# Ethics in IT

## Class 9

## Lab 2

UNITED TRUST

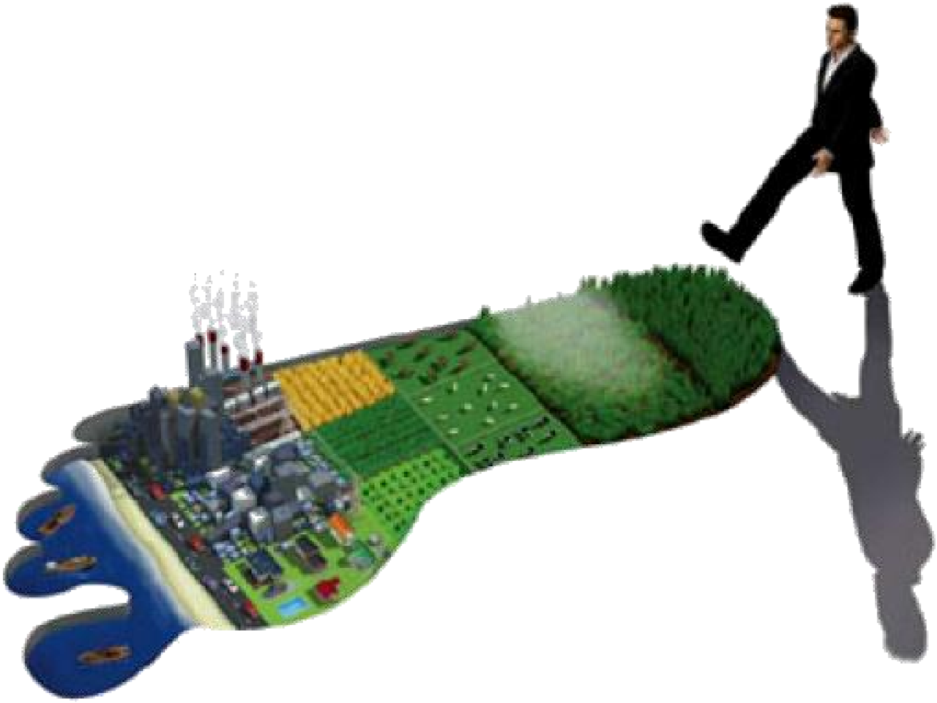
bdeducation
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা

## Lab Objectives:

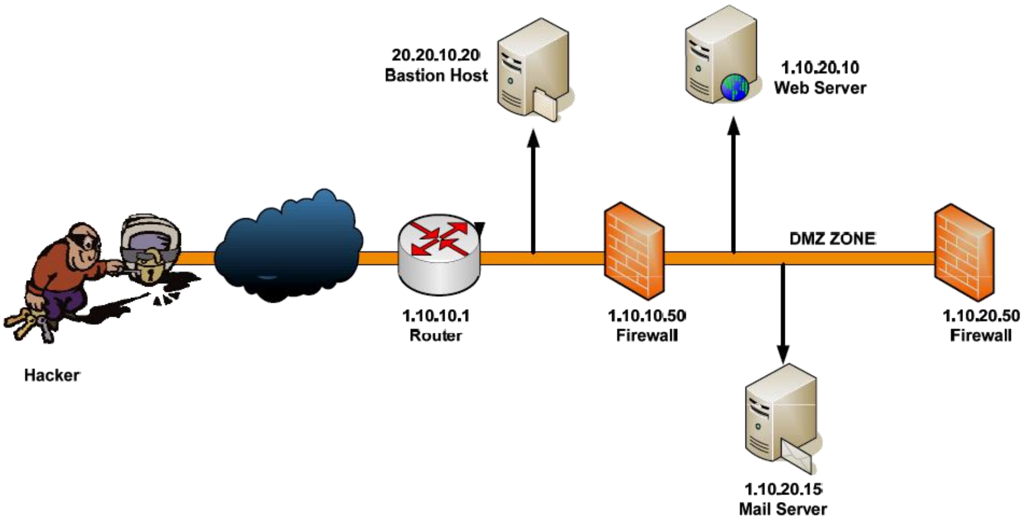
- Footprinting
- Sniffing

## Footprinting

Footprinting is a part of reconnaissance process which is used for gathering possible information about a target computer system or network.



Footprinting could be both passive and active. Reviewing a company’s website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.



Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

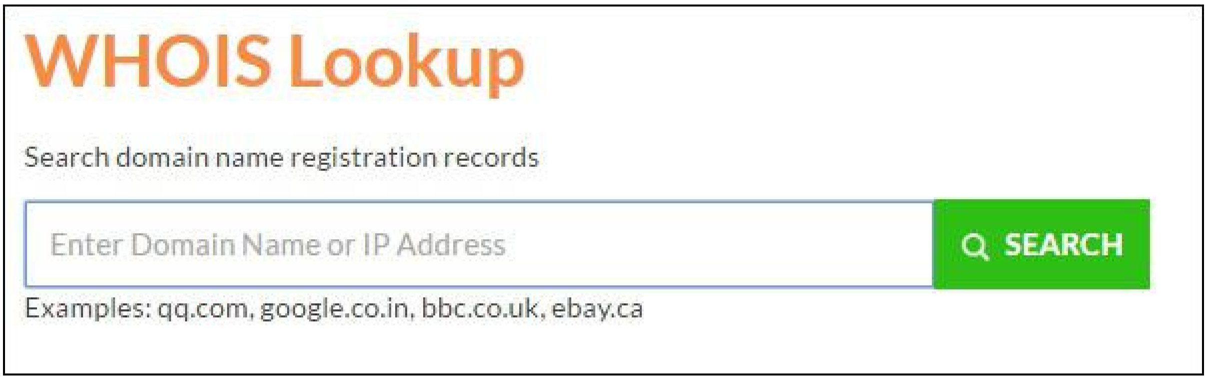
During this phase, a hacker can collect the following information −

- √ Domain name
- √ IP Addresses
- √ Namespaces
- √ Employee information
- √ Phone numbers
- √ E-mails
- √ Job Information

In the following section, we will discuss how to extract the basic and easily accessible information about any computer system or network that is linked to the Internet.

## Domain Name Information

You can use http://www.whois.com/whois website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.



WHOIS Lookup

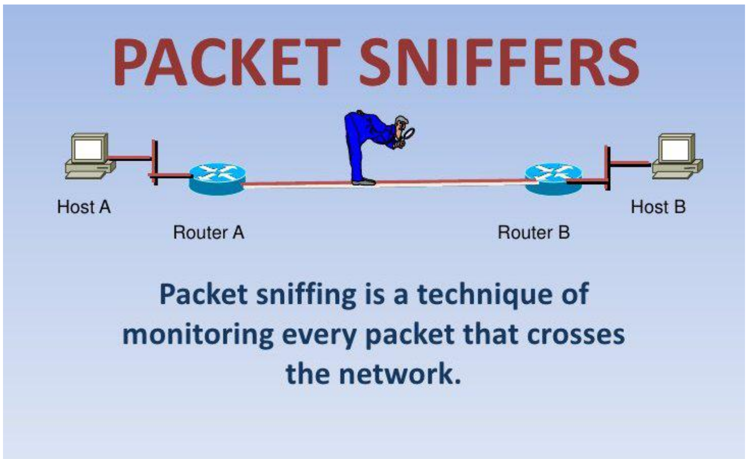
Search domain name registration records

Examples: qq.com, google.co.in, bbc.co.uk, ebay.ca

It's always recommended to keep your domain name profile a private one which should hide the information from potential hackers.

## Ethical Hacking - 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.



PACKET SNIFFERS

Packet sniffing is a technique of monitoring every packet that crosses the network.

## What can be sniffed?

One can sniff the following sensitive information from a network −

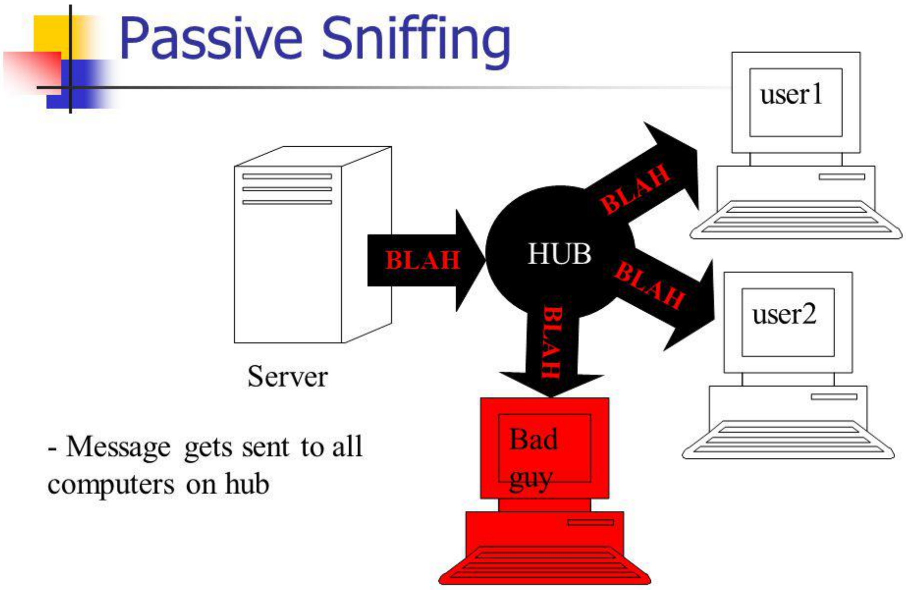
- √ Email traffic
- √ FTP passwords
- √ Web traffics
- √ Telnet passwords
- √ Router configuration
- √ Chat sessions
- √ DNS traffic

## 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.



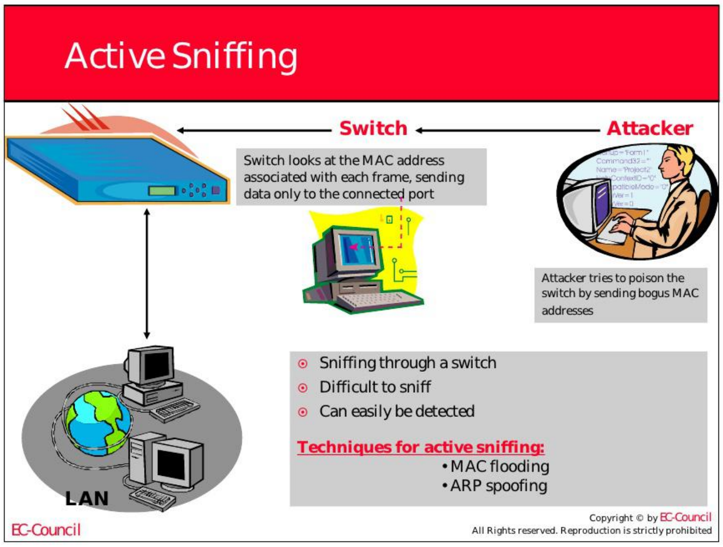
Passive Sniffing

- Message gets sent to all computers on hub

The good news is that hubs are almost obsolete nowadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

### *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.



## Active Sniffing

Switch

Attacker

Switch looks at the MAC address associated with each frame, sending data only to the connected port

Attacker tries to poison the switch by sending bogus MAC addresses

LAN

- Sniffing through a switch
- Difficult to sniff
- Can easily be detected

**Techniques for active sniffing:**

- MAC flooding
- ARP spoofing

EC-Council

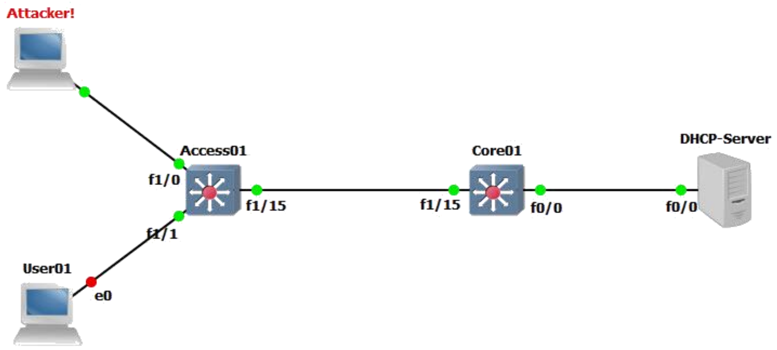
Copyright © by EC-Council
All Rights reserved. Reproduction is strictly prohibited

It involves injecting address resolution packets (ARP) into a target network to flood on the switch content addressable memory (CAM) table. CAM keeps track of which host is connected to which port.

Following are the Active Sniffing Techniques −

√ MAC Flooding

**MAC-ADDRESS FLOODING / DHCP STARVATION ATTACK**



- √ DNS Poisoning
- √ Spoofing Attacks
- √ ARP Poisoning