

# Malicious Attacks

# Contents

---

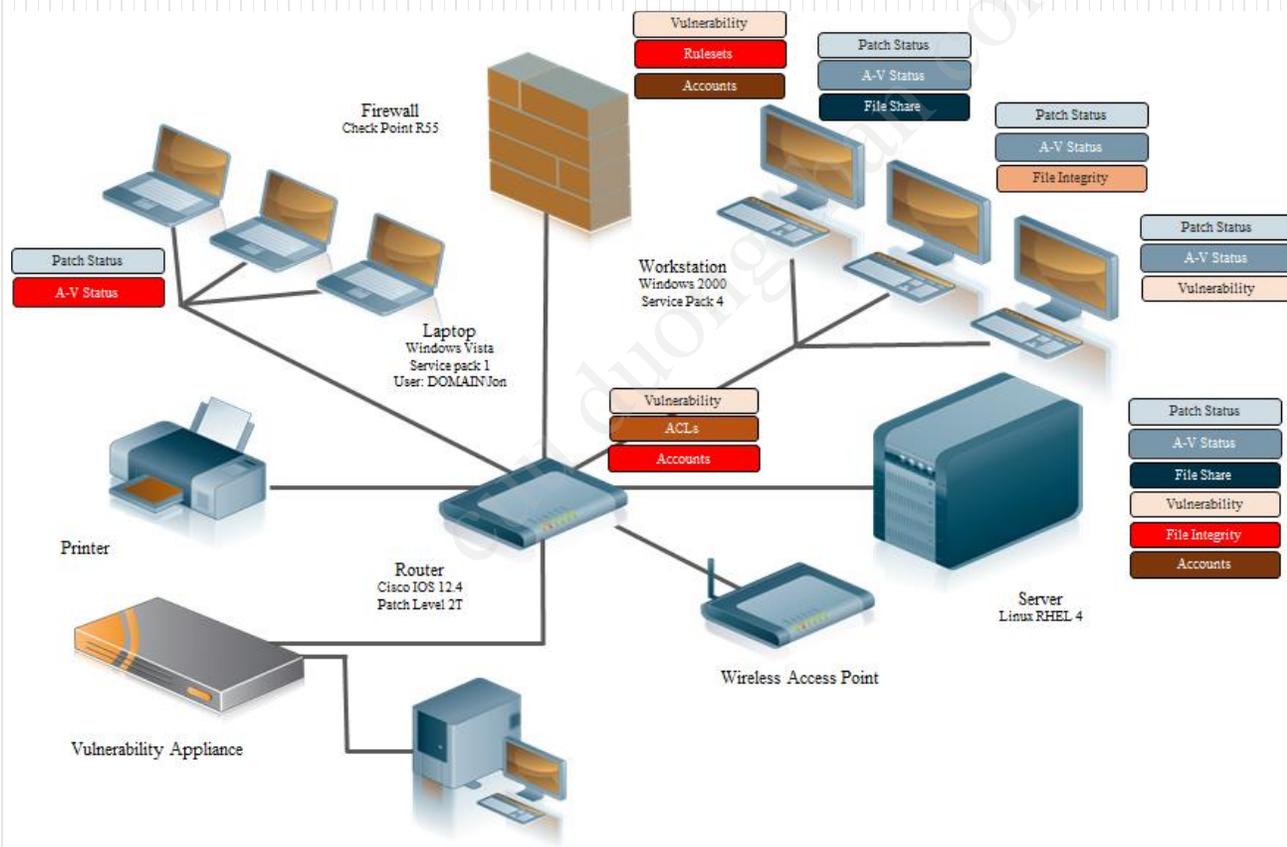
- 1) Malicious Attack
- 2) Attack Tools
- 3) The common types of malicious attacks
- 4) Malicious Software

# 1. Malicious Attack

---

# What Is a Malicious Attack?

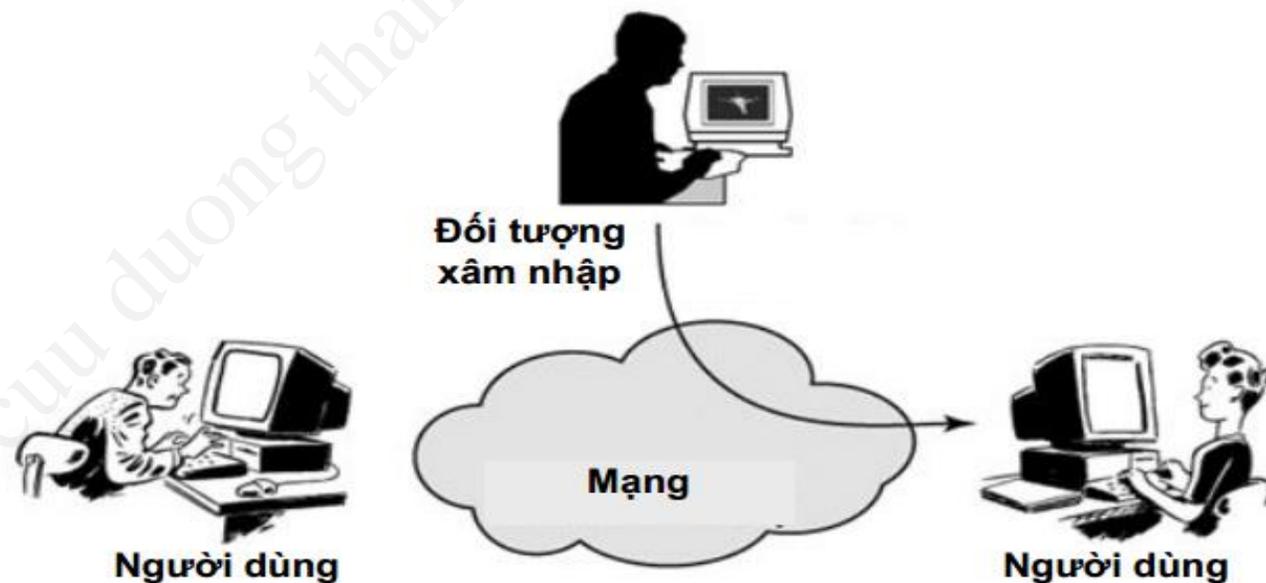
- An attack on a computer system or network asset succeeds by exploiting a vulnerability in the system.



# What Is a Malicious Attack?

An attack can consist of all or a combination of these four categories:

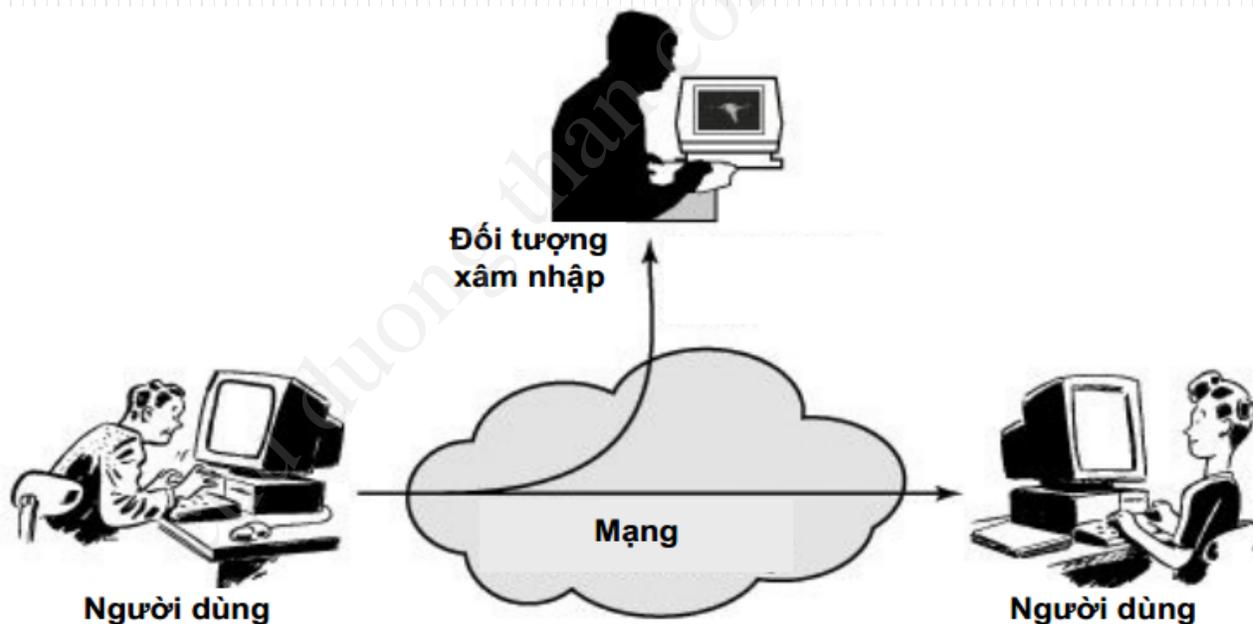
a) **Fabrications:** involve the creation of some deception in order to trick unsuspecting users.



Hình 1.8: Xâm nhập kiểu Fabrication

# What Is a Malicious Attack?

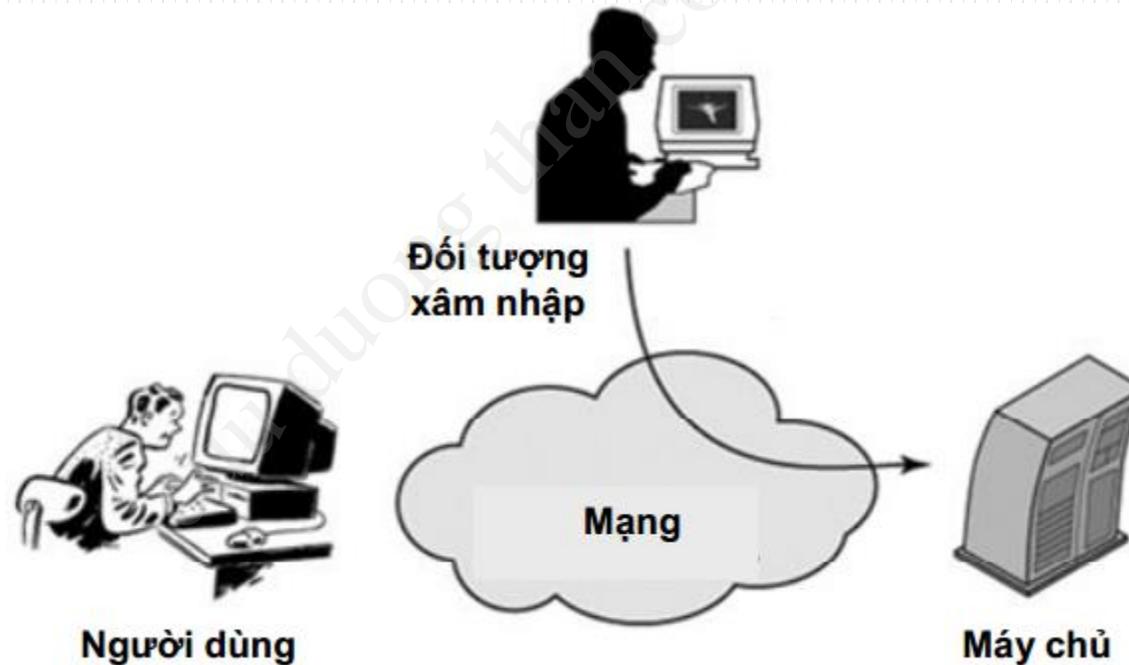
**b) Interceptions:** involve eavesdropping on transmissions and redirecting them for unauthorized use.



**Hình 1.6:** *Xâm nhập kiểu Interception*

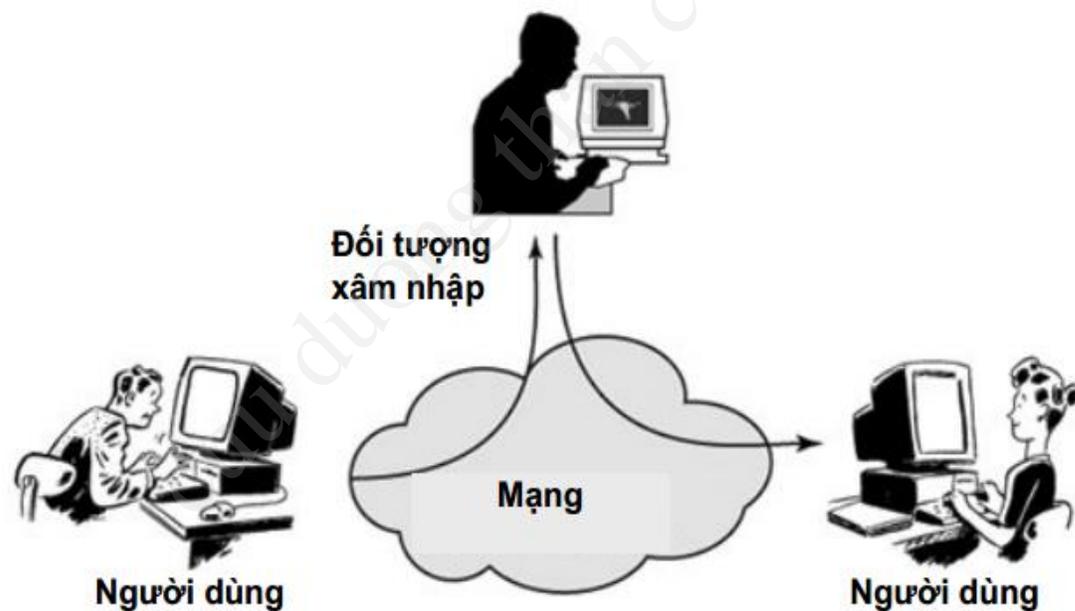
# What Is a Malicious Attack?

- c) **Interruptions:** An interruption causes a break in a communication channel, which blocks the transmission of data.



# What Is a Malicious Attack?

- d) **Modifications:** A modification is the alteration of data contained in transmissions or files



Hình 1.7: Xâm nhập kiểu Modification

## 2. Attack Tools

---

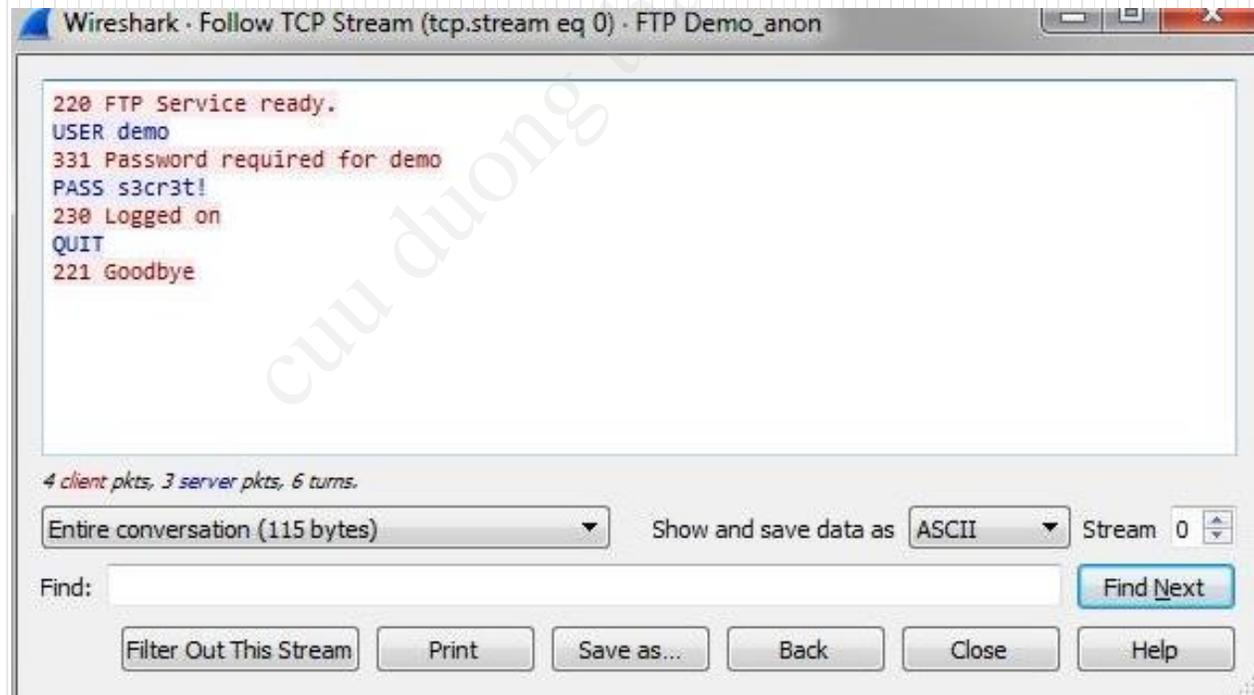
# Attack Tools

---

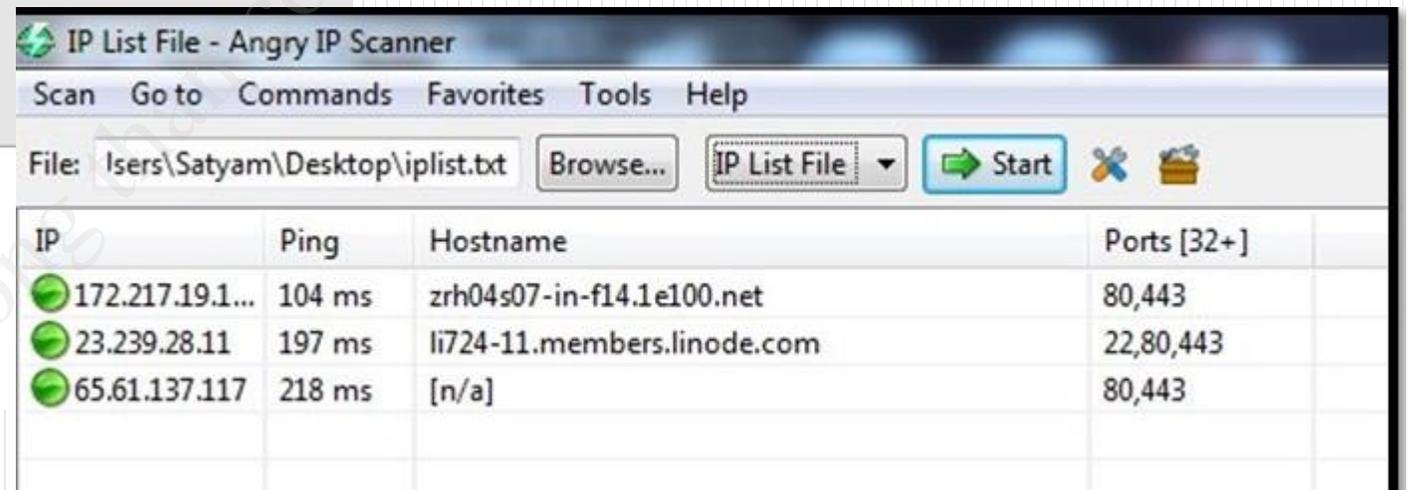
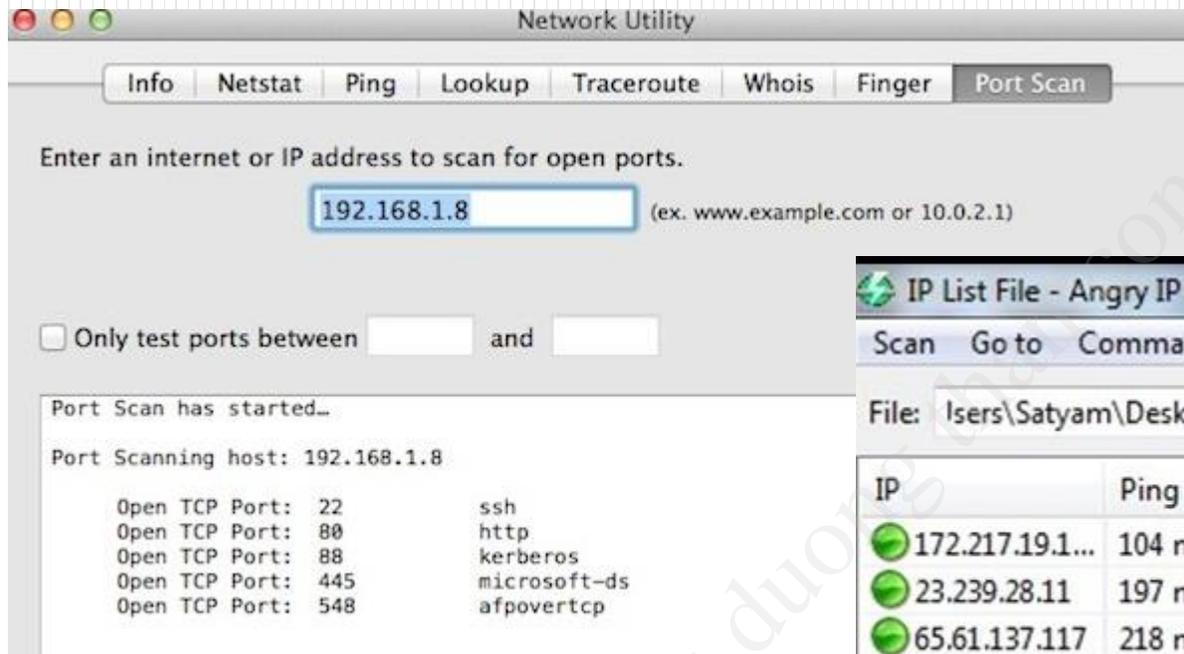
- Protocol analyzers
- Port scanners
- OS fingerprint scanners
- Vulnerability scanners
- Exploit software
- Wardialers
- Password crackers
- Keystroke loggers

# Protocol Analyzers

- A **protocol analyzer** or **packet sniffer** is a software program that enables a computer to monitor and capture network traffic.
- Every data packet can be seen and captured by the sniffer.



# Port Scanners



# OS Fingerprint Scanners

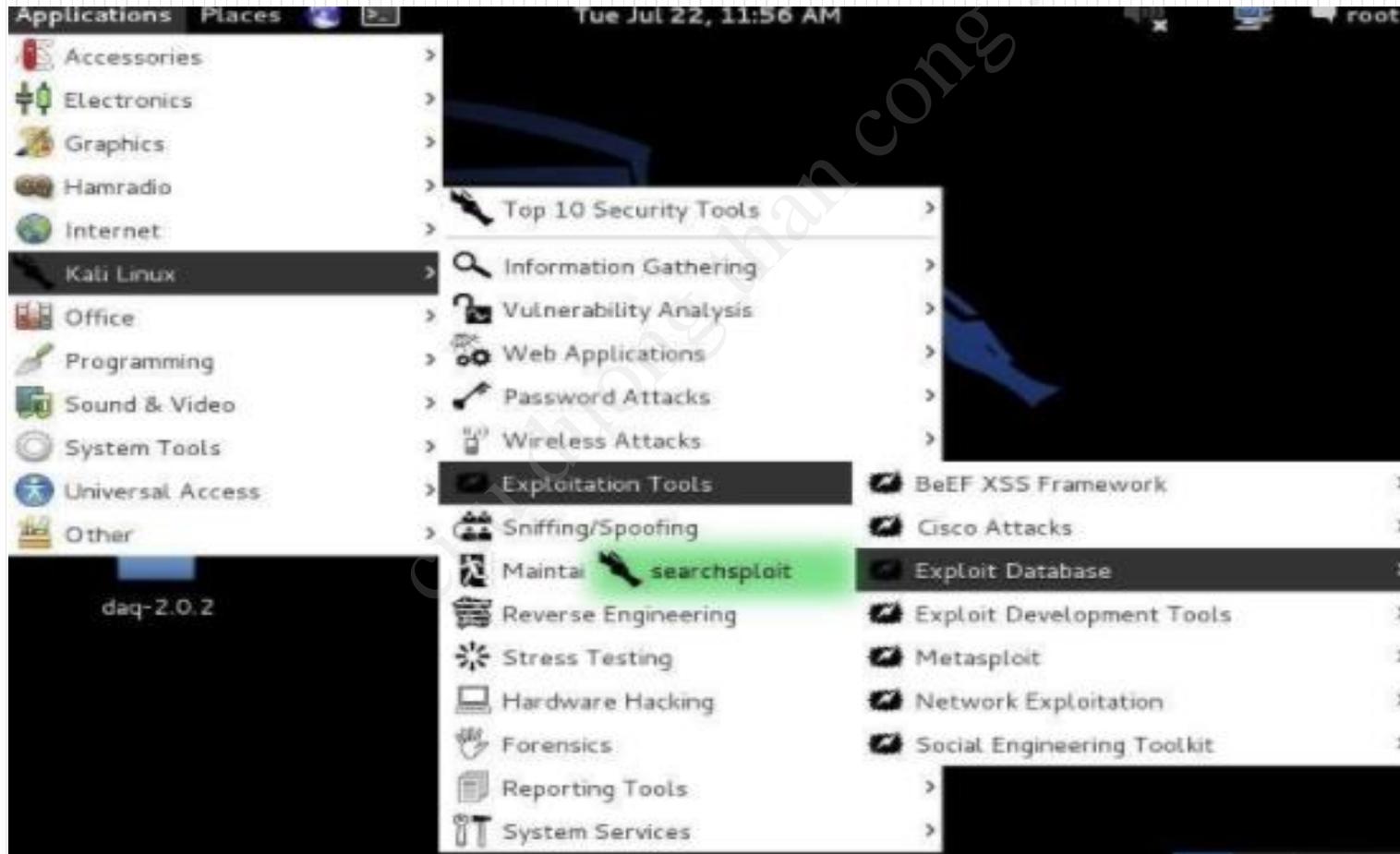
---

- An operating system (OS) fingerprint scanner is a software program that allows an attacker to send a variety of packets to an IP host device, hoping to determine the target device's operating system (OS) from the responses

**#nmap -O ip\_address**

# Exploit Software

- It is a program that can be used to exploit a weakness on the system



# Vulnerability Scanners

---

- A vulnerability scanner is a software program that is used to identify and, when possible, verify vulnerabilities on an IP host device
- Nexpose
- Nessus
- Kali Linux

# Password Crackers

---

- It is a software program that performs one of two functions: a brute-force password attack to gain unauthorized access to a system or recovery of passwords stored as a cryptographic hash on a computer system.
- Kali Linux

# Keystroke Loggers

- It is a type of surveillance software or hardware that can record to a log file every keystroke a user makes with a keyboard.



# 3. The common types of malicious attacks

---

# Password attacks

---

- **Brute-Force Password Attack:** the attacker tries different passwords on a system until one of them is successful.
- **Dictionary Password Attack:** a simple password-cracker program takes all the words from a dictionary file and attempts to log on by entering each dictionary entry as a password.

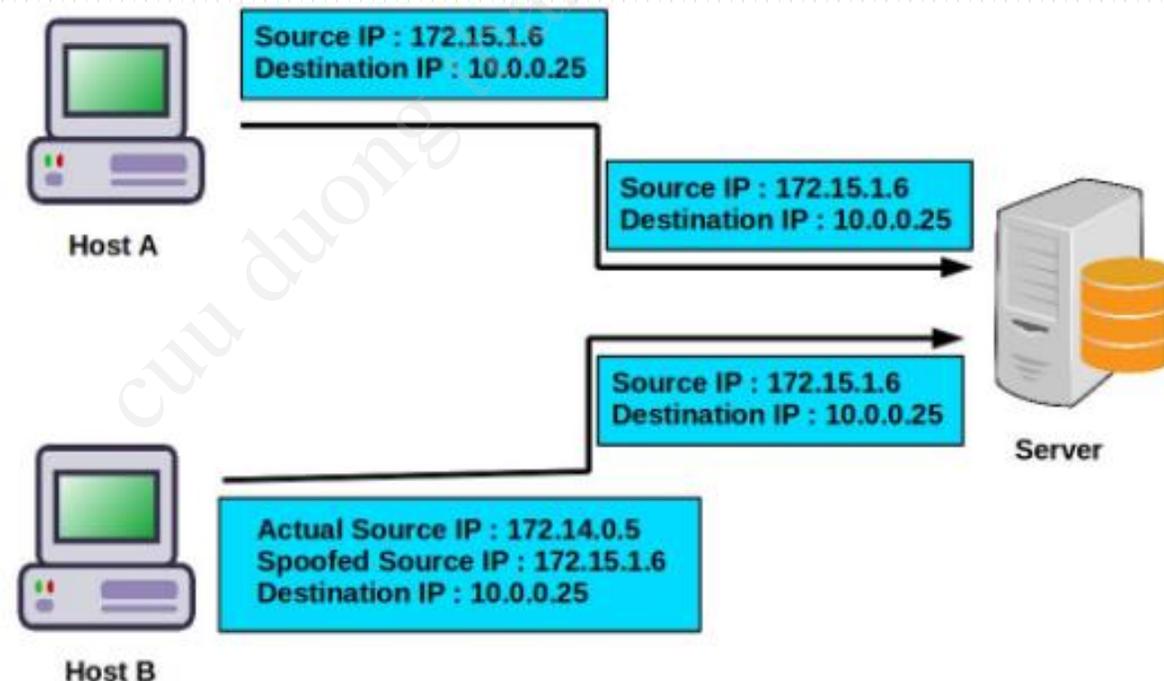
# IP Address Spoofing

---

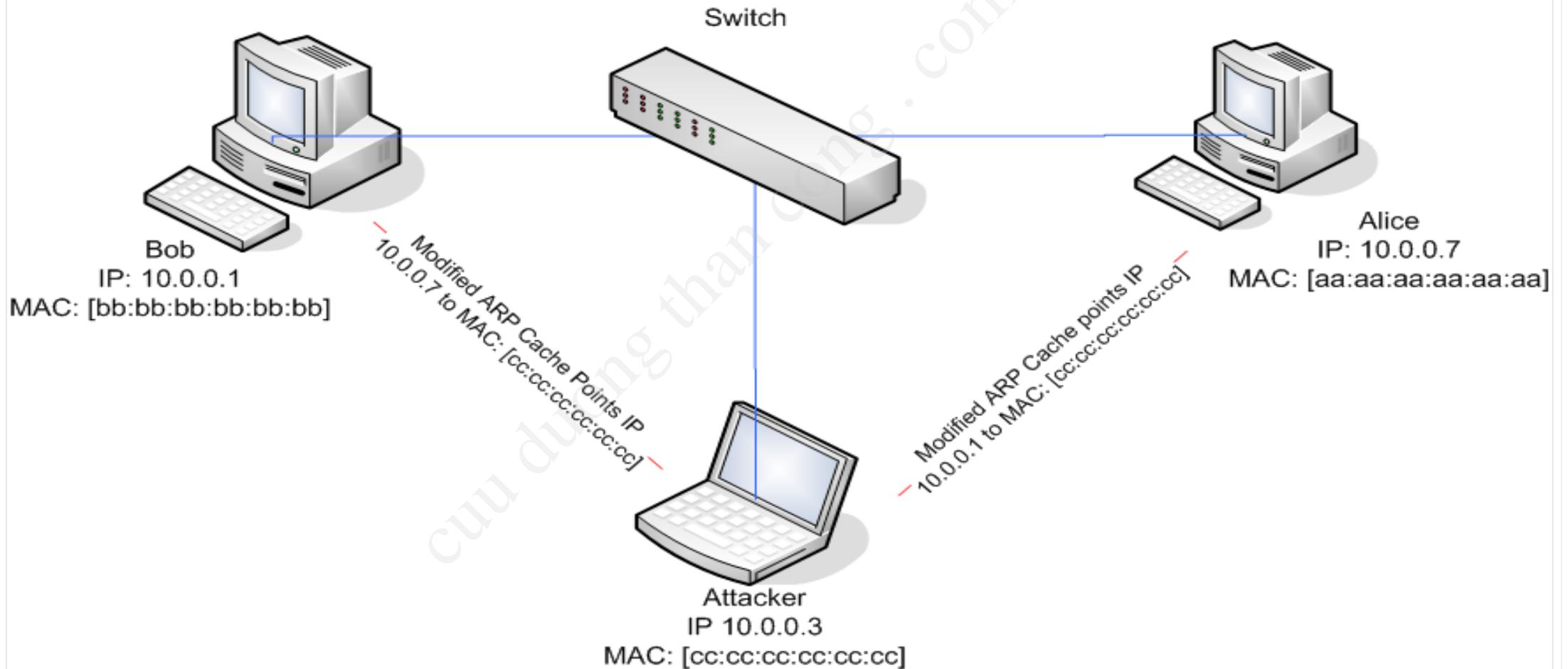
- **Spoofing** is a type of attack in which one person, program, or computer disguises itself as another person, program, or computer to gain access to some resource.
  - **IP spoofing**
  - **Address resolution protocol (ARP) poisoning**

# IP Address Spoofing

- **IP spoofing** is the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of hiding the identity of the sender or impersonating another computing system



# Address resolution protocol (ARP) poisoning



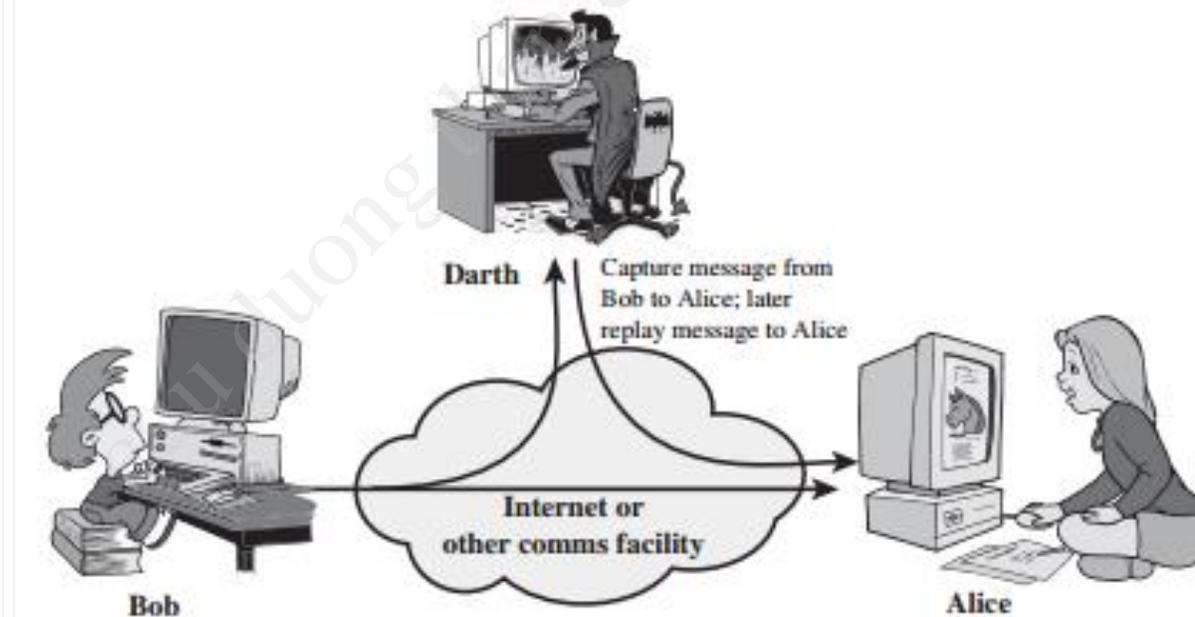
# Hijacking

---

- Hijacking is a type of attack in which the attacker takes control of a session between two machines and masquerades as one of them.
- Types of hijacking:
  - Man-in-the-middle hijacking
  - Browser or URL hijacking
  - Session hijacking

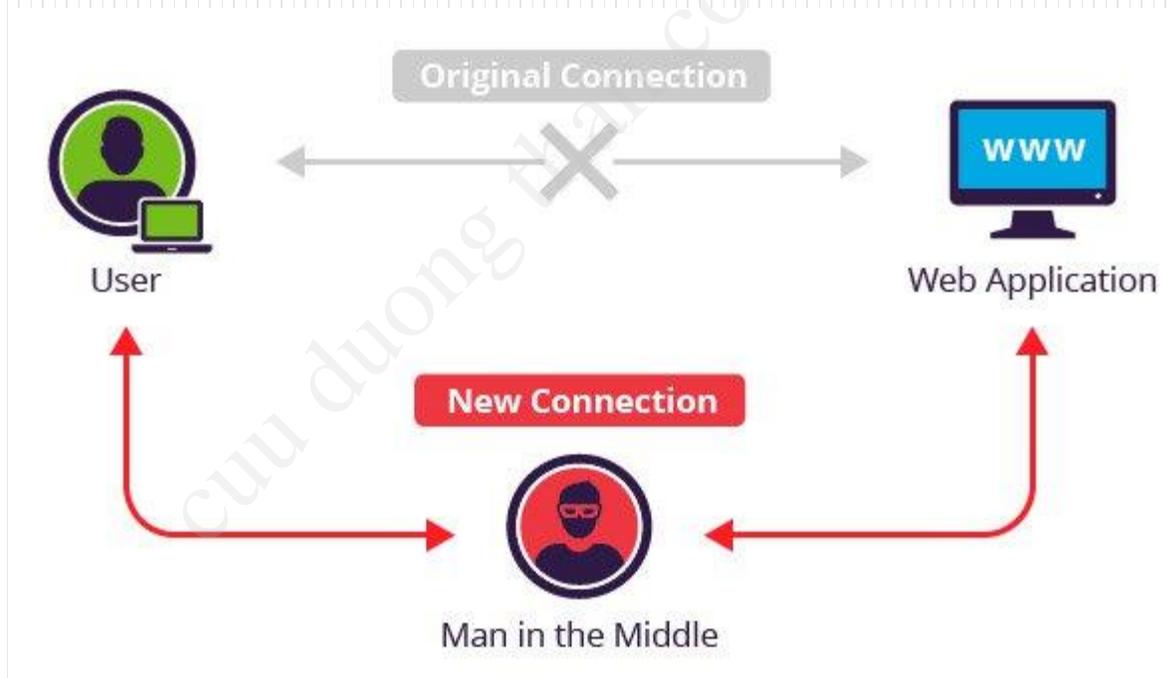
# Replay Attacks

- Replay attacks involve capturing data packets from a network and retransmitting them to produce an unauthorized effect.



# Man-in-the-Middle Attacks

- An attacker intercepts messages between two parties before transferring them on to their intended destination



# Social Engineering

Social engineering involves tricking authorized users into carrying out actions for unauthorized users.

- Phishing
- Spear phishing
- Baiting
- Pretexting

-- Ngày Thứ 4, 25/07/12, NguyenThi LanHuong <lhuor[redacted]m> đã viết:

Từ: NguyenThi LanHuong <lhuor[redacted].com>

Chủ đề: Danh sach tang luong Cui Nam 2012

Đến: duor[redacted].com

Ngày: Thứ Tư, 25 tháng 7, 2012, 11:09

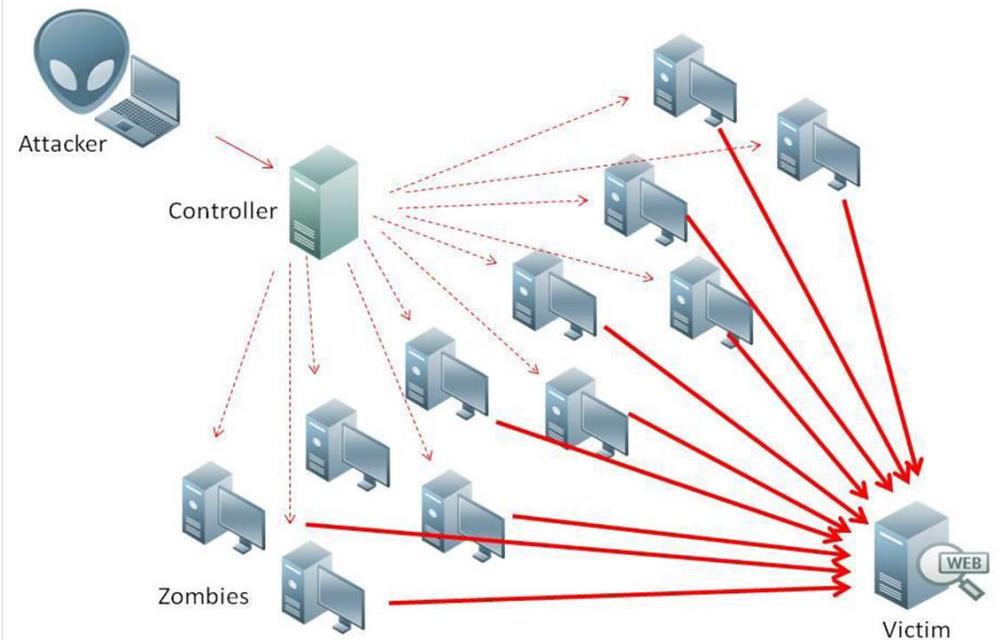
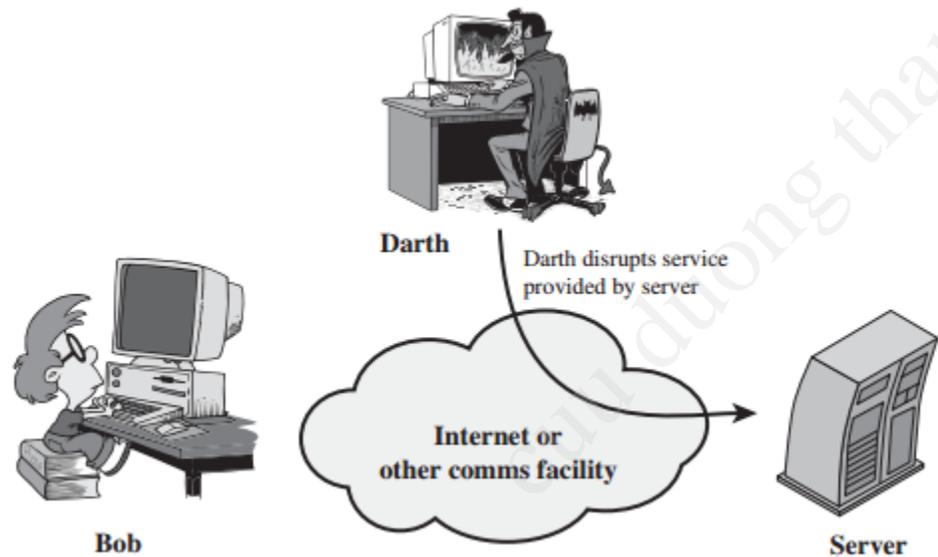
Chu y Danh sach co loi ko? .

 **DanhSachTangLuong.xls**  
77K [View](#) [Open as a Google spreadsheet](#) [Download](#)



# Denial of service - DOS

- A **Denial-of-Service (DoS)** attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users



Distributed Denial of Service

# 4. Malicious Software

---

# What Is Malicious Software?

---

- Malicious software - Malware, commonly known as malware, is any software that brings harm to a computer system.

## Malware exists in two main categories:

- **Infecting programs:** actively attempt to copy themselves to other computers. (Viruses, Worms)
- **Hiding programs:** Trojan horses, Rootkits, Spyware

# Viruses

---

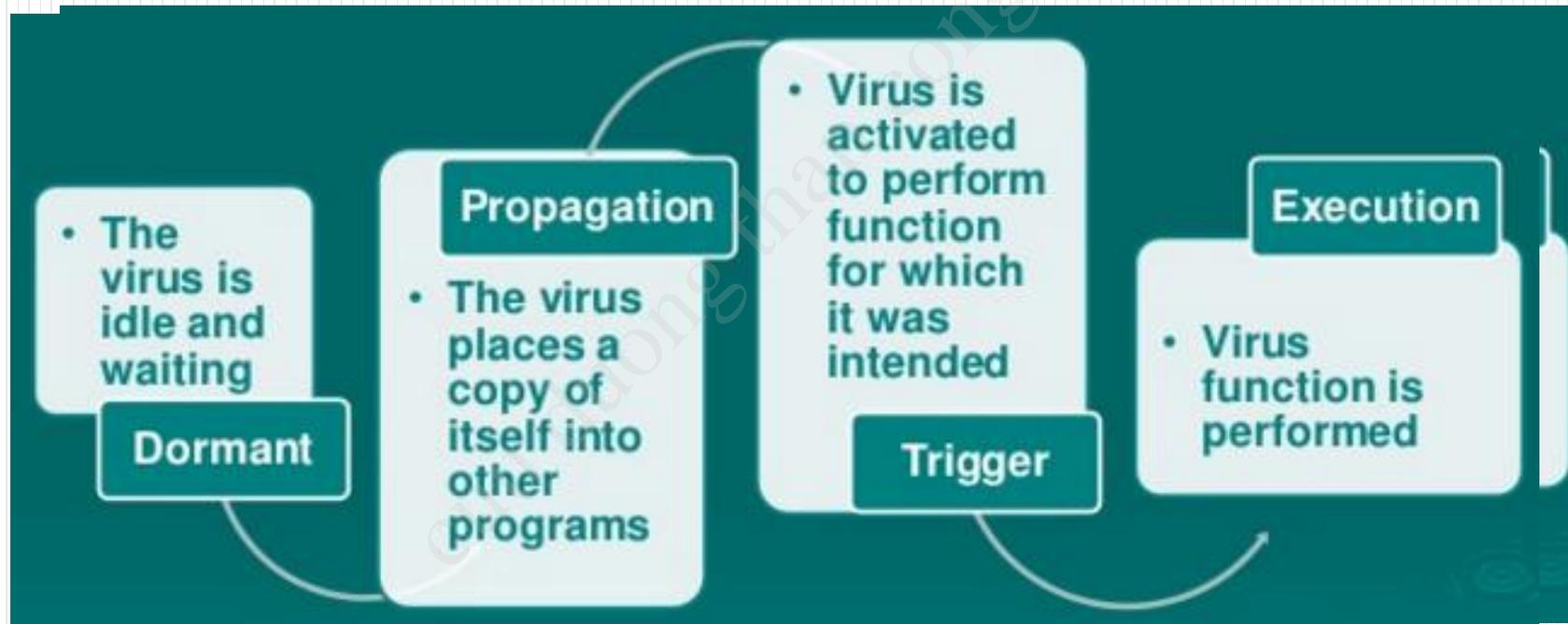
- A computer virus is a software program that attaches itself to or copies itself into another program on a computer.

## **Virus has three parts:**

- Infection mechanism: How a virus spreads
- Trigger: The means of deciding whether to deliver the payload or not
- Payload: What the virus does, besides spread.

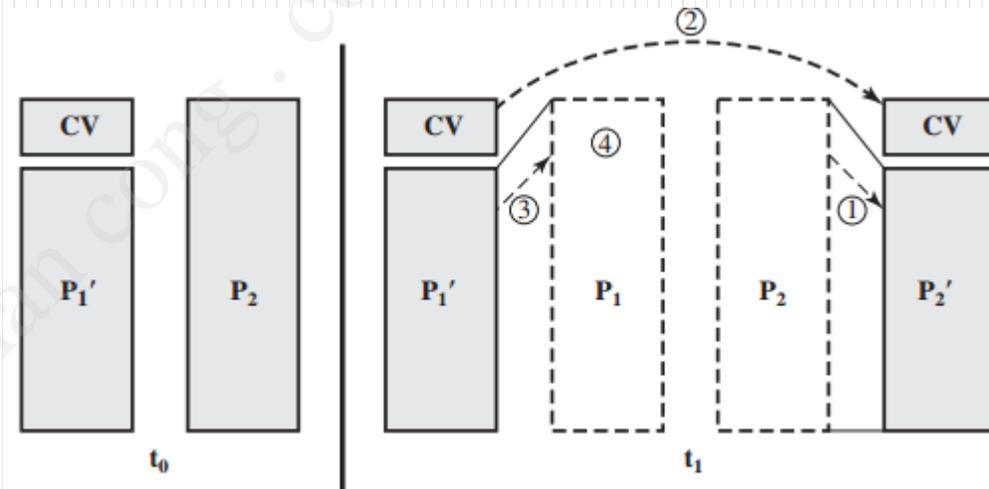
# Viruses

- 4 Phases of virus:



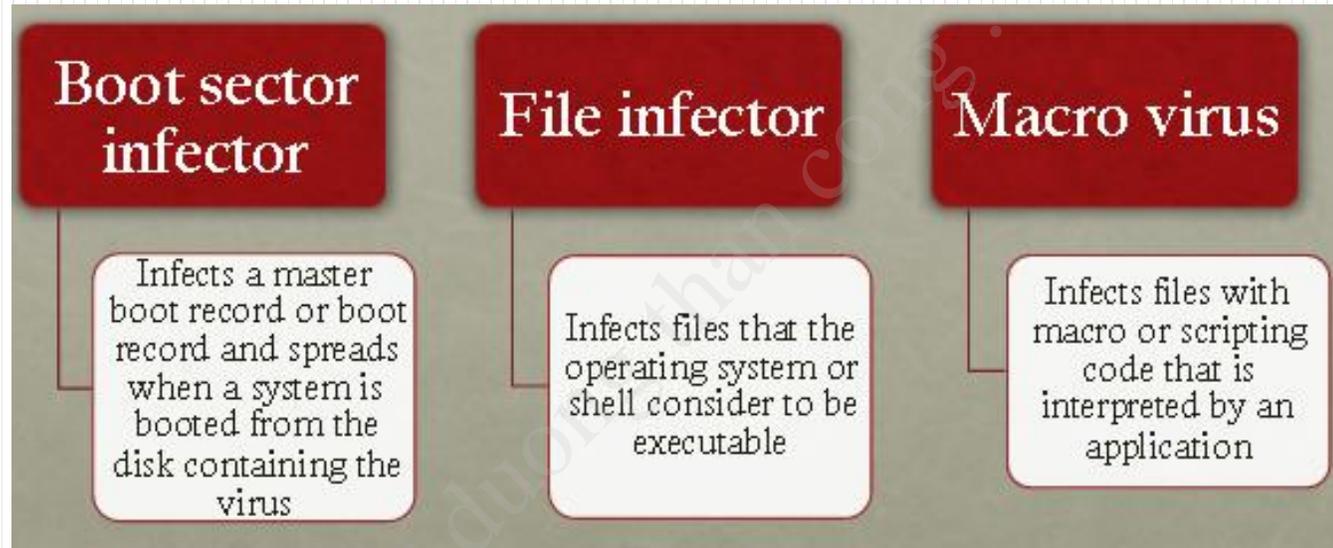
# Viruses

```
program CV :=  
{goto main;  
 01234567;  
  
  subroutine infect-executable :=  
    {loop:  
      file := get-random-executable-file;  
      if (first-line-of-file = 01234567) then goto loop;  
      (1) compress file;  
      (2) prepend CV to file;  
    }  
  
  main:  main-program :=  
    {if ask-permission then infect-executable;  
      (3) uncompress rest-of-file;  
      (4) run uncompressed file;  
    }
```



# Viruses

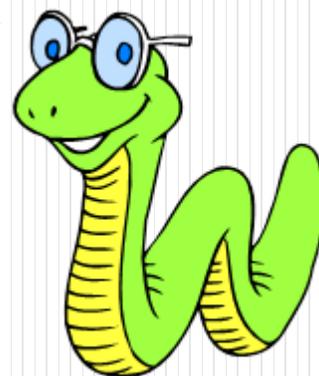
---



# WORM

---

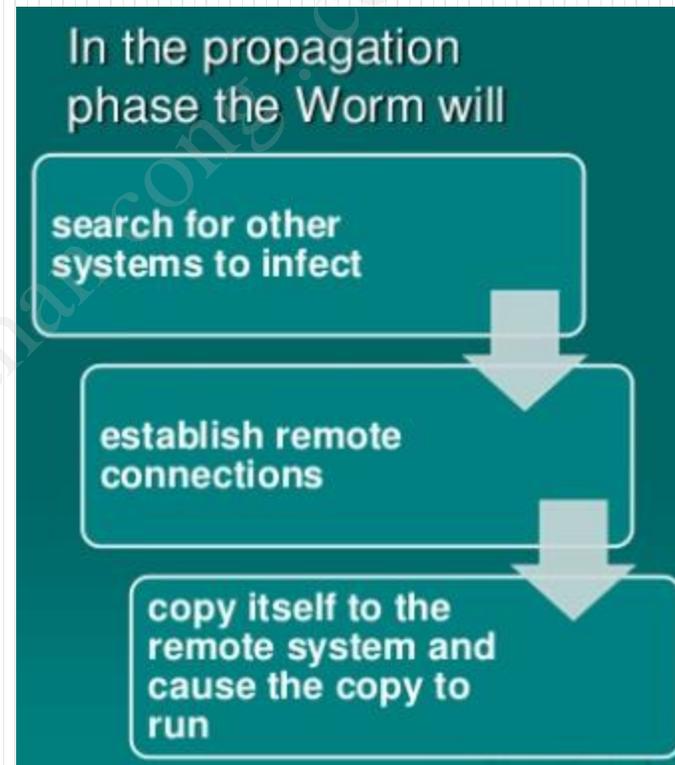
- The worm is a standalone program. that replicates and sends copies of itself to other computers, generally across a network, without any user input or action.
- Self replicating approaches:
  - Email
  - File sharing
  - Remote execution
  - Remote login



# WORM

---

- Phases:
  - Dormant
  - Propagation
  - Trigger
  - Execution



# Trojan horses

---

- A Trojan horse, also called a Trojan, is malware that masquerades as a useful program.
- A Trojan is different from a virus as it does not copy its code to other hosts or boot areas

# Rootkits

---

- Collection of attacker tools installed after an intruder has gained access
  - Log cleaners
  - File/process/user hiding tools
  - Network sniffer
  - Backdoor programs
- Rootkits often work with other malware.

# Spyware

---

- Spyware is software that aims to gather information about a person or organization without their knowledge, that may send such information to another entity without the consumer's consent

---

**Thanks**