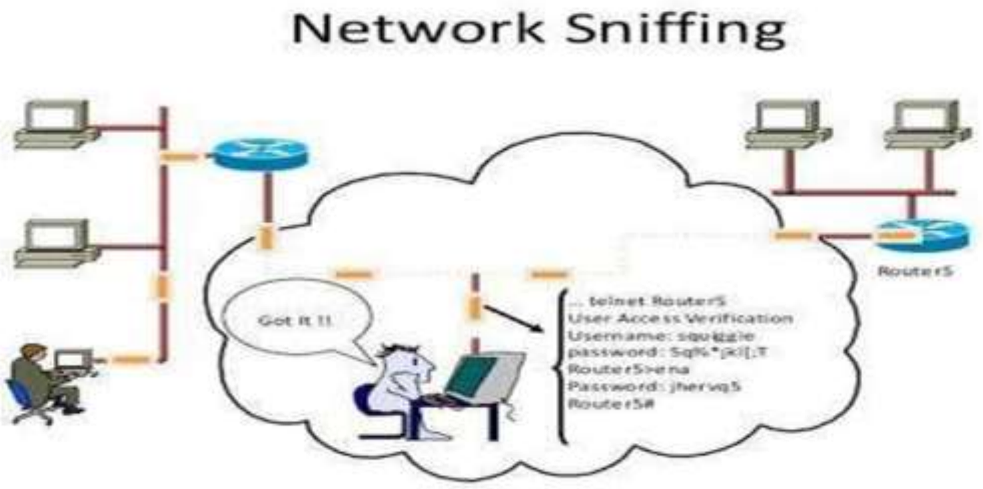
NETWORK SNIFFERS AND TOOLS IN CYBER SECURITY

[1]Rachana R. Buch, [2]Sachi N. Shah
[1]Assistant Professor, [2]Assistant Professor
[1]Department of Computer Engineering
[1]Atmiya University, Rajkot, India

Abstract:In the cyber world, there are numerous kinds of programmers which is utilized to hack username, passwords and personal details, account subtle elements, and touchy data about the client through their gadget or network. A procedure of catching, interpreting, and investigating network activity is called network sniffing. Network sniffers are same as a programmer which is gathered or assemble data from the Network i.e. IP address, MAC address, Hostname and so forth through which they can keep an eye on the network movement or they watch or gather a log of packets by packet sniffing. Network sniffers have utilized a few tools like Wireshark, Kismet, hping, TCPdump, and Windump for checking packets which are traverses the network.

Index Terms: **Cyber Security, Network sniffers, Packet Sniffers, Tools, Wireshark, hping, Kismet, TCPdump, and Windump.**

I. Introduction to Network Sniffers:



```
... telnet Router5
User Access Verification
Username: squiggle
password: Sq%*jk![;T
Router5>ena
Password: jhervq5
Router5#
```

fig.1 how network sniffer works

1.1 Network Sniffing:

The procedure of catching, decoding, and analyzing network movement is called network sniffing. [2]

Network Sniffing is a technique of observing each packet that crosses the network.

Network sniffing is a tool that can enable you to find network issues by enabling you to catch and view packet level data on your network it likewise screens or sniffs out the data flowing over computer network links in real time. [2]

A few sniffers work with TCP/IP packets yet more sophisticated tools can work with numerous other network protocols and at lower levels including Ethernet frames.[14]

1.2 Network Sniffer types:

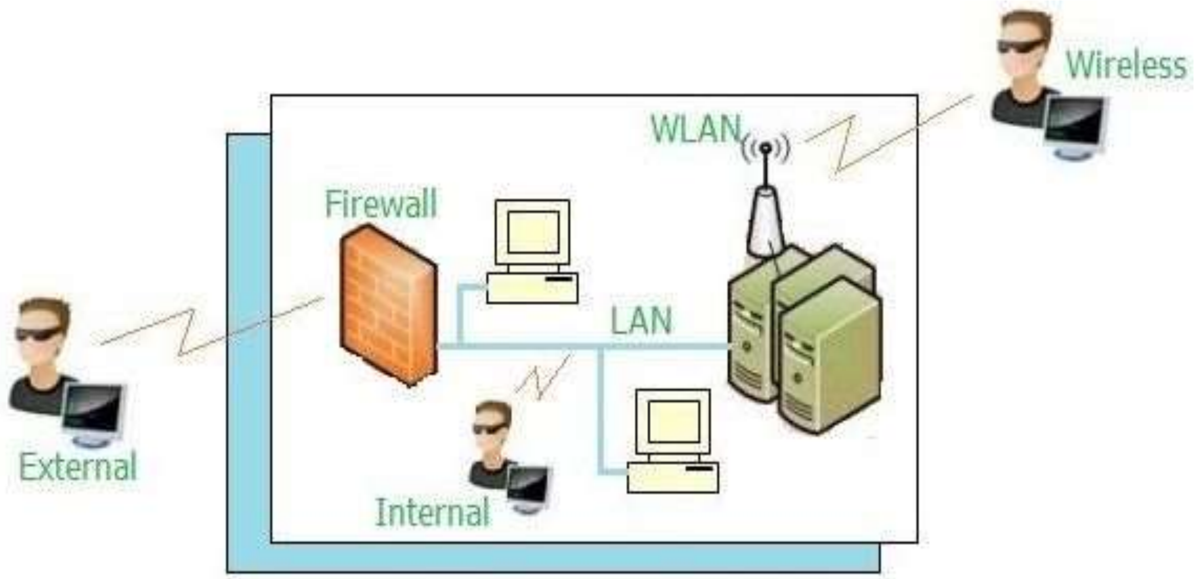


fig. 2 working of network sniffers and its working area

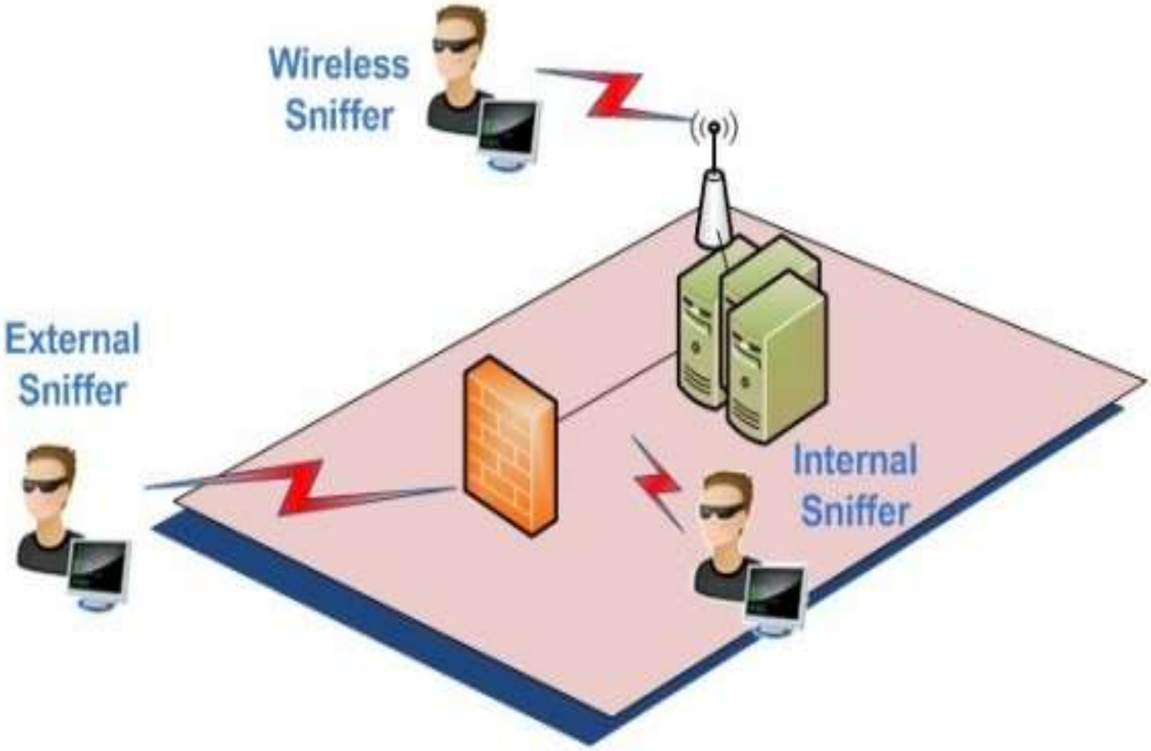


fig.3 types of network sniffers

1.3 What is network sniffing used for?

A typical use of network sniffer is to analyze network traffic and bandwidth utilization so that underlying troubles in the network can be identified.[11]

It analyses network issue and identifies network abuse by inward and outside clients additionally used to gain information for affecting network intrusion. [2]

It keeps an eye on other system clients and gathers touchy data, for example, log in details, individual subtle elements and make a report on network statistics. It filters suspect content from network traffic and verifies internal control system effectively, such as firewall, web filter, access control. [2]

1.4 Advantages of Network Sniffing:

- It captures packets and analyses packets and furthermore analyses the traffic of a network and makes a record.
- It decrypts packets and makes it in plain text or readable format. [2]
- It gathers relevant data like IP address, which protocol is used, hostname or server name and other sensitive data. [10]

1.5 Disadvantages of Network Sniffing:

✓ With positive uses, there are likewise some negative uses.

▪ Getting special and private data of exchange, like username, passwords, account which is the main reason behind most unlawful uses of sniffing tools. [3]

▪ A few sniffers can even change the targeted computer's data and harm the system. Recording email or text and resuming its content.

▪ Intruding on the security of a network or to gain higher level authority. [9]

II. Packet Sniffing:

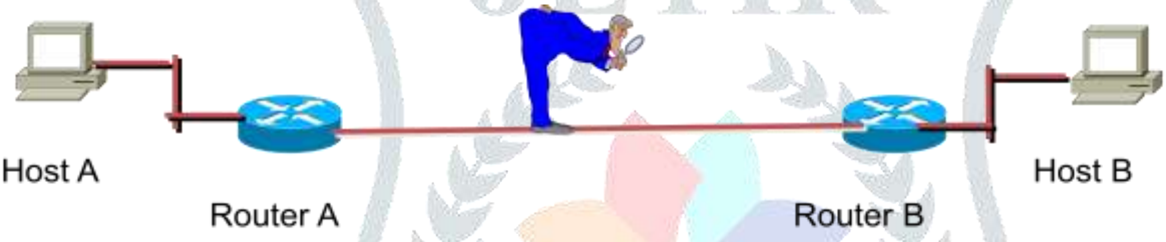


fig. 4 packet sniffing

Packet sniffing is a method of checking each packet that crosses the network. A network sniffer is also called as a Packet sniffer. [8]

A packet analyzer is a piece of software or hardware designed to intercept information as it is transmitted over a network and decode the information into a format that is readable for people. [2]

A packet sniffer is a software application that uses a network connector card in promiscuous mode to catch all network packets.

Wireless sniffers are packet analyzers particularly made for catching information on wireless networks. Wireless sniffers are commonly referred to as wireless packet sniffers or wireless network sniffers. [11] [14]

2.1 How does a Sniffer Work?

Sniffers also work differently depending on the type of network they are in.

1. **Shared Ethernet:**[18]In a Shared Ethernet environment, all hosts are associated with a similar transport and compete with each other for bandwidth. [3]

In such environment packets implied for one machine are received by all various machines. [18]

Therefore, when a machine comp 1 needs to converse with comp 2 in such an environment, it sends a packet on the network with the destination MAC address of comp 2 alongside its own source MAC address. [18]

All the computers on the shared Ethernet (comp 3 and comp 4) compare frame’s destination MAC address with their own. In the event that the two don't coordinate, the frame is quietly discarded. [2] [18]

A machine running a sniffer disrupts this rule and accepts all frames. Such a machine is said to have been put into promiscuous mode and can successfully tune in to all the traffic on the network. [18]

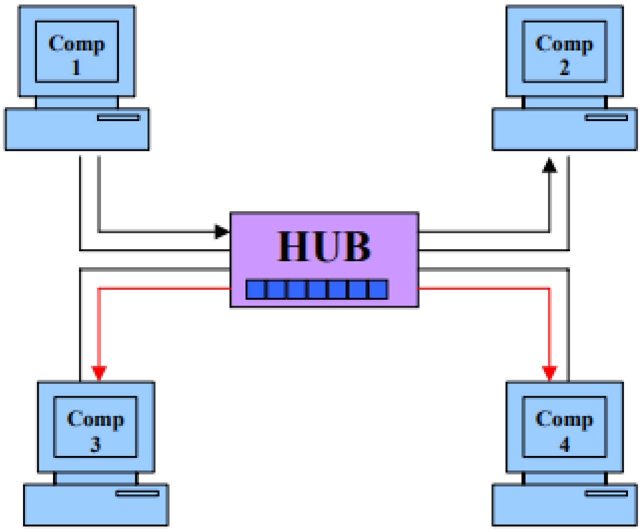


fig. 5 a shared ethernet network[18]

2. **Switched Ethernet:** [18]An Ethernet environment in which the hosts are connected to switch rather than a hub is called a Switched Ethernet.

The switch keeps up a table monitoring every computer's MAC addresses and the physical port on the switch to which that MAC address is connected and conveys packets destined for a specific machine correspondingly. [18]

The switch is an intelligent device that sends packets to the destined computer just and does not communicate it to every one of the machines on the network, as in the past case. [18]

These outcomes in better utilization of the available bandwidth and enhanced security.

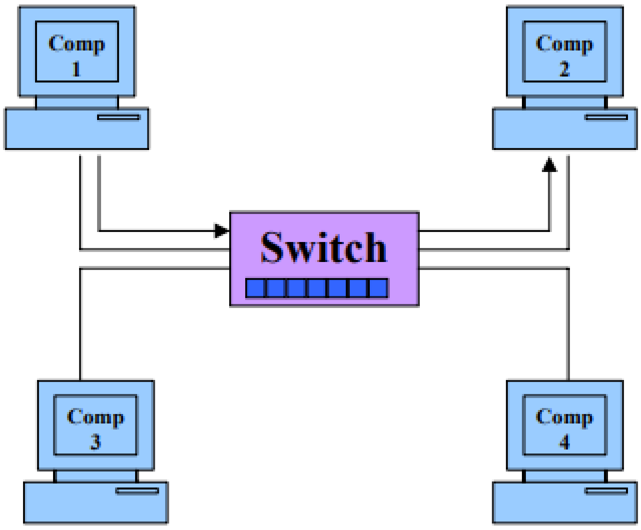


fig. 6 a switched network[18]

2.2 How can I detect a packet sniffer?

- **Ping method:** Most "packet sniffers" keep running on normal machines with a normal TCP/IP stack. This implies that if you send a request to these machines, they will react. The trick is to send a request to IP address of the machine, however not to its Ethernet adapter.[19]

- **ARP method:** In this technique, an attacker sends a fake ARP message to the local LAN. The objective of ARP spoofing is to hijack a system and an attacker wants to join his MAC address with the IP address of another host. The outcome is that any traffic implied for that IP address will be sent to the attacker. [19]

Now that you are familiar with ARP Spoofing, we will show you how we can implement it via Ettercap.[18] [19]

- **DNS method:** Many sniffing programs do automatic reverse-DNS lookups on the IP addresses they see. Thusly, a promiscuous mode can be identified by looking for the DNS traffic that it produces. This method can distinguish double homed machines and can work remotely.[19]

  This same technique works locally. Configure the detector in promiscuous mode itself, then send out IP datagrams to bad addresses and watch for the DNS lookups.

III. Packet Sniffer Mitigation:

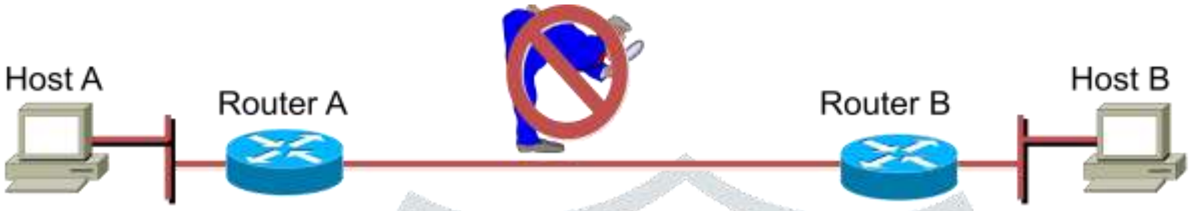


fig. 7 packet sniffer mitigation

The following techniques and tools can be used to reduce severity against the sniffers:

1. **Authentication:** Using strong authentication, such as one-time passwords or two-way authentication, is the first option for defense against packet sniffers. [11]
2. **Switched infrastructure:** Deploy a switched infrastructure to counter the use of packet sniffers in your environment. [11] [10]
3. **Anti-sniffer tools:** Use these tools to employ software and hardware designed to detect the use of sniffers on a network. [9]
4. **Cryptography:** The most effective method for countering packet sniffers does not prevent or detect packet sniffers, but rather renders them irrelevant. [8]

IV. Tools which are used in network sniffer:

4.1 Wireshark:

It is a GUI based option to tcpdump it otherwise called Network/Packet Protocol Analyzer Tool, it will attempt to catch network packets and tries to display that packet data as detailed as possible.[1] [12]

One of the best open source packet analyzer tool available today for UNIX and Windows.[1] [13]

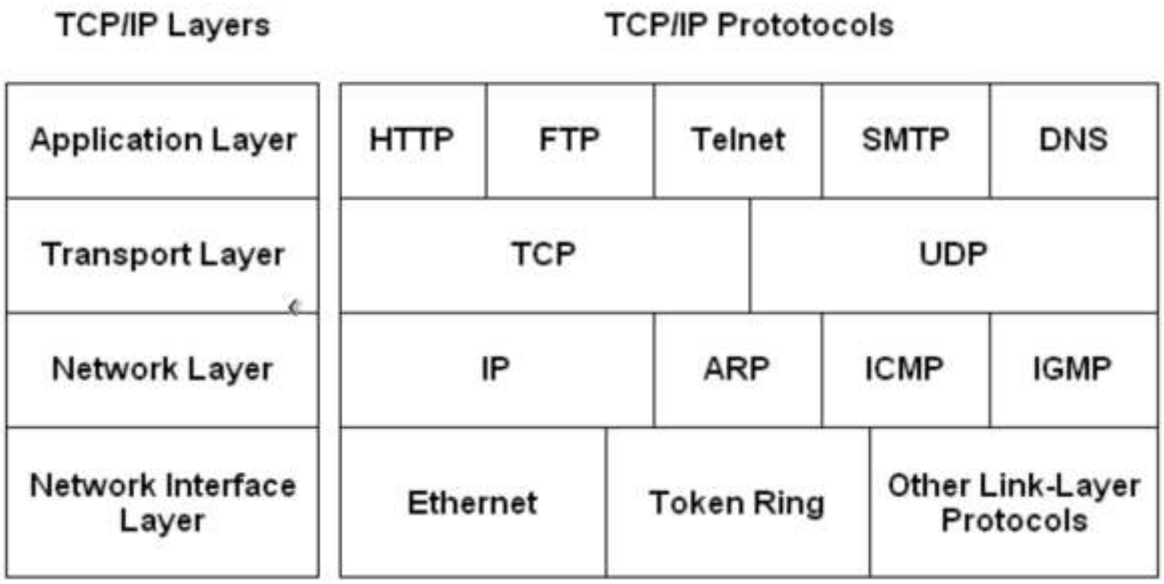
4.1.1 Features of Wireshark:

- Open source software which is available for UNIX and windows. [12]
- Live Capture from many network media and it saved that captured packet data with detailed protocol information. [1] [13]
- Import and export files of any other capture program.[1]
- Search and Filter packets on many criteria.
- Colorize packet display based on filters.[12] [1]

4.1.2 Some Intended Purposes:

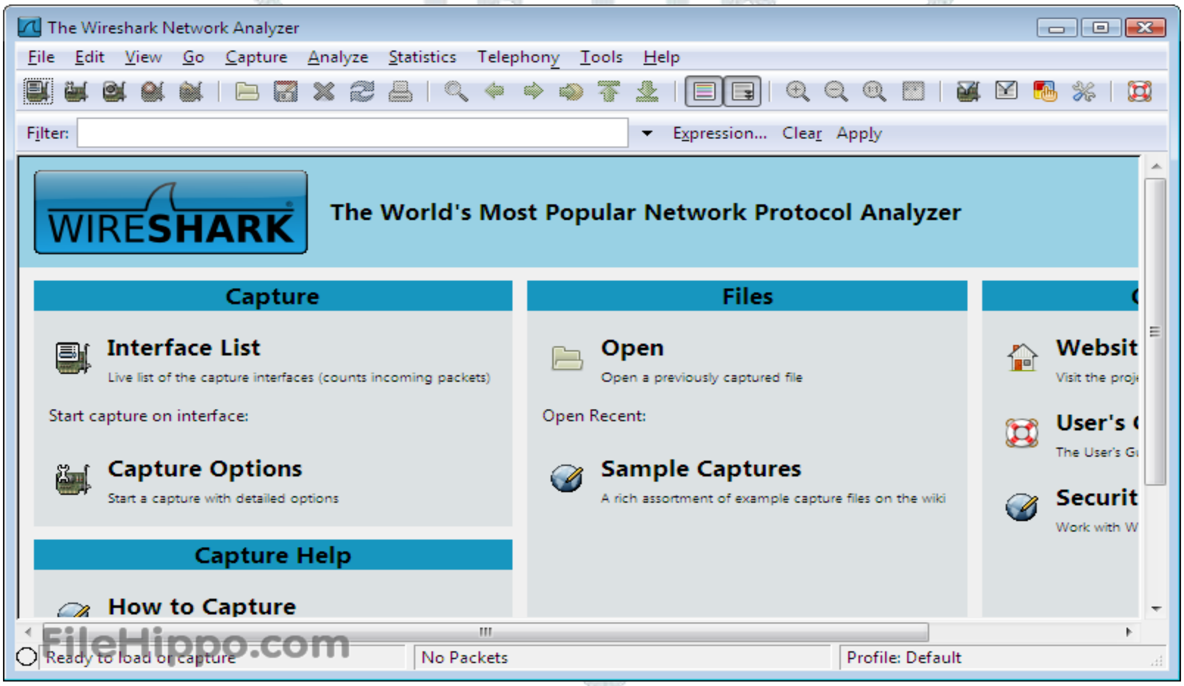
- Network Administrators use it to troubleshoot network problems.
- Network Security engineer uses it to examine network problem.
- People use it to learn network protocols and packet traffic over a network.[1] [2]
- Wireshark will not manipulate things on the network, it will only measure the things from the network.

4.1.3 List of Protocol Used:



TCP/IP Layers	TCP/IP Prototocols				
Application Layer	HTTP	FTP	Telnet	SMTP	DNS
Transport Layer	TCP		UDP		
Network Layer	IP		ARP	ICMP	IGMP
Network Interface Layer	Ethernet	Token Ring	Other Link-Layer Protocols		

fig. 8 list of protocols



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
WIRESHARK
Capture
Files
Capture Help
FileHippo.com

The World's Most Popular Network Protocol Analyzer

Interface List

Live list of the capture interfaces (counts incoming packets)

Start capture on interface:

Capture Options

Start a capture with detailed options

How to Capture

Open

Open a previously captured file

Open Recent:

Sample Captures

A rich assortment of example capture files on the wiki

Websit

Visit the proj

User's

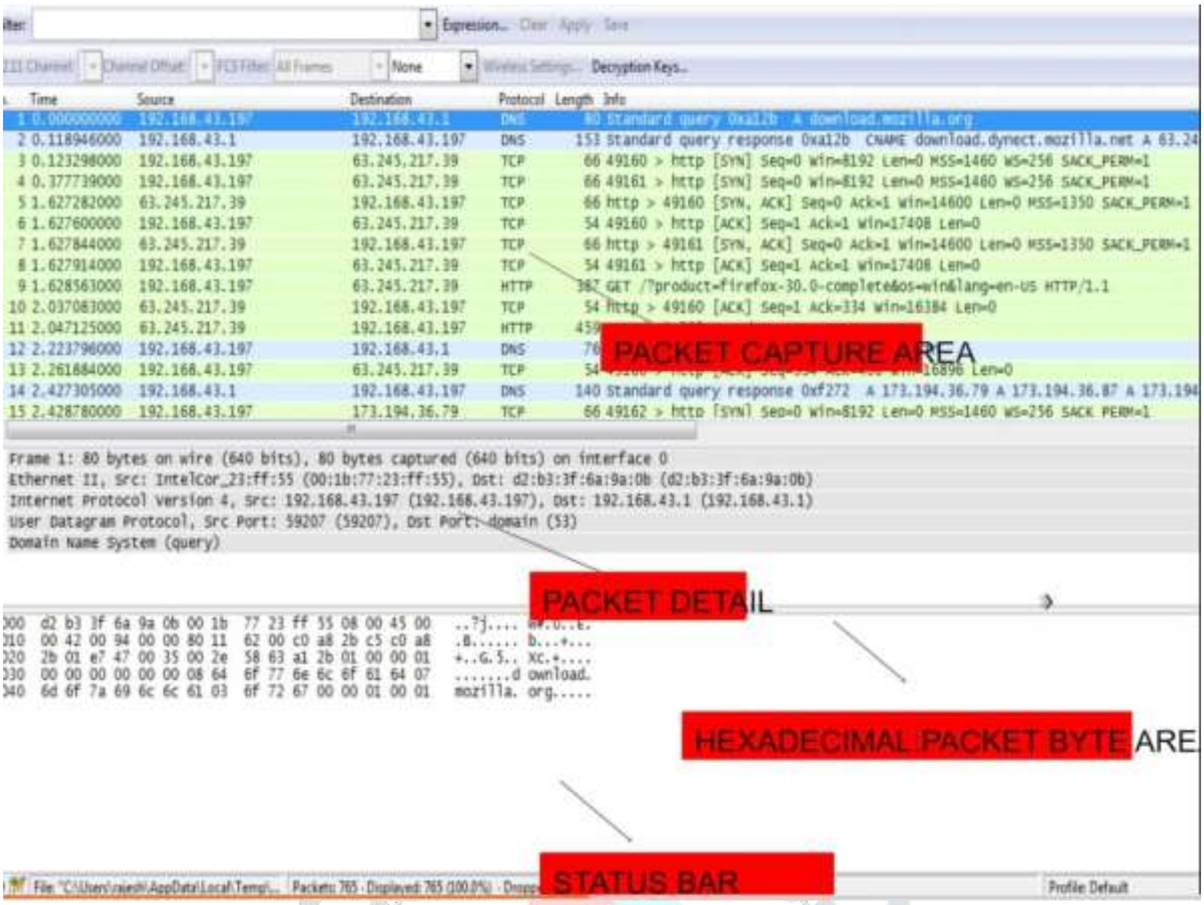
The User's G

Securit

Work with W

Ready to load or capture | No Packets | Profile: Default

fig. 9 main screens of wireshark[1]


Filter:
Expression... Clear Apply Save
Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...
PACKET CAPTURE AREA
PACKET DETAIL
HEXADECIMAL PACKET BYTE ARE
STATUS BAR
Profile: Default

```
.  Time         Source           Destination      Protocol Length Info
 1 0.000000000  192.168.43.197   192.168.43.1     DNS        80 Standard query 0xa12b  A download.mozilla.org
 2 0.118946000  192.168.43.1     192.168.43.197   DNS       153 Standard query response 0xa12b  CNAME download.dynect.mozilla.net A 63.24
 3 0.123298000  192.168.43.197   63.245.217.39    TCP        66 49160 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
 4 0.377739000  192.168.43.197   63.245.217.39    TCP        66 49161 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
 5 1.627282000  63.245.217.39    192.168.43.197   TCP        66 http > 49160 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1350 SACK_PERM=1
 6 1.627600000  192.168.43.197   63.245.217.39    TCP        54 49160 > http [ACK] Seq=1 Ack=1 Win=17408 Len=0
 7 1.627844000  63.245.217.39    192.168.43.197   TCP        66 http > 49161 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1350 SACK_PERM=1
 8 1.627914000  192.168.43.197   63.245.217.39    TCP        54 49161 > http [ACK] Seq=1 Ack=1 Win=17408 Len=0
 9 1.628563000  192.168.43.197   63.245.217.39    HTTP      387 GET /?product=firefox-30.0-complete&os=win&lang=en-US HTTP/1.1
10 2.037083000  63.245.217.39    192.168.43.197   TCP        54 http > 49160 [ACK] Seq=1 Ack=334 Win=16384 Len=0
11 2.047125000  63.245.217.39    192.168.43.197   HTTP      459
12 2.223796000  192.168.43.197   192.168.43.1     DNS        76
13 2.261884000  192.168.43.197   63.245.217.39    TCP        54                                   16896 Len=0
14 2.427305000  192.168.43.1     192.168.43.197   DNS       140 Standard query response 0xf272  A 173.194.36.79 A 173.194.36.87 A 173.194
15 2.428780000  192.168.43.197   173.194.36.79    TCP        66 49162 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

```
Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
Ethernet II, Src: IntelCor_23:ff:55 (00:1b:77:23:ff:55), Dst: d2:b3:3f:6a:9a:0b (d2:b3:3f:6a:9a:0b)
Internet Protocol Version 4, Src: 192.168.43.197 (192.168.43.197), Dst: 192.168.43.1 (192.168.43.1)
User Datagram Protocol, Src Port: 59207 (59207), Dst Port: domain (53)
Domain Name System (query)
```

```
000  d2 b3 3f 6a 9a 0b 00 1b  77 23 ff 55 08 00 45 00   ..?j.... w#.U..E.
010  00 42 00 94 00 00 80 11  62 00 c0 a8 2b c5 c0 a8   .B...... b...+...
020  2b 01 e7 47 00 35 00 2e  58 63 a1 2b 01 00 00 01   +..G.5.. Xc.+....
030  00 00 00 00 00 00 08 64  6f 77 6e 6c 6f 61 64 07   .......d ownload.
040  6d 6f 7a 69 6c 6c 61 03  6f 72 67 00 00 01 00 01   mozilla. org.....
```

```
File: "C:\Users\rajesh\AppData\Local\Temp\...  Packets: 765 · Displayed: 765 (100.0%) · Dropp...
```

fig. 10 packet analysis[1]

4.2 Hping:

Hping is a free packet generator and analyzer for the TCP/IP protocol distributed by Salvatore Sanfilippo (also known as Antirez). [4] [15]

It is one type of tester for network security.

The new form of hping, hping3, is scriptable utilizing the Tcl language (high level,general purpose language) and executes a engine for string based, intelligible depiction of TCP/IP packets, with the goal that the developer can compose contents identified with low-level TCP/IP packet manipulation and examination in a short time. [6] [15] [5]

Prior it was utilized to exploit idle scan scanning technique, yet nowadays it is actualized in the NMAP security scanner. It is a tool for security auditing and testing of firewalls and networks. [4]

hping is named after pinging in light of the fact that in default use it does likewise functionally - contacts another machine and gets it to answer. [4]

hping can also be utilized to craft and insert arbitrary byte sequences into packets. It is otherwise called crafting tool which is utilized for penetrating testers and IT security auditors. [4]

hping is a command-line oriented TCP/IP packet assembler/analyzer.

It supports TCP, UDP, ICMP, and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features. [15]

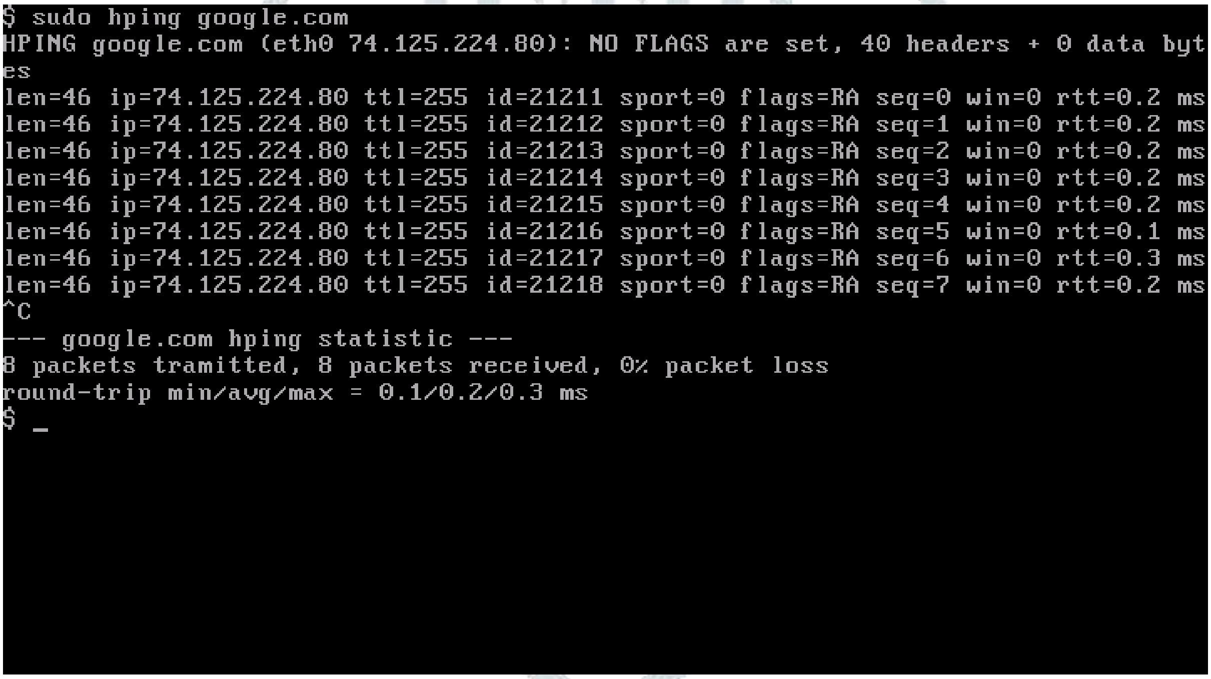
4.2.1 Testing hping can perform:

- Firewall testing.
- Advanced port scanning.
- Network testing, using different protocols, fragmentation.
- Manual path MTU(Maximum Transfer Unit) discovery.
- Advanced traceroute, under all the supported protocols.

- Remote OS fingerprinting.
- TCP/IP stacks auditing.
- hping can also be useful to students that are learning TCP/IP.

4.2.2 Examples of hping:

- Send TCP SYN packets to port 0 on host example.com
  hping example.com -S -V
- Send TCP SYN packets to port 443 on host example.com:
  hping example.com -S -V -p 443
- Send TCP packets to port 443 on host example.com with the SYN + ACK flag set:
  hping example.com -S -A -V -p 443
- Send TCP packets to port 443 on host example.com with the SYN + ACK + FINflags set:
  hping example.com -S -A -F -V -p 443
- Send TCP SYN packets every 5 seconds to port 443 on host example.com:
  hping example.com -S -V -p 443 -i 5



```
$ sudo hping google.com
HPING google.com (eth0 74.125.224.80): NO FLAGS are set, 40 headers + 0 data byt
es
len=46 ip=74.125.224.80 ttl=255 id=21211 sport=0 flags=RA seq=0 win=0 rtt=0.2 ms
len=46 ip=74.125.224.80 ttl=255 id=21212 sport=0 flags=RA seq=1 win=0 rtt=0.2 ms
len=46 ip=74.125.224.80 ttl=255 id=21213 sport=0 flags=RA seq=2 win=0 rtt=0.2 ms
len=46 ip=74.125.224.80 ttl=255 id=21214 sport=0 flags=RA seq=3 win=0 rtt=0.2 ms
len=46 ip=74.125.224.80 ttl=255 id=21215 sport=0 flags=RA seq=4 win=0 rtt=0.2 ms
len=46 ip=74.125.224.80 ttl=255 id=21216 sport=0 flags=RA seq=5 win=0 rtt=0.1 ms
len=46 ip=74.125.224.80 ttl=255 id=21217 sport=0 flags=RA seq=6 win=0 rtt=0.3 ms
len=46 ip=74.125.224.80 ttl=255 id=21218 sport=0 flags=RA seq=7 win=0 rtt=0.2 ms
^C
--- google.com hping statistic ---
8 packets tramitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.2/0.3 ms
$ _
```

fig. 11 execution of hping command

4.3 Kismet:

It is open source software or free software which is mainly used for wireless LANs. [7]

Kismet is a network identifier, packet sniffer, and intrusion identification framework for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic.

The program keeps running under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X. The client can also keep running on Microsoft Windows, although, besides outside drones, there's only supported wireless hardware available as packet source.[7]

Kismet also incorporates wireless IDS (Intrusion location system) features such as identifying active wireless sniffing programs including NetStumbler, and in addition various wireless network attacks.

Kismet also underpins logging of the geographical coordinates of the network if the input from a GPS receiver is also accessible. It is generally utilized and cutting-edge open source wireless monitoring tool.[7]

Kismet recognizes networks by passively gathering packets and distinguishing networks, which enables it to identify hidden networks and the presence of non-beaconing networks by means of data traffic.[7]

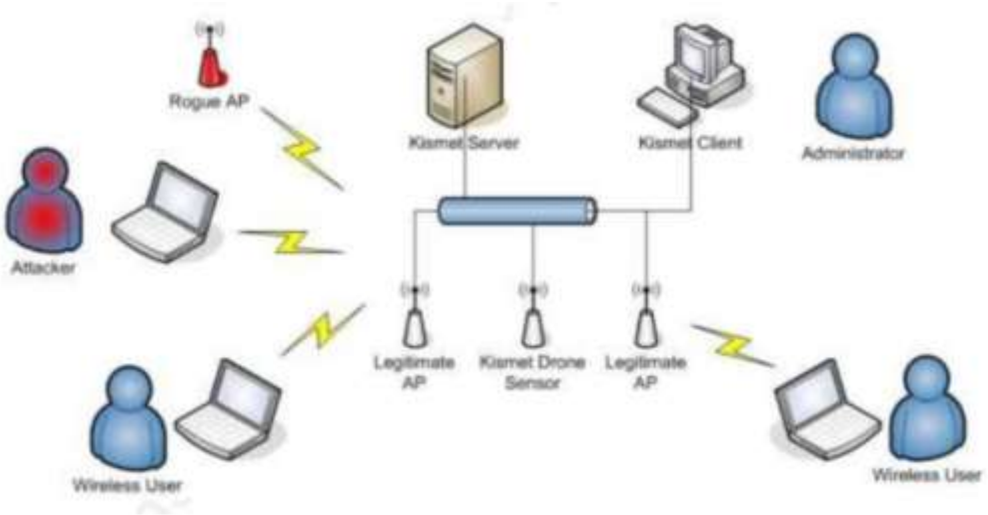


fig. 12 the architecture of kismet[7]

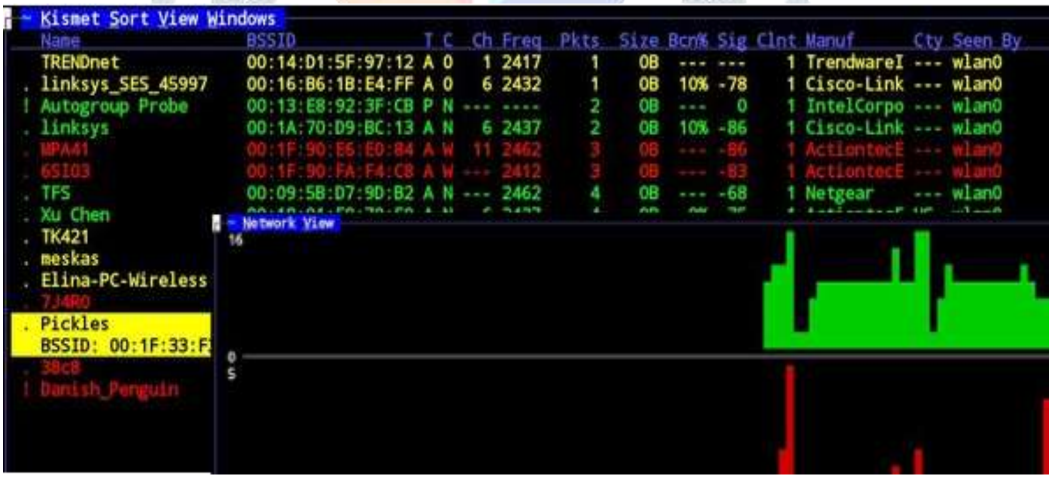
4.3.1 Features:

- Without sending any log report of packets, it is able to detect the presence of both wireless access points and wireless clients and to associate them with each other.

- Kismet main feature is the ability to log all sniffed packets and save them in a tcpdump/Wireshark or Airsnort compatible file format. [7]

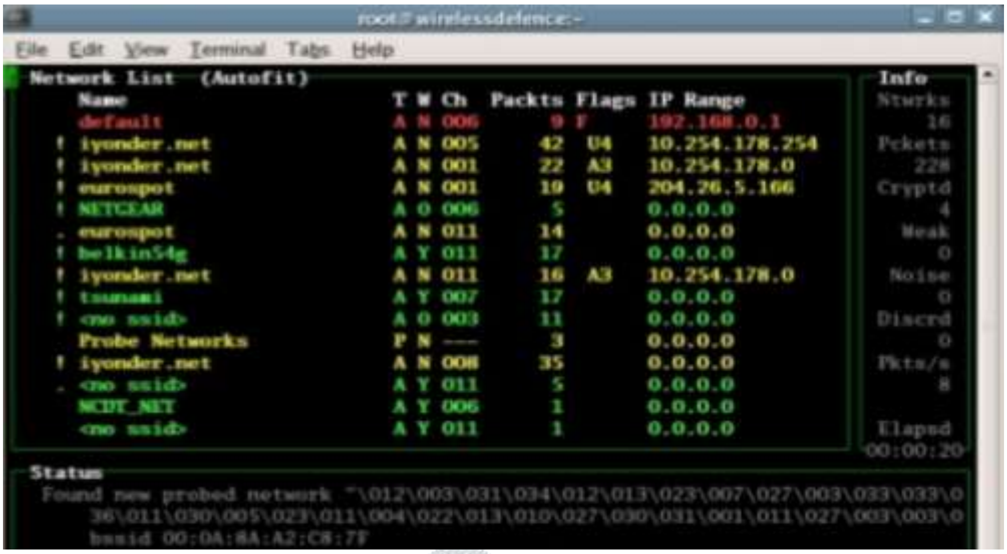
- Kismet can also capture "Per-Packet Information" headers.

- Kismet has a feature like it can detect default or "not configured" networks, probe requests, and determine what level of wireless encryption is used on a given access point.



```
~ Kismet Sort View Windows
   Name                BSSID             T C  Ch Freq  Pkts  Size Bcn% Sig Clnt Manuf      Cty Seen By
   TRENDnet            00:14:D1:5F:97:12 A O   1 2417     1    0B  --- ---    1 TrendwareI --- wlan0
 . linksys_SES_45997   00:16:B6:1B:E4:FF A O   6 2432     1    0B  10% -78    1 Cisco-Link --- wlan0
 ! Autogroup Probe     00:13:E8:92:3F:CB P N --- ----     2    0B  ---   0    1 IntelCorpo --- wlan0
 . linksys             00:1A:70:D9:BC:13 A N   6 2437     2    0B  10% -86    1 Cisco-Link --- wlan0
 . WPA41               00:1F:90:E6:E0:84 A W  11 2462     3    0B  --- -86    1 ActiontecE --- wlan0
 . 6SI03               00:1F:90:FA:F4:C8 A W --- 2412     3    0B  --- -83    1 ActiontecE --- wlan0
 . TFS                 00:09:5B:D7:9D:B2 A N --- 2462     4    0B  --- -68    1 Netgear    --- wlan0
 . Xu Chen
 . TK421               ~ Network View
 . meskas              16
 . Elina-PC-Wireless
 . 7J4R0
 . Pickles
   BSSID: 00:1F:33:F
 . 38c8                0
 ! Danish_Penguin      5
```

fig. 13 screen of kismet software



```
 Network List  (Autofit)                                       Info
     Name                      T W Ch   Packts Flags IP Range   Ntwrks
     default                   A N 006      9 F     192.168.0.1      16
   ! iyonder.net               A N 005     42  U4   10.254.178.254 Pckets
   ! iyonder.net               A N 001     22  A3   10.254.178.0    228
   ! eurospot                  A N 001     19  U4   204.26.5.166   Cryptd
   ! NETGEAR                   A O 006      5       0.0.0.0           4
   . eurospot                  A N 011     14       0.0.0.0        Weak
   ! belkin54g                 A Y 011     17       0.0.0.0           0
   ! iyonder.net               A N 011     16  A3   10.254.178.0   Noise
   ! tsunami                   A Y 007     17       0.0.0.0           0
   ! <no ssid>                 A O 003     11       0.0.0.0        Discrd
     Probe Networks            P N ---      3       0.0.0.0           0
   ! iyonder.net               A N 008     35       0.0.0.0        Pkts/s
   . <no ssid>                 A Y 011      5       0.0.0.0           8
     NCDT_NET                  A Y 006      1       0.0.0.0
     <no ssid>                 A Y 011      1       0.0.0.0        Elapsd
                                                                 00:00:20
 Status
  Found new probed network "\012\003\031\034\012\013\023\007\027\003\033\033\0
     36\011\030\005\023\011\004\022\013\010\027\030\031\001\011\027\003\003\0
     bssid 00:0A:8A:A2:C8:7F
```

fig. 14 screen of kismet software

Above both figures indicates different color in kismet screen. In that, Yellow color shows un-encrypted network, Red color shows default setting used by software and Green color identifies a secure network.

Unlike other wireless network detectors in working passively, Kismet is able to detect the presence of both wireless access points and wireless clients and to associate them together. [7]

In order to find as many networks as possible Kismet supports channel hopping. It means that it constantly changes from channel to channel non-sequentially, in a user-defined sequence.

It will also capture more packets because adjacent channels overlap.

4.4 Tcpdump:[16]

TCPdump is free and open source software and it is under the BSD license. It is a common packet analyzer that keeps running under command line.

It enables the user to show TCP/IP and different packets being transmitted or received over a network to which the computer is attached.[17] [16]

Tcpdumpworks on most Unix based operating system -like Solaris, BSD, macOS, HP-UX, Android, and AIX among others. [16]

In those systems, tcpdump uses the libpcap library to capture packets Tcpdump prints the contents of network packets. It can read packets from a network interface card or from a previously created saved packet file. Tcpdump can write packets to standard output or a file.[17]

It is also conceivable to utilize tcpdump for the particular purpose of intercepting and showing the interchanges of another user or computer. A user with the necessary privileges on a system acting as a router or gateway through which unencrypted traffic such as Telnet or HTTP passes can utilize tcpdump to see login IDs, passwords, the URLs and content of websites being seen, or some other unencrypted data.[17] [16]

The user may optionally apply a BPF-based filter to limit the number of packets seen by tcpdump.

4.4.1 Privileges Required:

In some Unix based operating systems, a user must have superuser privileges to use tcpdump because the packet capturing mechanisms on those systems require elevated privileges.[17]

However, the -Z option may be used to drop privileges to a specific unprivileged user after capturing has been set up.

Other hands, the packet capturing mechanism can be configured to allow non-privileged users to use it; if that is done, superuser privileges are not required.

4.5 Windump:

WinDump is free and it is released under a BSD-style license. It is used as a port of tcpdump for windows. [16]

It can run under Windows 95, 98, ME, NT, 2000, XP, 2003 and Vista.

WinDump captures using the Winpcap library and drivers, which are freely downloadable from the WinPcap.org website

WinDump is the Windows version of tcpdump, the command line network analyzer for UNIX. WinDump is fully compatible with tcpdump and can be used to watch, diagnose and save to disk network traffic according to various complex rules. [16]

WinDump captures using theWinPcap library and drivers, which are freely downloadable from the WinPcap.org website. WinDump supports 802.11b/g wireless capture and troubleshooting through the Riverbed AirPcap adapter. [16]

4.5.1 How to protect yourself from a sniffer on your system:

1. **Switch:** To date with the cost and price decreasing a managed switch has become a main sniffer defense tool both effective and economic. [9]
2. **Encryption:** Encrypting your data can reduce the effects of sniffer to access your private information. A sniffer can capture all data but it cannot decode and read encrypted data. [11]
3. **One time password:** Secure Key and other one-time password techniques make it insignificant to sniffer account information. Secure Key based on the principle that a remote host has gained a password which will not be transmitted on an insecure network. The secure feature of S/key is that passwords do not need to be transferred on a network and same challenge/response can appear only once. [10]
4. **Rejecting promiscuous mode:** A Sniffer can work only in promiscuous mode, so it is crucial whether your system is in such mode or not. In the past, most network interface cards of DOS compatible computers did not support promiscuous mode but now it is the reverse. [18] [8]

Conclusion:

Network sniffing is a technique that can help you find network problems by enabling you to capture and view packet level data on your network it also monitors that data flowing over computer network links in real time. We can measure traffic over the network and gather information about packets and make a record of it in a readable format to the user. We can also analyze bandwidth utilization to identify issues of the network.

References:

1. https://www.wireshark.org/docs/
2. http://www.monitis.com/blog/best-free-network-sniffers/
3. https://www.colasoft.com/resources/network-sniffer.php
4. http://www.hping.org/
5. https://tools.kali.org/information-gathering/hping3
6. https://searchsecurity.techtarget.com/feature/Hping-How-to-better-understand-how-hackers-attack
7. https://www.kismetwireless.net/
8. https://www.ijariit.com/manuscripts/v3i6/V3I6-1369.pdf
9. http://www.ijettjournal.org/volume-4/issue-5/IJETT-V4I5P160.pdf
10. http://airccse.org/journal/ijcses/papers/4313ijcses02.pdf
11. http://ijsetr.org/wp-content/uploads/2015/07/IJSETR-VOL-4-ISSUE-7-2470-2474.pdf
12. http://www.wireless-nets.com/resources/tutorials/sniff_packets_wireshark.html
13. https://en.wikiversity.org/wiki/Wireshark/TCP
14. http://www.ijsrp.org/research-paper-0416/ijsrp-p5259.pdf
15. http://thesprawl.org/research/hping/
16. http://www.ijccts.org/books_pdf_dwd/A%20Research%20Study%20on%20Packet%20Sniffing%20Tool%20%20TCPDUMP.pdf
17. https://jiva.io/assets/files/FJiva_PerformanceEvaluationOfTcpdump.pdf
18. http://www.just.edu.jo/~tawalbeh/nyit/incs745/presentations/Sniffers.pdf
19. https://cs.baylor.edu/~donahoo/tools/sniffer/sniffingFAQ.htm