Telent

Install telnet :

[root]

```
apt-get install telnetd
```

```
apt-get install openbsd-inetd
```

```
service openbsd-inetd start
```

check port 23 is listening

```
netstat -ano | grep LISTEN
```

Install packet capture:

```
apt-get install tshark
```

Start Packet Capture:

Collect the IP address of this machine.

```
tshark -i any -w telnet_capture.pcap port 23
```

From Another machine

```
telnet <Collected IP Address>
```

Go back to Telnet Server and do `ctrl+c` to stop the packet capture.

```
Python3
```

```
>>> import pyshark
>>> cap = pyshark.FileCapture('/opt/telnet_capture.pcap')
>>> cap
>>> print (cap[0])
```

Refer : Output for Telnet

For SSH

check port 22 is listening

```
netstat -ano | grep LISTEN
```

```
tshark -i any -w telnet_capture.pcap port 22
```

From Another machine

```
ssh root@<Collected IP Address>
```

type password

Go back to SSH Server and do `ctrl+c` to stop the packet capture.

```
Python3
```

```
>>> import pyshark
>>> cap = pyshark.FileCapture('/opt/telnet_capture.pcap')
>>> cap
>>> print (cap[0])
```

Refer : Output for SSH

Output for Telnet

```
------------------------

Packet (Length: 68)
Layer SLL
:       Packet type: Unicast to us (0)
        Link-layer address type: Ethernet (1)
        Link-layer address length: 6
        Source: 00:50:56:c0:00:08
        Unused: 0000
        Protocol: IPv4 (0x0800)
Layer IP
:       0100 .... = Version: 4
        .... 0101 = Header Length: 20 bytes (5)
        Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
        Total Length: 52
        Identification: 0xef70 (61296)
        010. .... = Flags: 0x2, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 128
        Protocol: TCP (6)
        Header Checksum: 0x7d80 [validation disabled]
        Header checksum status: Unverified
        Source Address: 192.168.6.1
        Destination Address: 192.168.6.129
Layer TCP
:       Source Port: 53604
        Destination Port: 23
        Stream index: 0
        Conversation completeness: Incomplete (0)
        ..0. .... = RST: Absent
        ...0 .... = FIN: Absent
        .... 0... = Data: Absent
        .... .0.. = ACK: Absent
        .... ..0. = SYN-ACK: Absent
        .... ...0 = SYN: Absent
        Completeness Flags: [ Null ]
        TCP Segment Len: 0
        Sequence Number: 0    (relative sequence number)
        Sequence Number (raw): 1165935044
        Next Sequence Number: 1    (relative sequence number)
        Acknowledgment Number: 0
        Acknowledgment number (raw): 0
        1000 .... = Header Length: 32 bytes (8)
        Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Accurate ECN: Not set
        .... 0... .... = Congestion Window Reduced: Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
```

```
       .... .... ..1. = Syn: Set
       Expert Info (Chat/Sequence): Connection establish request (SYN): server port 23
       Connection establish request (SYN): server port 23
       Severity level: Chat
       Group: Sequence
       .... .... ...0 = Fin: Not set
       TCP Flags: ··········S·
       Window: 64240
       Calculated window size: 64240
       Checksum: 0x0d8e [unverified]
       Checksum Status: Unverified
       Urgent Pointer: 0
       Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale,
No-Operation (NOP), No-Operation (NOP), SACK permitted
       TCP Option - Maximum segment size: 1460 bytes
       Kind: Maximum Segment Size (2)
       Length: 4
       MSS Value: 1460
       TCP Option - No-Operation (NOP)
       TCP Option - Window scale: 8 (multiply by 256)
       Shift count: 8
       Multiplier: 256
       TCP Option - SACK permitted
       Timestamps
       Time since first frame in this TCP stream: 0.000000000 seconds
       Time since previous frame in this TCP stream: 0.000000000 seconds
       Kind: No-Operation (1)
       Kind: Window Scale (3)
       Kind: No-Operation (1)
       Kind: No-Operation (1)
       Kind: SACK Permitted (4)
       Length: 3
       Length: 2
       TCP Option - No-Operation (NOP)
       TCP Option - No-Operation (NOP)
```

Output for SSH

```
Packet (Length: 68)
Layer SLL
:       Packet type: Unicast to us (0)
        Link-layer address type: Ethernet (1)
        Link-layer address length: 6
        Source: 00:50:56:c0:00:08
        Unused: 0000
        Protocol: IPv4 (0x0800)
Layer IP
:       0100 .... = Version: 4
        .... 0101 = Header Length: 20 bytes (5)
        Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
        Total Length: 52
        Identification: 0xef9a (61338)
        010. .... = Flags: 0x2, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 128
        Protocol: TCP (6)
        Header Checksum: 0x7d56 [validation disabled]
        Header checksum status: Unverified
        Source Address: 192.168.6.1
        Destination Address: 192.168.6.129
Layer TCP
:       Source Port: 54124
        Destination Port: 22
        Stream index: 0
        Conversation completeness: Incomplete (0)
        ..0. .... = RST: Absent
        ...0 .... = FIN: Absent
        .... 0... = Data: Absent
        .... .0.. = ACK: Absent
        .... ..0. = SYN-ACK: Absent
        .... ...0 = SYN: Absent
        Completeness Flags: [ Null ]
        TCP Segment Len: 0
        Sequence Number: 0    (relative sequence number)
        Sequence Number (raw): 2781456290
        Next Sequence Number: 1    (relative sequence number)
        Acknowledgment Number: 0
        Acknowledgment number (raw): 0
        1000 .... = Header Length: 32 bytes (8)
        Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Accurate ECN: Not set
        .... 0... .... = Congestion Window Reduced: Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        Expert Info (Chat/Sequence): Connection establish request (SYN): server port 22
        Connection establish request (SYN): server port 22
        Severity level: Chat
        Group: Sequence
        .... .... ...0 = Fin: Not set
        TCP Flags: ··········S·
        Window: 64240
        Calculated window size: 64240
        Checksum: 0xc55d [unverified]
        Checksum Status: Unverified
        Urgent Pointer: 0
        Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale,
No-Operation (NOP), No-Operation (NOP), SACK permitted
        TCP Option - Maximum segment size: 1460 bytes
        Kind: Maximum Segment Size (2)
        Length: 4
        MSS Value: 1460
        TCP Option - No-Operation (NOP)
        TCP Option - Window scale: 8 (multiply by 256)
        Shift count: 8
        Multiplier: 256
        TCP Option - SACK permitted
        Timestamps
        Time since first frame in this TCP stream: 0.000000000 seconds
        Time since previous frame in this TCP stream: 0.000000000 seconds
        Kind: No-Operation (1)
        Kind: Window Scale (3)
        Kind: No-Operation (1)
        Kind: No-Operation (1)
        Kind: SACK Permitted (4)
        Length: 3
        Length: 2
        TCP Option - No-Operation (NOP)
        TCP Option - No-Operation (NOP)
```