Malicious Attacks

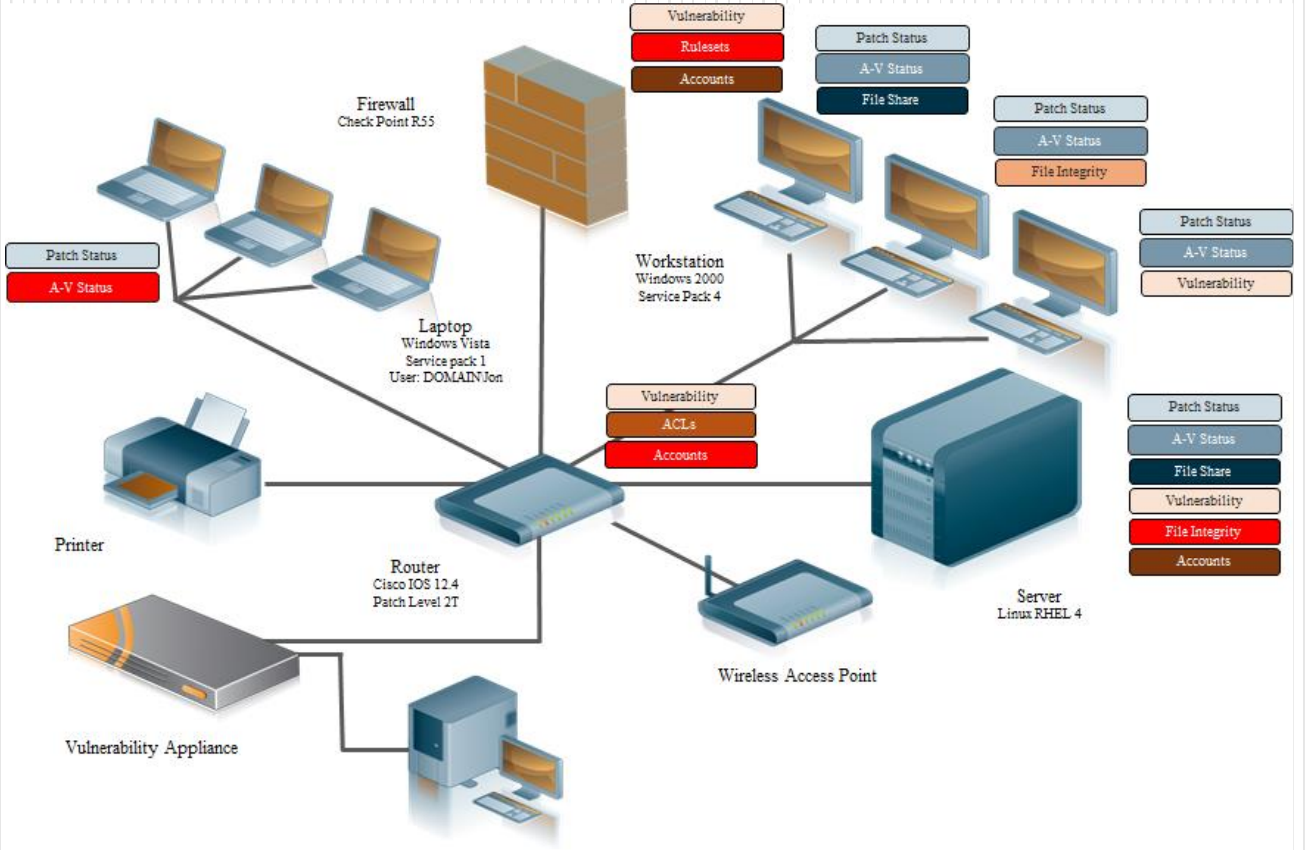
Contents

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

1.Malicious Attack

What Is a Malicious Attack?

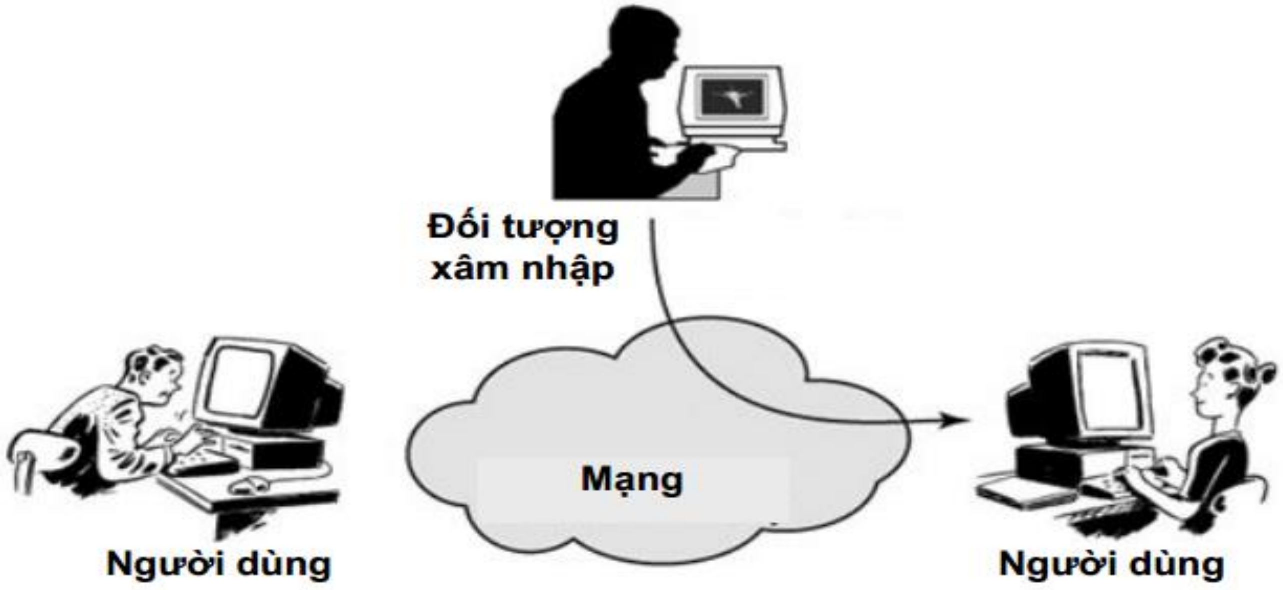
- An attack on a computer system or network asset succeeds by exploiting a vulnerability in the system.



What Is a Malicious Attack?

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

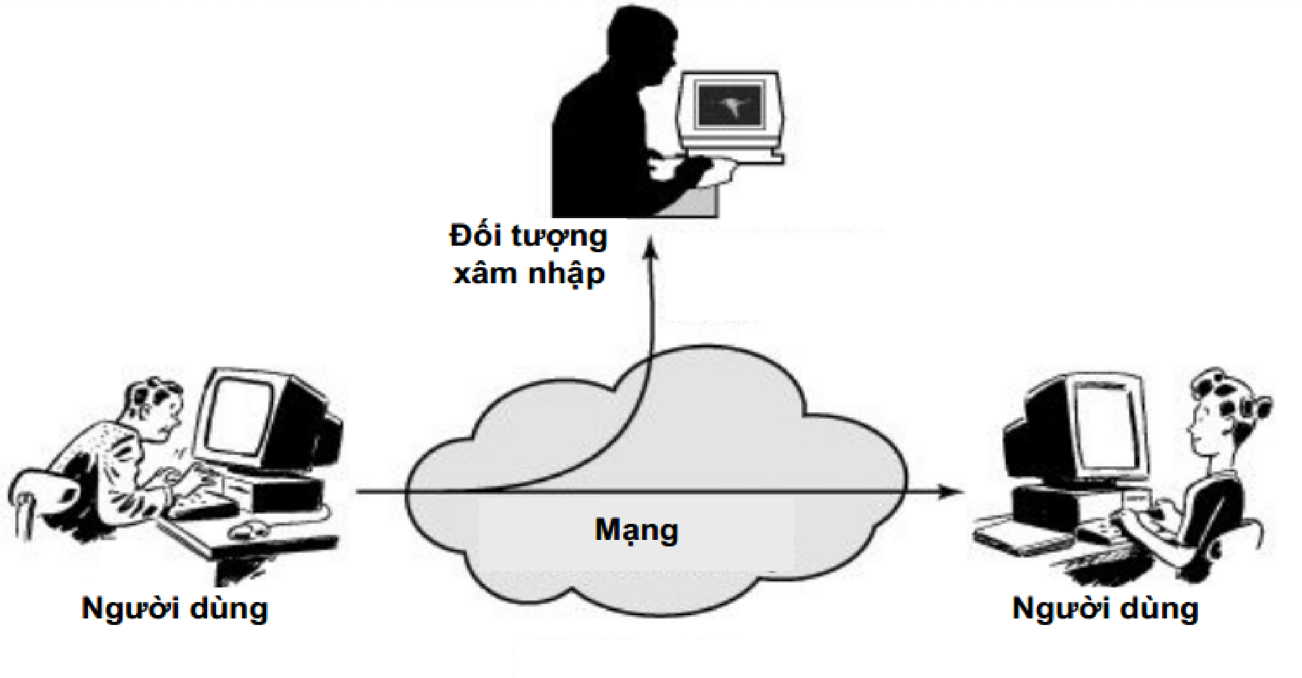
a) **Fabrications**: involve the creation of some deception in order to trick unsuspecting users.



Hình 1.8: *Xâm nhập kiểu Farbrication*

What Is a Malicious Attack?

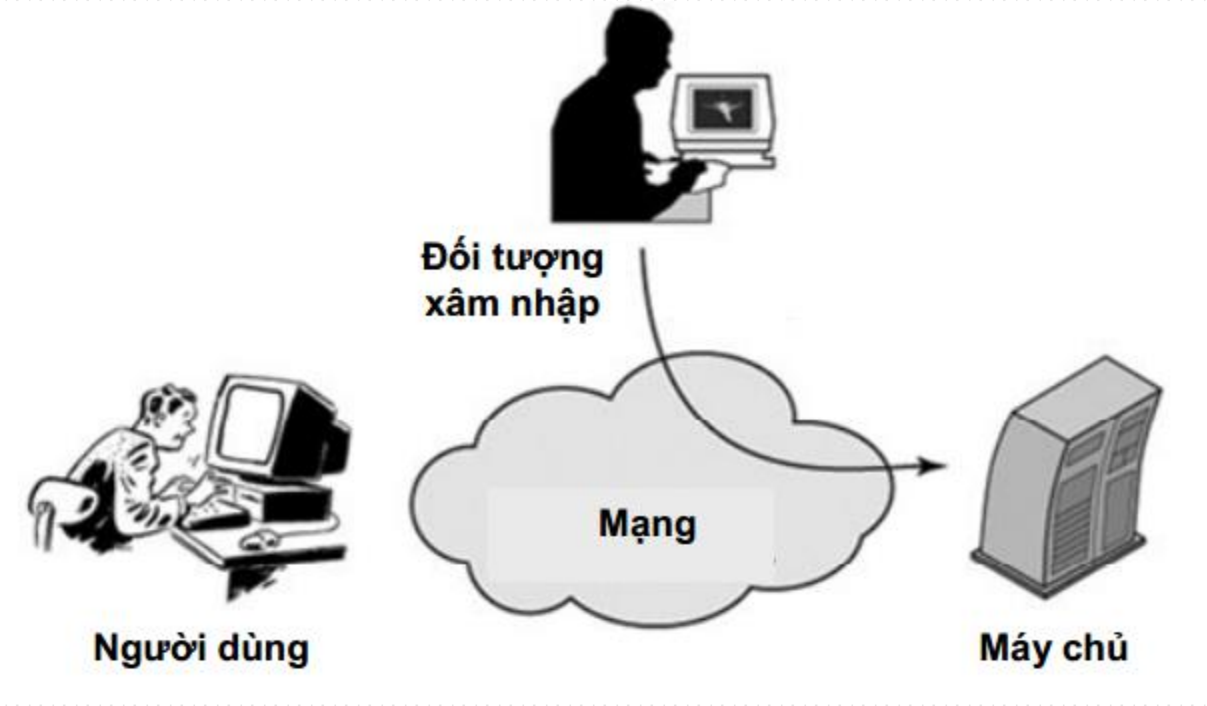
b) Interceptions: involve eavesdropping on transmissions and redirecting them for unauthorized use.



Hình 1.6: *Xâm nhập kiểu Interception*

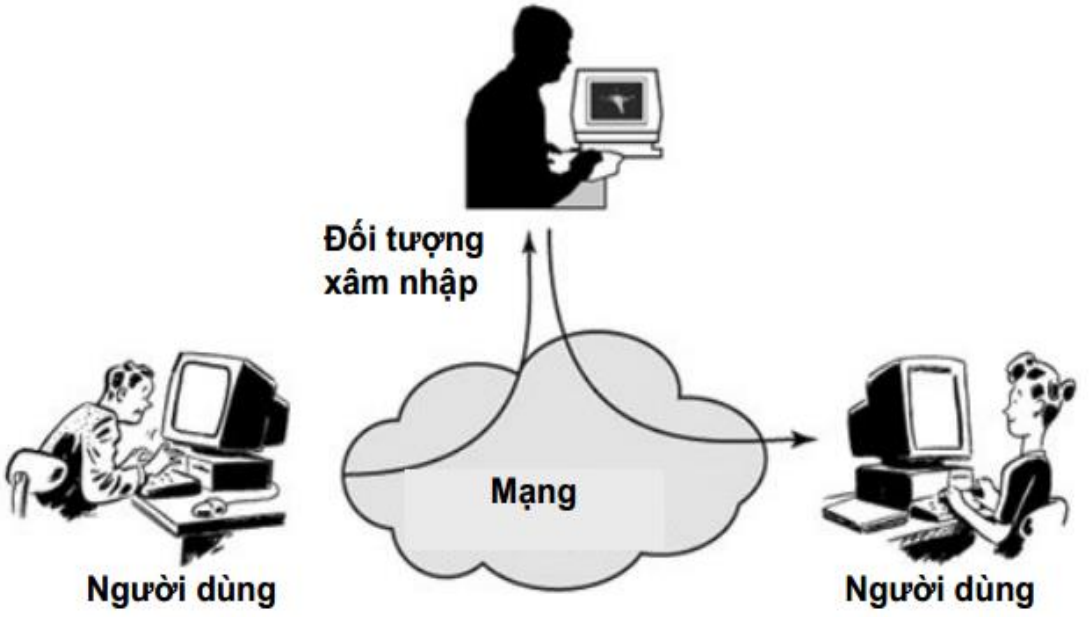
What Is a Malicious Attack?

- 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*

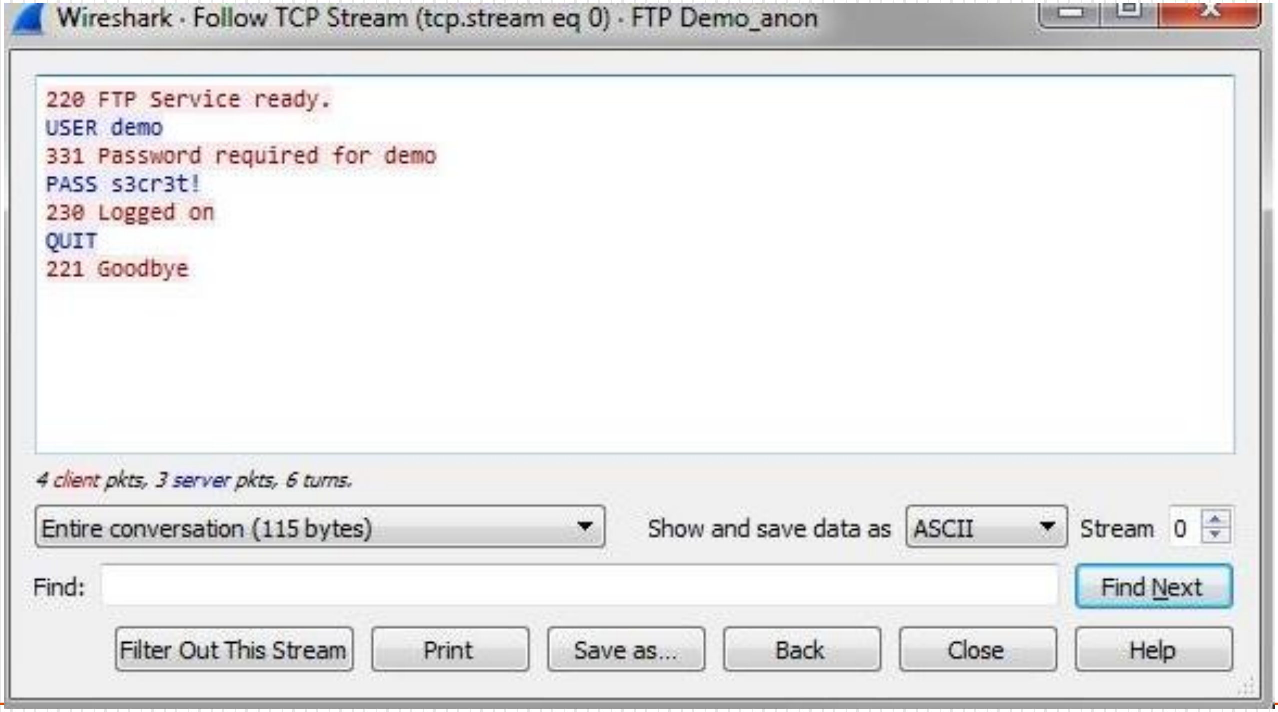
2. Attack Tools

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.


Wireshark · Follow TCP Stream (tcp.stream eq 0) · FTP Demo_anon

```
220 FTP Service ready.
USER demo
331 Password required for demo
PASS s3cr3t!
230 Logged on
QUIT
221 Goodbye
```

4 client pkts, 3 server pkts, 6 turns.

Entire conversation (115 bytes)

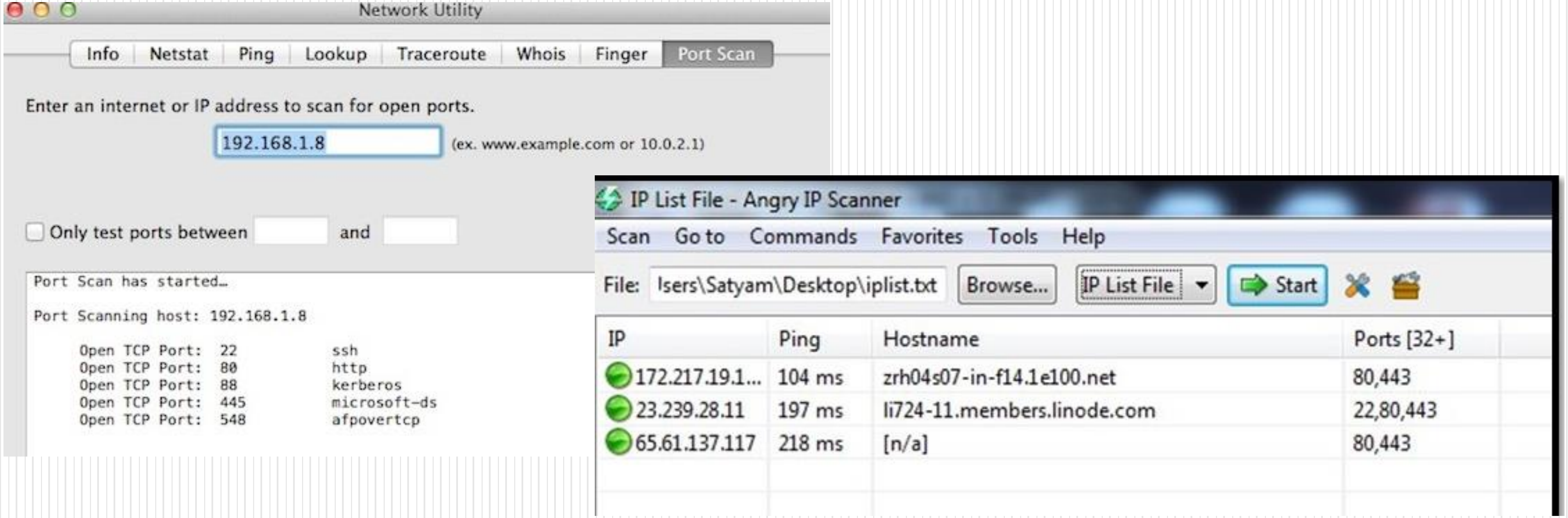
Show and save data as: ASCII

Stream: 0

Find:

Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help

Port Scanners



Enter an internet or IP address to scan for open ports.

192.168.1.8 (ex. www.example.com or 10.0.2.1)

□ Only test ports between and

```
Port Scan has started…

Port Scanning host: 192.168.1.8

     Open TCP Port:  22          ssh
     Open TCP Port:  80          http
     Open TCP Port:  88          kerberos
     Open TCP Port:  445         microsoft-ds
     Open TCP Port:  548         afpovertcp
```

File: lsers\Satyam\Desktop\iplist.txt

IP	Ping	Hostname	Ports [32+]
172.217.19.1...	104 ms	zrh04s07-in-f14.1e100.net	80,443
23.239.28.11	197 ms	li724-11.members.linode.com	22,80,443
65.61.137.117	218 ms	[n/a]	80,443

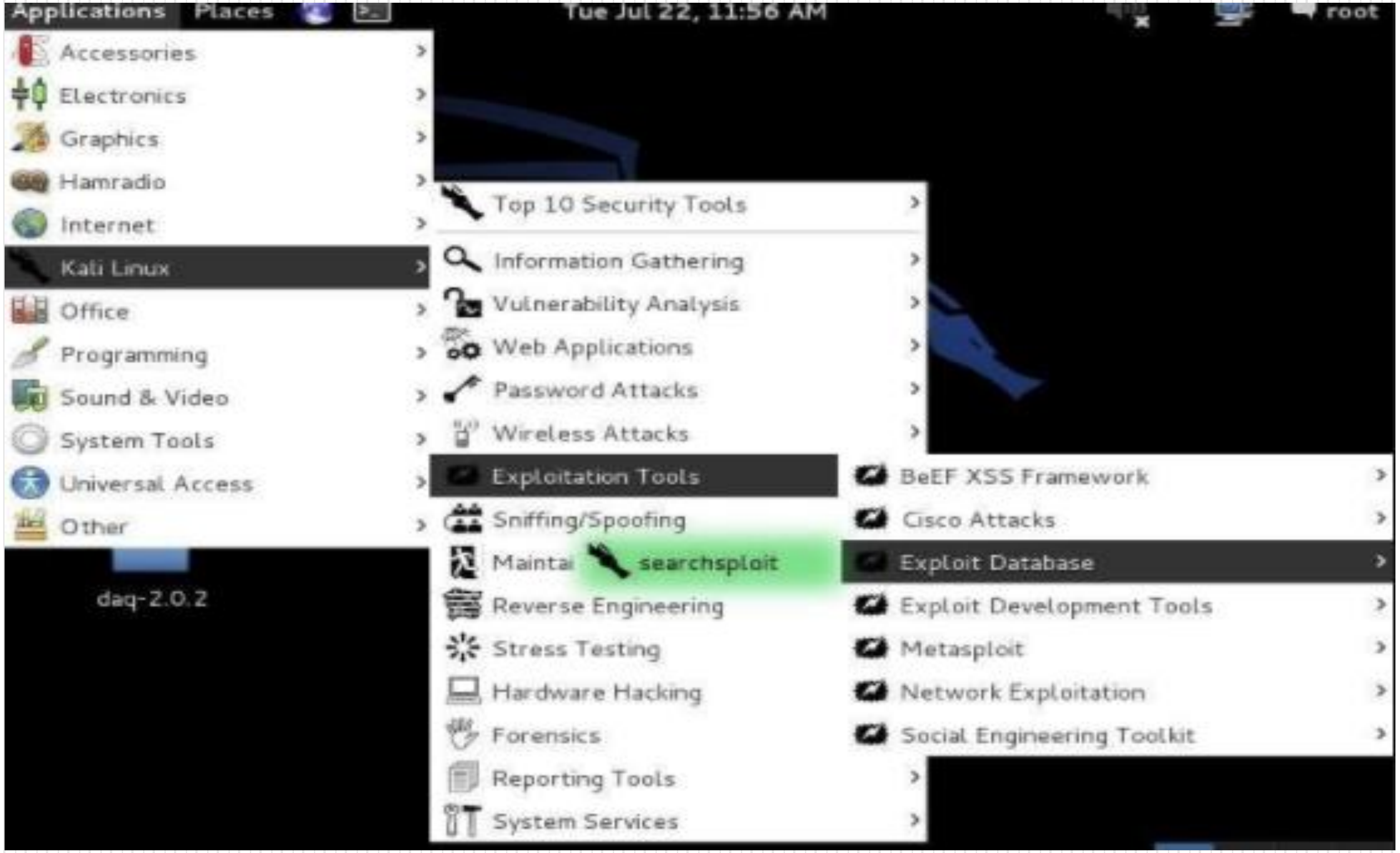
OS Fingerprint Scanners

- 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

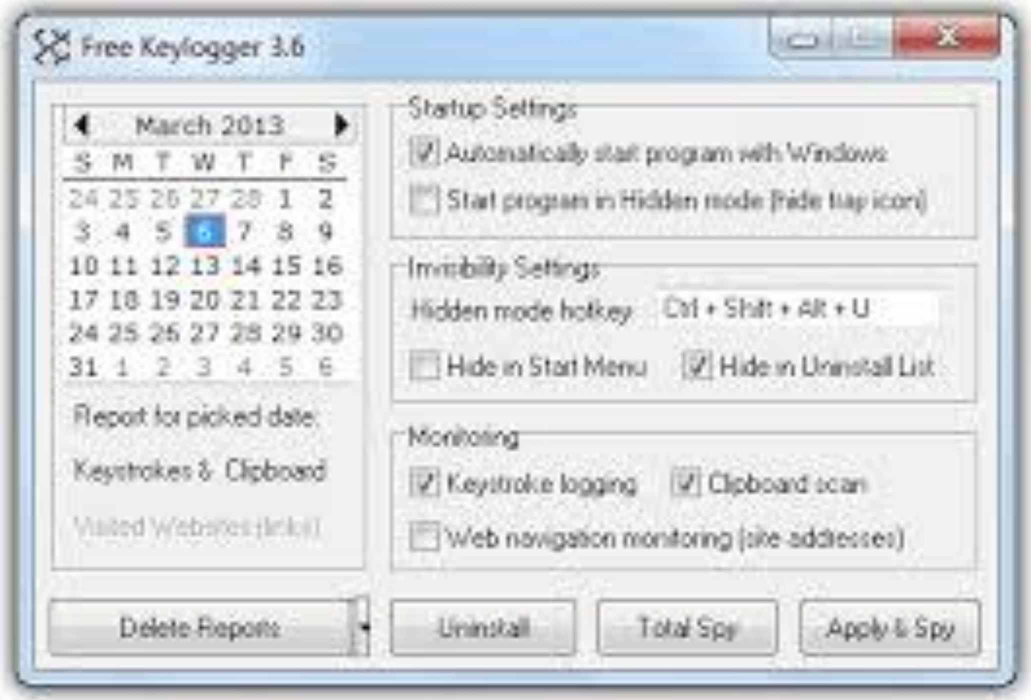
- A vulnerability scanner is a software program that is used to identify and, when possible, verify vulnerabilities on an IP host device
- Nexpose
- Nessus
- Kali Linux

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.



Free Keylogger 3.6

March 2013

S	M	T	W	T	F	S
24	25	26	27	28	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Report for picked date:

Keystrokes & Clipboard

Visited Websites (links)

Startup Settings

☑ Automatically start program with Windows

□ Start program in Hidden mode (hide tray icon)

Invisibility Settings

Hidden mode hotkey: Ctrl + Shift + Alt + U

□ Hide in Start Menu ☑ Hide in Uninstall List

Monitoring

☑ Keystroke logging ☑ Clipboard scan

□ Web navigation monitoring (site addresses)

3. The common types of malicious attacks

Password attacks

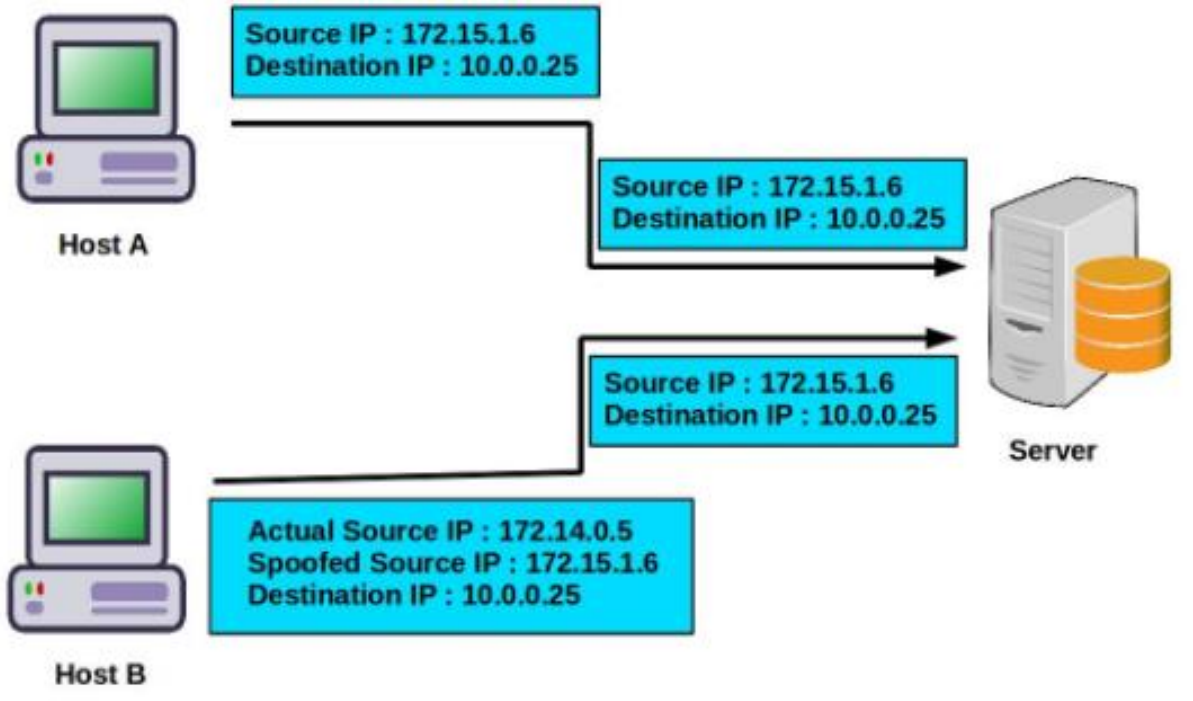
- **Brute-Force Password Attack:** the attacker tries different passwords on a system until one of them is successful.
- **Dictionary Password Attack**: a simple password-cracker program takes all the words from a dictionary file and attempts to log on by entering each dictionary entry as a password.

IP Address Spoofing

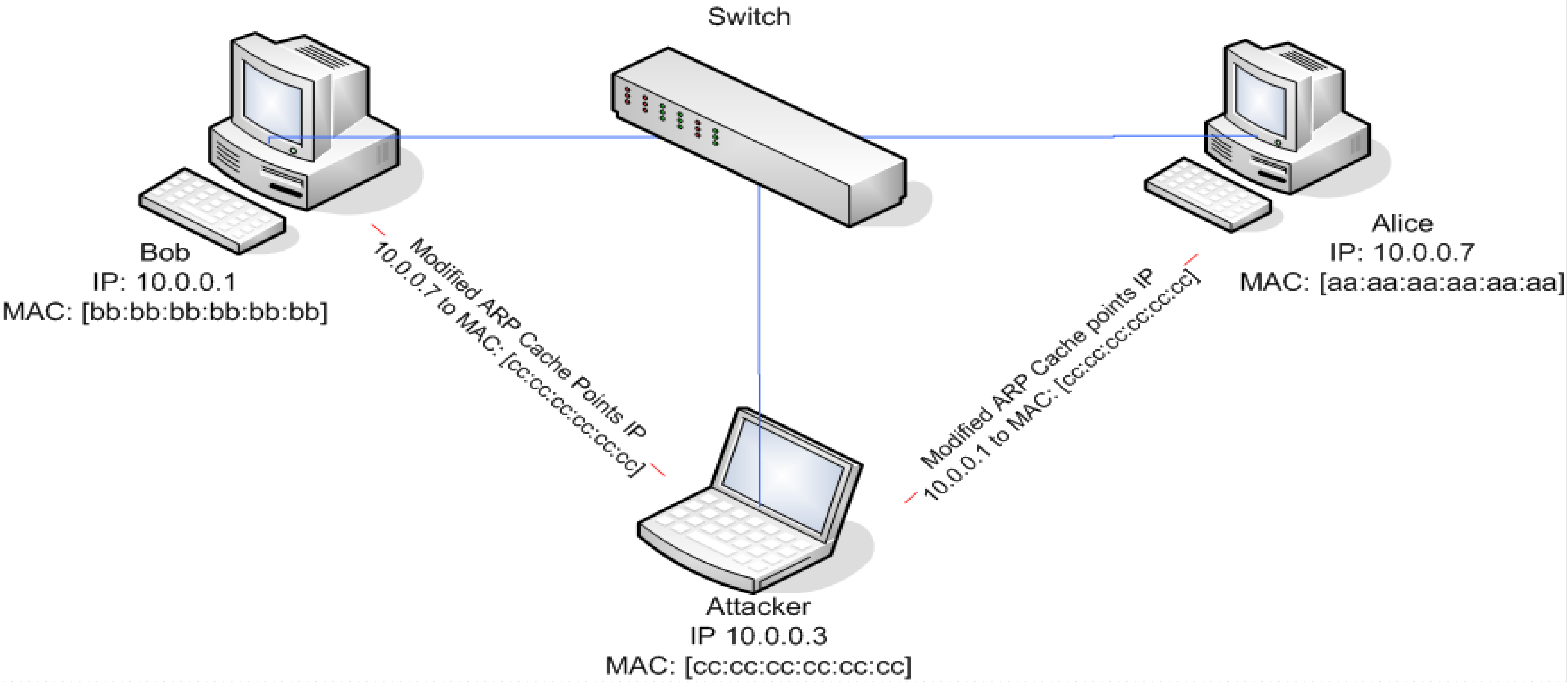
- **Spoofing** is a type of attack in which one person, program, or computer disguises itself as another person, program, or computer to gain access to some resource.
  - **IP spoofing**
  - **Address resolution protocol (ARP) poisoning**

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


Source IP : 172.15.1.6
Destination IP : 10.0.0.25
Host A
Source IP : 172.15.1.6
Destination IP : 10.0.0.25
Server
Source IP : 172.15.1.6
Destination IP : 10.0.0.25
Actual Source IP : 172.14.0.5
Spoofed Source IP : 172.15.1.6
Destination IP : 10.0.0.25
Host B

Address resolution protocol (ARP) poisoning

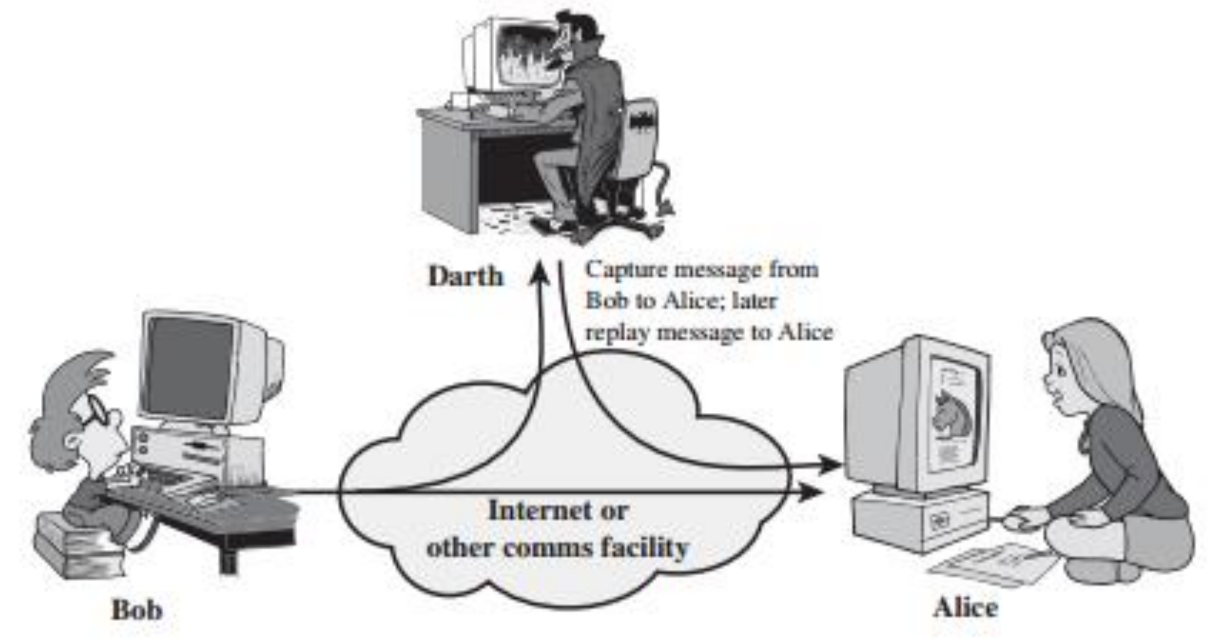

Switch
Bob
IP: 10.0.0.1
MAC: [bb:bb:bb:bb:bb:bb]
Alice
IP: 10.0.0.7
MAC: [aa:aa:aa:aa:aa:aa]
Modified ARP Cache Points IP 10.0.0.7 to MAC: [cc:cc:cc:cc:cc:cc]
Modified ARP Cache points IP 10.0.0.1 to MAC: [cc:cc:cc:cc:cc:cc]
Attacker
IP 10.0.0.3
MAC: [cc:cc:cc:cc:cc:cc]

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

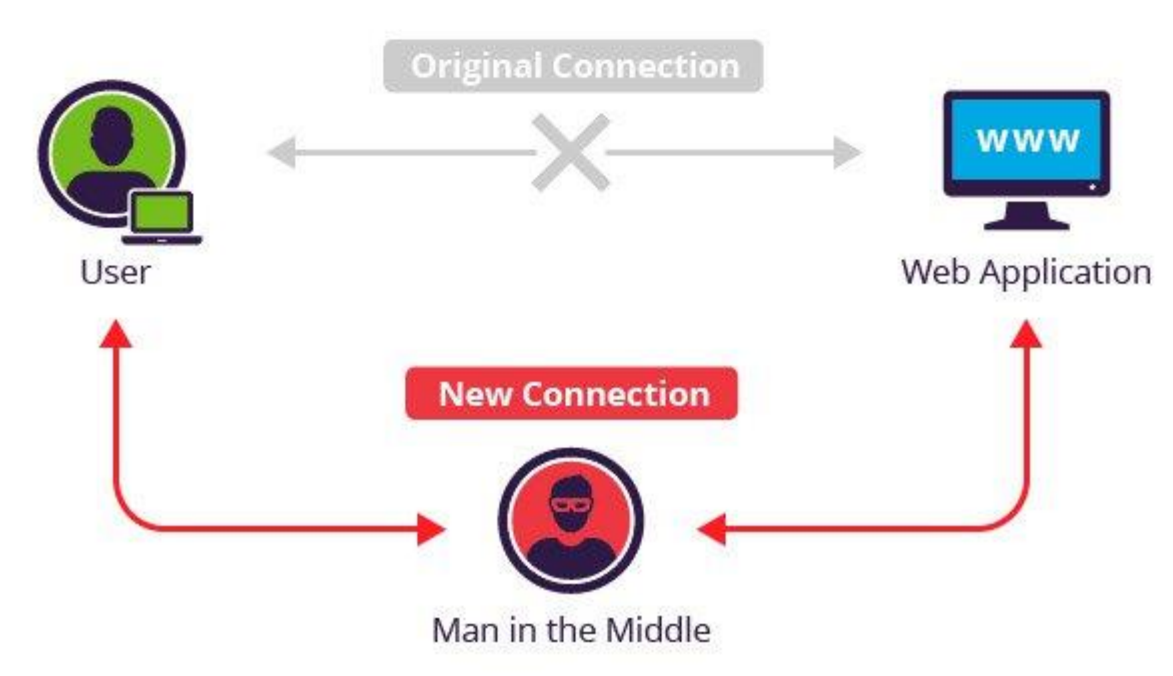
Replay Attacks

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


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Man-in-the-Middle Attacks

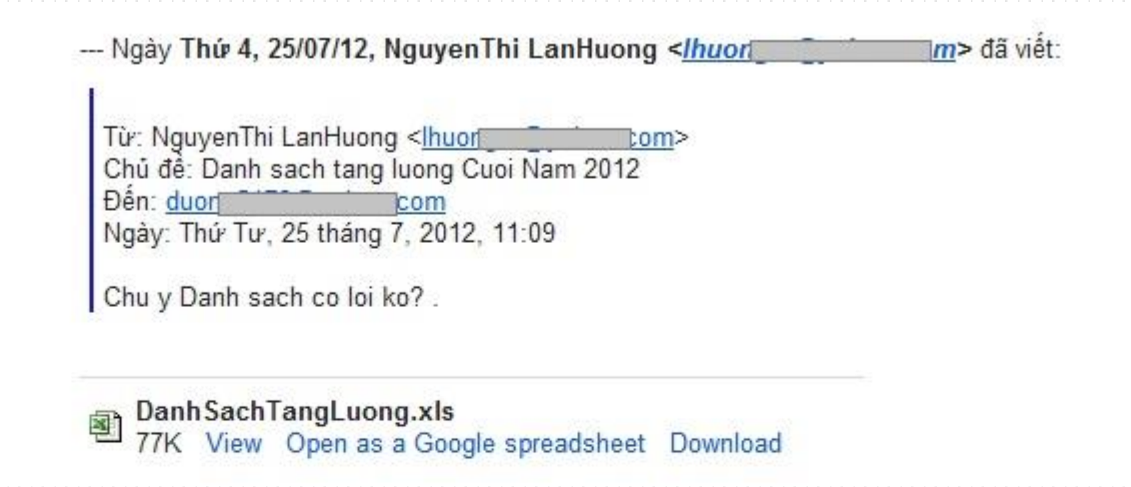
- An attacker intercepts messages between two parties before transferring them on to their intended destination



Social Engineering

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

- Phishing
- Spear phishing
- Baiting
- Pretexting

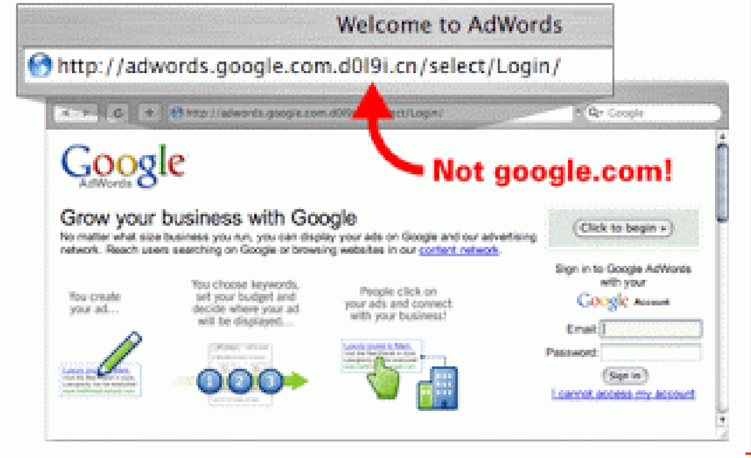


--- Ngày Thứ 4, 25/07/12, NguyenThi LanHuong <lhuon[redacted]m> đã viết:

Từ: NguyenThi LanHuong <lhuon[redacted]com>
Chủ đề: Danh sach tang luong Cuoi Nam 2012
Đến: duon[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



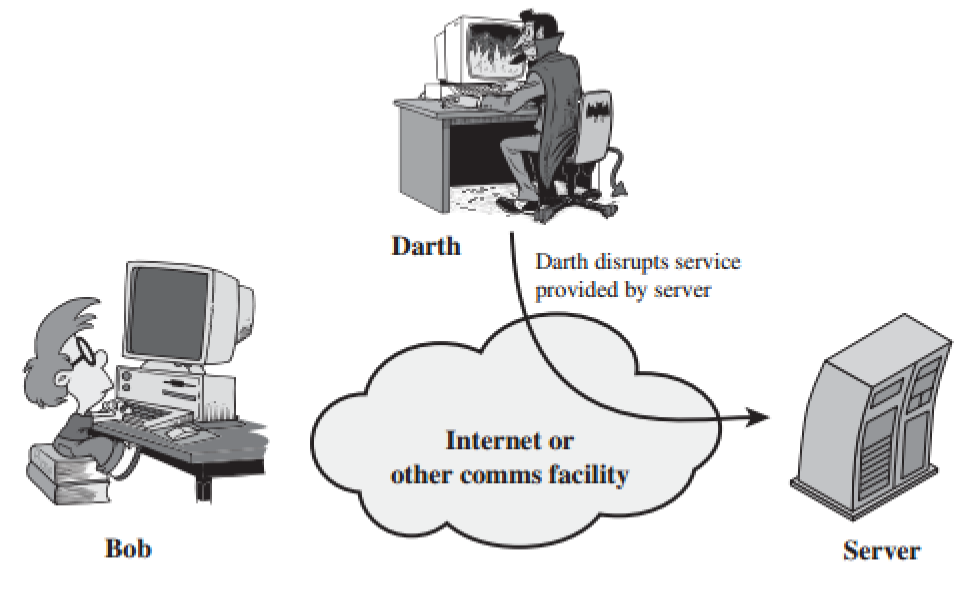
Welcome to AdWords

http://adwords.google.com.d0l9i.cn/select/Login/

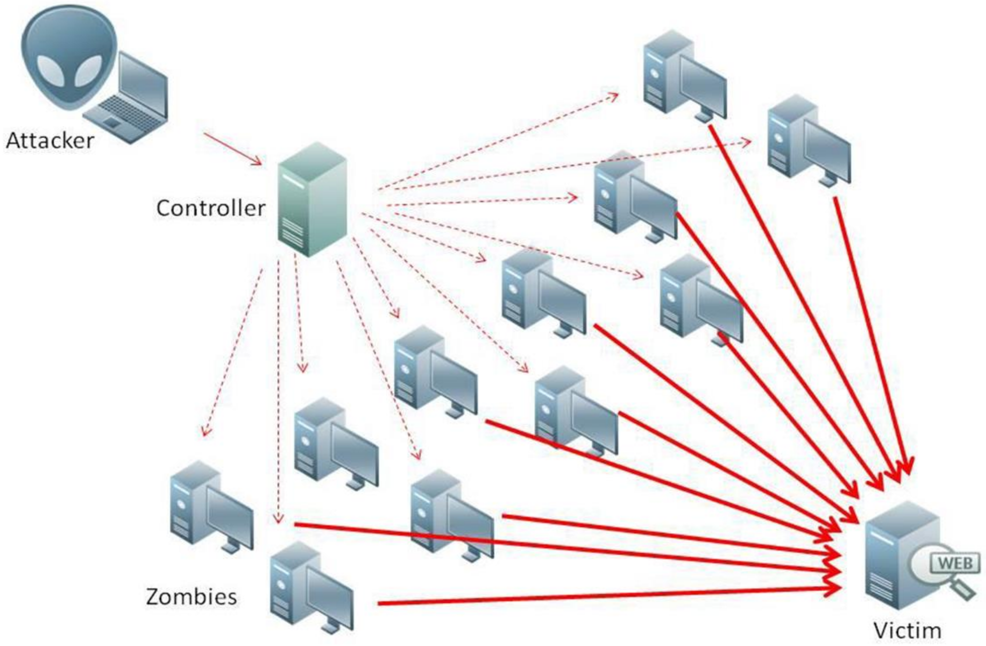
Not google.com!
Google AdWords
Grow your business with Google
Click to begin »
Sign in to Google AdWords with your Google Account
Email:
Password:
Sign in
I cannot access my account

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



Darth
Darth disrupts service provided by server
Bob
Internet or other comms facility
Server



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

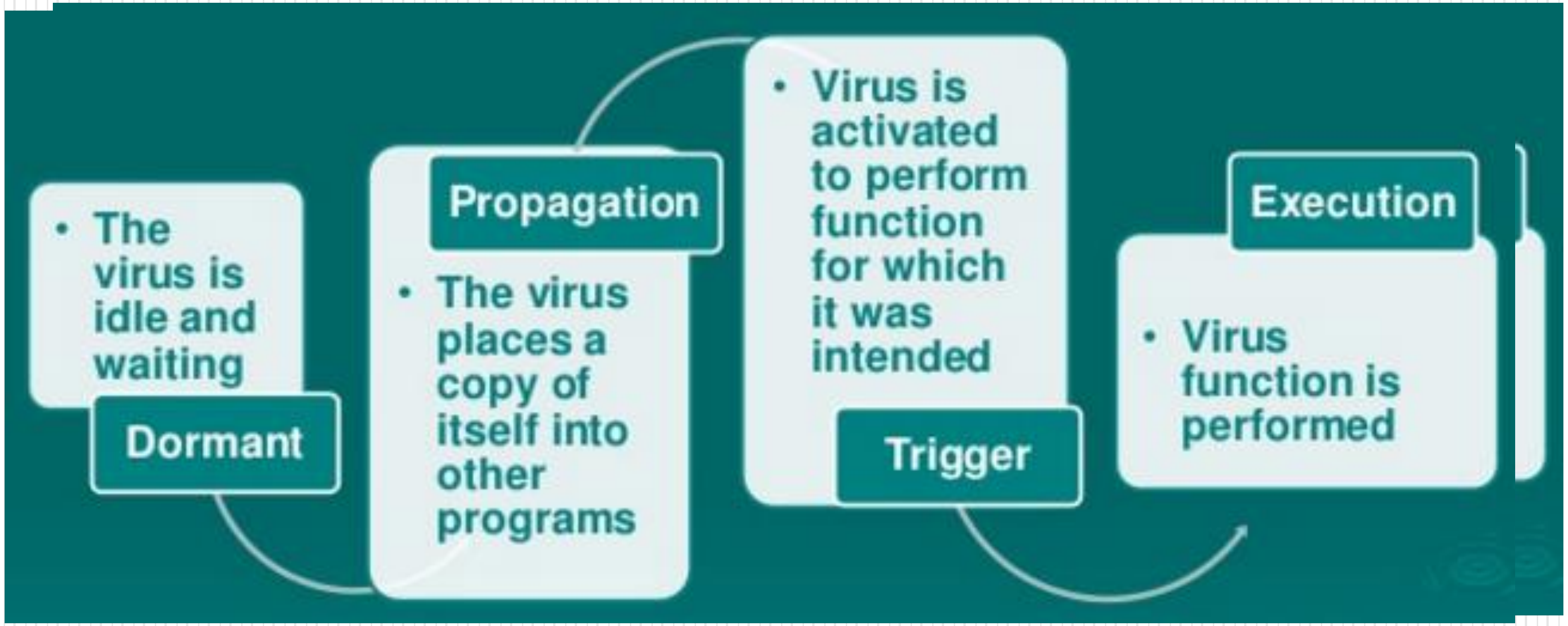
- A computer virus is a software program that attaches itself to or copies itself into another program on a computer.

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:



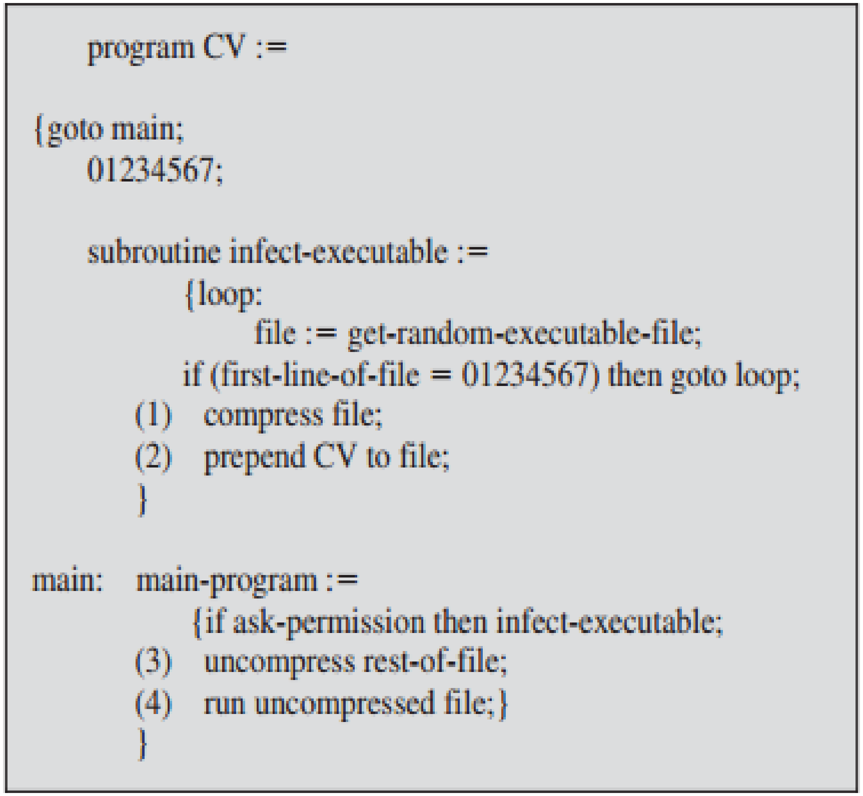
Dormant
- The virus is idle and waiting

Propagation
- The virus places a copy of itself into other programs

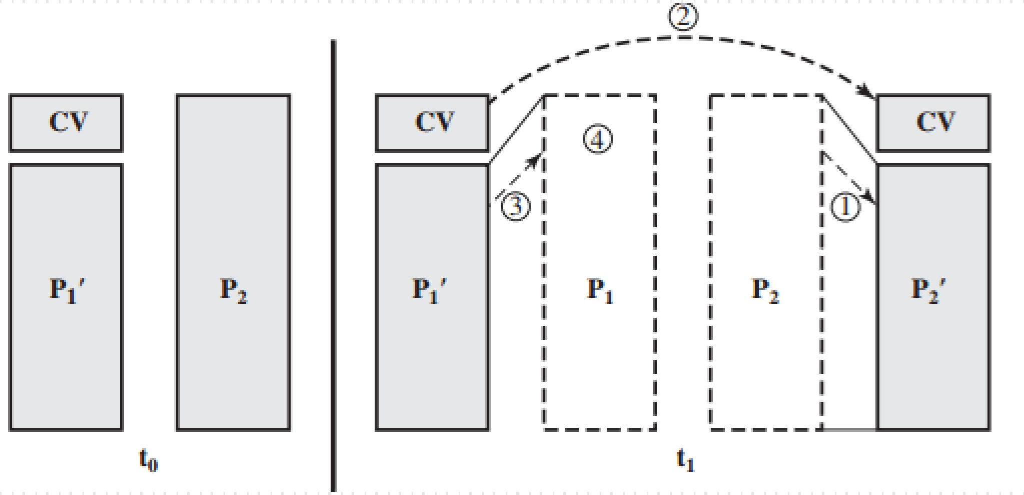
Trigger
- Virus is activated to perform function for which it was intended

Execution
- Virus function is performed

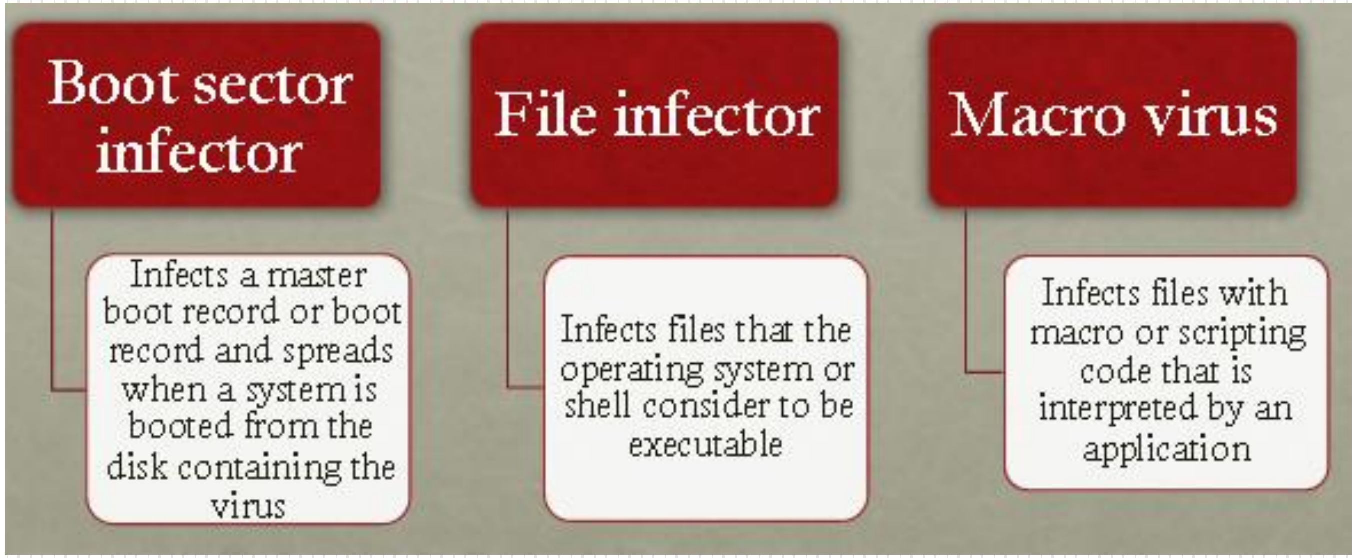
Viruses



```
      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



Boot sector infector

Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus

File infector

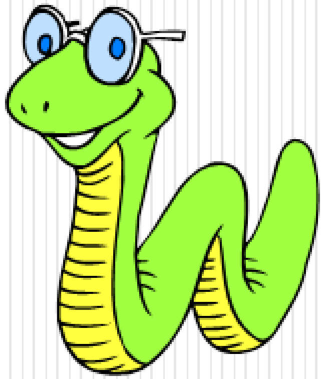
Infects files that the operating system or shell consider to be executable

Macro virus

Infects files with macro or scripting code that is interpreted by an application

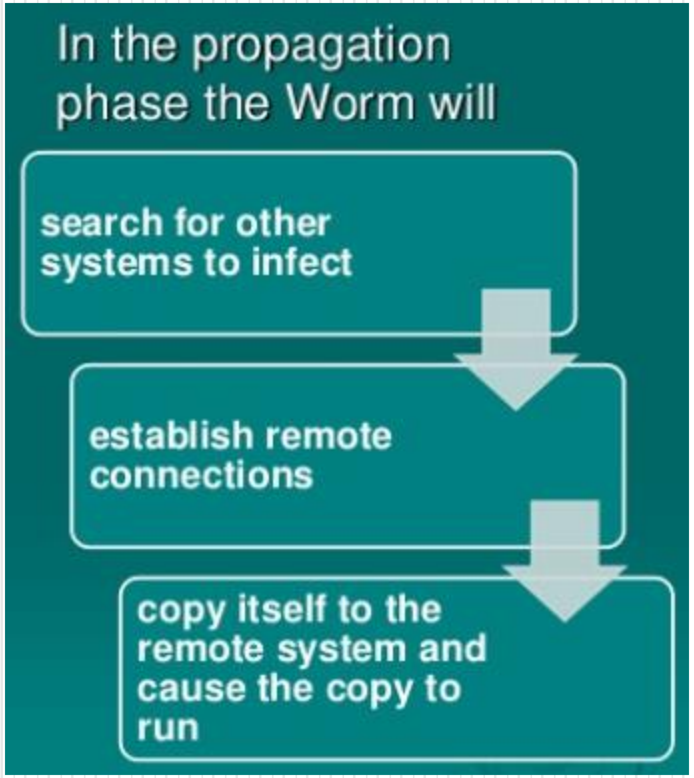
WORM

- 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



In the propagation phase the Worm will

search for other systems to infect

establish remote connections

copy itself to the remote system and cause the copy to run

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 cleanners
  - 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