BenchMark M3.srl

Remediation Phase

Index

INTRO

Objective of the Remediation Phase

The remediation phase aims to address and resolve vulnerabilities and weaknesses identified during the penetration test, in order to enhance the overall security of the system or application. This process involves implementing solutions and corrections to mitigate the identified risks and ensure greater resilience against future attack.

Key Activities

- Through analysis of vulnerabilities identified during the PT.
- Prioritization of corrective actions based on the severity and impact of vulnerabilities.
- Development and implementation of derailed mitigation plans for each vulnerability.
- Continuous monitoring to ensure the effectiveness of implemented solutions.
- Comprehensive documentation of remediation actions for audit and compliance purposes.

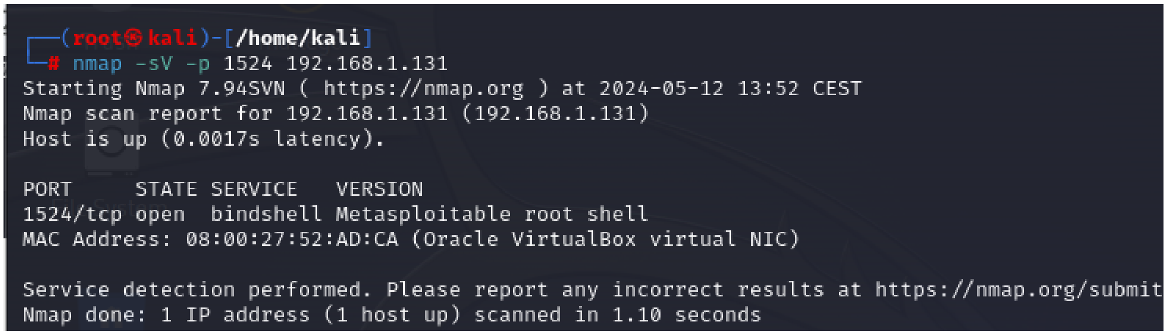
51988 - Bind Shell Backdoor Detection

To resolve the current issue, we employed the “fuser” utility to identify the running process.

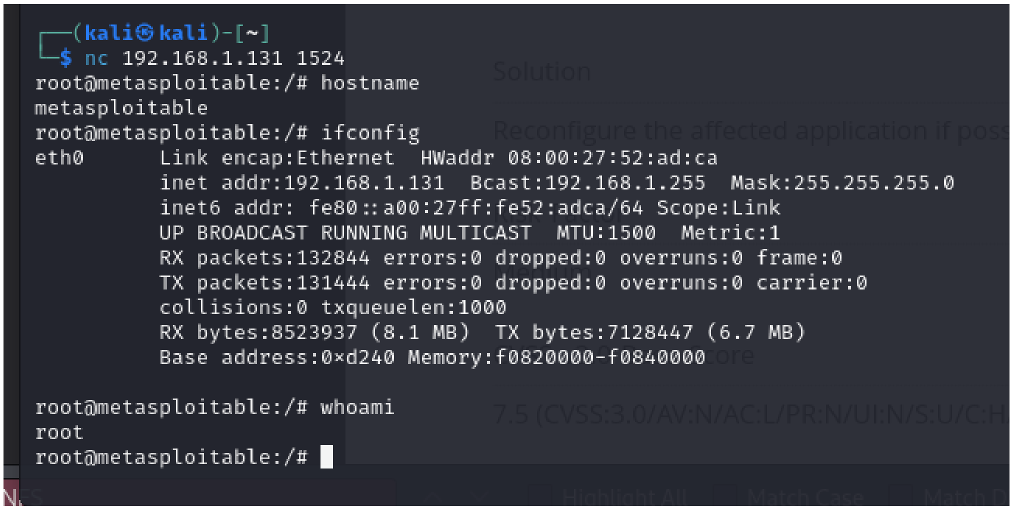
This tool was paired with “-k”, which sends a “kill” signal to processes using the specified resources and “-n tcp” specifies that we are seeking processes utilizing TCP network connections.

To ensure that the port was indeed open and accessible to a potential attacker, tests were conducted from a Kali Linux shell using the tools Nmap and Netcat.

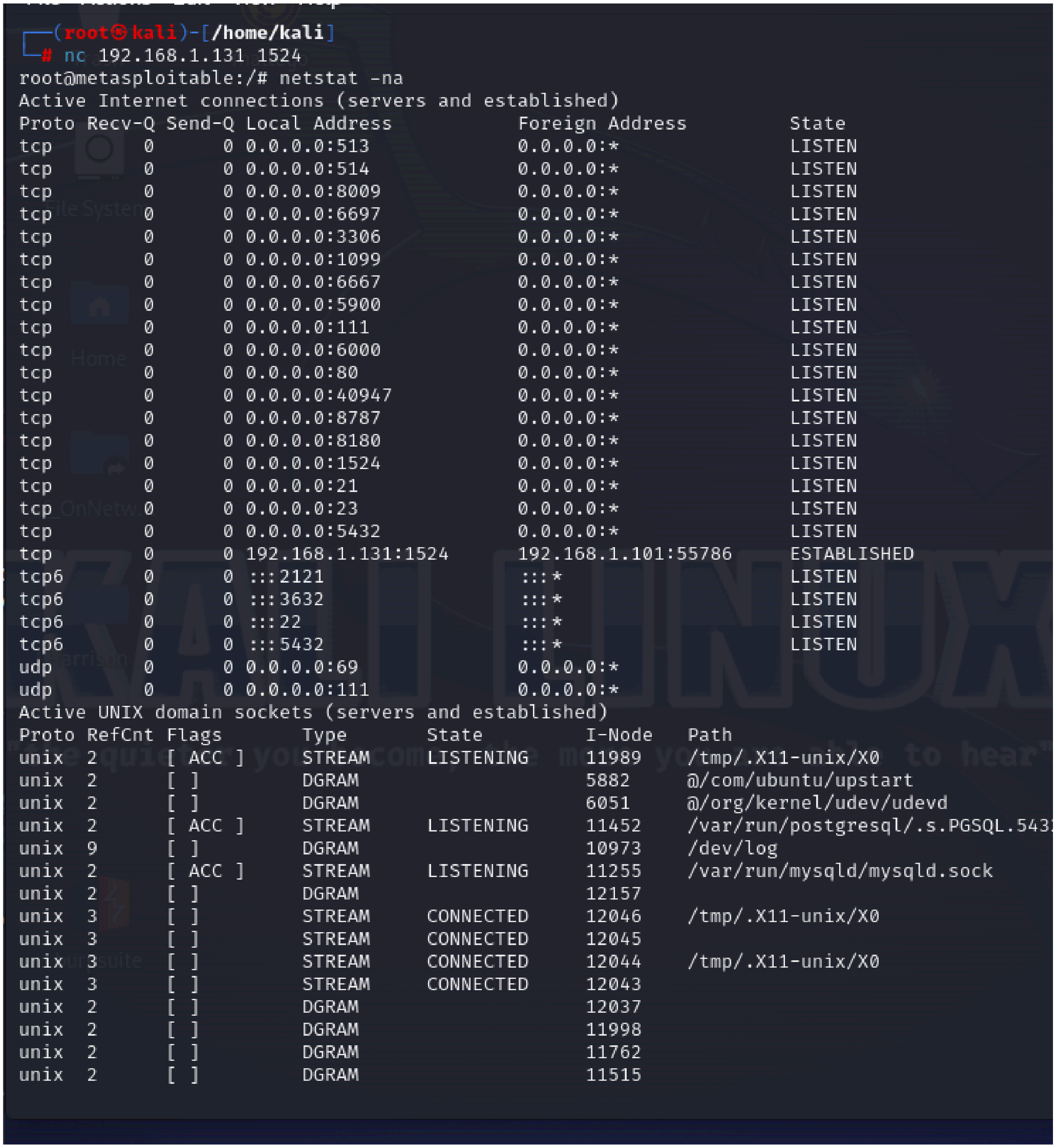
1) The screenshot of Nmap and Netcat were followed before the process was closed:



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -p 1524 192.168.1.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-12 13:52 CEST
Nmap scan report for 192.168.1.131 (192.168.1.131)
Host is up (0.0017s latency).

PORT     STATE SERVICE   VERSION
1524/tcp open  bindshell Metasploitable root shell
MAC Address: 08:00:27:52:AD:CA (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
```

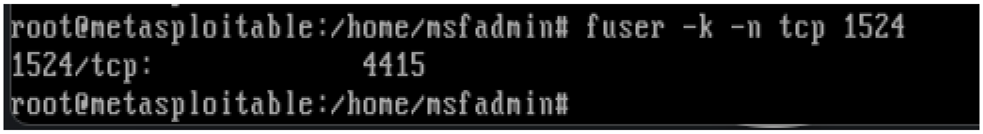


```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.1.131 1524
root@metasploitable:/# hostname
metasploitable
root@metasploitable:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:52:ad:ca
          inet addr:192.168.1.131  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe52:adca/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:132844 errors:0 dropped:0 overruns:0 frame:0
          TX packets:131444 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8523937 (8.1 MB)  TX bytes:7128447 (6.7 MB)
          Base address:0×d240 Memory:f0820000-f0840000

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

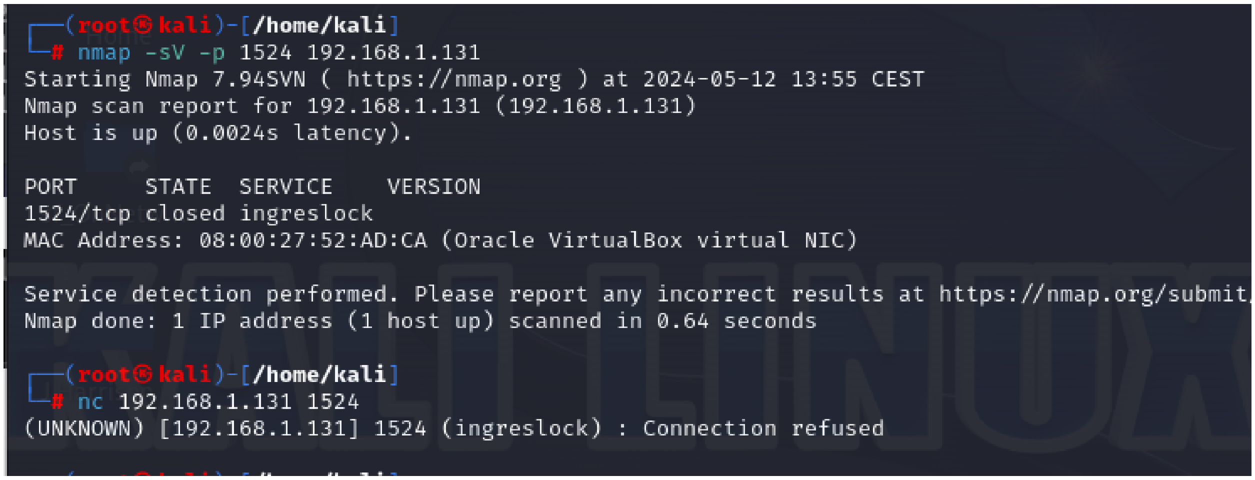


```
┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.1.131 1524
root@metasploitable:/# netstat -na
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:40947           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8180            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.131:1524      192.168.1.101:55786     ESTABLISHED
tcp6       0      0 :::2121                 :::*                    LISTEN
tcp6       0      0 :::3632                 :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::5432                 :::*                    LISTEN
udp        0      0 0.0.0.0:69              0.0.0.0:*
udp        0      0 0.0.0.0:111             0.0.0.0:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     11989    /tmp/.X11-unix/X0
unix  2      [ ]         DGRAM                    5882     @/com/ubuntu/upstart
unix  2      [ ]         DGRAM                    6051     @/org/kernel/udev/udevd
unix  2      [ ACC ]     STREAM     LISTENING     11452    /var/run/postgresql/.s.PGSQL.543
unix  9      [ ]         DGRAM                    10973    /dev/log
unix  2      [ ACC ]     STREAM     LISTENING     11255    /var/run/mysqld/mysqld.sock
unix  2      [ ]         DGRAM                    12157
unix  3      [ ]         STREAM     CONNECTED     12046    /tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     12045
unix  3      [ ]         STREAM     CONNECTED     12044    /tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     12043
unix  2      [ ]         DGRAM                    12037
unix  2      [ ]         DGRAM                    11998
unix  2      [ ]         DGRAM                    11762
unix  2      [ ]         DGRAM                    11515
```

2) Here is the screenshot of the process closure and the test from Kali Linux Shell



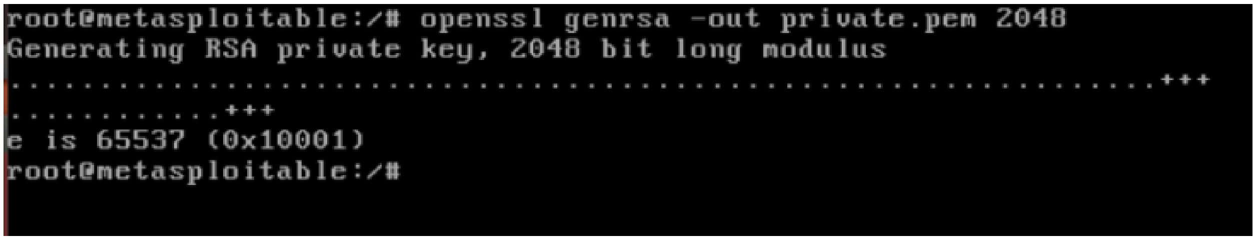
```
root@metasploitable:/home/msfadmin# fuser -k -n tcp 1524
1524/tcp:            4415
root@metasploitable:/home/msfadmin#
```



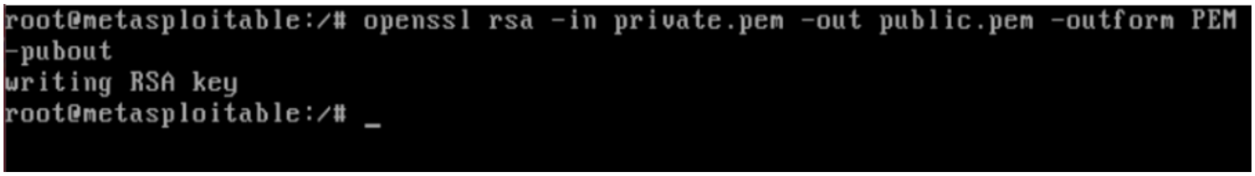
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -p 1524 192.168.1.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-12 13:55 CEST
Nmap scan report for 192.168.1.131 (192.168.1.131)
Host is up (0.0024s latency).

PORT     STATE  SERVICE    VERSION
1524/tcp closed ingreslock
MAC Address: 08:00:27:52:AD:CA (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds

┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.1.131 1524
(UNKNOWN) [192.168.1.131] 1524 (ingreslock) : Connection refused
```

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

To fix this issue was used the commands below to extract the public and private keys and wrote in to the files “public.pem” and “private.pem”



```
root@metasploitable:/# openssl genrsa -out private.pem 2048
Generating RSA private key, 2048 bit long modulus
.........................................................................+++
.............+++
e is 65537 (0x10001)
root@metasploitable:/#
```



```
root@metasploitable:/# openssl rsa -in private.pem -out public.pem -outform PEM
-pubout
writing RSA key
root@metasploitable:/# _
```

20007 - SSL Version 2 and 3 Protocol Detection

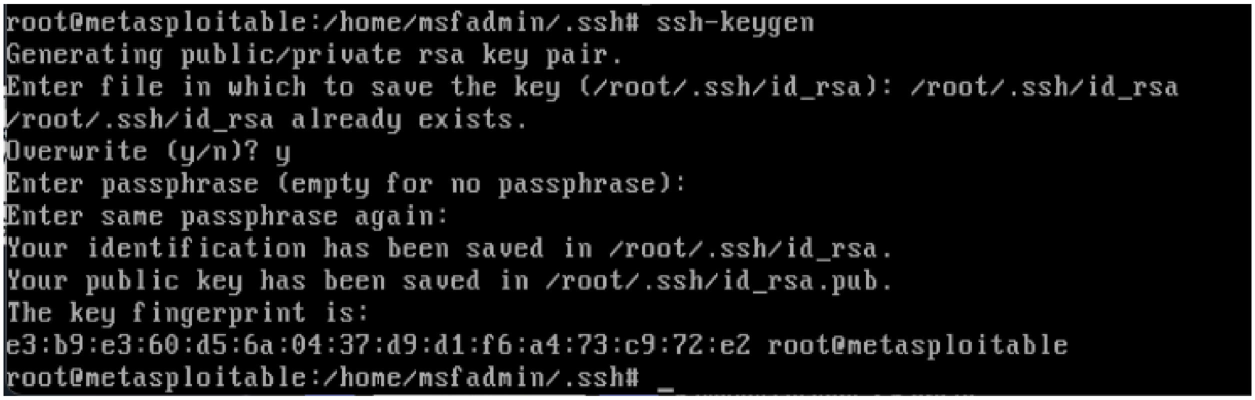
This was solved re-generated key material of SSL.

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

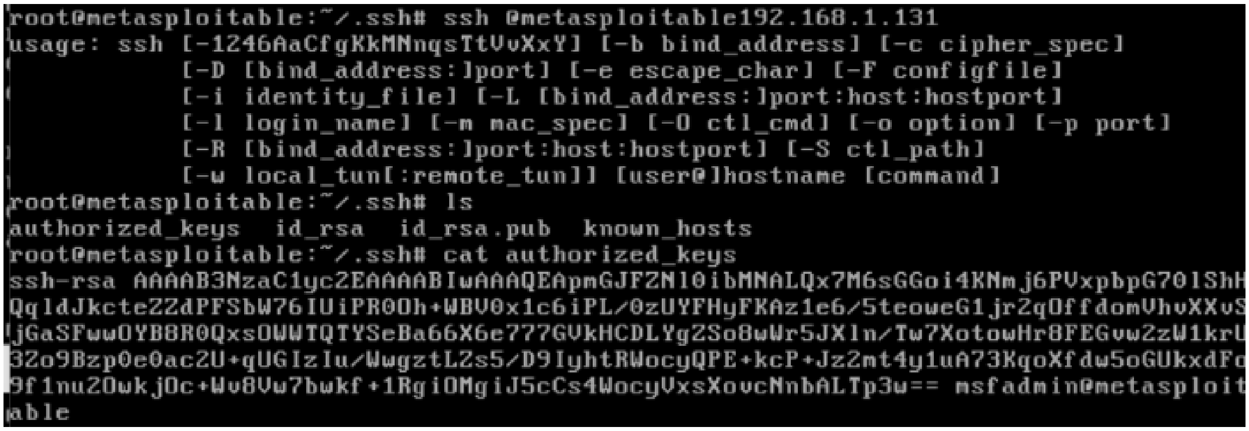
For this vulnerability was used the tool “ssh-keygen” to generate, manage and manipulate SSH (secure shell) key pairs on Unix- like operating systems and other systems compatible with SSH. (first figure)

SSH keys are used for passwordless authentication and encryption during SSH connections.

The “ssh-copy-id” command is a utility that simplifies the process of adding a user’s public key to the /.ssh/authorized_keys file on a remote server. (second figure)



```
root@metasploitable:/home/msfadmin/.ssh# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): /root/.ssh/id_rsa
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
e3:b9:e3:60:d5:6a:04:37:d9:d1:f6:a4:73:c9:72:e2 root@metasploitable
root@metasploitable:/home/msfadmin/.ssh# _
```



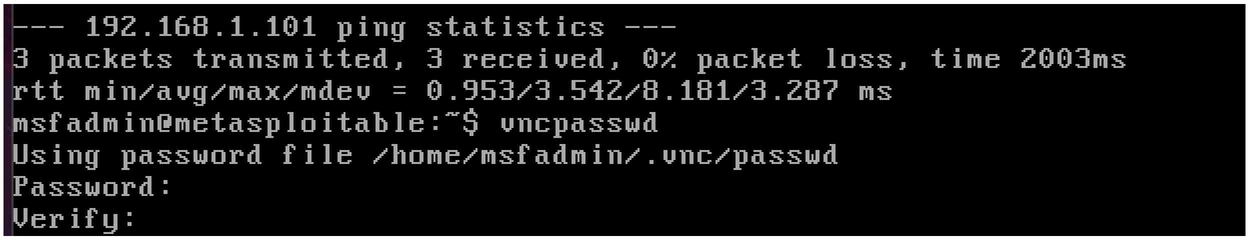
```
root@metasploitable:~/.ssh# ssh @metasploitable192.168.1.131
usage: ssh [-1246AaCfgKkMNnqsTtVvXxY] [-b bind_address] [-c cipher_spec]
           [-D [bind_address:]port] [-e escape_char] [-F configfile]
           [-i identity_file] [-L [bind_address:]port:host:hostport]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-R [bind_address:]port:host:hostport] [-S ctl_path]
           [-w local_tun[:remote_tun]] [user@]hostname [command]
root@metasploitable:~/.ssh# ls
authorized_keys  id_rsa  id_rsa.pub  known_hosts
root@metasploitable:~/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShH
QqldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jrZqOffdomVhvXXvS
jGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU
3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo
9f1nuZOwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@metasploit
able
```

61708 - VNC Server 'password' Password

The “vncpasswd” command is a utility included in VNC (Virtual Network Computing) software used to set or modify the password for remote access via VNC.

VNC is a system that allows controlling a computer remotely through a graphical interface.

The purpose of the “vncpasswd” command is to set or change the password for access via VNC.



```
--- 192.168.1.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.953/3.542/8.181/3.287 ms
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
```