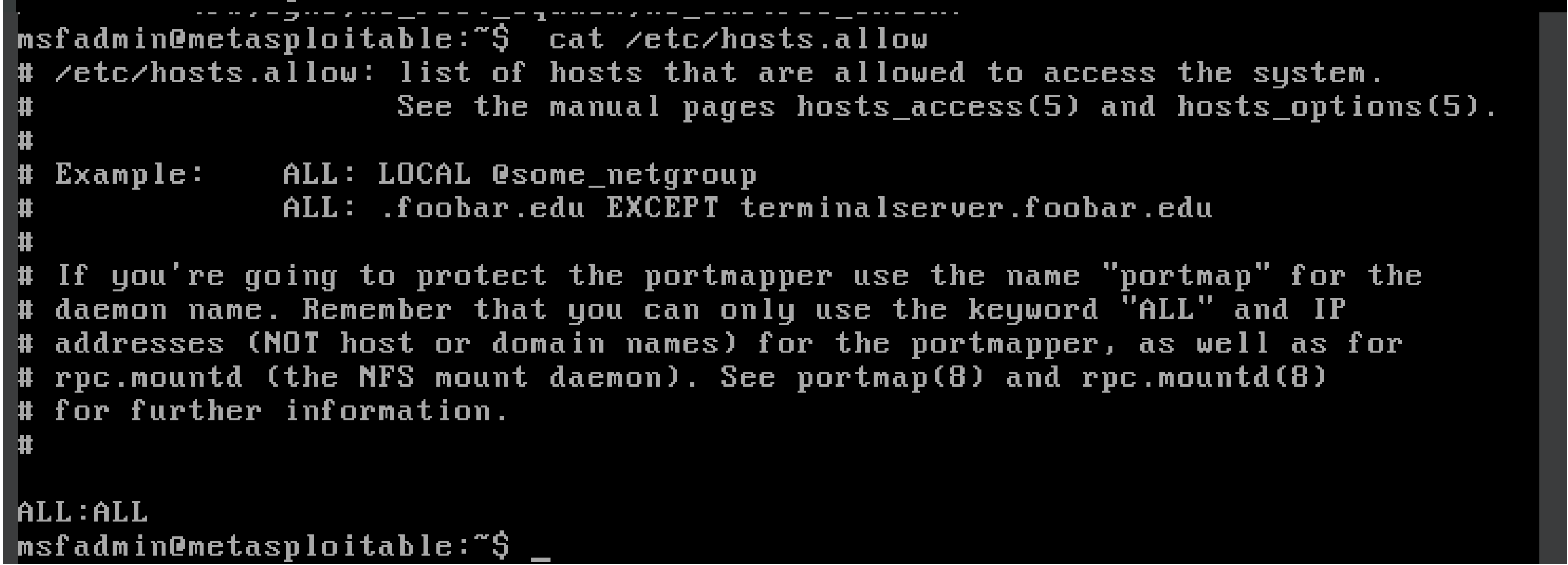
1. restrict access
2. Firewall rule

sudo nano /etc/exports

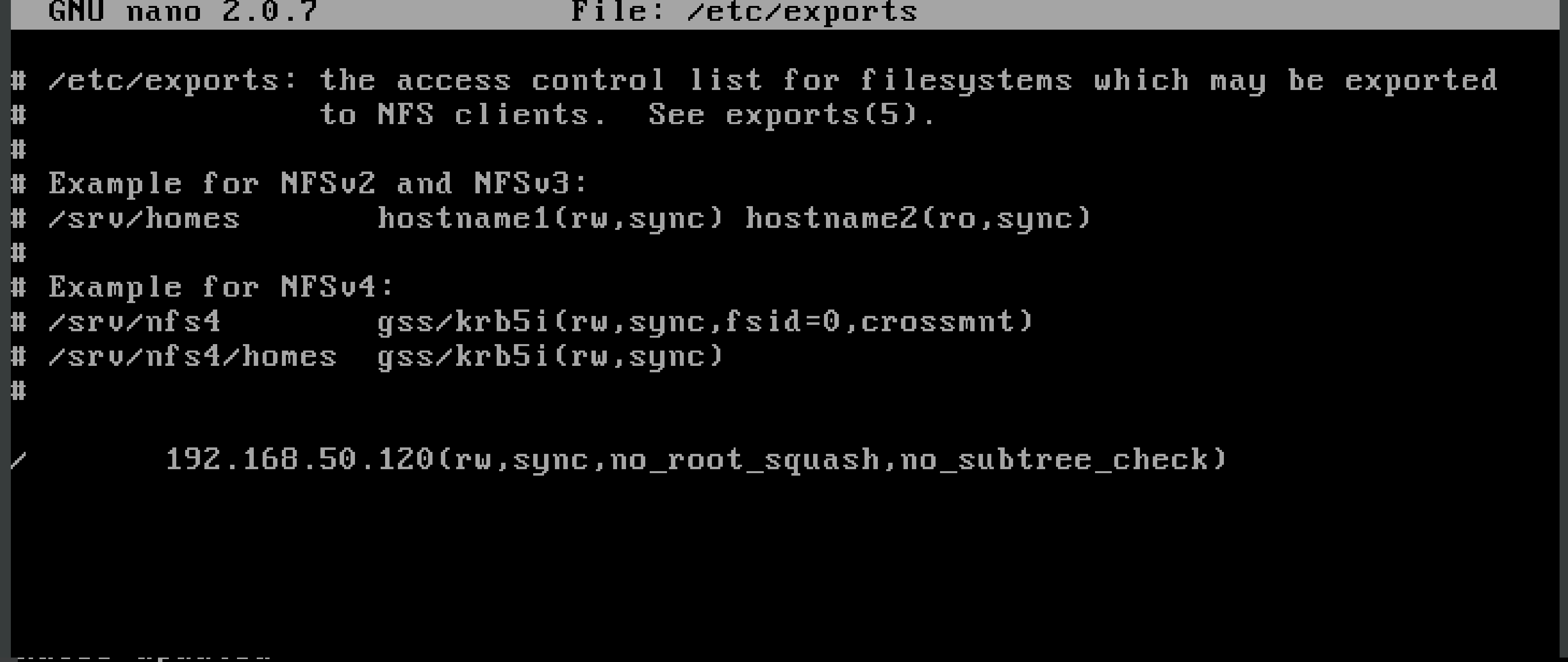
sudo ufw allow from 192.168.50.120 to any port 2049



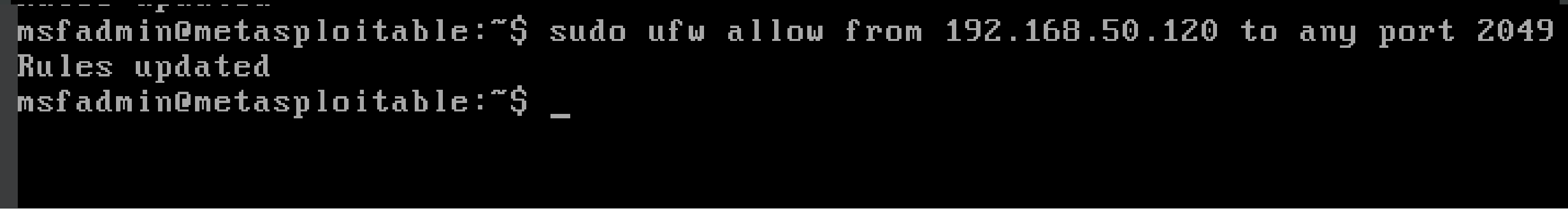
```
msfadmin@metasploitable:~$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4 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

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



```
msfadmin@metasploitable:~$  cat /etc/hosts.allow
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                   See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#

ALL:ALL
msfadmin@metasploitable:~$ _
```



```
  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)
#

/       192.168.50.120(rw,sync,no_root_squash,no_subtree_check)
```



```
msfadmin@metasploitable:~$ sudo ufw allow from 192.168.50.120 to any port 2049
Rules updated
msfadmin@metasploitable:~$ _
```

61708 - VNC Server 'password' Password

Machine: Kali

-We check if the port is open:
nmap -sV 192.168.50.120 5900

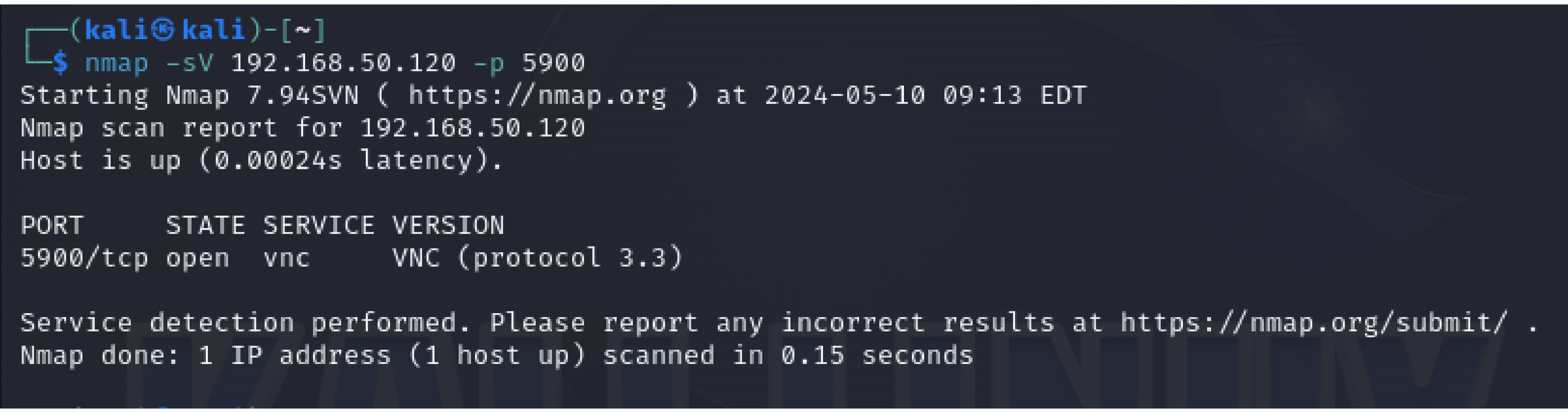
-We check if the password is actually weak:
msfconsole
search vnc_login
use 0
msf6 auxiliary(scanner/vnc/vnc_login) >show options
set rhosts 192.168.50.120
exploit
vncviewer 192.168.50.120

Machine: Metasploitable

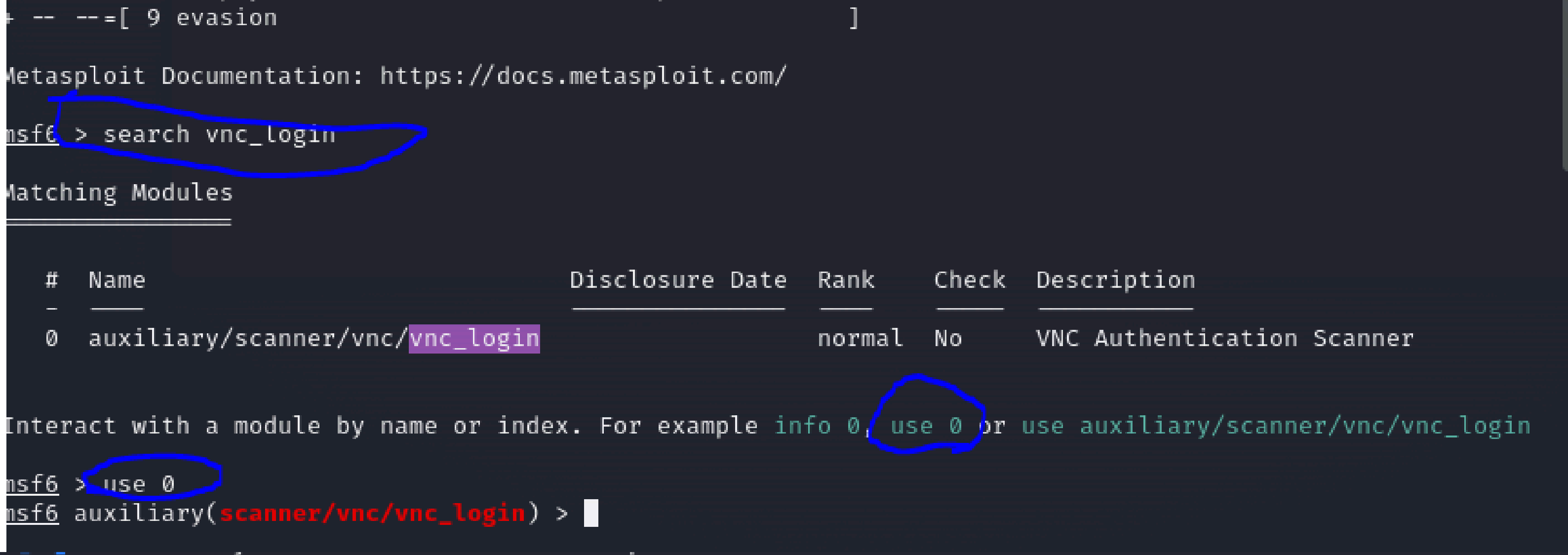
1. change password
2. add firewall rule

vncpasswd
password: MrN18fL

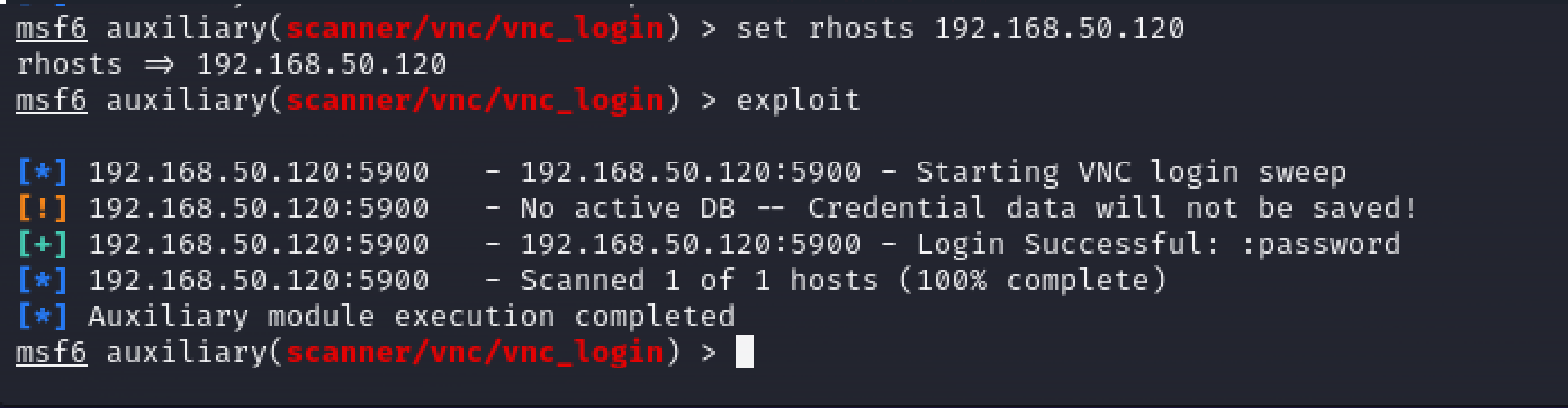
iptables
sudo iptables -A INPUT -p tcp --dport 5900 -j DROP



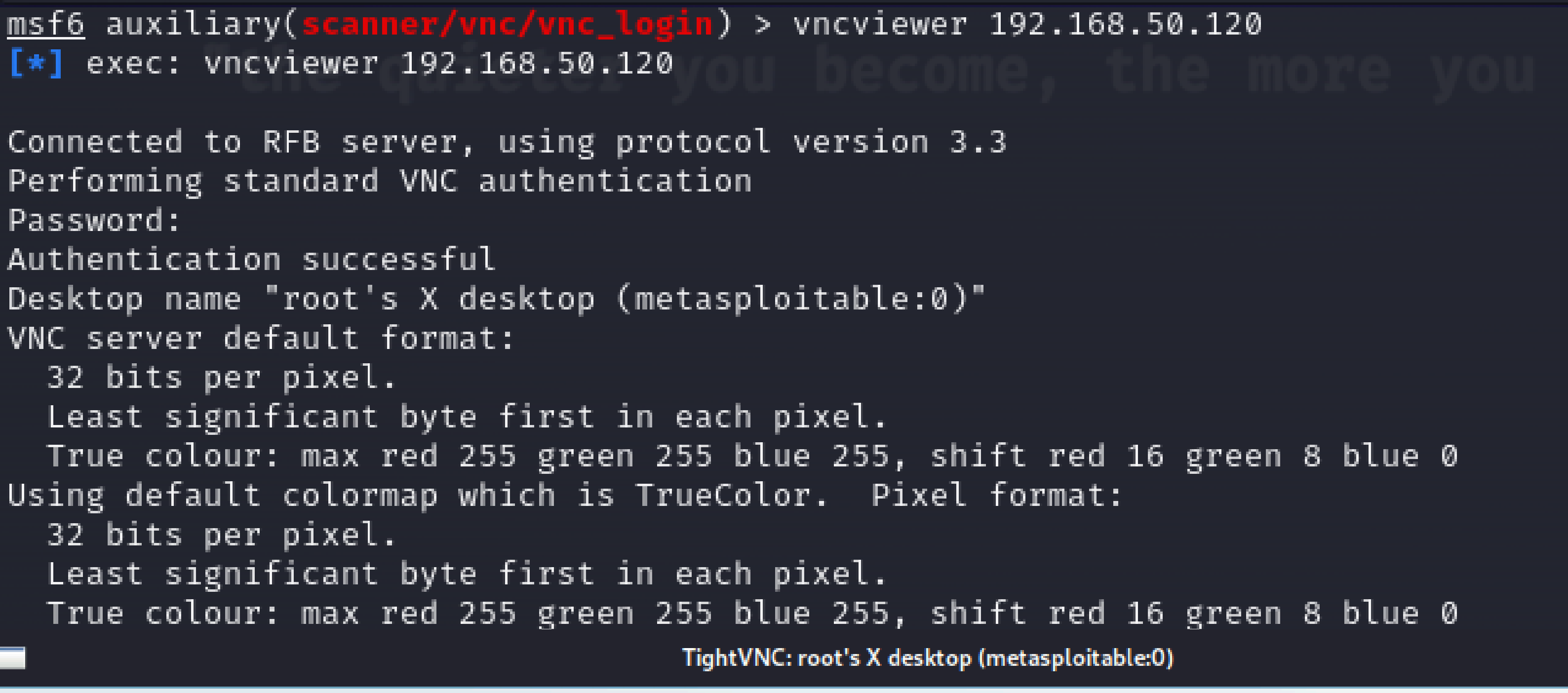
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.120 -p 5900
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 09:13 EDT
Nmap scan report for 192.168.50.120
Host is up (0.00024s latency).

PORT     STATE SERVICE VERSION
5900/tcp open  vnc     VNC (protocol 3.3)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```



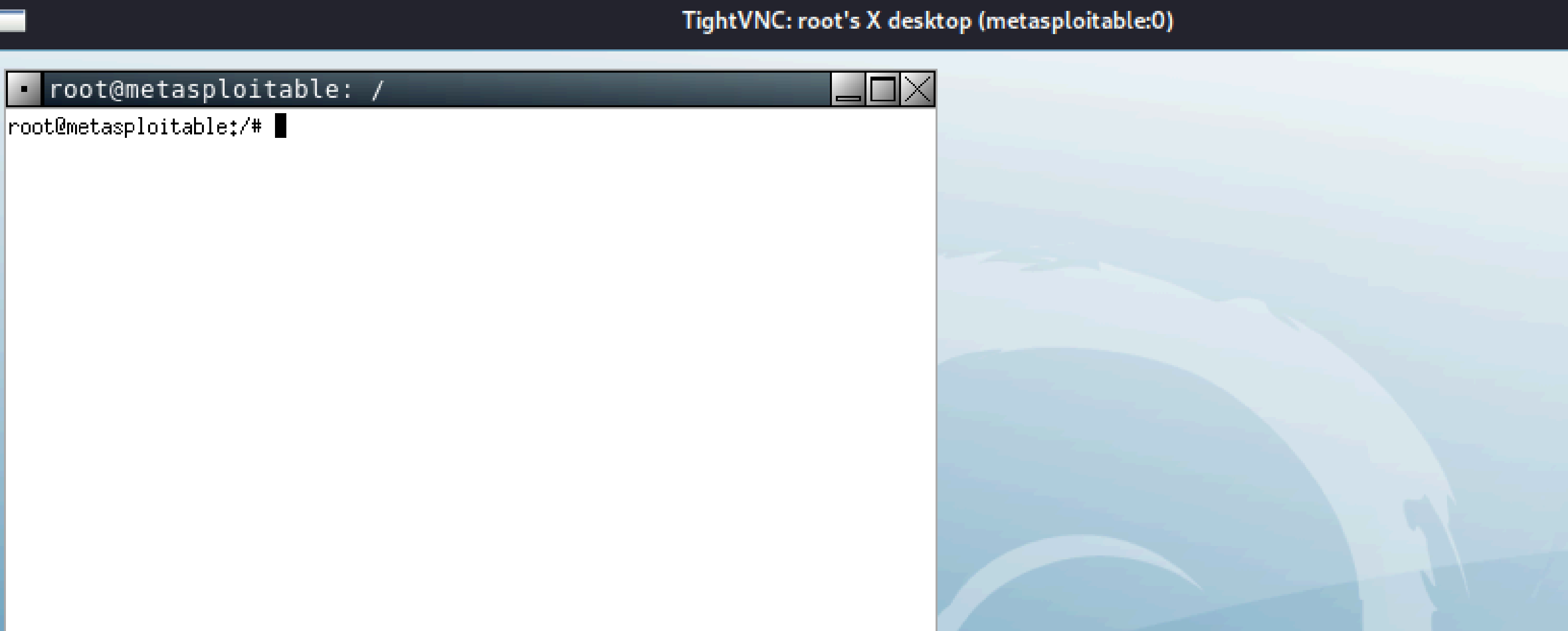
```
+ -- --=[ 9 evasion                                    ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vnc_login

Matching Modules
================

   #  Name                            Disclosure Date  Rank    Check  Description
   -  ----                            ---------------  ----    -----  -----------
   0  auxiliary/scanner/vnc/vnc_login                  normal  No     VNC Authentication Scanner


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/vnc/vnc_login

msf6 > use 0
msf6 auxiliary(scanner/vnc/vnc_login) > 
```



```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 192.168.50.120
rhosts => 192.168.50.120
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.50.120:5900   - 192.168.50.120:5900 - Starting VNC login sweep
[!] 192.168.50.120:5900   - No active DB -- Credential data will not be saved!
[+] 192.168.50.120:5900   - 192.168.50.120:5900 - Login Successful: :password
[*] 192.168.50.120:5900   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > 
```



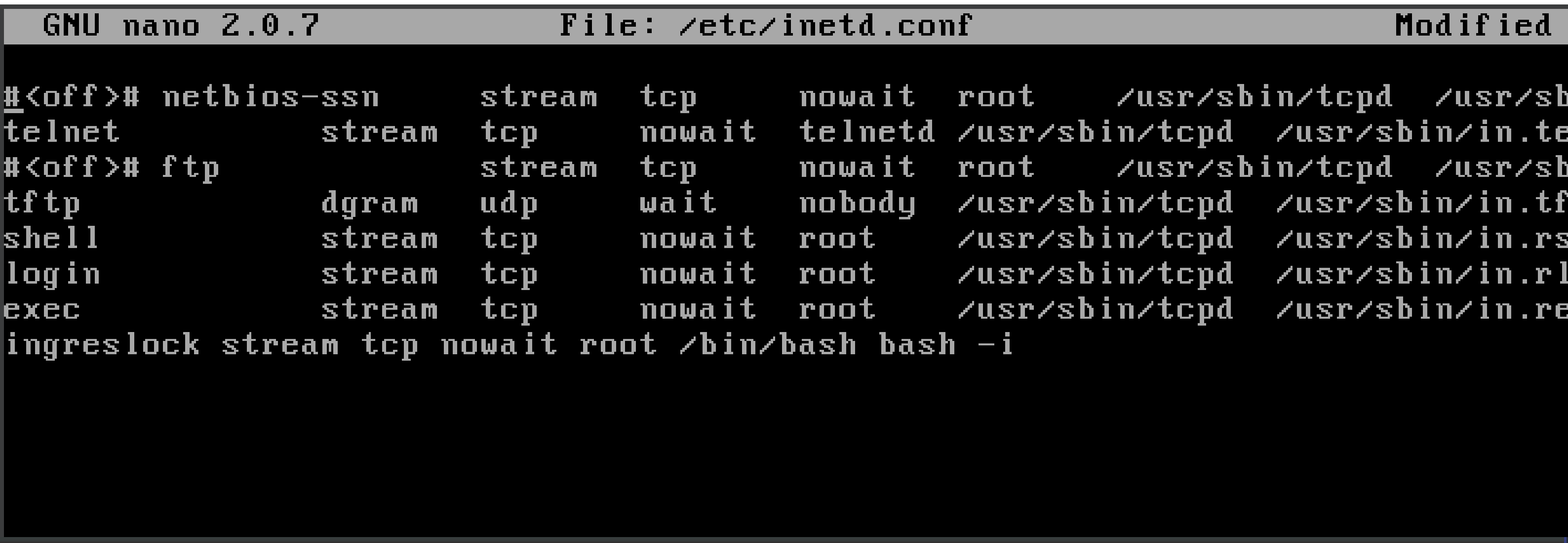
```
msf6 auxiliary(scanner/vnc/vnc_login) > vncviewer 192.168.50.120
[*] exec: vncviewer 192.168.50.120

Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```



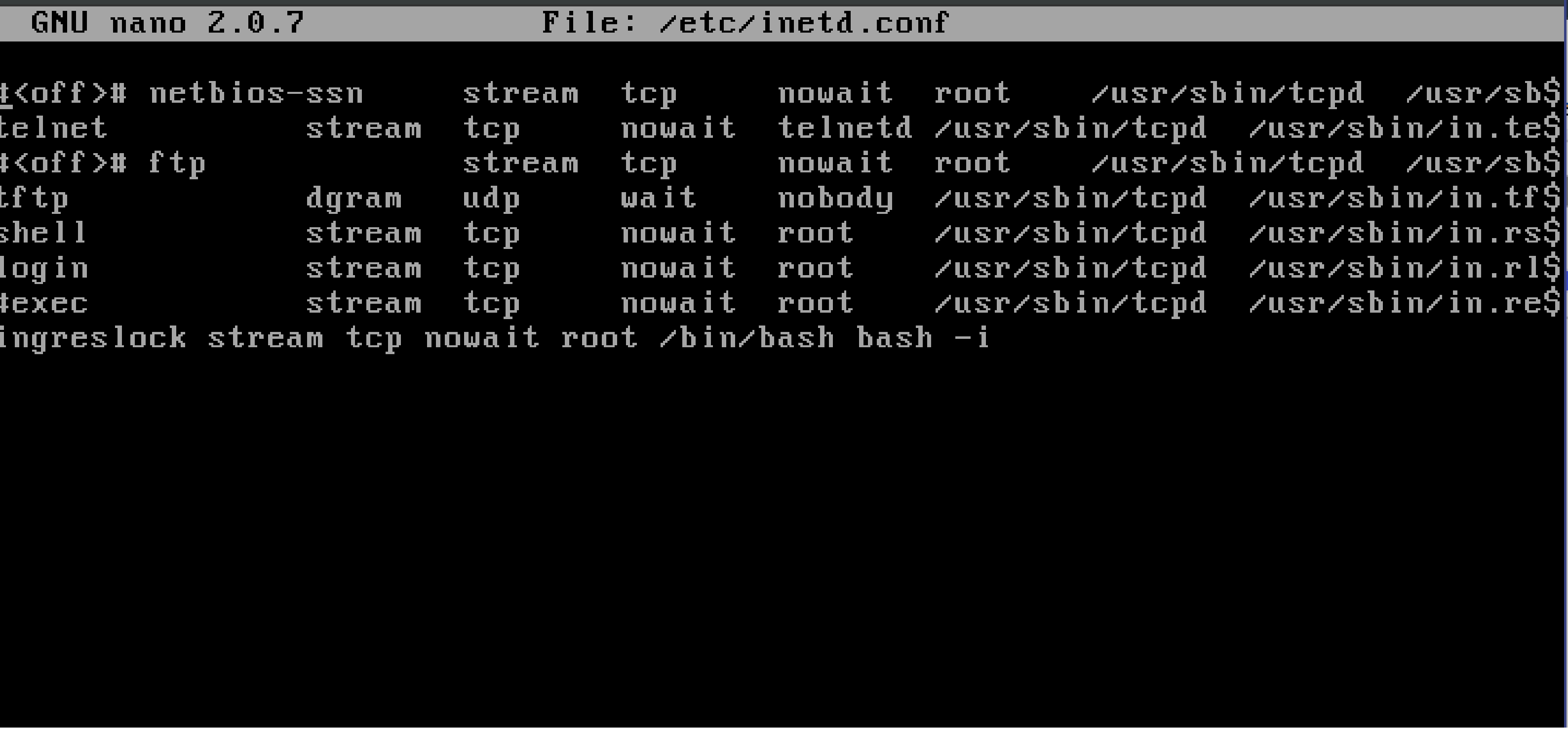
```
root@metasploitable:/# 
```

10203 rexecd Service Detection

- sudo nano /etc/inetd.conf
- commento # su stringa exec



```
  GNU nano 2.0.7               File: /etc/inetd.conf                     Modified

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl
exec            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re
ingreslock stream tcp nowait root /bin/bash bash -i
```

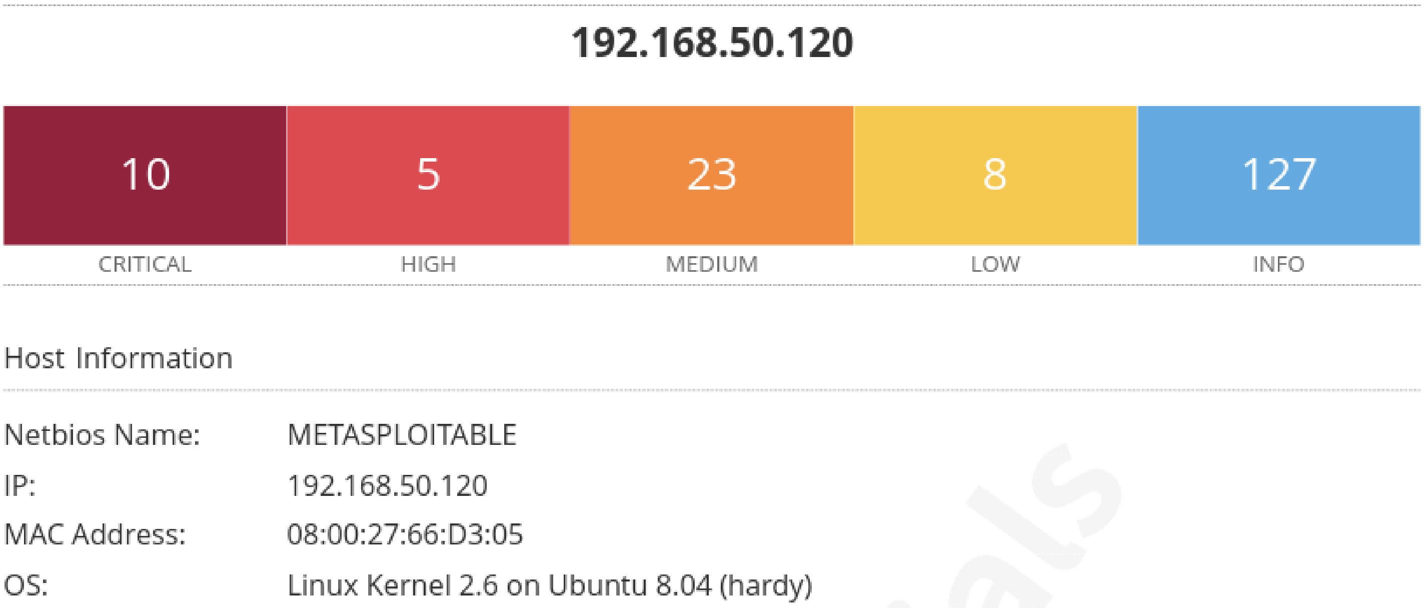


```
  GNU nano 2.0.7               File: /etc/inetd.conf

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
#exec           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i
```

5.

POST REMEDIATION SCANSION

INITIAL SCANSION (PRE-REMEDIATION)



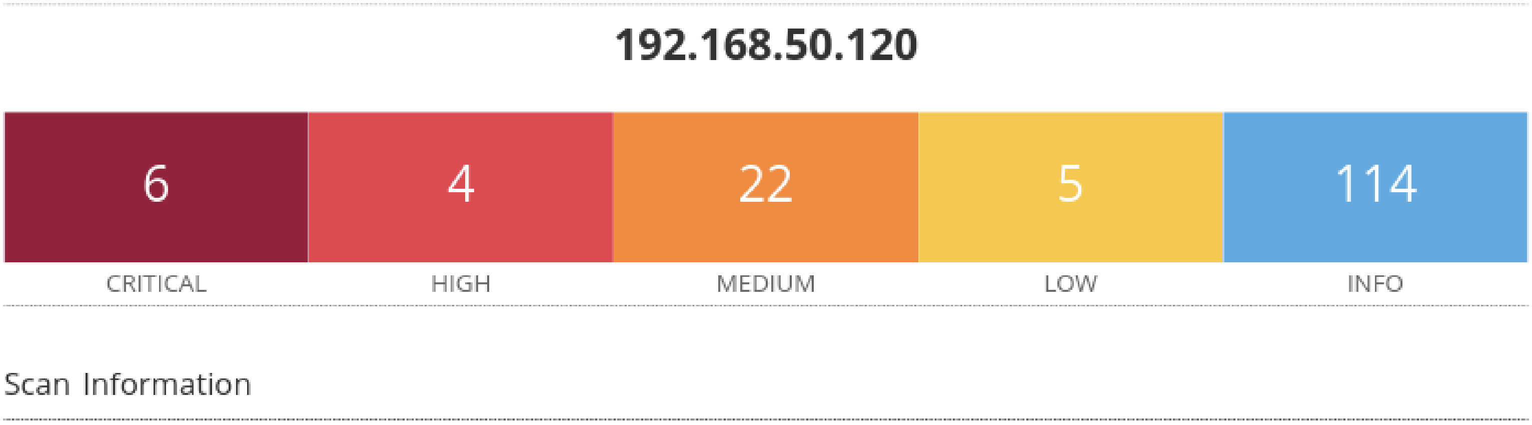
192.168.50.120

10	5	23	8	127
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.120
MAC Address:	08:00:27:66:D3:05
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

POST-REMEDIATION



192.168.50.120

6	4	22	5	114
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Conclusion

we can see that we were able to resolve 4 critical vulnerabilities inside the system.

point 1

Many security issues can be solved by applying a proper firewall rule or stricter authorization.

point 2

A lot of services need to be upgraded or updated to solve their potential exploitation.

Thank you.