Network Security

Class 10

Lab 25

UNITED TRUST

bdeducation
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা

Lab Objectives:

- sniffing

What is Sniffing?

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools.

It is a form of “tapping phone wires” and get to know about the conversation. It is also called wiretapping applied to the computer networks.

There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.

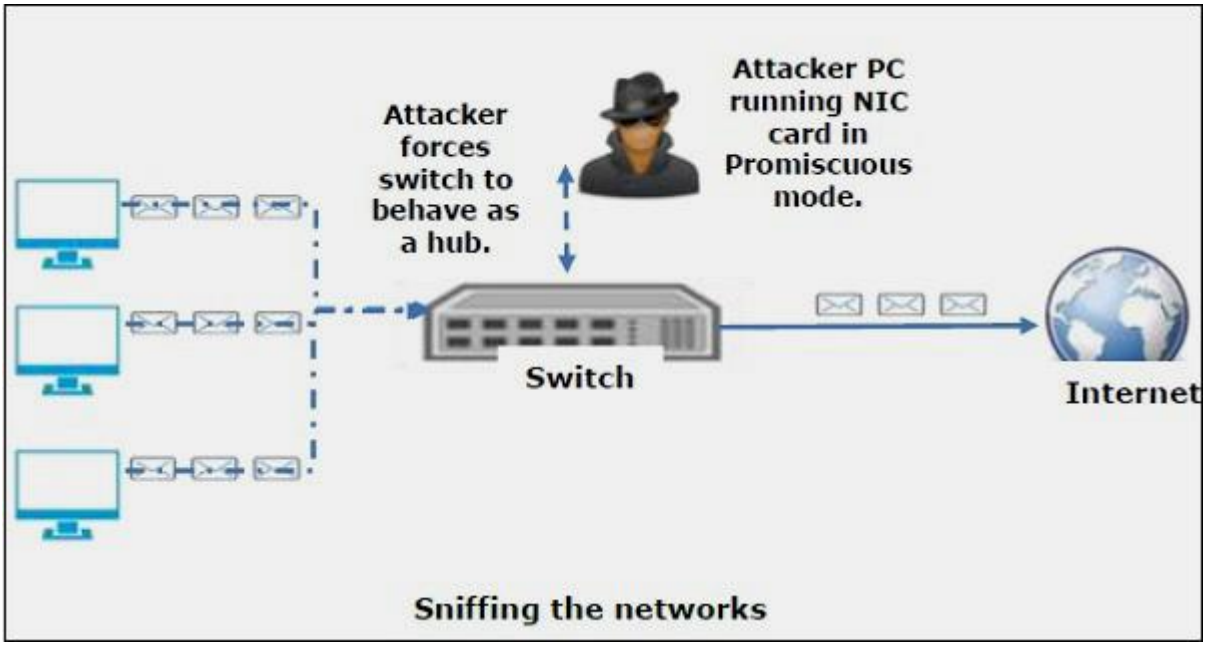
What can be sniffed?

One can sniff the following sensitive information from a network −

- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

How it works

A sniffer normally turns the NIC of the system to the promiscuous mode so that it listens to all the data transmitted on its segment.

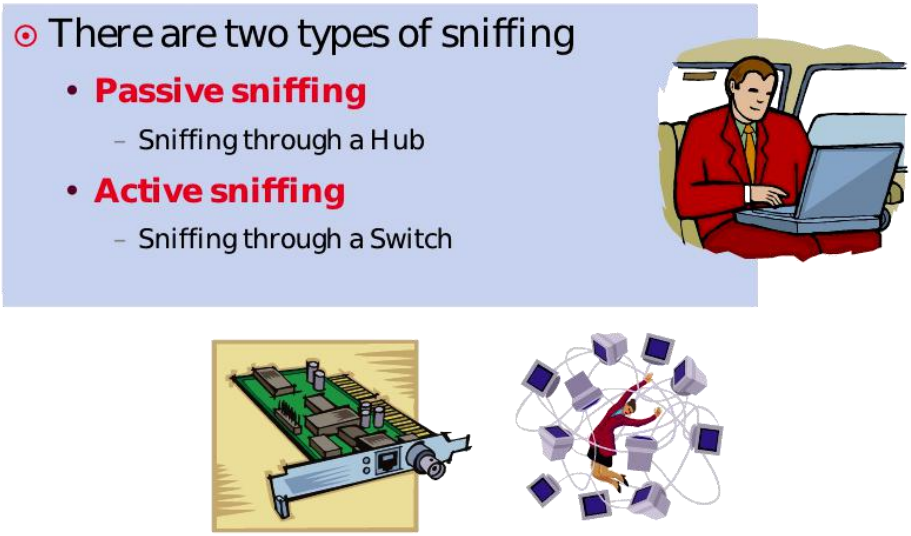


Network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC.

A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

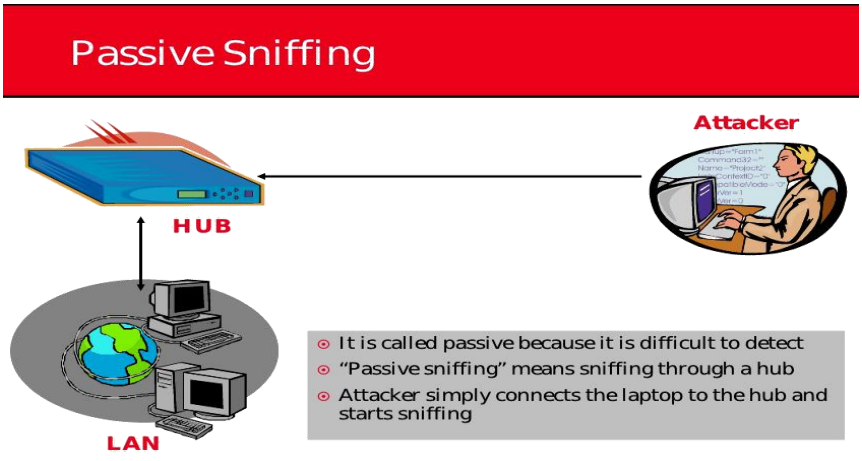
Types of Sniffing

Sniffing can be either Active or Passive in nature.



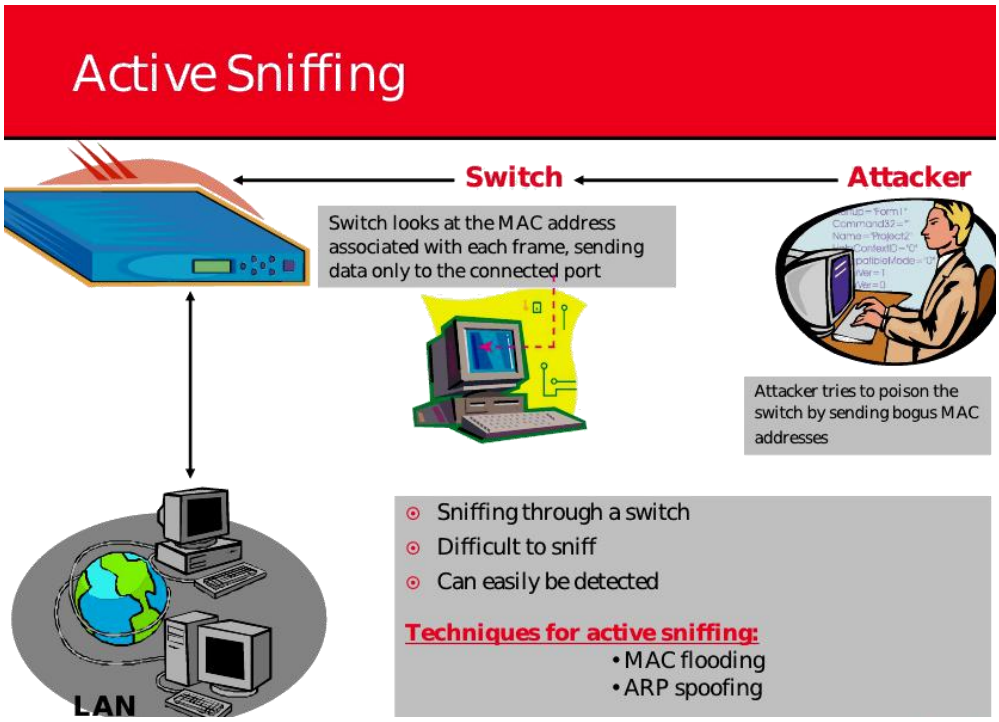
Passive Sniffing

In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.



Active Sniffing

In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network.



Sniffing Tools

There are so many tools available to perform sniffing over a network, and they all have their own features to help a hacker analyze traffic and dissect the information. Sniffing tools are extremely common applications. We have listed here some of the interesting ones −

- ***BetterCAP*** – BetterCAP is a powerful, flexible and portable tool created to perform various types of MITM attacks against a network.

```
new@kali:~/code/dec$ sudo bettercap -T 192.168.2.2 --proxy -P POST
                                                  |_| v1.5.8
http://bettercap.org/

[I] Starting [ spoofing:✓ discovery:✘ sniffer:✓ tcp-proxy:✘ http-proxy:✓ https-p
roxy:✘ sslstrip:✓ http-server:✘ dns-server:true ] ...

[I] [wlan0] 192.168.2.7 : D0:53:49:E5:EB:29 / wlan0 ( Liteon Technology )
[I] [GATEWAY] 192.168.2.1 : 00:17:7C:43:8B:61 ( Smartlink Network Systems Limite
d )
[I] [DNS] Starting on 192.168.2.7:5300 ...
[I] [HTTP] Proxy starting on 192.168.2.7:8080 ...
[I] [TARGET] 192.168.2.2 : A0:32:99:41:38:ED ( Lenovo (Beijing) )
```

- ***Ettercap*** – Ettercap is a comprehensive suite for man-in-the-middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

- ***Wireshark*** – It is one of the most widely known and used packet sniffers. It offers a tremendous number of features designed to assist in the dissection and analysis of traffic.

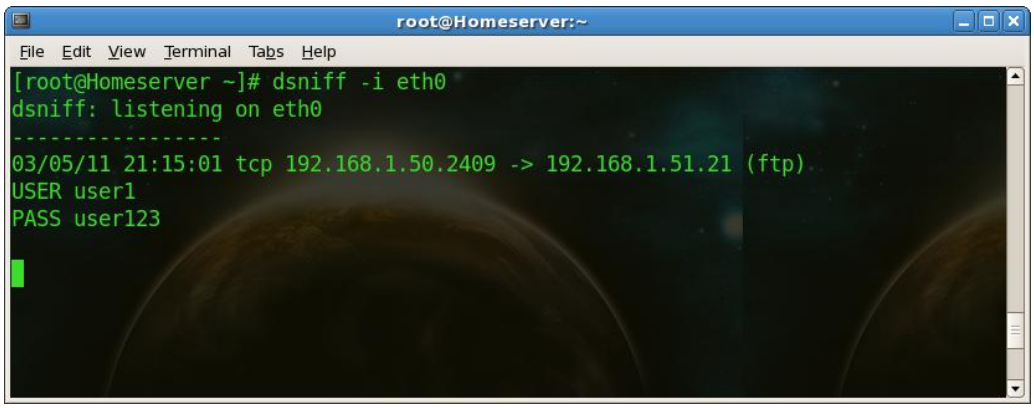
- ***Tcpdump*** – It is a well-known command-line packet analyzer. It provides the ability to intercept and observe TCP/IP and other packets during transmission over the network. Available at www.tcpdump.org.

TCPDUMP

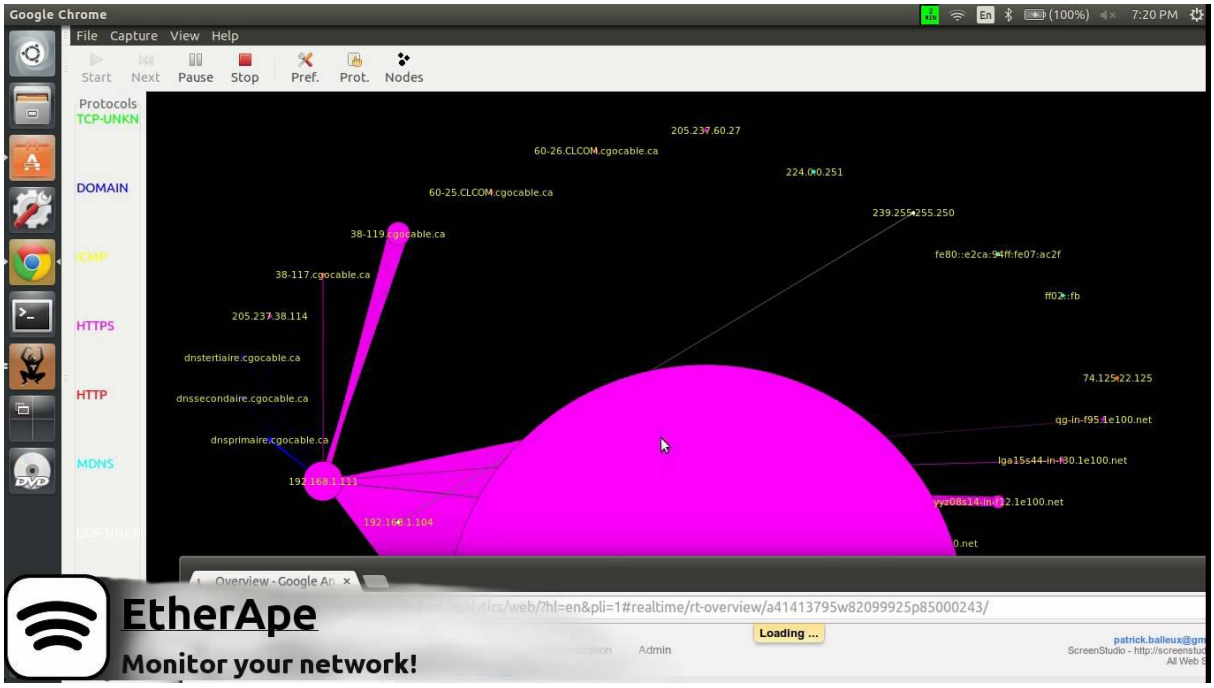
- ***WinDump*** – A Windows port of the popular Linux packet sniffer tcpdump, which is a command-line tool that is perfect for displaying header information.

- ***OmniPeek*** – Manufactured by WildPackets, OmniPeek is a commercial product that is the evolution of the product EtherPeek.

- ***Dsniff*** – A suite of tools designed to perform sniffing with different protocols with the intent of intercepting and revealing passwords. Dsniff is designed for Unix and Linux platforms and does not have a full equivalent on the Windows platform.

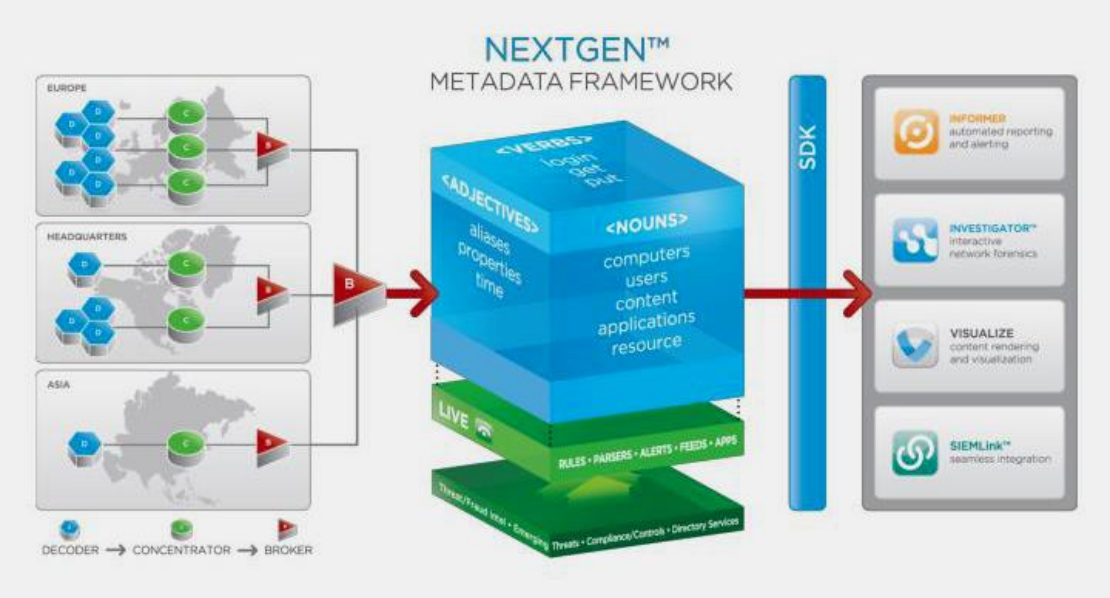


- ***EtherApe*** – It is a Linux/Unix tool designed to display graphically a system's incoming and outgoing connections.



- ***MSN Sniffer*** – It is a sniffing utility specifically designed for sniffing traffic generated by the MSN Messenger application.

- ***NetWitness NextGen*** – It includes a hardware-based sniffer, along with other features, designed to monitor and analyze all traffic on a network. This tool is used by the FBI and other law enforcement agencies.



A potential hacker can use any of these sniffing tools to analyze traffic on a network and dissect information. If you want to be a Network Security Specialist or Ethical Hacker you have use these sniffing tools to protect malicious attacker or hacker