VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology & Engineering

WINTER 2022 - 23

Programme : B.Tech **Due Date : 25-03-2022**
Course Title : Information Security Management **Course Code : CSE3502**

Name: SHUBHAM AGARWAL
RegNo: 19BIT0010

Q1) Commands for Port Scanning using NMAP

ANS

Procedure:

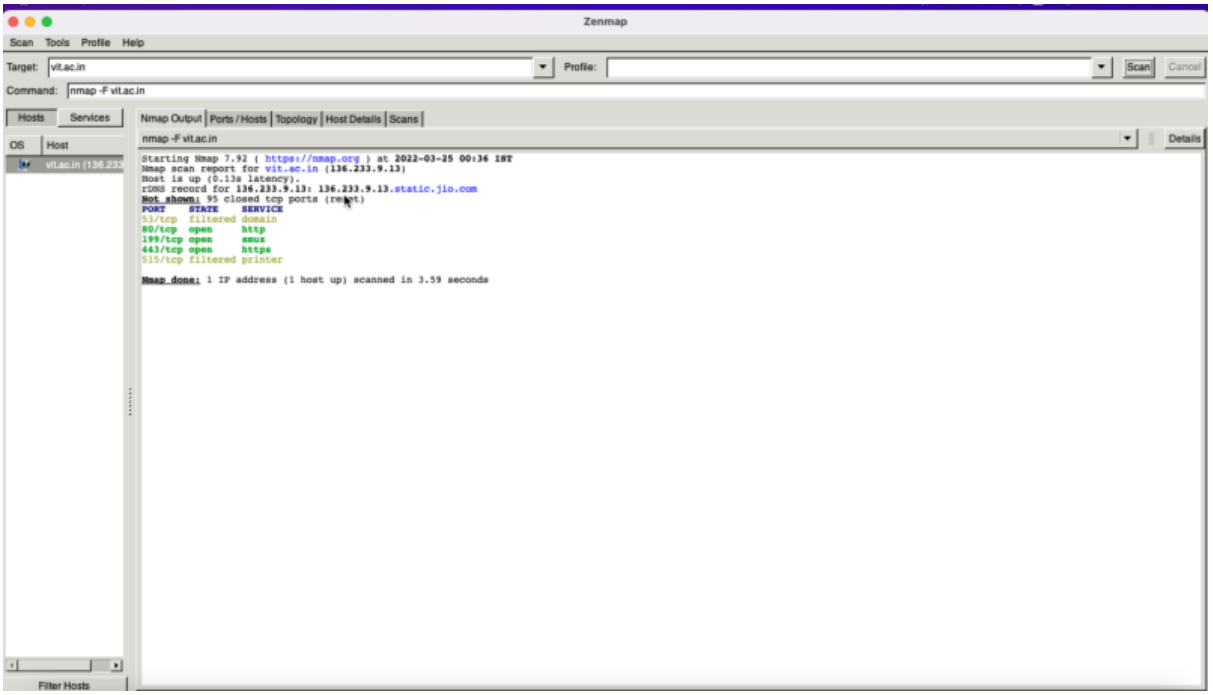
- After launching the nmap software, we begin by scanning the ports for vit.ac.in. Using the nmap -F vit.ac.in command. All of the active ports are returned to us. 136.233.9.13 is the IP address of vit.ac.in.

- Next, we'll use the command to execute aggressive port scanning.nmap -A vit.ac.in nmap -A vit.ac.in nmap -A vit.

- A scan for a specific port or a range of ports can also be performed.Providing port numbers The command nmap -p can be used to accomplish this.vit.ac.in. 50-85 vit.ac.in.

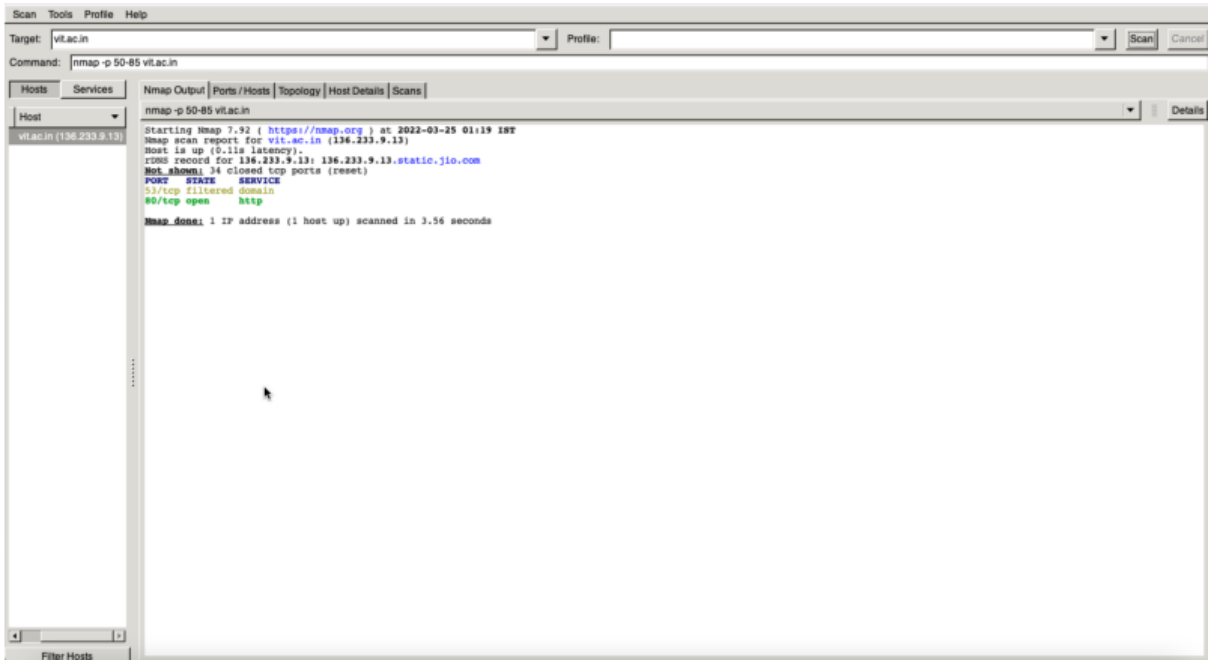
- Now we'll execute port scanning by specifying the name of the port.nmap -p ftp,http* vit.ac.in nmap -p ftp,http* vit.ac.in nmap -p ftp,http* vit.ac.in nmap -p ft After http, we use the * symbol to include https as well.Finally, we'll execute port scanning by providing protocol information and using the nmap command

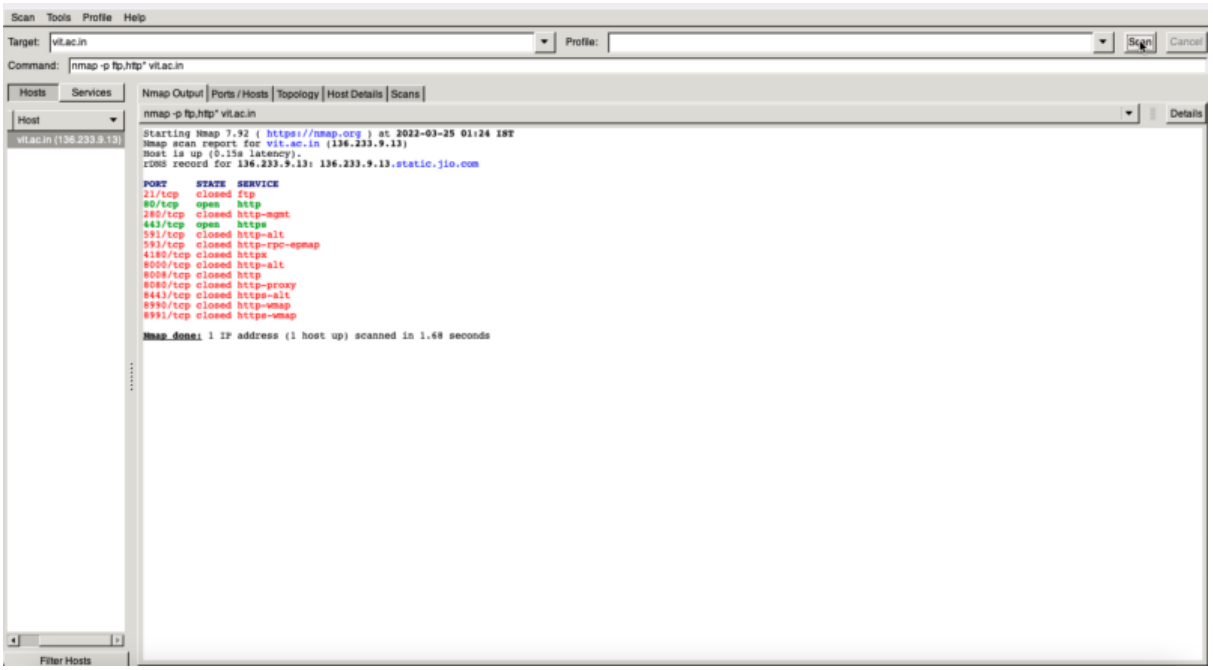
OUTPUT:

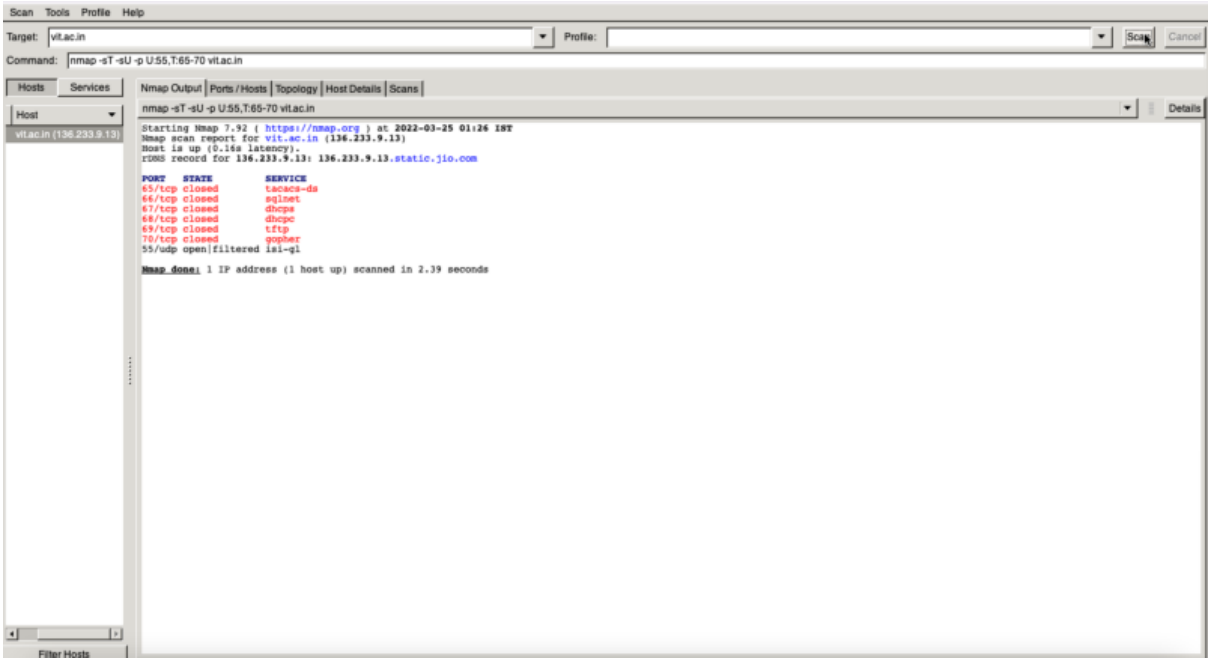

Zenmap
Scan Tools Profile Help
Target: vit.ac.in
Profile:
Scan
Cancel
Command: nmap -F vit.ac.in
Hosts
Services
OS
Host
vit.ac.in (136.233
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -F vit.ac.in
Details
Starting Nmap 7.92 (https://nmap.org) at 2022-03-25 00:36 IST
Nmap scan report for vit.ac.in (136.233.9.13)
Host is up (0.13s latency).
rDNS record for 136.233.9.13: 136.233.9.13.static.jio.com
Not shown: 95 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp filtered domain
80/tcp open http
199/tcp open smux
443/tcp open https
515/tcp filtered printer
Nmap done: 1 IP address (1 host up) scanned in 3.59 seconds
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: vit.ac.in
Profile:
Scan
Cancel
Command: nmap -A vit.ac.in
Hosts
Services
OS
Host
vit.ac.in (136.233
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -A vit.ac.in
Details
Starting Nmap 7.92 (https://nmap.org) at 2022-03-25 00:38 IST
sendto in send ip packet sd: sendto(19, packet, 60, 0, 136.233.9.13, 16) => No route to host
Offending packet: TCP 192.168.43.9:52087 > 136.233.9.13:80 S ttl=58 id=59958 iplen=15360 seq=1519721591 win=1 <wscale 10,nop,mss 1460,timestamp 4294967295 0,sackOK>
sendto in send ip packet sd: sendto(19, packet, 60, 0, 136.233.9.13, 16) => No route to host
Offending packet: TCP 192.168.43.9:52088 > 136.233.9.13:80 S ttl=45 id=59712 iplen=15360 seq=1519721592 win=63 <mss 1400,wscale 0,sackOK,timestamp 4294967295 0,eol>
sendto in send ip packet sd: sendto(19, packet, 60, 0, 136.233.9.13, 16) => No route to host
Offending packet: TCP 192.168.43.9:52089 > 136.233.9.13:80 S ttl=50 id=37638 iplen=15360 seq=1519721593 win=4 <timestamp 4294967295 0,nop,nop,wscale 5,nop,mss 640>
sendto in send ip packet sd: sendto(19, packet, 56, 0, 136.233.9.13, 16) => No route to host
Offending packet: TCP 192.168.43.9:52090 > 136.233.9.13:80 S ttl=40 id=31132 iplen=14336 seq=1519721594 win=4 <sackOK,timestamp 4294967295 0,wscale 10,eol>
sendto in send ip packet sd: sendto(19, packet, 60, 0, 136.233.9.13, 16) => No route to host
Offending packet: TCP 192.168.43.9:52091 > 136.233.9.13:80 S ttl=50 id=37313 iplen=15360 seq=1519721595 win=16 <mss 536,sackOK,timestamp 4294967295 0,wscale 10,eol>
sendto in send ip packet sd: sendto(19, packet, 56, 0, 136.233.9.13, 16) => No route to host
Offending packet: TCP 192.168.43.9:52092 > 136.233.9.13:80 S ttl=37 id=21535 iplen=14336 seq=1519721596 win=512 <mss 265,sackOK,timestamp 4294967295 0>
sendto in send ip packet sd: sendto(19, packet, 148, 0, 136.233.9.13, 16) => No route to host
Offending packet: ICMP 192.168.43.9 > 136.233.9.13 fragment ttl=53 id=20941 iplen=37888 frag offset=512 (incomplete)
sendto in send ip packet sd: sendto(19, packet, 178, 0, 136.233.9.13, 16) => No route to host
Offending packet: ICMP [192.168.43.9 > 136.233.9.13 Echo request (type=8/code=0) id=14559 seq=296] IP [ttl=53 id=25560 iplen=45568]
sendto in send ip packet sd: sendto(19, packet, 328, 0, 136.233.9.13, 16) => No route to host
Offending packet: UDP 192.168.43.9:51996 > 136.233.9.13:30545 ttl=58 id=4162 iplen=18433
send ip packet in send closedudp probe: No route to host (65)
sendto in send ip packet sd: sendto(19, packet, 60, 0, 136.233.9.13, 16) => No route to host
Offending packet: TCP 192.168.43.9:52093 > 136.233.9.13:80 S ttl=51 id=63938 iplen=15360 seq=1519721591 win=1 <wscale 10,nop,mss 1460,timestamp 4294967295 0,sackOK>
Omitting future Sendto error messages now that 10 have been shown. Use -d2 if you really want to see them.
send ip packet in send closedudp probe: No route to host (65)
send ip packet in send closedudp probe: No route to host (65)
send ip packet in send closedudp probe: No route to host (65)
send ip packet in send closedudp probe: No route to host (65)
send ip packet in send closedudp probe: No route to host (65)
send ip packet in send closedudp probe: No route to host (65)
Nmap scan report for vit.ac.in (136.233.9.13)
Host is up (0.12s latency).
rDNS record for 136.233.9.13: 136.233.9.13.static.jio.com
Not shown: 995 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp filtered domain
80/tcp open http
| fingerprint-strings:
| GetRequest:
| HTTP/1.1 302 Object Moved
| Location: https://vit.ac.in/?-
| event transid=38616022284 event clientip=106.208.72.135& event clientport=2366& event attackname=HTTP+RFC+Violation& event threatcategory=HTTP+RFC+Violations
| Content-Type: text/html
| Cache-Control: private
| Connection: close
| Content-Length: 320
| <head>
| <script type="text/javascript">
| event transid='3861602228';
| </script>
| <body> This object may be found <a HREF="https://vit.ac.in/?-
| event transid=38616022284 event clientip=106.208.72.135& event clientport=2366& event attackname=HTTP+RFC+Violation& event threatcategory=HTTP+RFC+Violations">here </body>
| HTTPOptions:

Scan Tools Profile Help
Target: vit.ac.in
Profile:
Scan
Cancel
Command: nmap -A vit.ac.in
Hosts
Services
OS
Host
vit.ac.in (136.233
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -A vit.ac.in
Details
| <body> This object may be found <a HREF="https://vit.ac.in/?-
| event transid=38616022304 event clientip=106.208.72.135& event clientport=1931& event attackname=HTTP+RFC+Violation& event threatcategory=HTTP+RFC+Violations">here </body>
199/tcp open smux Linux SNMP multiplexer
443/tcp open ssl/http Apache httpd (off)
515/tcp filtered printer
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.92%I=7%D=3/25%Time=623CC1B6%P=x86_64-apple-darwin17.7.0%
SF:r(GetRequest,273,"HTTP/1\.1\x20302\x20Object\x20Moved\r\nLocation:\x20h
SF:ttps://vit\.ac\.in/\?
SF:\.72\.135&
SF:1& event threatcategory=HTTP\+RFC\+Violations\r\nContent-Type:\x20text/h
SF:tml\r\nCache-Control:\x20private\r\nConnection:\x20close\r\nContent-Len
SF:gth:\x20320\r\n\r\n<head>\n<script\x20type=\"text/javascript\">\n\x20\x
SF:20var\x20
SF:ect\x20may\x20be\x20found\x20<a\x20HREF=\"https://vit\.ac\.in/\?
SF:transid=38616022284 event clientip=106\.208\.72\.135& event clientport=
SF:2366& event attackname=HTTP\+RFC\+Violation& event threatcategory=HTTP\
SF:+RFC\+Violations\">here\x20</body>");r(HTTPOptions,273,"HTTP/1\.1\x
SF:20302\x20Object\x20Moved\r\nLocation:\x20https://vit\.ac\.in/\?
SF:ransid=38616022294 event clientip=106\.208\.72\.135& event clientport=1
SF:9294 event attackname=HTTP\+RFC\+Violation& event threatcategory=HTTP\+
SF:RFC\+Violations\r\nContent-Type:\x20text/html\r\nCache-Control:\x20priv
SF:ate\r\nConnection:\x20close\r\nContent-Length:\x20320\r\n\r\n<head>\n<s
SF:cript\x20type=\"text/javascript\">\n\x20\x20var\x20
SF:602229';\n</script>\n<body>\x20This\x20object\x20may\x20be\x20found\x20
SF:<a\x20HREF=\"https://vit\.ac\.in/\?
SF:entip=106\.208\.72\.135& event clientport=1929& event attackname=HTTP\+
SF:RFC\+Violation& event threatcategory=HTTP\+RFC\+Violations\">here\x
SF:20</body>");r(RTSPRequest,273,"HTTP/1\.1\x20302\x20Object\x20Moved\r\nL
SF:ocation:\x20https://vit\.ac\.in/\?
SF:ntip=106\.208\.72\.135& event clientport=1931& event attackname=HTTP\+R
SF:FC\+Violation& event threatcategory=HTTP\+RFC\+Violations\r\nContent-Ty
SF:pe:\x20text/html\r\nCache-Control:\x20private\r\nConnection:\x20close\r
SF:\nContent-Length:\x20320\r\n\r\n<head>\n<script\x20type=\"text/javascri
SF:pt\">\n\x20\x20var\x20
SF:t clientport=1931& event attackname=HTTP\+RFC\+Violation& event threatc
SF:ategory=HTTP\+RFC\+Violations\">here\x20</body>");
Device type: firewall
Running (JUST GUESSING): Fortinet embedded (87%)
OS CPE: cpe:/h:fortinet:fortigate_100d
Aggressive OS guesses: Fortinet FortiGate 100D firewall (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 23/tcp)
HOP RTT ADDRESS
1 ... 30
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 92.20 seconds


Scan Tools Profile Help
Target: vit.ac.in
Profile:
Scan
Cancel
Command: nmap -p 50-85 vit.ac.in
Hosts
Services
Host
vit.ac.in (136.233.9.13)
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p 50-85 vit.ac.in
Details
Starting Nmap 7.92 (https://nmap.org) at 2022-03-25 01:19 IST
Nmap scan report for vit.ac.in (136.233.9.13)
Host is up (0.11s latency).
rDNS record for 136.233.9.13: 136.233.9.13.static.jio.com
Not shown: 34 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp filtered domain
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 3.56 seconds
Filter Hosts


Scan Tools Profile Help
Target: vit.ac.in
Profile:
Scan
Cancel
Command: nmap -p ftp,http* vit.ac.in
Hosts
Services
Host
vit.ac.in (136.233.9.13)
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p ftp,http* vit.ac.in
Details
Starting Nmap 7.92 (https://nmap.org) at 2022-03-25 01:24 IST
Nmap scan report for vit.ac.in (136.233.9.13)
Host is up (0.15s latency).
rDNS record for 136.233.9.13: 136.233.9.13.static.jio.com
PORT STATE SERVICE
21/tcp closed ftp
80/tcp open http
280/tcp closed http-mgmt
443/tcp open https
591/tcp closed http-alt
593/tcp closed http-rpc-epmap
4180/tcp closed httpx
8000/tcp closed http-alt
8008/tcp closed http
8080/tcp closed http-proxy
8443/tcp closed https-alt
8990/tcp closed http-wmap
8991/tcp closed https-wmap
Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
Filter Hosts



Q2) Commands for Port Redirection and Tunneling using SSH

PROCEDURE:

I. On the system, open a terminal and change the working directory to

II. Using the cd.. command, navigate to the root directory. II. Using the command, install the open ssh server on the machine.

install openssl-server sudo apt-get

III. Now, run the command sudo service ssh start to start the server.

IV. We use the sudo command to test the ssh server's functionality.ssh status service

V. Now we'll use the to execute port redirection for localhost.kali@localhost ssh -L 127.0.0.1:80:8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8

VI. Finally, we'll use the to conduct port redirection for the remote host.kali@10.0.2.15 ssh -R 127.0.0.1:443:136.233.9.13:443

OUTPUT:

```
┌──(root㉿kali)-[~]
└─# sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
     Active: active (running) since Thu 2022-03-24 13:27:52 EDT; 2h 43min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 1167 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1168 (sshd)
      Tasks: 1 (limit: 2294)
     Memory: 2.2M
        CPU: 322ms
     CGroup: /system.slice/ssh.service
             └─1168 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Mar 24 13:29:50 kali sshd[1187]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=::1  user=root
Mar 24 13:29:52 kali sshd[1187]: Failed password for root from ::1 port 51094 ssh2
Mar 24 13:30:00 kali sshd[1187]: Failed password for root from ::1 port 51094 ssh2
Mar 24 13:30:08 kali sshd[1187]: Failed password for root from ::1 port 51094 ssh2
Mar 24 13:30:10 kali sshd[1187]: Connection closed by authenticating user root ::1 port 51094 [preauth]
Mar 24 13:30:10 kali sshd[1187]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=::1  user=root
Mar 24 13:30:50 kali sshd[1191]: Accepted password for kali from ::1 port 51096 ssh2
Mar 24 13:30:50 kali sshd[1191]: pam_unix(sshd:session): session opened for user kali(uid=1000) by (uid=0)
Mar 24 13:38:00 kali sshd[1266]: Accepted password for kali from 10.0.2.15 port 51608 ssh2
Mar 24 13:38:00 kali sshd[1266]: pam_unix(sshd:session): session opened for user kali(uid=1000) by (uid=0)
```

```
┌──(root㉿kali)-[~]
└─# ssh -L 127.0.0.1:80:8.8.8.8:80 kali@localhost
kali@localhost's password:
Linux kali 5.10.0-kali9-amd64 #1 SMP Debian 5.10.46-4kali1 (2021-08-09) 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: Thu Mar 24 13:38:00 2022 from 10.0.2.15
┌──(Message from Kali developers)
│
│  We have kept /usr/bin/python pointing to Python 2 for backwards
│  compatibility. Learn how to change this and avoid this message:
│  ⇒ https://www.kali.org/docs/general-use/python3-transition/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
```

```
┌──(kali㉿kali)-[~]
└─$ ssh -R 127.0.0.1:443:136.233.9.13:443 kali@10.0.2.15
kali@10.0.2.15's password:
Linux kali 5.10.0-kali9-amd64 #1 SMP Debian 5.10.46-4kali1 (2021-08-09) 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: Thu Mar 24 16:18:00 2022 from ::1
┌──(Message from Kali developers)
│
│  We have kept /usr/bin/python pointing to Python 2 for backwards
│  compatibility. Learn how to change this and avoid this message:
│  ⇒ https://www.kali.org/docs/general-use/python3-transition/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
```