IT APP. SEC. LAB FILE

To- Dr. Gopal Rawat

Name- Dhairya Jain
Sap ID- 500105432
Batch- CSF-B1

Aim- *Wireshark Installation & Configuration*, SSH, Telnet

To do the following:

- Install Wireshark
- Perform packet capturing and log the reports

Metasploitable ip address:

```
msfadmin@metasploitable:~$  ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:78:f6:e4
          inet addr:192.168.0.100  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe78:f6e4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4644 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3519 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:358054 (349.6 KB)  TX bytes:598653 (584.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:16436  Metric:1
          RX packets:197 errors:0 dropped:0 overruns:0 frame:0
          TX packets:197 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:70953 (69.2 KB)  TX bytes:70953 (69.2 KB)
```

Preforming ssh attack on metasploitable

```
┌──(root㉿kali)-[/home/dhairya]
└─# ssh -oHostKeyAlgorithms=+ssh-dss msfadmin@192.168.0.100
msfadmin@192.168.0.100's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Thu Feb  1 00:14:05 2024 from 192.168.0.117
msfadmin@metasploitable:~$
```

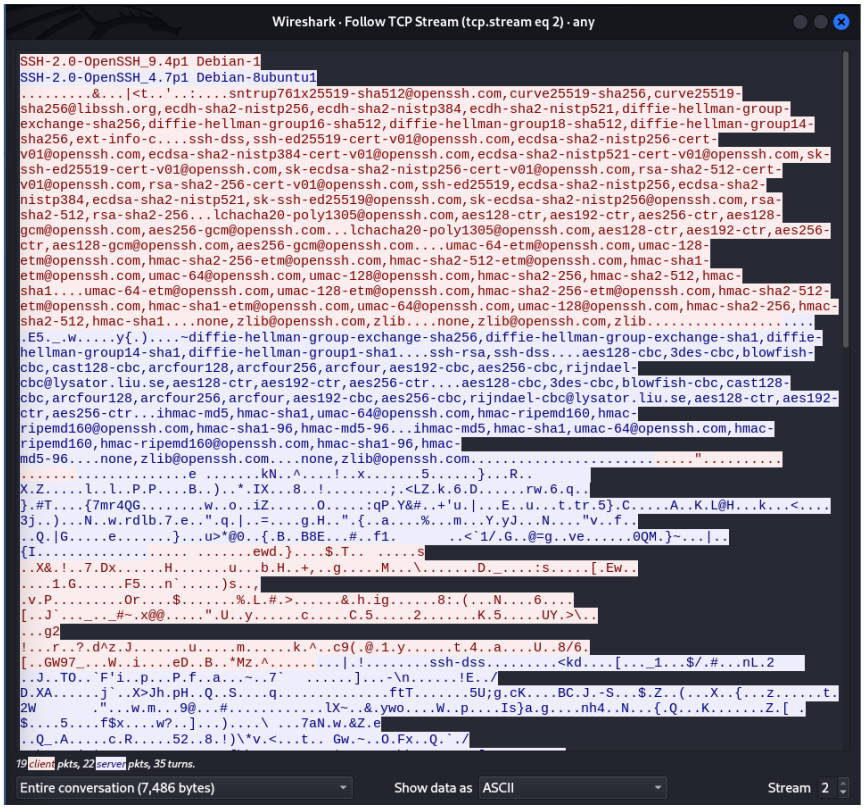
Capturing ssh packets in wire shark

*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssh

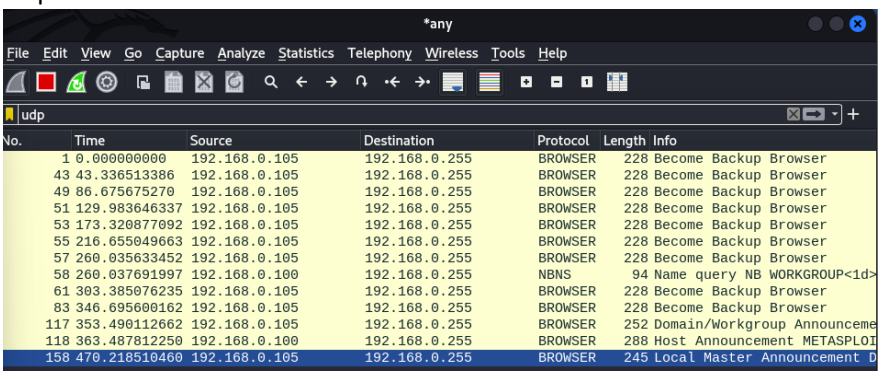
No.	Time	Source	Destination	Protocol	Length	Info
5	11.895504349	192.168.0.117	192.168.0.100	SSHv2	100	Client: Protocol (SSH-2.0-Op
7	11.903027115	192.168.0.100	192.168.0.117	SSHv2	106	Server: Protocol (SSH-2.0-Op
9	11.903909375	192.168.0.117	192.168.0.100	SSHv2	1580	Client: Key Exchange Init
10	11.904590067	192.168.0.100	192.168.0.117	SSHv2	852	Server: Key Exchange Init
12	11.906201846	192.168.0.117	192.168.0.100	SSHv2	92	Client: Diffie-Hellman Group
13	11.910279614	192.168.0.100	192.168.0.117	SSHv2	476	Server: Diffie-Hellman Group
14	11.913366684	192.168.0.117	192.168.0.100	SSHv2	468	Client: Diffie-Hellman Group
15	11.929452125	192.168.0.100	192.168.0.117	SSHv2	980	Server: Diffie-Hellman Group
16	11.934868666	192.168.0.117	192.168.0.100	SSHv2	84	Client: New Keys
18	11.969354288	192.168.0.117	192.168.0.100	SSHv2	108	Client: Encrypted packet (le
20	11.972299388	192.168.0.100	192.168.0.117	SSHv2	108	Server: Encrypted packet (le
21	11.972830155	192.168.0.117	192.168.0.100	SSHv2	124	Client: Encrypted packet (le
24	12.022168905	192.168.0.100	192.168.0.117	SSHv2	124	Server: Encrypted packet (le
26	20.987946794	192.168.0.117	192.168.0.100	SSHv2	204	Client: Encrypted packet (le
28	20.990351211	192.168.0.100	192.168.0.117	SSHv2	92	Server: Encrypted packet (le
30	20.991532871	192.168.0.117	192.168.0.100	SSHv2	124	Client: Encrypted packet (le
31	21.001043150	192.168.0.100	192.168.0.117	SSHv2	108	Server: Encrypted packet (le
32	21.001631548	192.168.0.117	192.168.0.100	SSHv2	508	Client: Encrypted packet (le
33	21.006475287	192.168.0.100	192.168.0.117	SSHv2	156	Server: Encrypted packet (le
34	21.007245212	192.168.0.100	192.168.0.117	SSHv2	604	Server: Encrypted packet (le
36	21.015601427	192.168.0.100	192.168.0.117	SSHv2	124	Server: Encrypted packet (le
40	32.173436534	192.168.0.117	192.168.0.100	SSHv2	124	Client: Encrypted packet (le
41	32.175707775	192.168.0.100	192.168.0.117	SSHv2	204	Server: Encrypted packet (le



Tcp

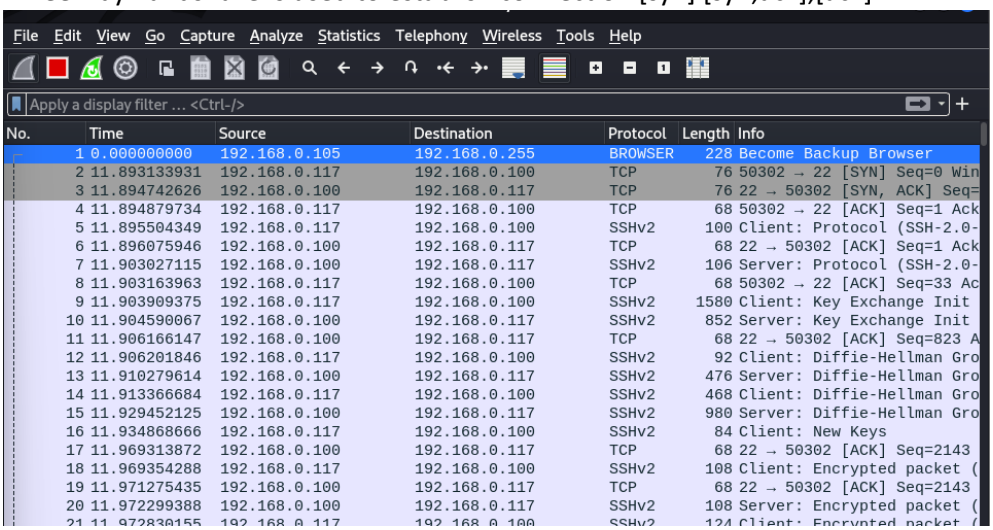
No.	Time	Source	Destination	Protocol	Length	Info
2	11.893133931	192.168.0.117	192.168.0.100	TCP	76	50302 → 22 [SYN] Seq=0 Win=
3	11.894742626	192.168.0.100	192.168.0.117	TCP	76	22 → 50302 [SYN, ACK] Seq=0
4	11.894879734	192.168.0.117	192.168.0.100	TCP	68	50302 → 22 [ACK] Seq=1 Ack=
5	11.895504349	192.168.0.117	192.168.0.100	SSHv2	100	Client: Protocol (SSH-2.0-O
6	11.896075946	192.168.0.100	192.168.0.117	TCP	68	22 → 50302 [ACK] Seq=1 Ack=
7	11.903027115	192.168.0.100	192.168.0.117	SSHv2	106	Server: Protocol (SSH-2.0-O
8	11.903163963	192.168.0.117	192.168.0.100	TCP	68	50302 → 22 [ACK] Seq=33 Ack
9	11.903909375	192.168.0.117	192.168.0.100	SSHv2	1580	Client: Key Exchange Init
10	11.904590067	192.168.0.100	192.168.0.117	SSHv2	852	Server: Key Exchange Init
11	11.906166147	192.168.0.100	192.168.0.117	TCP	68	22 → 50302 [ACK] Seq=823 Ac
12	11.906201846	192.168.0.117	192.168.0.100	SSHv2	92	Client: Diffie-Hellman Grou
13	11.910279614	192.168.0.100	192.168.0.117	SSHv2	476	Server: Diffie-Hellman Grou
14	11.913366684	192.168.0.117	192.168.0.100	SSHv2	468	Client: Diffie-Hellman Grou
15	11.929452125	192.168.0.100	192.168.0.117	SSHv2	980	Server: Diffie-Hellman Grou
16	11.934868666	192.168.0.117	192.168.0.100	SSHv2	84	Client: New Keys
17	11.969313872	192.168.0.100	192.168.0.117	TCP	68	22 → 50302 [ACK] Seq=2143 A
18	11.969354288	192.168.0.117	192.168.0.100	SSHv2	108	Client: Encrypted packet (l
19	11.971275435	192.168.0.100	192.168.0.117	TCP	68	22 → 50302 [ACK] Seq=2143 A
20	11.972299388	192.168.0.100	192.168.0.117	SSHv2	108	Server: Encrypted packet (l
21	11.972830155	192.168.0.117	192.168.0.100	SSHv2	124	Client: Encrypted packet (l
23	12.008821348	192.168.0.100	192.168.0.117	TCP	68	22 → 50302 [ACK] Seq=2183 A
24	12.022168905	192.168.0.100	192.168.0.117	SSHv2	124	Server: Encrypted packet (l
25	12.067256937	192.168.0.117	192.168.0.100	TCP	68	50302 → 22 [ACK] Seq=2081 A
26	20.987946794	192.168.0.117	192.168.0.100	SSHv2	204	Client: Encrypted packet (l
27	20.989293762	192.168.0.100	192.168.0.117	TCP	68	22 → 50302 [ACK] Seq=2239 A
28	20.990351211	192.168.0.100	192.168.0.117	SSHv2	92	Server: Encrypted packet (l
29	20.990384187	192.168.0.117	192.168.0.100	TCP	68	50302 → 22 [ACK] Seq=2217 A
30	20.991532871	192.168.0.117	192.168.0.100	SSHv2	124	Client: Encrypted packet (l
31	21.001043150	192.168.0.100	192.168.0.117	SSHv2	108	Server: Encrypted packet (l
32	21.001631548	192.168.0.117	192.168.0.100	SSHv2	508	Client: Encrypted packet (l
33	21.006475287	192.168.0.100	192.168.0.117	SSHv2	156	Server: Encrypted packet (l

Udp



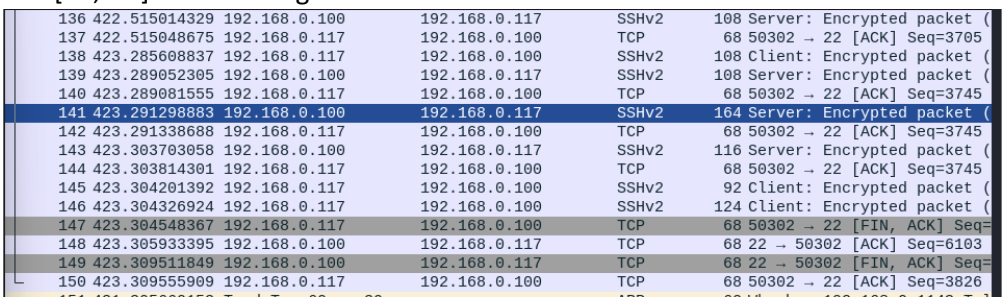
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
43	43.336513386	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
49	86.675675270	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
51	129.983646337	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
53	173.320877092	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
55	216.655049663	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
57	260.035633452	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
58	260.037691997	192.168.0.100	192.168.0.255	NBNS	94	Name query NB WORKGROUP<1d>
61	303.385076235	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
83	346.695600162	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
117	353.490112662	192.168.0.105	192.168.0.255	BROWSER	252	Domain/Workgroup Announceme
118	363.487812250	192.168.0.100	192.168.0.255	BROWSER	288	Host Announcement METASPLOI
158	470.218510460	192.168.0.105	192.168.0.255	BROWSER	245	Local Master Announcement D

Three way handshake is used to establish connection [syn] [syn,ack],[ack]



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.105	192.168.0.255	BROWSER	228	Become Backup Browser
2	11.893133931	192.168.0.117	192.168.0.100	TCP	76	50302 → 22 [SYN] Seq=0 Win
3	11.894742626	192.168.0.100	192.168.0.117	TCP	76	22 → 50302 [SYN, ACK] Seq=
4	11.894879734	192.168.0.117	192.168.0.100	TCP	68	50302 → 22 [ACK] Seq=1 Ack
5	11.895504349	192.168.0.117	192.168.0.100	SSHv2	100	Client: Protocol (SSH-2.0-
6	11.896075946	192.168.0.100	192.168.0.117	TCP	68	22 → 50302 [ACK] Seq=1 Ack
7	11.903027115	192.168.0.100	192.168.0.117	SSHv2	106	Server: Protocol (SSH-2.0-
8	11.903163963	192.168.0.117	192.168.0.100	TCP	68	50302 → 22 [ACK] Seq=33 Ac
9	11.903909375	192.168.0.117	192.168.0.100	SSHv2	1580	Client: Key Exchange Init
10	11.904590067	192.168.0.100	192.168.0.117	SSHv2	852	Server: Key Exchange Init
11	11.906166147	192.168.0.100	192.168.0.117	TCP	68	22 → 50302 [ACK] Seq=823 A
12	11.906201846	192.168.0.117	192.168.0.100	SSHv2	92	Client: Diffie-Hellman Gro
13	11.910279614	192.168.0.100	192.168.0.117	SSHv2	476	Server: Diffie-Hellman Gro
14	11.913366684	192.168.0.117	192.168.0.100	SSHv2	468	Client: Diffie-Hellman Gro
15	11.929452125	192.168.0.100	192.168.0.117	SSHv2	980	Server: Diffie-Hellman Gro
16	11.934868666	192.168.0.117	192.168.0.100	SSHv2	84	Client: New Keys
17	11.969313872	192.168.0.100	192.168.0.117	TCP	68	22 → 50302 [ACK] Seq=2143
18	11.969354288	192.168.0.117	192.168.0.100	SSHv2	108	Client: Encrypted packet (
19	11.971275435	192.168.0.100	192.168.0.117	TCP	68	22 → 50302 [ACK] Seq=2143
20	11.972299388	192.168.0.100	192.168.0.117	SSHv2	108	Server: Encrypted packet (

Got [fin,ack] while closing connection



136	422.515014329	192.168.0.100	192.168.0.117	SSHv2	108	Server: Encrypted packet (
137	422.515048675	192.168.0.117	192.168.0.100	TCP	68	50302 → 22 [ACK] Seq=3705
138	423.285608837	192.168.0.117	192.168.0.100	SSHv2	108	Client: Encrypted packet (
139	423.289052305	192.168.0.100	192.168.0.117	SSHv2	108	Server: Encrypted packet (
140	423.289081555	192.168.0.117	192.168.0.100	TCP	68	50302 → 22 [ACK] Seq=3745
141	423.291298883	192.168.0.100	192.168.0.117	SSHv2	164	Server: Encrypted packet (
142	423.291338688	192.168.0.117	192.168.0.100	TCP	68	50302 → 22 [ACK] Seq=3745
143	423.303703058	192.168.0.100	192.168.0.117	SSHv2	116	Server: Encrypted packet (
144	423.303814301	192.168.0.117	192.168.0.100	TCP	68	50302 → 22 [ACK] Seq=3745
145	423.304201392	192.168.0.117	192.168.0.100	SSHv2	92	Client: Encrypted packet (
146	423.304326924	192.168.0.117	192.168.0.100	SSHv2	124	Client: Encrypted packet (
147	423.304548367	192.168.0.117	192.168.0.100	TCP	68	50302 → 22 [FIN, ACK] Seq=
148	423.305933395	192.168.0.100	192.168.0.117	TCP	68	22 → 50302 [ACK] Seq=6103
149	423.309511849	192.168.0.100	192.168.0.117	TCP	68	22 → 50302 [FIN, ACK] Seq=
150	423.309555909	192.168.0.117	192.168.0.100	TCP	68	50302 → 22 [ACK] Seq=3826

telnet:

```
┌──(root㉿kali)-[/home/dhairya]
└─# telnet 192.168.0.100
Trying 192.168.0.100...
Connected to 192.168.0.100.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

telnet

No.	Time	Source	Destination	Protocol	Length	Info
24	18.655407230	192.168.0.117	192.168.0.100	TELNET	101	Telnet Data ...
34	28.624662952	192.168.0.100	192.168.0.117	TELNET	80	Telnet Data ...
36	28.626705550	192.168.0.100	192.168.0.117	TELNET	113	Telnet Data ...
38	28.632034972	192.168.0.117	192.168.0.100	TELNET	147	Telnet Data ...
40	28.636518907	192.168.0.100	192.168.0.117	TELNET	71	Telnet Data ...
41	28.636899689	192.168.0.117	192.168.0.100	TELNET	71	Telnet Data ...
42	28.641744286	192.168.0.100	192.168.0.117	TELNET	71	Telnet Data ...
43	28.642493433	192.168.0.117	192.168.0.100	TELNET	71	Telnet Data ...
44	28.645480756	192.168.0.100	192.168.0.117	TELNET	666	Telnet Data ...
46	28.687688502	192.168.0.100	192.168.0.117	TELNET	90	Telnet Data ...
147	88.647034712	192.168.0.100	192.168.0.117	TELNET	105	Telnet Data ...
183	215.453942452	192.168.0.117	192.168.0.100	TELNET	101	Telnet Data ...
192	225.439584121	192.168.0.100	192.168.0.117	TELNET	80	Telnet Data ...
194	225.441373603	192.168.0.100	192.168.0.117	TELNET	113	Telnet Data ...
196	225.442506475	192.168.0.117	192.168.0.100	TELNET	147	Telnet Data ...
198	225.445587637	192.168.0.100	192.168.0.117	TELNET	71	Telnet Data ...
199	225.445834235	192.168.0.117	192.168.0.100	TELNET	71	Telnet Data ...
200	225.448217560	192.168.0.100	192.168.0.117	TELNET	71	Telnet Data ...
201	225.448476235	192.168.0.117	192.168.0.100	TELNET	71	Telnet Data ...
202	225.451115604	192.168.0.100	192.168.0.117	TELNET	666	Telnet Data ...
204	225.496331799	192.168.0.100	192.168.0.117	TELNET	90	Telnet Data ...

```
▸ Frame 24: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 192.168.0.117, Dst: 192.168.0.100
```

Telnet: Protocol | Packets: 211 · Displayed: 21 (10.0%) | Profile: Default

Wireshark · Follow TCP Stream (tcp.stream eq 0) · any

```
..&..&........... ..!.."..'.....#..... ..#..'..&..&........!.."..... .....#.....'.............G......
.38400,38400....#.kali:1....'..DISPLAY.kali:1......XTERM-256COLOR.............
_
_ __ ___  ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
Login timed out after 60 seconds.
```