

EXPERIMENT NO. 9

AIM: Analyzing network packet stream using tcpdump and wireshark. service tests using nc.

RESULT:

tcpdump:

tcpdump is a packet sniffing and packet analyzing tool for a System Administrator to troubleshoot connectivity issues in Linux. It is used to capture, filter, and analyze network traffic such as TCP/IP packets going through your system. It is many times used as a security tool as well. It saves the captured information in a pcap file, these pcap files can then be opened through Wireshark or through the command tool itself.

Installing tcpdump tool in Linux

Sudo apt install tcpdump

Working with tcpdump command

1. To capture the packets of current network interface

```
sudo tcpdump
```

This will capture the packets from the current interface of the network through which the system is connected to the internet.

2. To capture packets from a specific network interface

```
sudo tcpdump -i wlp2s0
```

This command will now capture the packets from wlp2s0 network interface.

- 3) To display all available interfaces

```
sudo tcpdump -D
```

wireshark:

Wireshark is a software tool used to monitor the network traffic through a network interface. It is the most widely used network monitoring tool today.

Wireshark is loved equally by system administrators, network engineers, network enthusiasts, network security professionals and black hat hackers. The extent of its popularity is such, that experience with Wireshark is considered as a valuable/essential trait in a computer networking related professional.

There are many reasons why Wireshark is so popular :

- ⑩ It has a great GUI as well as a conventional CLI(T Shark).
- ⑩ It offers network monitoring on almost all types of network standards (ethernet, wlan, Bluetooth etc)
- ⑩ It is open source with a large community of backers and developers.
- ⑩ All the necessary components for monitoring, analysing and documenting the network traffic are present. It is free to use.

Wireshark installation:

`sudo apt install wireshark` command is used to install wireshark in linux

Enter Y to continue

You can give appropriate option according to your need. After this the wireshark will be downloaded to the system

On launching Wireshark, you will see a screen like this:

The basic features of Wireshark are:

1) Packet Monitor: This segment visually shows the packets flowing inside the network. There are colour codes for each type of packets. The packets are shown

with following information :

1. Source address
2. Destination address
3. Packet type
4. Hex dump of the packet
5. Contents of the packet in text
6. Source port(if applicable)
7. Destination port(if applicable)

2) Import from a capture file:

This feature lets you import packets dump from a capture file to analyse further. There are many formats supported by Wireshark, some of them are:

- ⑩ pcapng
- ⑩ libpcap
- ⑩ Oracle snoop and atmsnoop
- ⑩ Finisar (previously Shomiti) Surveyor captures
- ⑩ Microsoft Network Monitor captures
- ⑩ Novell LANalyzer captures
- ⑩ AIX iptrace captures
- ⑩ Cinco Networks NetXray captures
- ⑩ Network Associates Windows-based Sniffer and Sniffer Pro captures
- ⑩ Network General/Network Associates DOS-based Sniffer (compressed or uncompressed) captures
- ⑩ AG Group/WildPackets/Savvius
EtherPeek/TokenPeek/AiroPeek/EtherHelp/PackageGrabber captures
- ⑩ RADCOM's WAN/LAN Analyzer captures
- ⑩ Network Instruments Observer version 9 captures
- ⑩ Lucent/Ascend router debug output
- ⑩ HP-UX's nettl

- ⑩ Toshiba's ISDN routers dump output
- ⑩ ISDN4BSD i4btrace utility
- ⑩ Traces from the EyeSDN USB S0
- ⑩ IPLog format from the Cisco Secure Intrusion Detection System
- pppd logs (pppdump format)
- ⑩ the output from VMS's TCPIPtrace/TCPtrace/UCX\$TRACE utilities
- ⑩ the text output from the DBS Etherwatch VMS utility
- ⑩ Visual Networks' Visual UpTime traffic capture
- ⑩ the output from CoSine L2 debug
- ⑩ the output from Accellent's 5Views LAN agents
- ⑩ Endace Measurement Systems' ERF format captures
- ⑩ Linux Bluez Bluetooth stack hcidump -w traces
- ⑩ Catapult DCT2000 .out files
- ⑩ Gammu generated text output from Nokia DCT3 phones in Netmonitor mode
- ⑩ IBM Series (OS/400) Comm traces (ASCII & UNICODE)
- ⑩ Juniper Netscreen snoop captures
- ⑩ Symbian OS btsnoop captures
- ⑩ Tamosoft CommView captures
- ⑩ Textronix K12xx 32bit .rf5 format captures
- ⑩ Textronix K12 text file format captures
- ⑩ Apple PacketLogger captures
- ⑩ Captures from Aethra Telecommunications' PC108 software

3) **Export to a capture file:** Wireshark lets you save the results as a capture file to continue working on them at later point of time. The supported formats are:

- ⑩ pcapng (*.pcapng)

- ⑩ libpcap, tcpdump and various other tools using tcpdump's capture format (*.pcap, *.cap, *.dmp)
- ⑩ Accellent 5Views (*.5vw)
- ⑩ HP-UX's nettl (*.TRC0, *.TRC1)
- ⑩ Microsoft Network Monitor – NetMon (*.cap)
- ⑩ Network Associates Sniffer – DOS (*.cap, *.enc, *.trc, *.fdc, *.syc)
- ⑩ Network Associates Sniffer – Windows (*.cap)
- ⑩ Network Instruments Observer version 9 (*.bfr)
- ⑩ Novell LANalyzer (*.tr1)
- ⑩ Oracle (previously Sun) snoop (*.snoop, *.cap)
- ⑩ Visual Networks Visual UpTime traffic (*.*)

Netcat:

Netcat (or nc in short) is a simple yet powerful **networking command-line tool** used for performing any operation in Linux related to TCP, UDP, or UNIX-domain sockets.

Netcat can be used for port scanning, port redirection, as a port listener (for incoming connections); it can also be used to open remote connections and so many other things. Besides, you can use it as a backdoor to gain access to a target server.

Installing netcat on linux:

```
sudo apt-get install netcat
```

Port scanning:

Netcat can be used for port scanning: to know **which ports are open** and running services on a target machine. It can scan a single or multiple or a range of open ports.

The `-z` option sets nc to simply scan for listening daemons, without actually sending any data to them. The `-v` option enables verbose mode and `-w` specifies a timeout for connection that can not be established.

Syntax:

```
nc -vz IP_address port
```

Connection timed out:

A *connection timed out* response indicates that your connection is not working, which could mean your firewall is blocking the port. Test the connection status by adding a rule that accepts connections on the required port.

Connection succeeded

If the initial connection succeeds, Netcat can connect to the service. Look at the connection in more detail.

Syntax:

```
nc -vt IP Address Port
```

Closing the connection

You can terminate the connection by either pressing Ctrl-C or type the service-specific quit command.