

# Report

Objective: Remediation of Critical Vulnerabilities

VM: Kali, Metasploitable

Tools: Nessus, Nmap, Msfconsole, Netcat



|   |                        |                   |  |                       |       |     |
|---|------------------------|-------------------|--|-----------------------|-------|-----|
| <input type="checkbox"/>  | Host                   | Vulnerabilities ▾ |  |                       |       |     |
| <input type="checkbox"/>  | 192.168.50.101         | 10                | 5  | 24                    | 5     | 120 |
| Hosts 1 Vulnerabilities 60 Remediations 2 Notes 2 VPR Top Threats 1 History 5 |                        |                   |  |                       |       |     |
| Filter ▾  | Search Vulnerabilities |                   | Q  | 60 Vulnerabilities    |       |     |
| <input type="checkbox"/>  | Sev                    | Score             | Name   | Family                | Count | ⚙   |
| <input type="checkbox"/>  | CRITICAL               | 10.0 *            | NFS Exported Share Information Disclosure                | RPC                   | 1     | 🔄 ✎ |
| <input type="checkbox"/>  | CRITICAL               | 10.0              | Unix Operating System Unsupported Version Detection      | General               | 1     | 🔄 ✎ |
| <input type="checkbox"/>  | CRITICAL               | 10.0 *            | VNC Server 'password' Password                           | Gain a shell remotely | 1     | 🔄 ✎ |
| <input type="checkbox"/>  | CRITICAL               | 9.8               | Apache Tomcat AJP Connector Request Injection (Ghostcat) | Web Servers           | 1     | 🔄 ✎ |
| <input type="checkbox"/>  | CRITICAL               | 9.8               | Bind Shell Backdoor Detection                            | Backdoors             | 1     | 🔄 ✎ |
| <input type="checkbox"/>  | CRITICAL               | ...               | 📁 SSL (Multiple Issues)                                  | Gain a shell remotely | 3     | 🔄 ✎ |
| <input type="checkbox"/>  | MIXED                  | ...               | 📁 SSL (Multiple Issues)                                  | Service detection     | 3     | 🔄 ✎ |
| <input type="checkbox"/>  | HIGH                   | 7.5               | NFS Shares World Readable                                | RPC                   | 1     | 🔄 ✎ |
| <input type="checkbox"/>  | HIGH                   | 7.5               | Samba Badlock Vulnerability                              | General               | 1     | 🔄 ✎ |

## Vulnerability n. 1

☐ CRITICAL

9.8 Bind Shell Backdoor Detection

Backdoors

1

Port 1524, has the xinetd super server daemon running on it.

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 |

Proof of concept:

To exploit it is as simple as using Netcat command to get root access of the machine.

```
File Actions Edit View Help
zsh: corrupt history file /home/filip/.zsh_history
(filip@KaLinux)-[~]
$ nc 192.168.50.101 1524
root@metasploitable:/# whoami
root
root@metasploitable:/#
```

Solution:

This is exploitable due to the Ingreslock backdoor on the machine. To fix it we will need to delete the last line inside:

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo nano /etc/inetd.conf
GNU nano 2.0.7 File: /etc/inetd.conf
#<off># netbios-ssn      stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
telnet                 stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/inetd.$
#<off># ftp              stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
tftp                  dgram   udp     wait    nobody   /usr/sbin/tcpd  /usr/sbin/inetd.$
shell                 stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
login                 stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
exec                  stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
#ingreslock stream tcp nowait root /bin/bash bash -i
```

This one

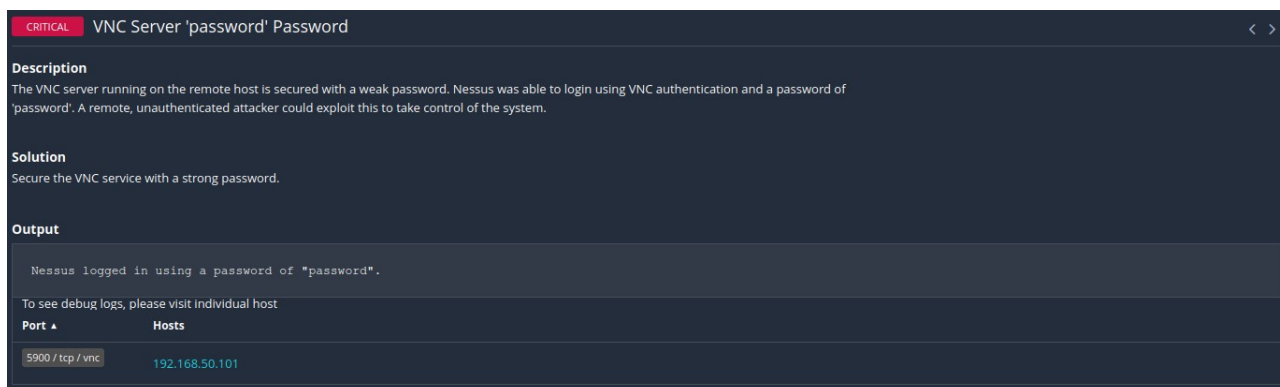
Afterwards if we try to exploit it again from Kali:

```
(filip@KaLinux)-[~]
$ nc 192.168.50.101 1524
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection refused
(filip@KaLinux)-[~]
```

## Vulnerability n. 2

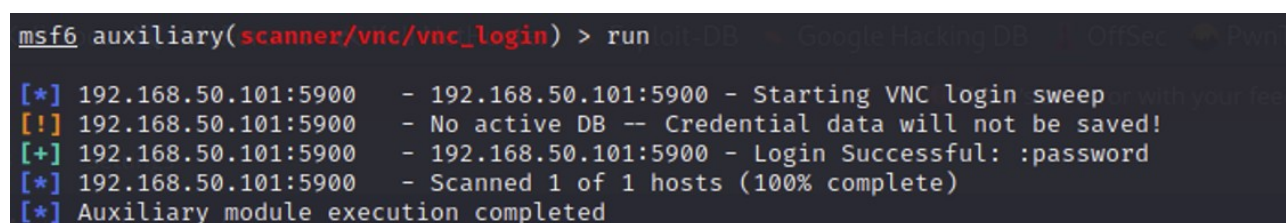


This is a simple misconfiguration, where the default password wasn't changed.



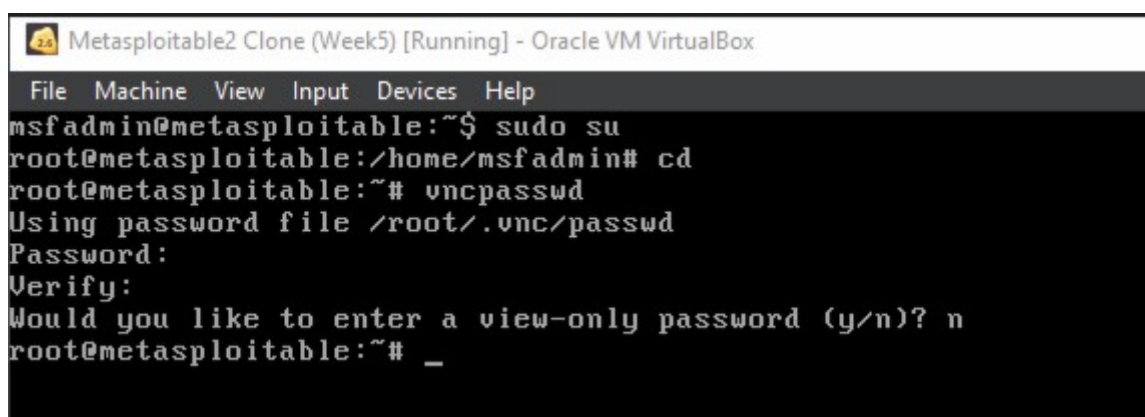
Proof of Concept:

This can be checked with msfconsole using Kali:

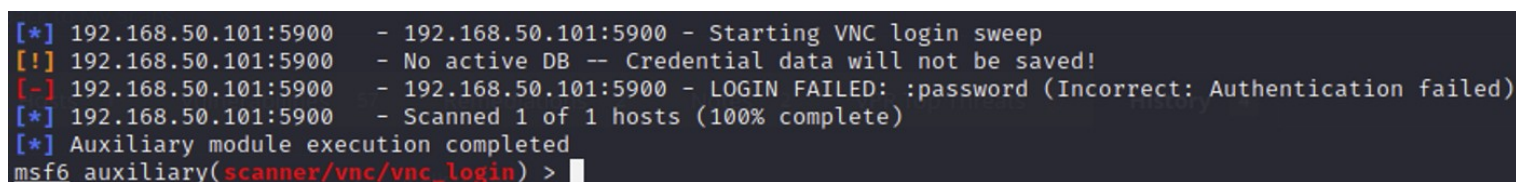


Solution:

Changing the password.



After changing the password we should get failed Authentication on next try of exploiting it.



## Vulnerability n. 3

CRITICAL

10.0 \* NFS Exported Share Information Disclosure

RPC

1

CRITICAL

NFS Exported Share Information Disclosure

**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.

**Output**

```
The following NFS shares could be mounted :

+ /
+ Contents of / :
- .
- ..
- bin
- boot
- cdrom
- dev
- etc
- home
- initrd
- initrd.img
- lib
- lost+found
- media
- mnt
- nohup.out
- opt
- proc
- root
- sbin
- srv
- sys
- tmp
- usr
- var
- vmlinuz

less...
```

To see debug logs, please visit individual host

| Port ▲               | Hosts          |
|----------------------|----------------|
| 2049 / udp / rpc-nfs | 192.168.50.101 |

POC: missing, in order to exploit and install of nfs-common is needed on Kali

Solution:

There are many ways to harden the NFS service  
one of them is:

```
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ sudo nano /etc/exports
```

Here once again we will modify the last line

```
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)
#
/mnt/newdisk 192.168.50.101(rw,sync,no_root_squash,no_subtree_check)
```

After remediation:

Host

Vulnerabilities

192.168.50.101

7

4

24

5

120

Hosts 1

Vulnerabilities 55

Remediations 2

Notes 2

VPR Top Threats 1

History 5

Filter

Search Vulnerabilities

55 Vulnerabilities

| Sev                 | Score | Name   | Family                | Count |                         |
|---------------------|-------|--|-----------------------|-------|-------------------------|
| <div>CRITICAL</div> | 10.0  | Unix Operating System Unsupported Version Detection      | General               | 1     | <div></div> <div></div> |
| <div>CRITICAL</div> | 9.8   | Apache Tomcat AJP Connector Request Injection (Ghostcat) | Web Servers           | 1     | <div></div> <div></div> |
| <div>CRITICAL</div> | ...   | <div>2</div> SSL (Multiple Issues)                       | Gain a shell remotely | 3     | <div></div> <div></div> |
| <div>MIXED</div>    | ...   | <div>2</div> SSL (Multiple Issues)                       | Service detection     | 3     | <div></div> <div></div> |
| <div>HIGH</div>     | 7.5   | Samba Badlock Vulnerability                              | General               | 1     | <div></div> <div></div> |
| <div>MIXED</div>    | ...   | <div>15</div> SSL (Multiple Issues)                      | General               | 27    | <div></div> <div></div> |