Ethical Hacking

Session 7

Sniffing Network Scanning

Learning Objectives 1-2

1. Explain sniffing
2. Describe the working of sniffers
3. Explain types of sniffing
4. Describe sniffing tools
5. Explain sniffing prevention techniques

Learning Objectives 2-2

6
- Explain ways to detect sniffing

7
- Describe packet sniffing

8
- Explain sniffing using Wireshark tool

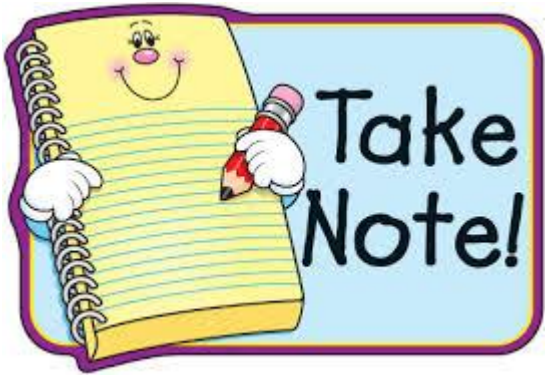
Introduction

- **Sniffer:**
  - Is a program that monitors, analyses and identifies any problem in network traffic.
  - Helps a network manager to maintain traffic flow efficiently.
  - Captures data that is transmitted on the network with the help of sniffers.

Sniffers 1-2

- Sniffers are referred to as ‘Data Interception Technology’ that networks use to transmit messages between computers and also help in identifying messages that are not useful.
- There are legal and illegal ways of sniffing that help monitor network security, network traffic, to hack passwords and files from the network.
- A packet-capturing or frame-capturing tool is called a sniffer, which displays captured data that is transmitted from one host to another on the network.

Sniffers 2-2



1. ‘Packet’ means the Network layer or the data at Layer 3 of the OSI model which contains IP addresses.
2. ‘Frame’ means the Data Link layer or the data at Layer 2 which contains MAC addresses.

Working of Sniffers 1-7

- Computers are used to perform tasks such as sharing files, emails, Web browsing and so on.
- Computers are connected to the LAN. The two addresses to a computer that is connected to the LAN are:

MAC Address	IP Address
• This address helps identify all the nodes that are located in the network and accumulated on the network card. MAC addresses are used by Ethernet protocol to generate frames that transmit data through the machine.	• This address is commonly used in place of a MAC address. • The Data Link Layer uses MAC address of the destined machine.

Working of Sniffers 2-7

- The IP network is located by the Network Layer as and when the Data Link Protocol requires and interprets the MAC address of the target machine in a table.
- This is also referred to as the Address Resolution Protocol (ARP) cache.
- If the IP address is unable to find entry, the ARP sends a request packet to all computers that are located in the network.

Working of Sniffers 3-7

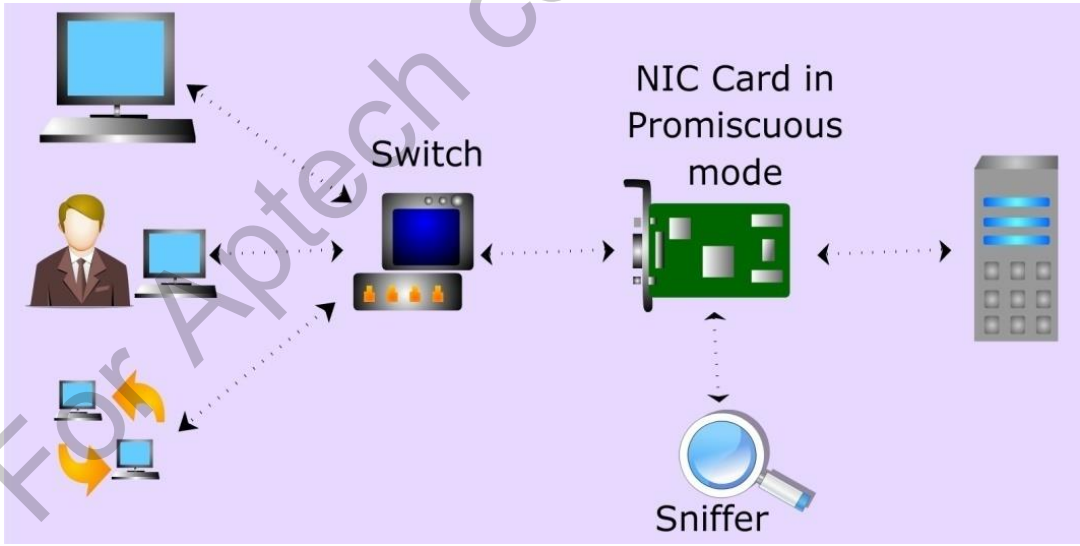
- The machine uses a similar address to respond to the source machine using the MAC address.
- The MAC address is inserted to the source machine ARP cache to interact with the destination machine.
- Packets are captured by the Sniffer software that is meant for a particular destination MAC address, also known as ‘promiscuous mode’.

Working of Sniffers 4-7

- The system on the network reads and responds only to traffic sent directly to the MAC address.
- However, the presence of hacking tools change the system's Network Interface Controller (NIC) to promiscuous mode that reads all traffic and sends it to the sniffer for processing.
- By installing special driver software, the promiscuous mode gets enabled on a network card.

Working of Sniffers 5-7

- A promiscuous mode driver is used as a hacking tool for sniffing.
- It is recommended that the driver supports the required mode when using hacking tools as all Windows drivers do not support promiscuous mode as shown in the figure.



Working of Sniffers 6-7

- Unencrypted data is vulnerable to sniffing.
- Following are the most commonly captured protocols that are used in Sniffer:

HyperText Transfer Protocol (HTTP)	Post Office Protocol (POP3)
• The default version of HTTP Basic authentication has a number of loopholes that are used for sending passwords across the wire in plain text by many Websites.	• The data and passwords are sent in clear text all through the network.

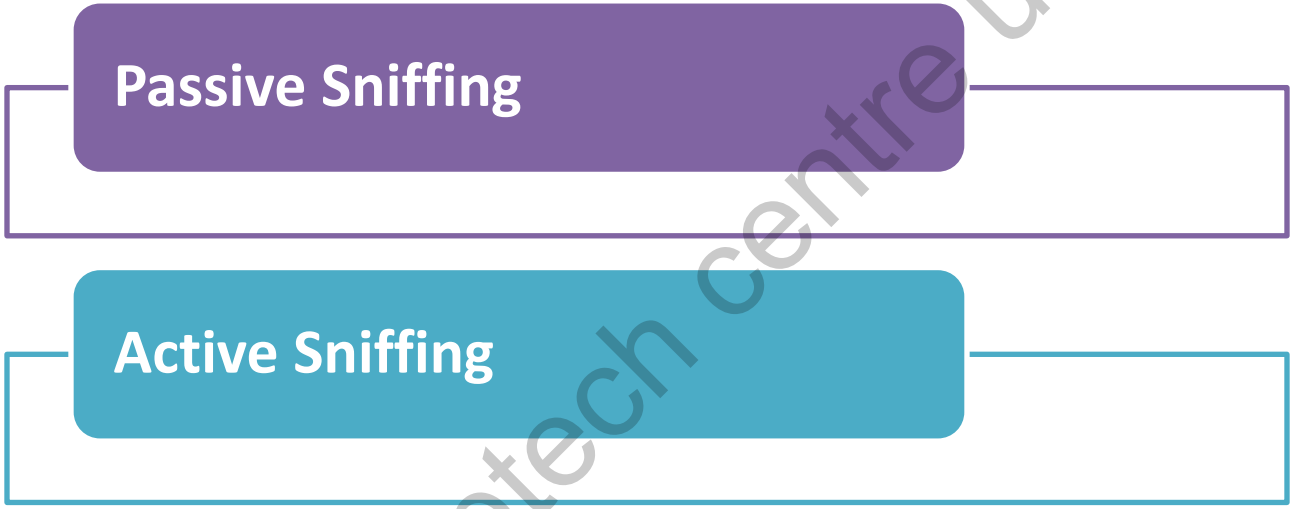
Working of Sniffers 7-7

Simple Network Management Protocol (SNMP)	File Transfer Protocol (FTP)
• SNMP passwords are sent in clear texts throughout the network.	• Passwords and data are sent in clear text all through the network.

- Hackers view these protocols and collect usernames and passwords.

Types of Sniffing 1-11

- Sniffing is of two types:



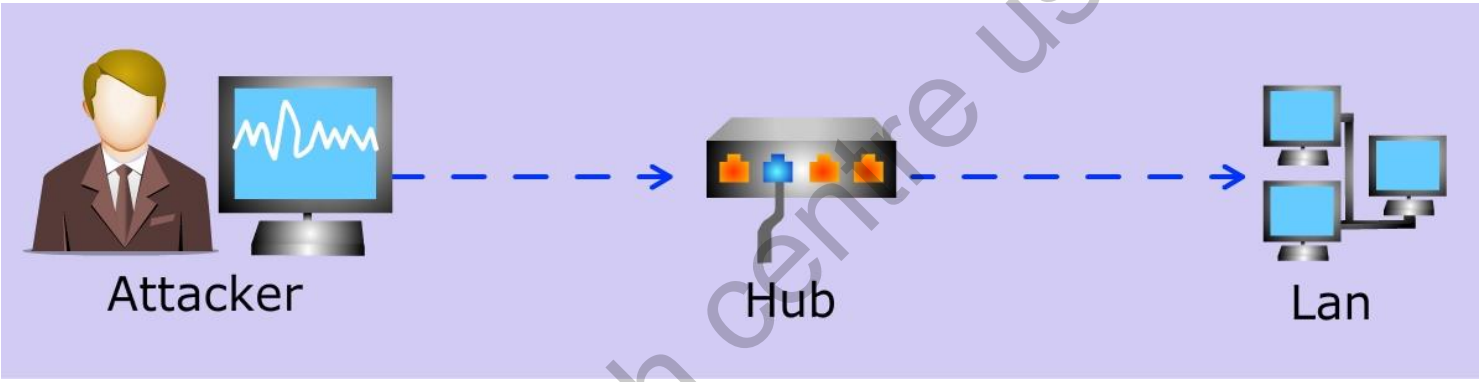
Types of Sniffing 2-11

Passive Sniffing

- Is used for listening and accumulating traffic in a network.
- Is used in a network system that is attached by hubs or wireless media.
- Displays the traffic to all the hosts on the network.
- Helps a passive packet sniffer to capture traffic going to and from all hosts connected via the hub.

Types of Sniffing 3-11

- Passive sniffing is not detectable as shown in the figure.



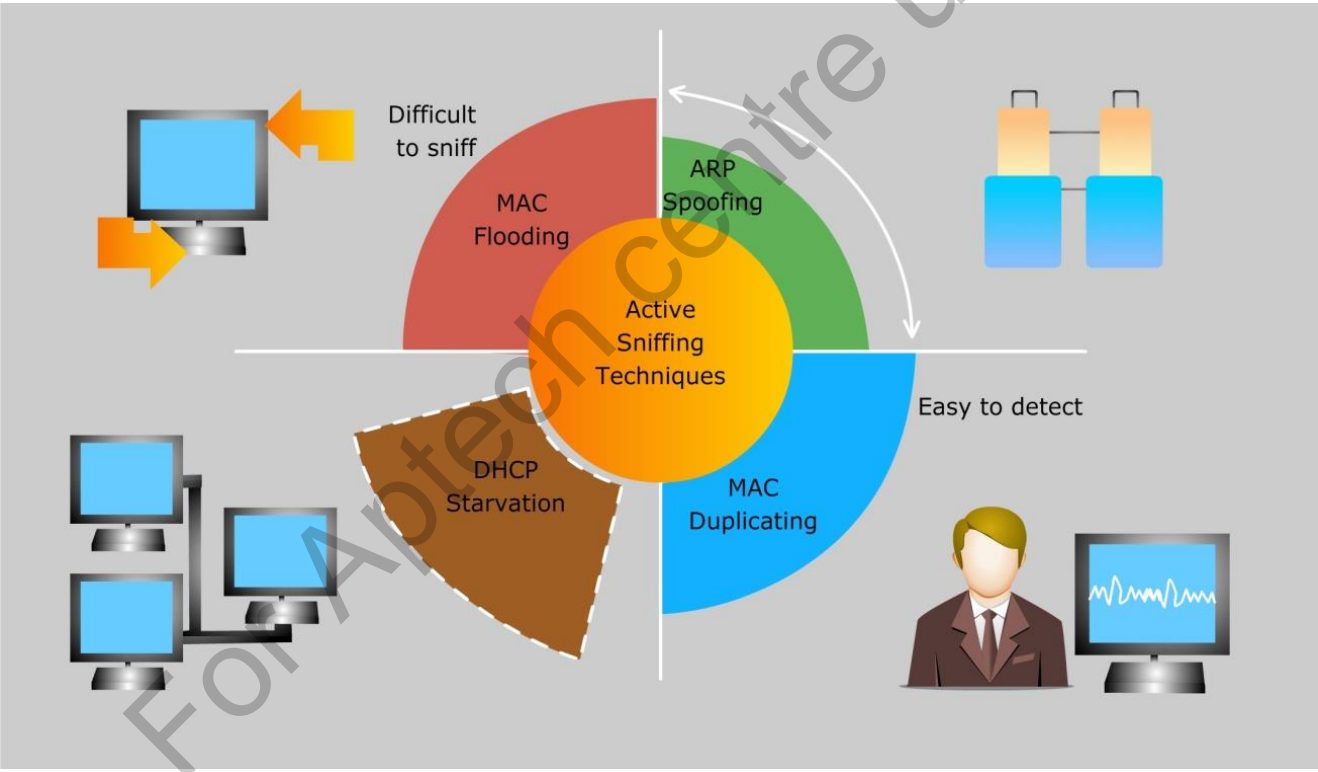
Types of Sniffing 4-11

Active Sniffing

- Is used by injecting Address Resolution Protocol (ARP) packets in a network, which causes traffic.
- Does not send packets.
- Checks the packets sent by other recipients.

Types of Sniffing 5-11

- Active sniffing is done on a switched network and is detectable as shown in the figure.



Types of Sniffing 6-11

- Span port or port mirroring can be used to duplicate data to another port and monitor legal traffic by network administrators.

- Active sniffing can be performed in two ways to ensure that the switch sends traffic to the system running the sniffer. These are:

ARP Sniffing or Spoofing

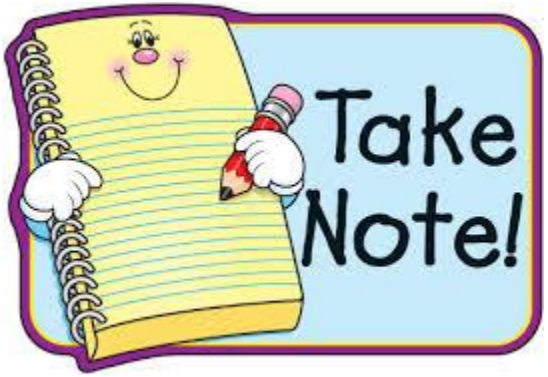
DNS Spoofing or Poisoning

Types of Sniffing 7-11

ARP Sniffing or Spoofing

- In this type of sniffing, the attacker sends fake ARP messages on a LAN to connect the MAC address of the attacker to the IP address of another host.
- As a result, the traffic sends the IP address to the attacker.
- ARP spoofing allows the hacker to change the traffic, stop the traffic or capture data frames on the LAN.

Types of Sniffing 8-11



Switches are redesigned so that they are not vulnerable to flooding.

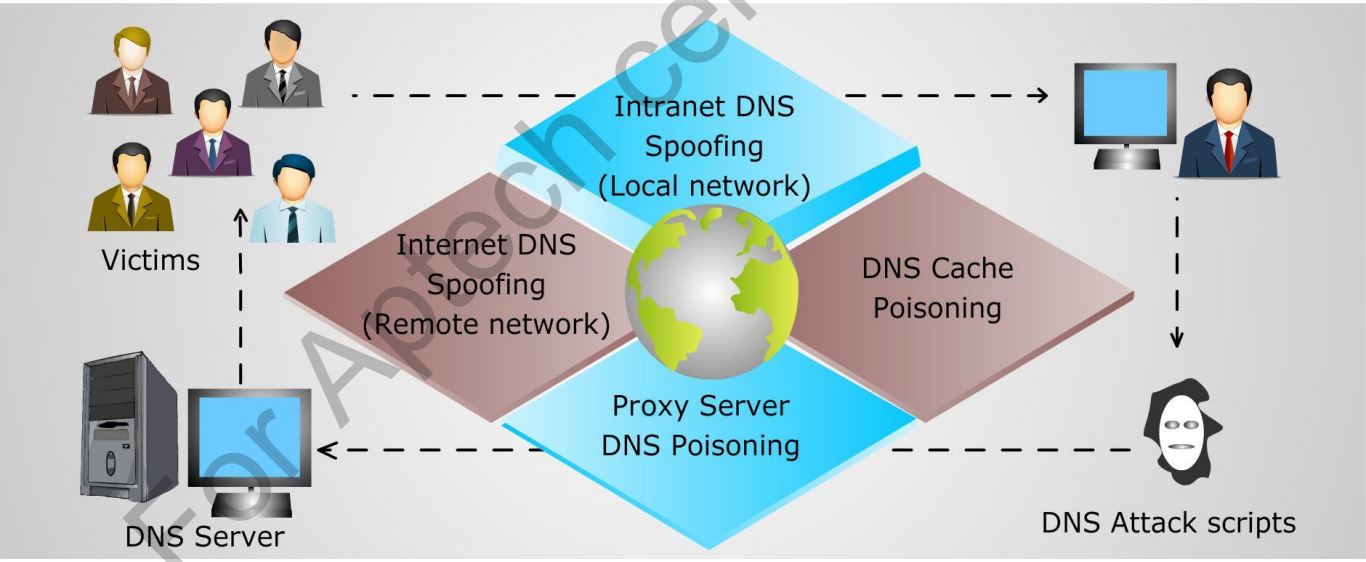
Types of Sniffing 9-11

DNS Spoofing or Poisoning

- In this type of sniffing, the DNS server is made to believe that the information received is valid.
- The poisoned information is cached and affects the users.
- When the user requests a Website URL, the DNS server looks up the address to find the corresponding IP address.
- If the DNS server is poisoned, the user is redirected to a fake Website.

Types of Sniffing 10-11

- An attacker can use fake ARP messages to divert all the communications between two computers to exchange all the traffic as shown in the figure.
- Following figure shows different DNS spoofing techniques.



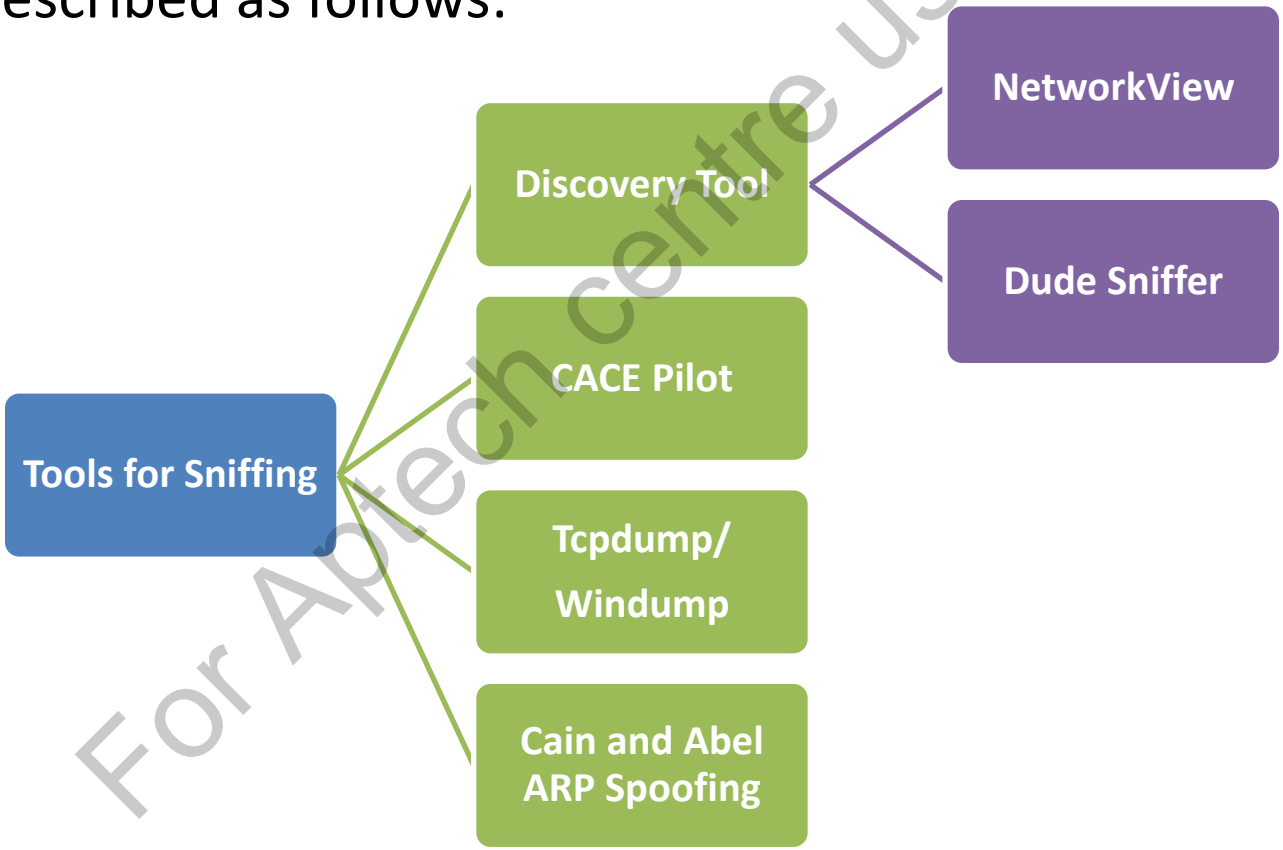
Types of Sniffing 11-11

- DNS spoofing techniques include:

Intranet Spoofing	• The device acts as if it is on the same internal network.
Internet Spoofing	• The device acts as if it is on the Internet.
Proxy Server DNS Poisoning	• The DNS entries are modified on a proxy server that redirects the user to a different host system.
DNS Cache Poisoning	• The DNS entries are modified on any system that redirects the user to a different host.

Tools for Sniffing 1-8

- There are many tools used for sniffing. Some of these tools are described as follows:



Tools for Sniffing 2-8

- **Cain and Abel ARP Spoofing:**
  - Is also known as a Windows-based password recovery tool.
  - Have involved two programs:
    - **Cain**: Considered as the GUI of the program.
    - **Abel**: The Windows service that offers a remote console on the intended machine.
  - Supports large characteristics so that passwords from the LAN to different routing protocols can be recovered.

Tools for Sniffing 3-8

- **Cain and Abel ARP Spoofing:**
  - Helps to recover encrypted passwords and cached passwords with the help of Dictionary, Brute–force and Cryptanalysis attacks.
  - Also known as ARP Poison Routing (APR) that allows sniffing packets of different products on switched LAN.
  - Controls the IP traffic of many hosts. Encrypted protocols such as HTTPS and SSH–1 are also studied by APR.

Tools for Sniffing 4-8

- **CACE Pilot:**
  - Is a sniffing tool that is used for both wired and wireless network that helps identify network problems.

Tools for Sniffing 5-8

- **CACE Pilot:**
  - The features of CACE Pilot are as follows:

Reports can be created directly from the user's customised views.

Multi-gigabyte trace files can be opened and analysed easily.

Quick and easy visualisation of off-line traffic statistics.

Easy identification of traffic of interest through network analysis metrics that is known as 'Views'.

Monitor long-duration network traffic with a mechanism called 'Watches' that provides flexible trigger-alerts.

Tools for Sniffing 6-8

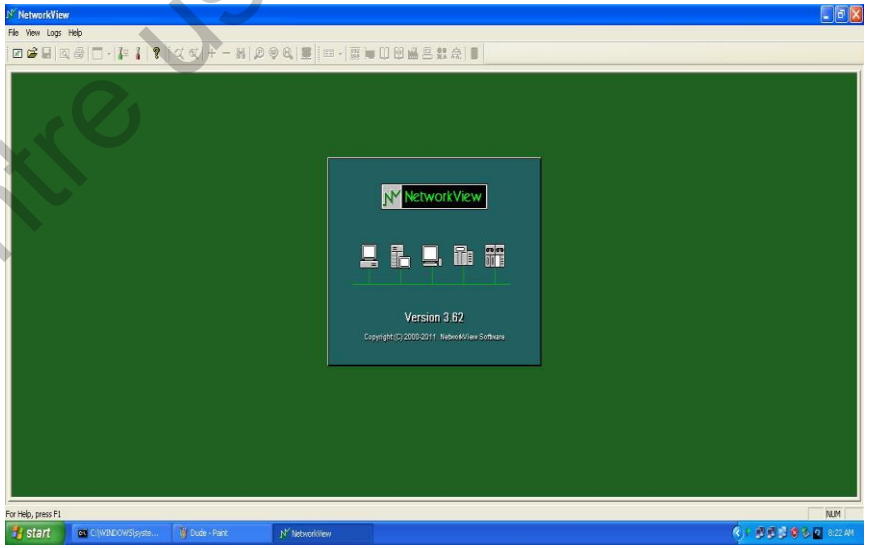
- **Tcpdump/Windump:**
  - Is a software that monitors the traffic on a network.
  - Is a UNIX tool that collects network data, decodes the information and displays the output.
  - Is considered a powerful command line interface packet sniffer that runs on Linux and Windows.

Tools for Sniffing 7-8

- **The Discovery tool:**

NetworkView

- NetworkView is a Windows management and discovery tool that discovers TCP/IP nodes and routes with the help of DNS, NetBIOS, Ports, SNMP and WMI as shown in the figure.

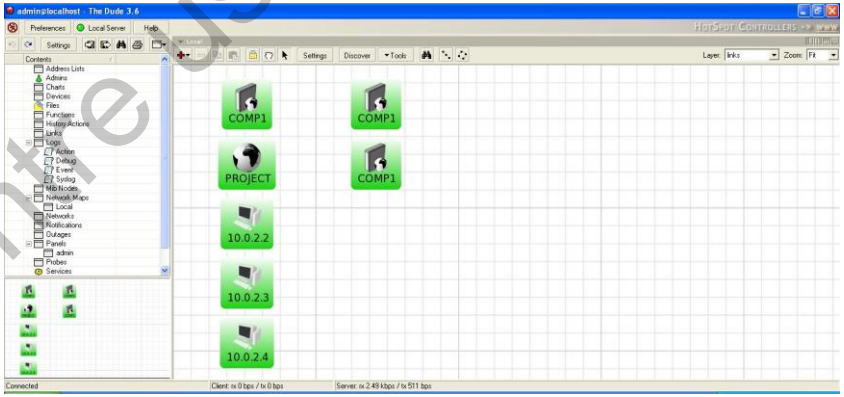


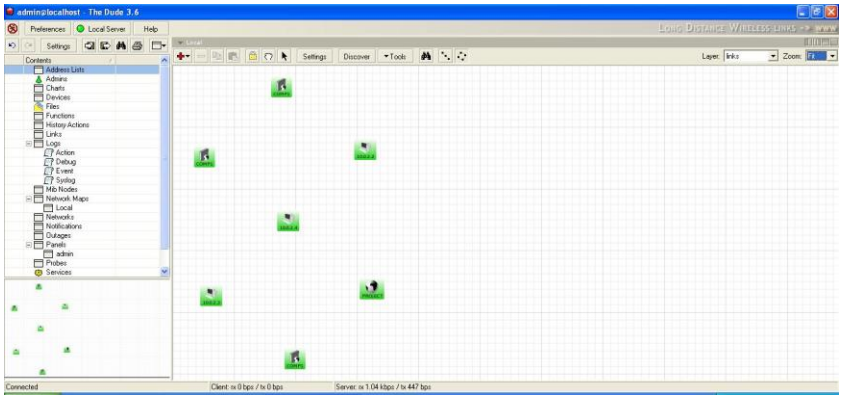
Tools for Sniffing 8-8

- **The Discovery tool:**

Dude Sniffer

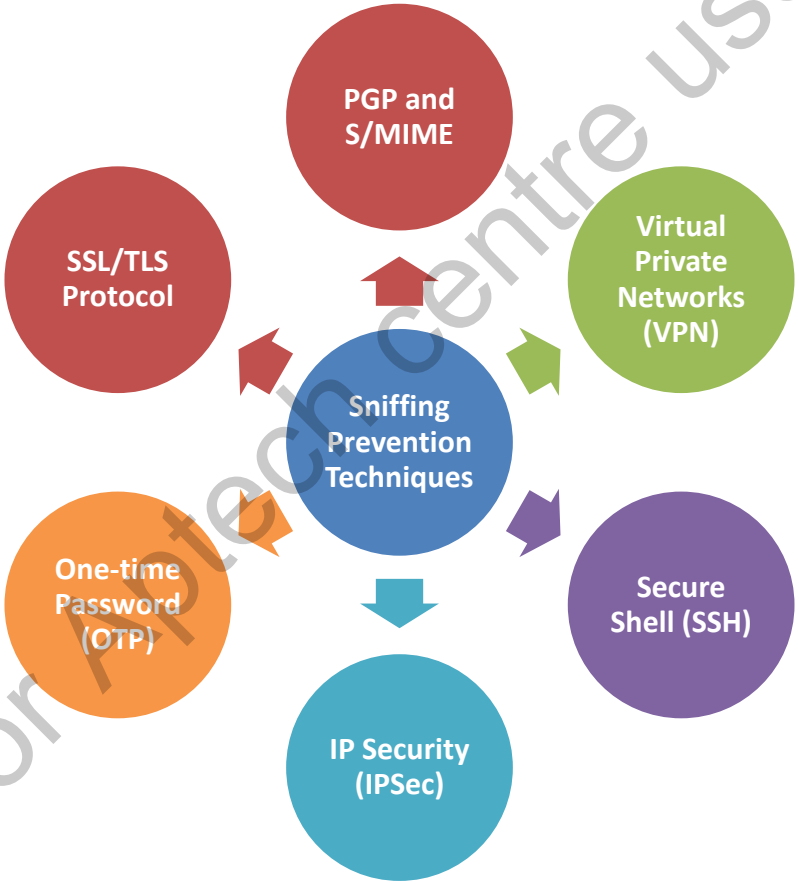
- The Dude Sniffer is a discovery tool that is used to scan all the devices that are inside the specified subnets and also draws a complete layout map as shown in the figures.





Sniffing Prevention Techniques 1-7

- Sniffing can be prevented by using the following techniques:



Sniffing Prevention Techniques 2-7

PGP and S/MIME

- **Pretty Good Privacy (PGP):**
  - is an application that protects email messages and files.
  - is based on strong cryptographic algorithms such as IDEA, RSA and SHA-1.
- **Secure/Multipurpose Internet Mail Extensions (S/MIME):**
  - is a standard for public key encryption and signing of MIME data.
  - is on an IETF standards track and defined in a number of documents, most importantly RFCs (3369, 3370, 3850, 3851).

Sniffing Prevention Techniques 3-7

- **Virtual Private Network:**
  - VPN uses Internet protected access to users that maintain privacy and tunnelling protocols such as the Layer Two Tunnelling Protocol (L2TP) that encrypts the data at the sending end and decrypts at the receiving end.
  - The data is sent through a tunnel.
  - Data that is not encrypted properly is not allowed to enter the tunnel.

Sniffing Prevention Techniques 4-7

- **Secure Shell (SSH):**
  - This is a cryptographic network protocol.
  - It provides secure network services such as data communication, remote command execution and remote command-line login.
  - This is done by connecting two networked computers through a server, a secure channel and a client that uses SSH server and SSH client programs.

Sniffing Prevention Techniques 5-7

- **IP Security (IPSec):**
  - This protocol is used to protect Internet Protocol (IP) communications that authenticate and encrypt each IP packet of a communication session.
  - This is done at the beginning of the session and at the time of negotiation of cryptographic keys that is used during the session.
  - IPSec protects the following the flow of data:
    - between two hosts (host-to-host)
    - between two security gateways (network-to-network)
    - between two security gateway and a host (network-to-host)

Sniffing Prevention Techniques 6-7

- **One-time Password (OTP):**
  - This password allows only one login transaction that is not vulnerable to replay attacks.
  - The attacker is unable to abuse it as the password becomes invalid after one transaction.

Sniffing Prevention Techniques 7-7

- **SSL/TLS Protocol:**
  - Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols.
  - They provide communication security over the Internet by using X.509 certificates and exchange asymmetric key.
  - The data that flows between them is encrypted using the session key, maintains confidentiality of the data and authenticates the codes of messages.
  - This protocol is commonly used in applications such as electronic mail, instant messaging, Voice-over-IP (VoIP), Web browsing and Internet faxing.

Ways to Detect Sniffing

- The ways to detect if there are any sniffers in the network are as follows:

Promiscuous Mode	IDS	Network Tools
• By checking which machine runs in the promiscuous mode, a network device can be intercepted to read each network packet that arrives. • Promiscuous detection tools are PromqryUI and Promiscan. • PromqryUI detects network interfaces that run in the promiscuous mode. Promiscan detects promiscuous applications that start and end without increasing the load of the network.	• By running IDS, changes in the router's MAC address can be checked and then authorities can be alerted about the change.	• By running network tools, it should be checked if there are packets. • For example, tools such as HP Performance Insight can be checked to analyse, centralise and consolidate traffic data spread over other technologies and resources.

Packet Sniffing

- A packet sniffer is also referred to as a protocol analyser, a network analyser or a packet analyser.

Definition and Concept 1-2

- The process of capturing any data or log traffic that passes over the local network is termed as packet sniffing.
- This process is used by a system or network administration to troubleshoot network problems and traffic.
- The sniffer captures each packet to decode the data and checks the contents of the packet to Request for Comment (RFC).

Definition and Concept 2-2

- The packet sniffers are able to capture all packets that are placed into promiscuous mode.

- Packet sniffers are used as network tools to monitor if the network is being compromised and they help maintain efficient network data transmission.

Packet Sniffing Techniques 1-3

- Traffic can be captured on all or parts of the network on a machine in the network.
- A malicious hacker can capture and analyse all network traffic if a packet sniffer is placed on a network in promiscuous mode.
- The username and password information in a network is transmitted in clear text and can be viewed by analysing the packets that are being transmitted.

Packet Sniffing Techniques 2-3

- Since packet sniffers capture packet information within a given subnet, an attacker cannot place a packet sniffer on their home ISP network to capture the network traffic within the corporate network.

- If Trojan is used to compromise a machine on the internal network, the attacker can run a packet sniffer from that machine, capture username and password information and compromise more machines on the network.

- Rogue packet sniffers are passive by nature and are not detected easily.

Packet Sniffing Techniques 3-3

- The packets travelling to the network interface are captured without indicating any traffic that would identify a machine that is running a packet sniffer.
- The only way to identify network interfaces on the network that are running in promiscuous mode is by locating rogue packet sniffers.
- For example, Ethereal is a packet sniffer that maintains and monitors a network.

How to Defend against Sniffing? 1-2

- Following are some countermeasures to defend against sniffing:

To block the traffic from getting collected locally, a user can use tough physical security and appropriate segmenting of the network.

Strong authentication credentials can be used as complete encrypt communication does not allow attackers to use sniffed packets. For example, encrypted sessions such as SSH, Internet Protocol Security (IPSec) and Secure Sockets Layer (SSL) can be used.

Programs such as ARP watch, Anti Sniff, Neped and so on, can be used to detect sniffer.

Passing credentials in plaintext over the wire should be avoided.

How to Defend against Sniffing? 2-2

- Data hashing and signing should be used.
- Digital signatures should be used and safe audit trails should be created.
- Resource and bandwidth throttling techniques should be employed.
- Input should be authenticated and filtered.
- A network Intrusion Detection System (IDS) should be used.
- IPv4 protocol should be avoided and instead IPv6 should be used.
- Static IP address and static ARP tables should be used.
- Network identification broadcasts should be switched off and unauthorised use should be restricted.

Wireshark: The Ultimate Sniffer 1-4

- **Wireshark:**
  - Is a network analysis tool.
  - Is used to capture packets in real time and display them in human-readable format and include filters, colour-coding and other features that monitor network traffic and inspect individual packets.

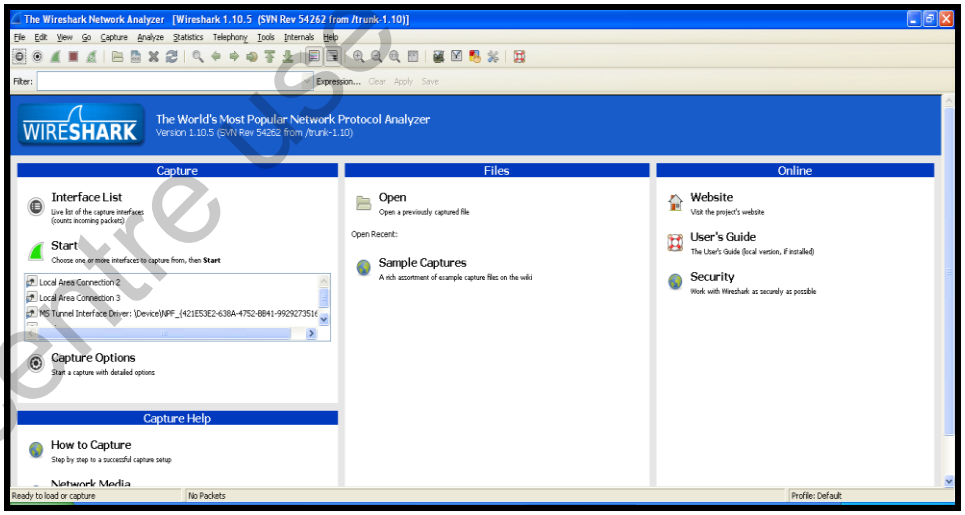
Wireshark: The Ultimate Sniffer 2-4

- Is considered as one of the best network protocol analysers and is used for the following reasons:

  - Browse the capture data
  - Network troubleshooting
  - Education
  - Software and communication
  - Develop protocol
  - Analysis
  - View summary and detail information for each packet

Wireshark: The Ultimate Sniffer 3-4

- Wireshark displays filter language and analyses the restructured stream of a Transmission Control Protocol (TCP) session. Wireshark can read live data from Ethernet.

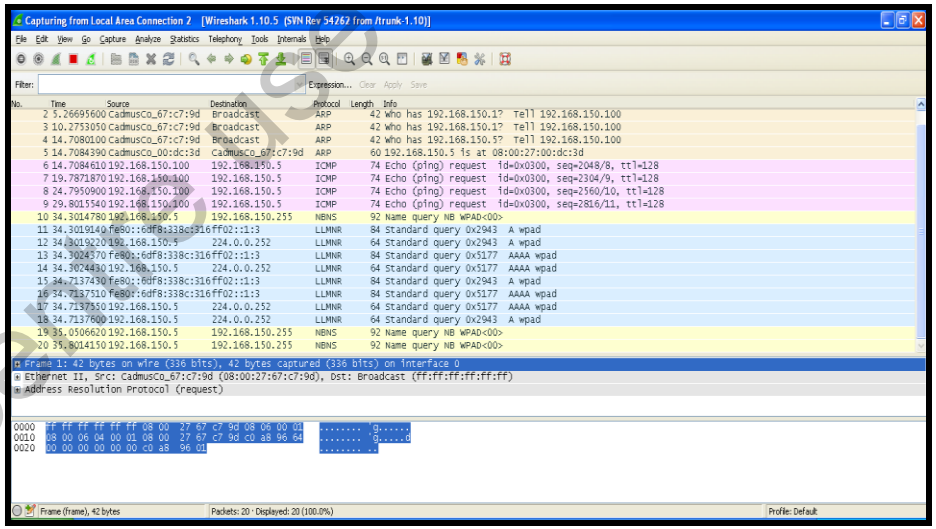


- Figure displays the Wireshark Network Analyzer.

Wireshark: The Ultimate Sniffer 4-4

- Wireshark has been written and developed by networking experts. It supports platforms such as UNIX, LINUX and Windows.

- Figure displays Wireshark Capturing from a Local Area Connection.



Wireshark Filters 1-3

- **Display Filters:**
  - Are used by Wireshark for viewing general packet filtering meant to examine network traffic and flow of traffic for a doubtful program.
  - Also helps troubleshoot the errors in a network.

Wireshark Filters 2-3

- Wireshark filters any field of any protocol. Display filters utilised in Wireshark are as follows:

ip.addr == 10.0.0.1: This sets a filter for any packet with 10.0.0.1, as either the source or dest

ip.addr==10.0.0.1&& ip.addr==10.0.0.2: This sets a conversation filter between the two defined IP addresses

http or dns: This sets a filter to display all http and dns

tcp.port==4000: This sets a filter for any TCP packet with 4000 as a source or dest port

Wireshark Filters 3-3

tcp.flags.reset==1: This displays all TCP resets

http.request: This displays all HTTP GET requests

tcp contains traffic: This shows all TCP packets which include a word 'traffic'. This display filter works best for searching on a certain string or user ID]

!(arp or icmp or dns): This helps to focus on the traffic of interest by disabling arp, icmp, dns or any protocols may be background noise.

udp contains 33:27:58: This sets a filter for the HEX values of 0x33 0x27 0x58 at any offset

tcp.analysis.retransmission: This shows all retransmissions inside the trace. Offers assistance while tracking down slow application performance and packet loss

Colour Coding 1-4

- Packets are highlighted in **green**, **blue** and **black** to identify the types of traffic.

- By default:
  - **Transmission Control Protocol (TCP) traffic appears in green**
  - **Domain Name System (DNS) traffic appears in dark blue**
  - **User Datagram Protocol (UDP) traffic appears in light blue**
  - **TCP packets with errors or those delivered out-of-order appear in black**

Colour Coding 2-4

- **Sample Captures:**
  - WiresharkWiki includes a page of sample capture files which can be loaded and inspected if there is nothing to inspect on the network.
  - The following step can be performed to capture file:

Step: Click **Start** → **All Programs** → **Wireshark** → Open the main screen and browse for a file.

Colour Coding 3-4

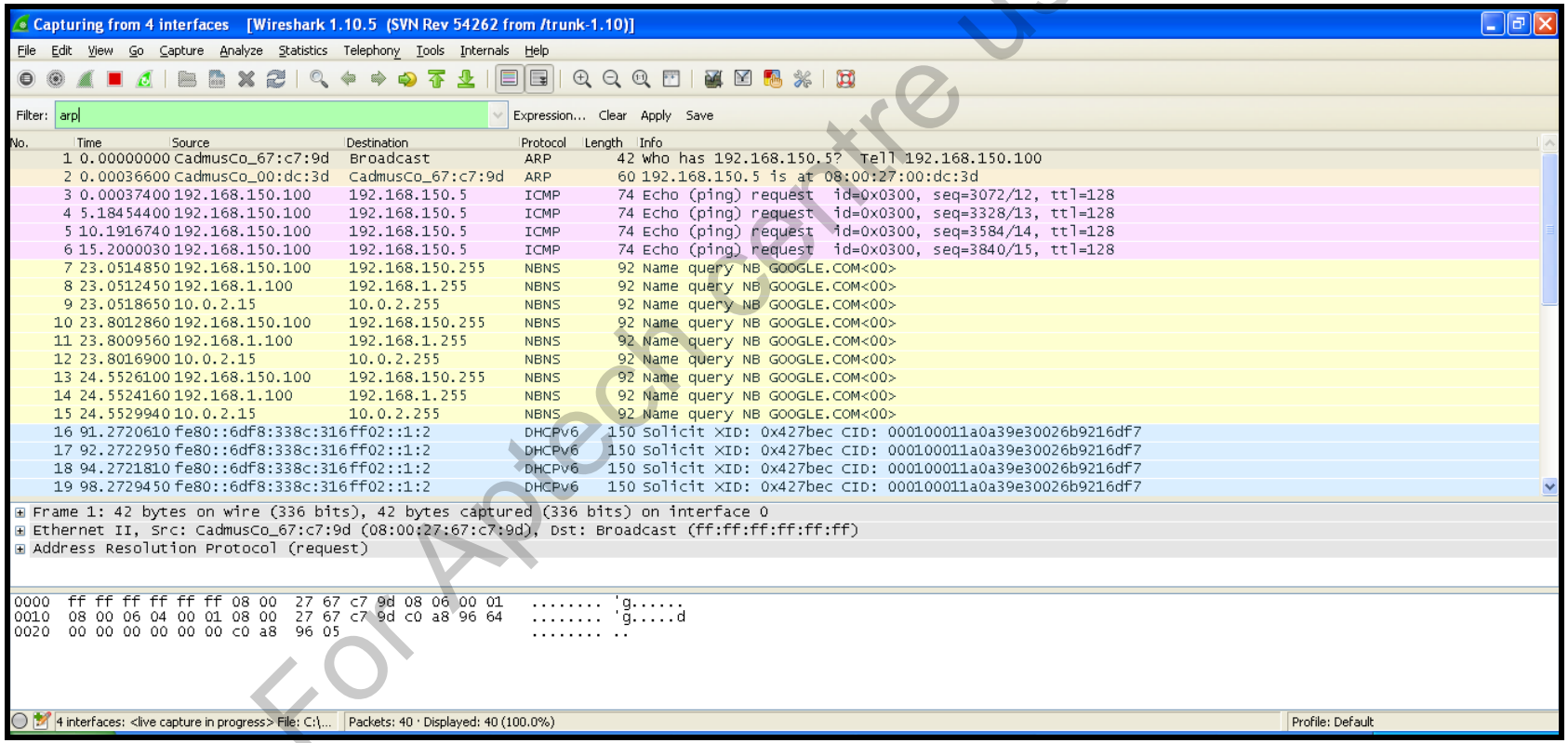
- **Filtering Packets:**
  - Wireshark filters are used to check traffic. The following step can be performed to filter the type of traffic:

Step: To apply a filter, enter the type of traffic in the **Filter** box and click **Apply** or press **Enter**.

  - For example, if dns is entered, only the DNS packets open. When a user begins typing, Wireshark assists to autocomplete the filter.

Colour Coding 4-4

- Following figure displays ARP Filtering Packets:



Summary 1-3

- Sniffers help a network manager to maintain the traffic flow efficiently.
- There are legal and illegal ways of sniffing that help monitor network security, network traffic, to hack passwords and files from the network.
- The two addresses to a computer that is connected to the LAN are, MAC addresses and IP address.
- An unencrypted data is vulnerable to sniffing.
- Passive sniffing is used for listening and accumulating the traffic in a network. It is used in a network system that is attached by hubs or wireless media.

Summary 2-3

- Active sniffing is used by injecting Address Resolution Protocol (ARP) packets if a network causes traffic.
- Promiscuous Mode checks which machine runs in the promiscuous mode, a network device can be intercepted to read each network packet that arrives.
- The process of capturing any data or log traffic that passes over the local network is termed as packet sniffing.
- A malicious hacker can capture and analyse all the network traffic if a packet sniffer is placed on a network in promiscuous mode.

Summary 3-3

- Rogue packet sniffers are passive by nature and are not detected easily. The packets travelling to the network interface are captured without indicating any traffic that would identify a machine that is running a packet sniffer.
- Wireshark is a network analysis tool. It is used to capture packets in real time and display them in human-readable format and include filters, colour-coding and other features that monitor network traffic and inspect individual packets.
- Wireshark is considered as one of the best network protocol analysers.
- Wireshark supports platforms such as UNIX, LINUX and Windows.