Information
Technology
Institute

ITI

Introduction to
Computer Networks & Cyber Security

Prepared By : Mohamed AboSehly

Part 2 (Cyber Security Essentials)

Cyber Security Essentials

Part 2 (Cyber Security Essentials)

- **Session Outlines**
  - **Information Security Goals**
    - Confidentiality ,Integrity, Availability
  - **Risks & Threats**
    - Threats & Vulnerabilities
    - Attackers methodology & Methods
    - Malware Types
  - **Security Defenses**
    - Firewalls (Static & Dynamic firewalls)
    - IDS /IPS
    - VPN
    - Proxy
    - Next generation Firewalls
  - **Encryption**
    - Symmetric & Asymmetric Key Cryptography

Part 2 _Introduction

- People use networks to exchange sensitive information with each other.
- People purchase products and do their banking over the Internet.
  - We rely on networks to be secure and to protect our identities and our private information
- Cyber Security is a <u>shared responsibility </u>that each person must accept when they connect to the network.

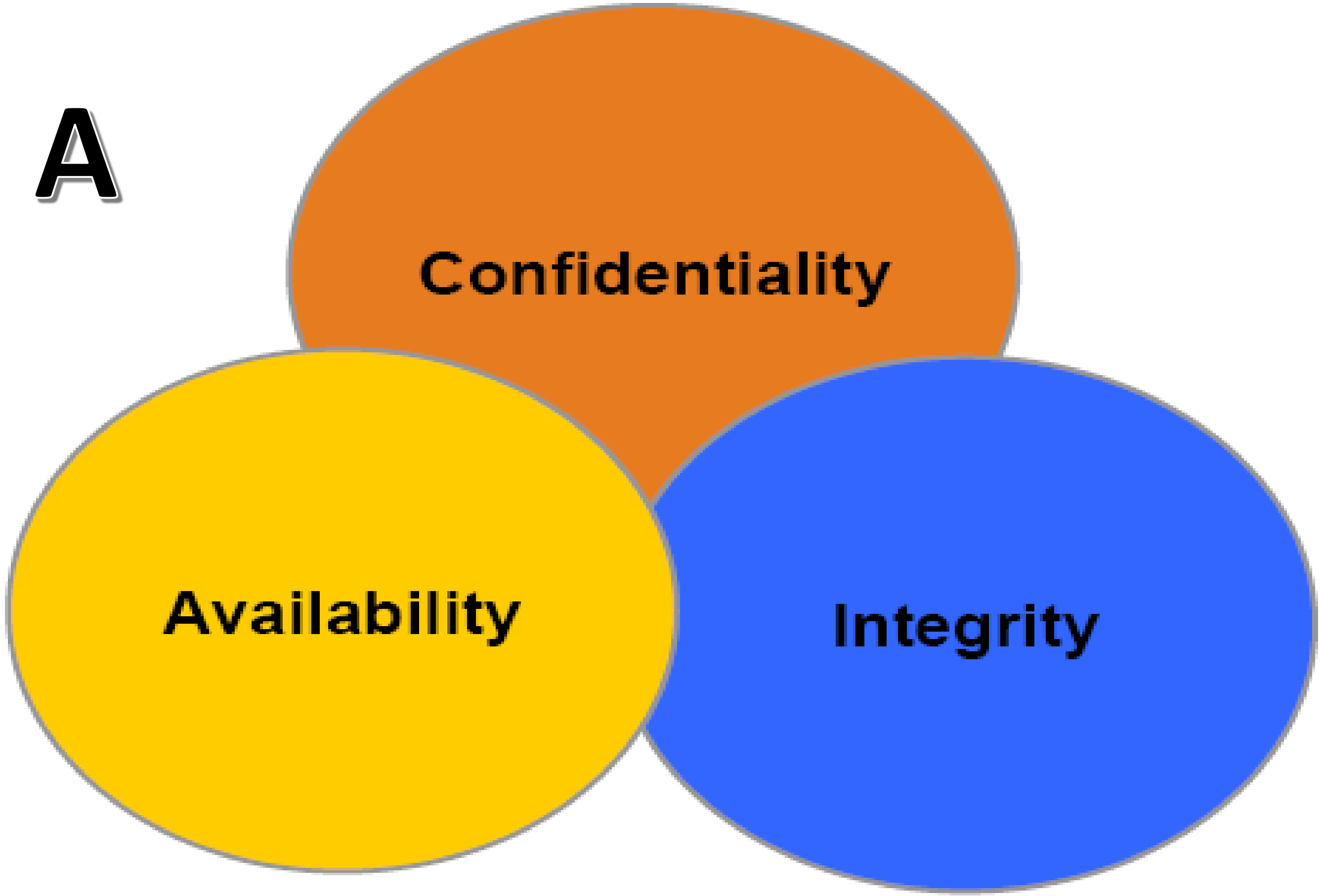
Part 2 _Cyber Security

- **Cyber Security**
  - **How to protect systems, networks, programs, devices and data from cyber attacks**
- **Network security** is the implementation of security devices, policies, and processes to **prevent the unauthorized access to network resources** or the alteration or destruction of resources or data.
- **Security involves protecting resources:**
  - **End-user resources**: PCs, Laptop, Tablets
  - **Network resources**: Routers, Switches
  - **Server resources**: Rack Mount, Blade servers

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY -

Part 2 _Security Goals

C . I . A



Part 2 _Security Goals

- Confidentiality
  - Ensuring that information is not revealed to unauthorized persons
  - Data transmitted or stored should only be revealed to an intended audience
- Integrity
  - Ensuring **consistency** of data
  - It should be possible to detect any modification of data
- Availability
  - Ensuring that legitimate users are not denied access to information and resources

Part 2 _Focus of Security is Risk

- Security deals with managing risk to your critical assets
- It's **impossible** to totally eliminate risk
- Security 99.9 % Not found Why ?
    - This can be seen through the different types of attacks that users face today.
    - New technologies / applications
    - New Vulnerabilities
    - the difficulties in defending against these attacks

Risk = Threat x Vulnerabilities x Impact

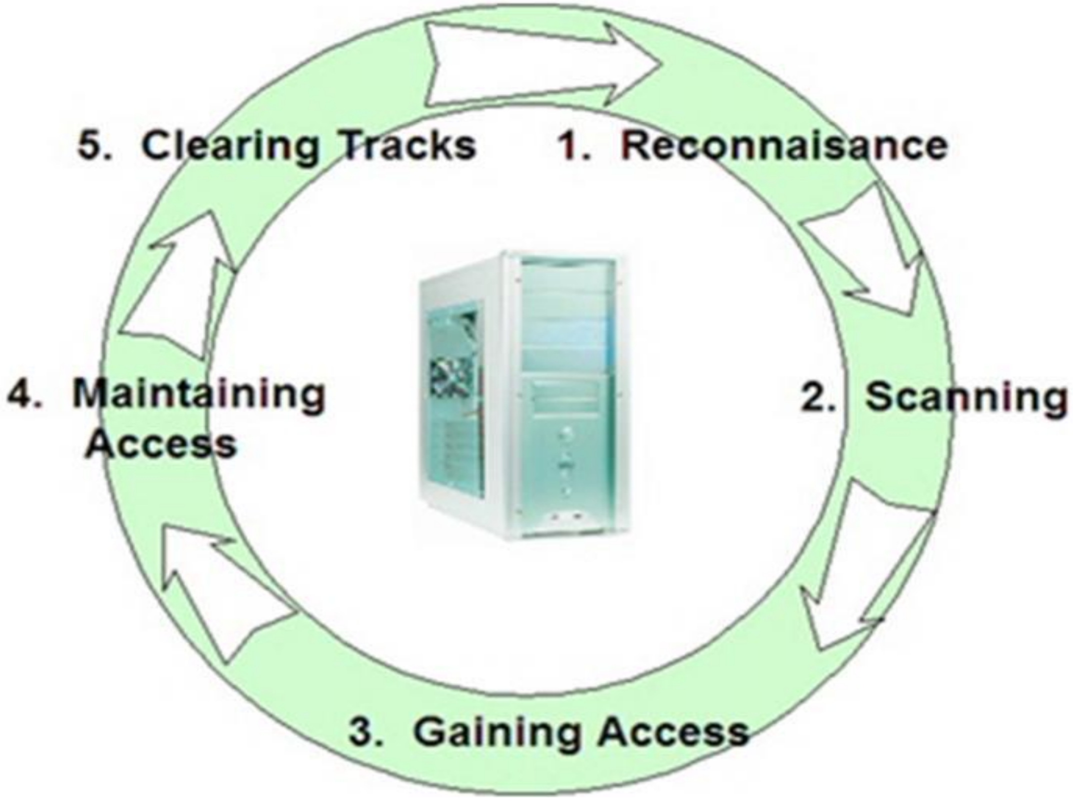
Vulnerability is the degree of weakness which is found in every network and device.
Threats is A person, thing, event or idea which poses danger to **an asset** in terms of that asset’s confidentiality, integrity, availability or legitimate use

Part 2 _Attackers Terminologies

- **Black hats**
  - Individuals with extraordinary computing skills, resorting to malicious or destructive activities.
  - Known as '**Crackers**.'
- **White Hats**
  - Individuals professing hacker skills and using them for defensive purposes.
  - Known as 'Security Analysts, **Ethical hacker**'.
- **Gray Hats**
  - Individuals who work both offensively and defensively at various times.

Part 2 _What does a Malicious Hacker Do?

- Reconnaissance
- Scanning
- Gaining access
- Maintaining access
- Covering tracks



Part 2 _Reconnaissance (Phase 1)

- Reconnaissance refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack.
- Gathering info about internal structure of organization, by browsing and search the internet

Part 2 _ Scanning (Phase 2)

- Scanning refers to pre-attack phase when the hacker scans the network with specific information gathered during reconnaissance.
- Scanning for open ports, operating systems, applications, open shares,

Lab

- In your lab use A port scanner tools to find the open ports on your device

Part 2 _Gaining Access (Phase 3)

- Gaining Access refers to the true attack phase. The hacker exploits the system.
- The exploit can occur over a LAN, locally, Internet.
- Examples include buffer overflows, denial of service, session hijacking etc.

Part 2 - Maintaining Access (Phase 4)

- Maintaining Access refers to the phase when the hacker tries to retain his ‘ownership’ of the system.
- Sometimes, hackers harden the system from other hackers as well (to own the system).

Part 2- Covering Tracks(Phase 5)

- Covering Tracks refers to the activities undertaken by the hacker to extend his misuse of the system without being detected.

- Reasons include need for continued use of resources, removing evidence of hacking, avoiding legal action etc.

- Hackers can remain undetected for long periods.

Part 2 _Attacks

Attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

Part 2 _Attack Types

- Passive Attack
- Active Attack
- Phishing Attack
- Hijack Attack
- Spoof Attack
- Buffer Overflow Attack
- Exploit Attack
- Password Attack

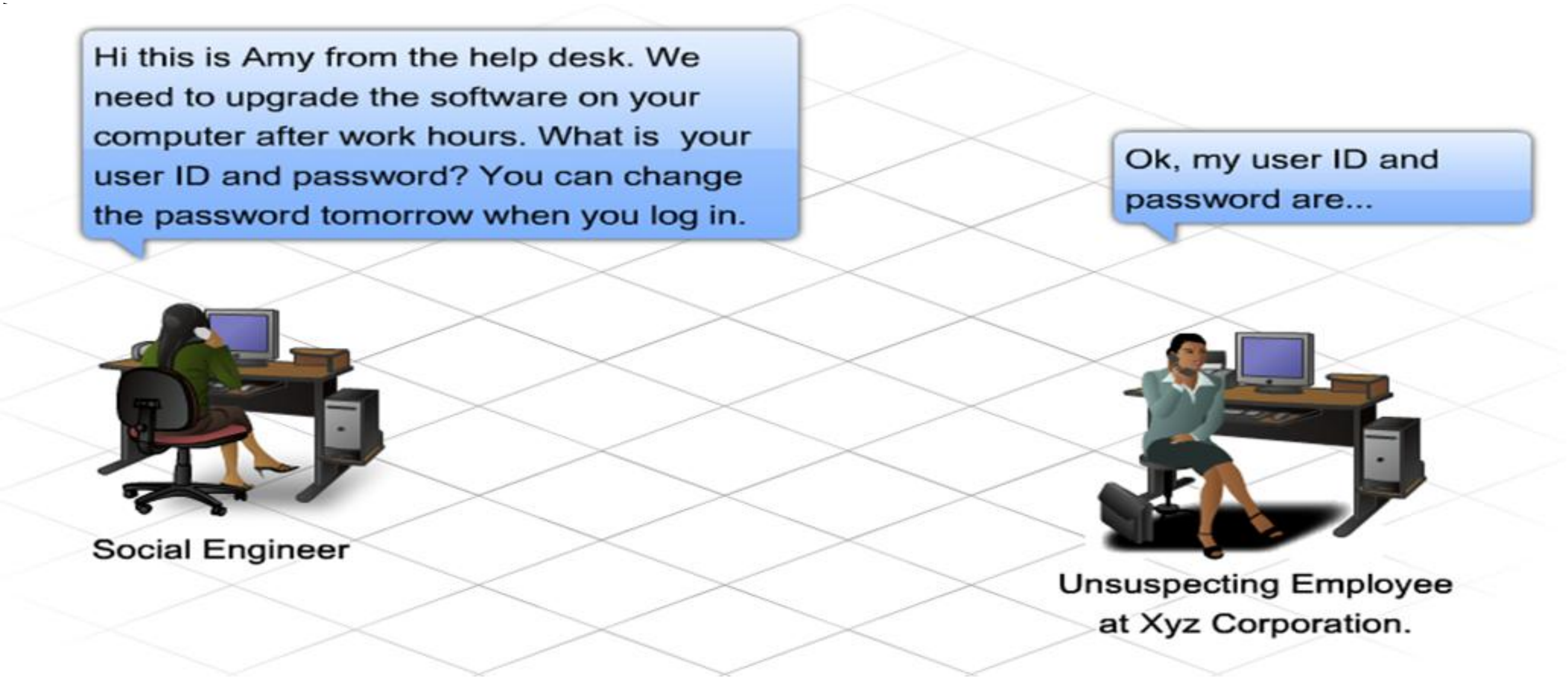
Part 2_Passive attack VS Active attack

- **Passive attack** attempts **to take the information** from the system and **does not affect any system resources and its operations.**
  - **Ex : Cookies , Spyware , Wireshark**

- **Active attack** attempts to **change** the system resources or affect their usual operations.
  - **Ex : Ransomware, Viruses, worms**

Part 2_ Social engineering

- **Social engineering** is a term that refers to the ability of something or someone to influence the behavior of a group of people

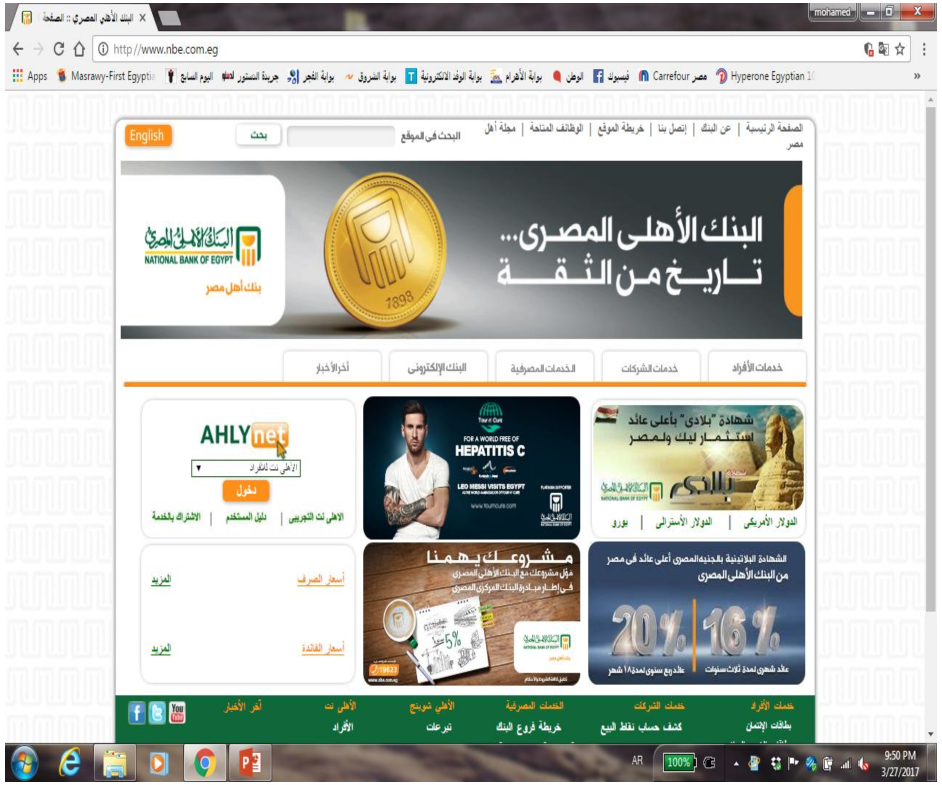

Hi this is Amy from the help desk. We need to upgrade the software on your computer after work hours. What is your user ID and password? You can change the password tomorrow when you log in.
Ok, my user ID and password are...
Social Engineer
Unsuspecting Employee at Xyz Corporation.

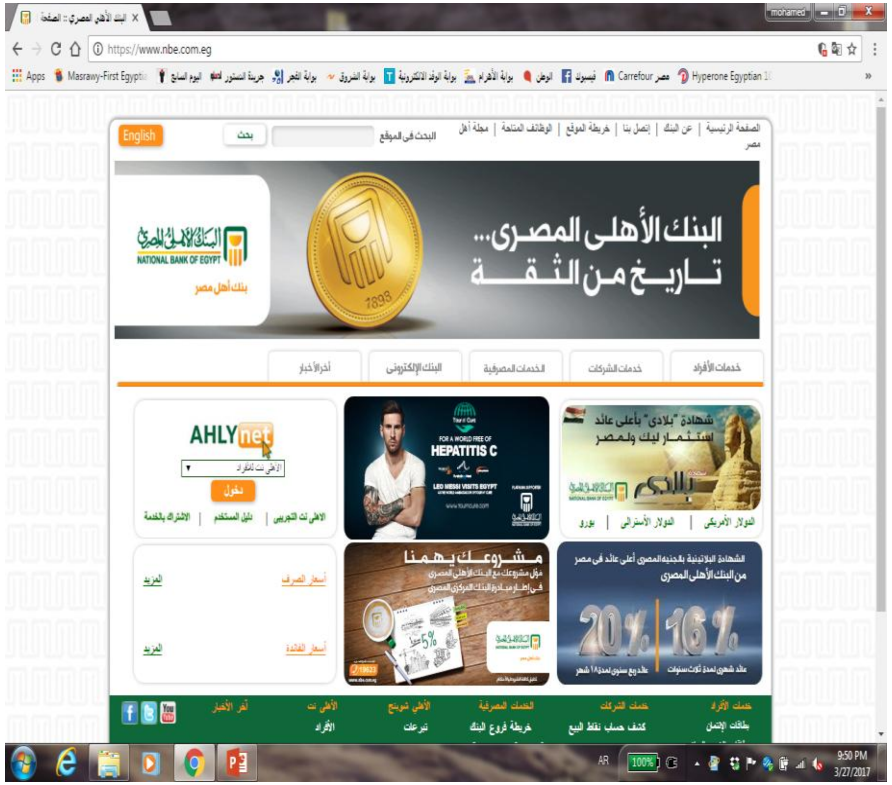
Part 2_PHISHING ATTACK

In **phishing attack**

- the hacker creates a fake web site that looks exactly like a popular site.
- **The phishing part of the attack is that the hacker sends**
  - **An e-mail message , Sms message**
- **trying to trick the user into clicking a link that leads to the fake site.**
  - When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

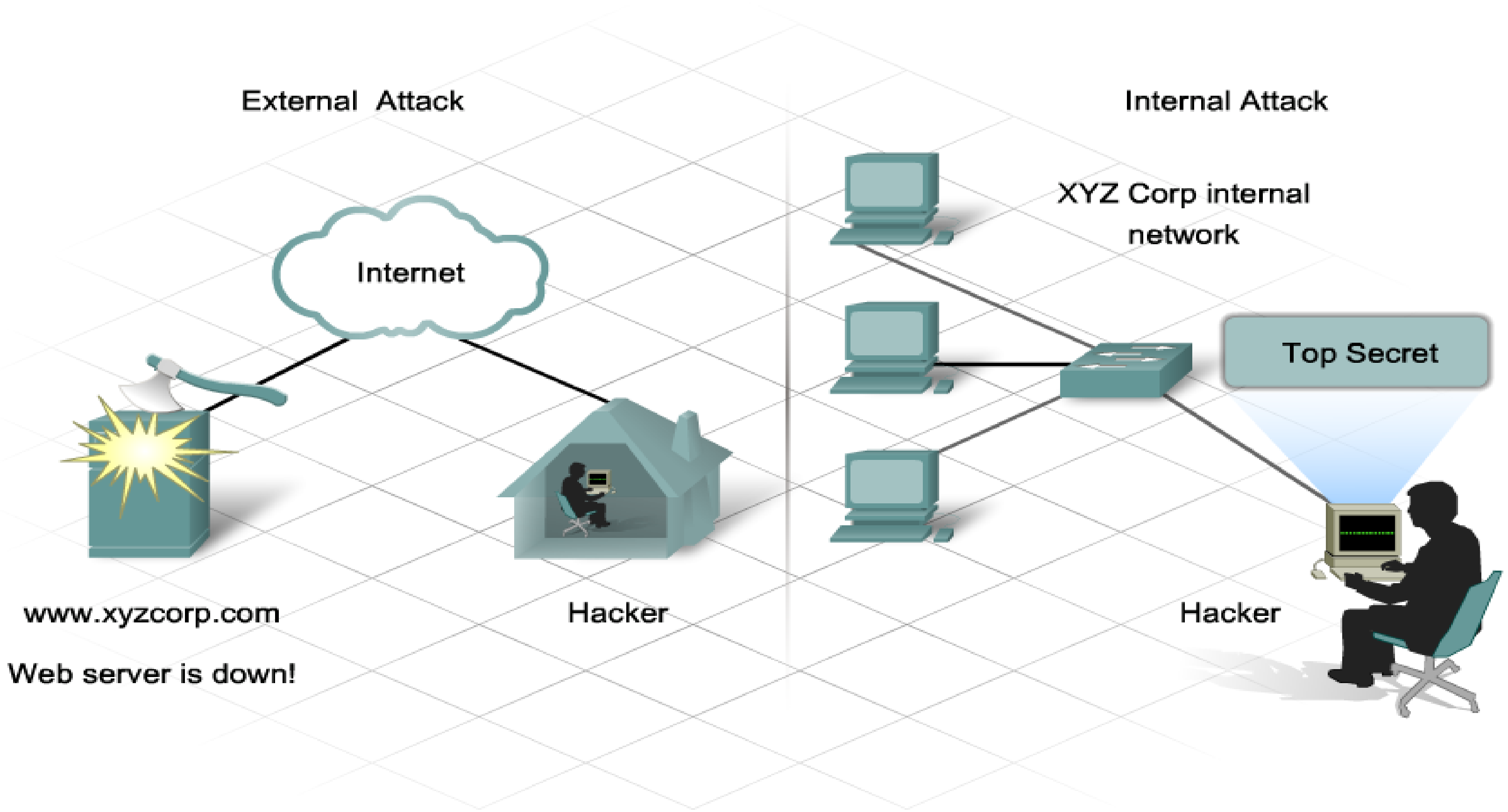
Part 2_Find the fake one ?





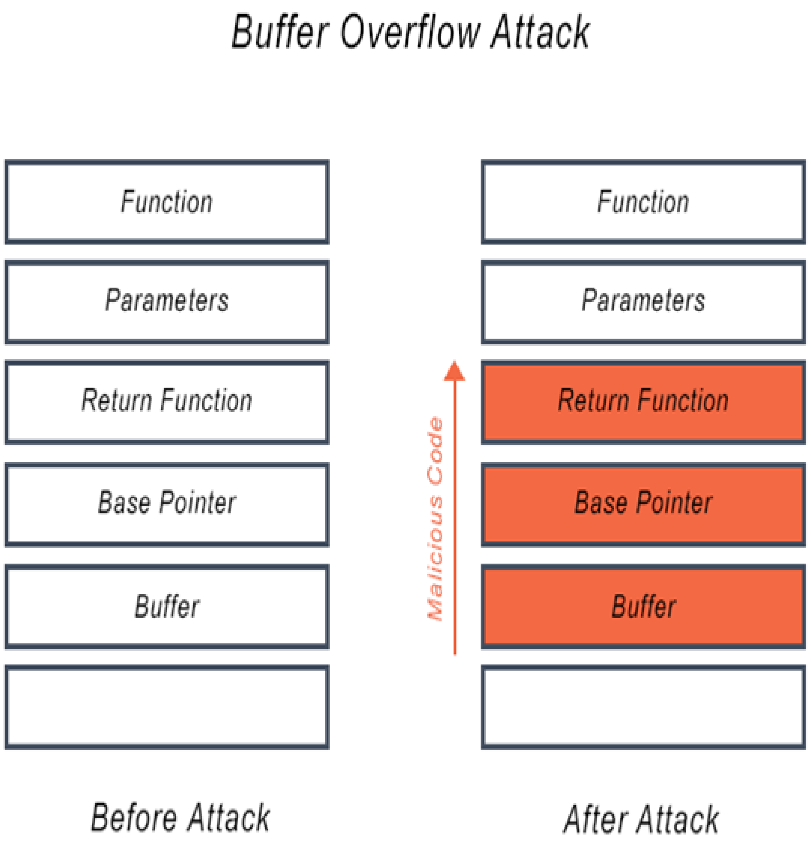
https://www.virustotal.com/gui/home/url

Part 2_Insider Attack



Part 2_BUFFER OVERFLOW ATTACK

A **buffer overflow** attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell.

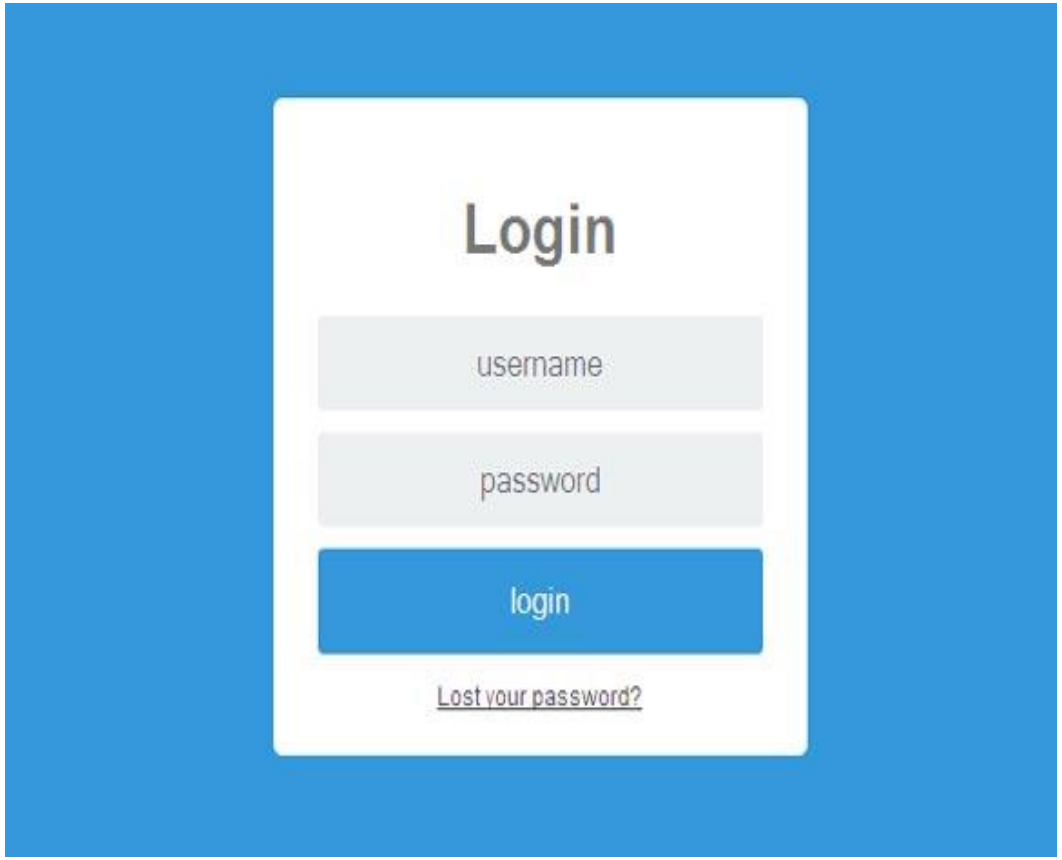


Part 2_PASSWORD ATTACK

An attacker tries to crack the passwords stored in a network account database or a password-protected file.

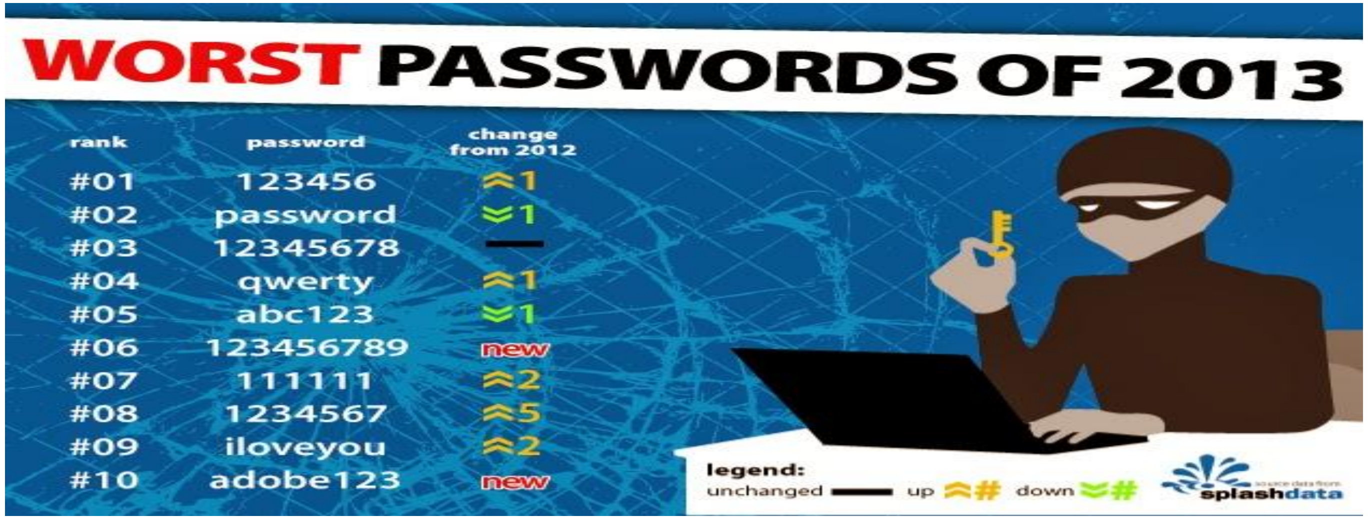
Part 2_types of password attack

- **Dictionary attack**
- **Brute-force attack**
- **Hybrid attack.**



Part 2_types of password attack

- A **dictionary attack** uses a word list file, which is a list of potential passwords.



WORST PASSWORDS OF 2013

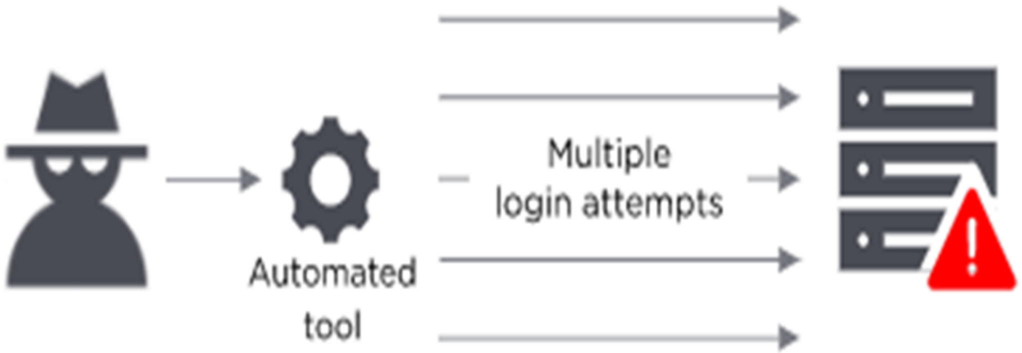
rank	password	change from 2012
#01	123456	▲1
#02	password	▼1
#03	12345678	—
#04	qwerty	▲1
#05	abc123	▼1
#06	123456789	new
#07	111111	▲2
#08	1234567	▲5
#09	iloveyou	▲2
#10	adobe123	new

legend: unchanged — up ▲# down ▼#

source data from splashdata

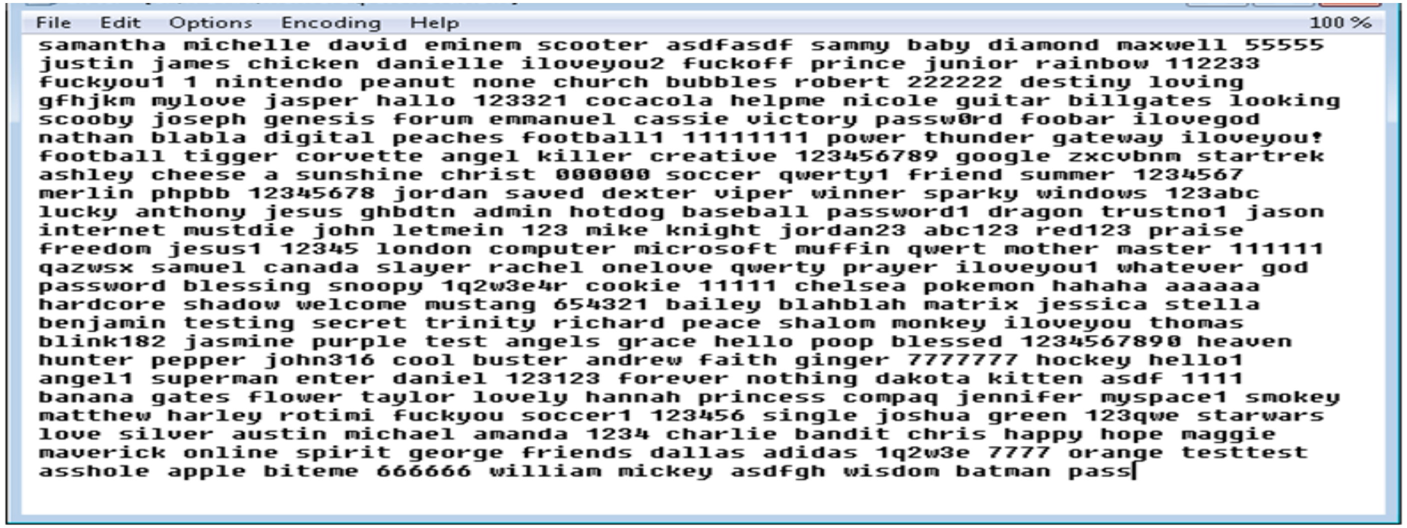
Part 2_TYPES OF PASSWORD ATTACK

- A **brute-force attack** is when the attacker tries every possible combination of characters.



Part 2_types of password attack

- A **hybrid attack** builds on the dictionary attack method by adding numerals and symbols to dictionary words



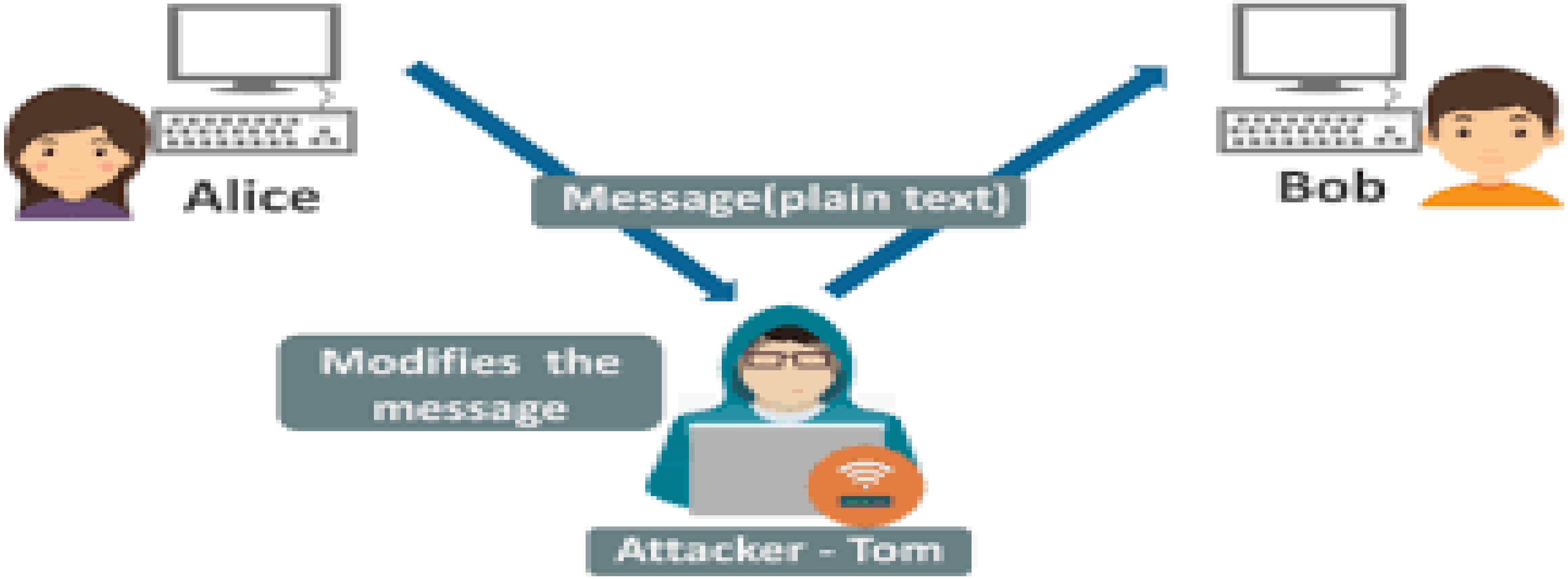
```
samantha michelle david eminem scooter asdfasdf sammy baby diamond maxwell 55555
justin james chicken danielle iloveyou2 fuckoff prince junior rainbow 112233
fuckyou1 1 nintendo peanut none church bubbles robert 222222 destiny loving
gfhjkm mylove jasper hallo 123321 cocacola helpme nicole guitar billgates looking
scooby joseph genesis forum emmanuel cassie victory passw0rd foobar ilovegod
nathan blabla digital peaches football1 11111111 power thunder gateway iloveyou!
football tigger corvette angel killer creative 123456789 google zxcvbnm startrek
ashley cheese a sunshine christ 000000 soccer qwerty1 friend summer 1234567
merlin phpbb 12345678 jordan saved dexter viper winner sparky windows 123abc
lucky anthony jesus ghbdtn admin hotdog baseball password1 dragon trustno1 jason
internet mustdie john letmein 123 mike knight jordan23 abc123 red123 praise
freedom jesus1 12345 london computer microsoft muffin qwert mother master 111111
qazwsx samuel canada slayer rachel onelove qwerty prayer iloveyou1 whatever god
password blessing snoopy 1q2w3e4r cookie 11111 chelsea pokemon hahaha aaaaaa
hardcore shadow welcome mustang 654321 bailey blahblah matrix jessica stella
benjamin testing secret trinity richard peace shalom monkey iloveyou thomas
blink182 jasmine purple test angels grace hello poop blessed 1234567890 heaven
hunter pepper john316 cool buster andrew faith ginger 7777777 hockey hello1
angel1 superman enter daniel 123123 forever nothing dakota kitten asdf 1111
banana gates flower taylor lovely hannah princess compaq jennifer myspace1 smokey
matthew harley rotimi fuckyou soccer1 123456 single joshua green 123qwe starwars
love silver austin michael amanda 1234 charlie bandit chris happy hope maggie
maverick online spirit george friends dallas adidas 1q2w3e 7777 orange testtest
asshole apple biteme 666666 william mickey asdfgh wisdom batman pass
```

Lab

- Check you compromised password and your data leakage at

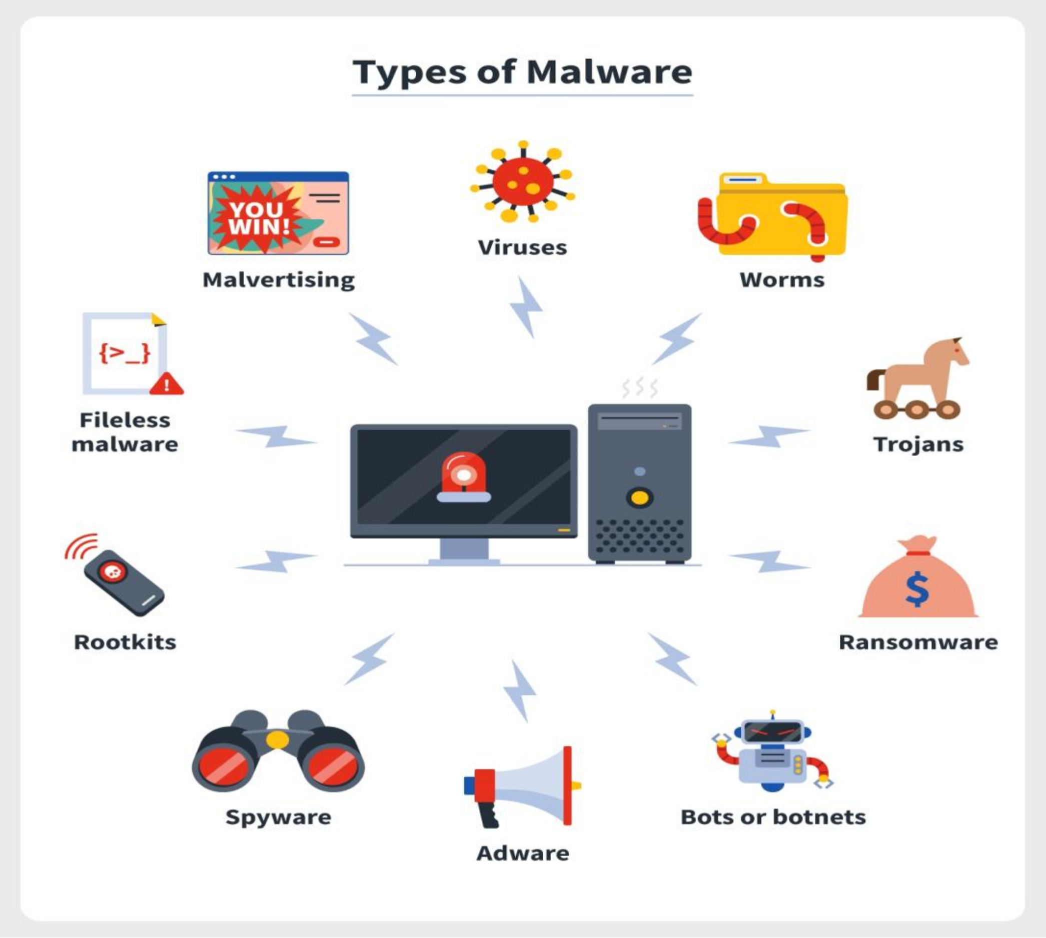
    - https://haveibeenpwned.com/

Part 2_Man in the middle Attack

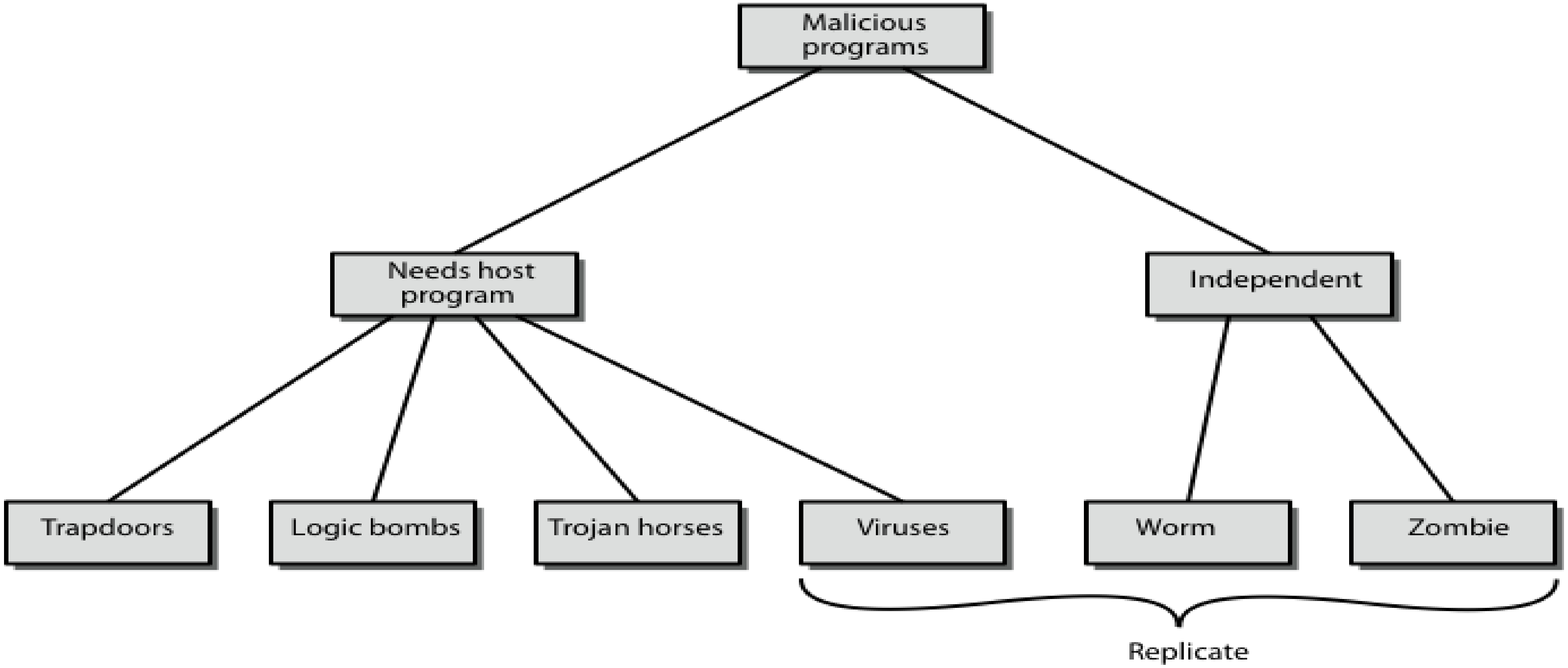


Part 2_Malware Types

- Malware Capabilities
  - Destruction of Data
  - Leaking Confidential Information
  - Providing Backdoor Access
  - Countless Other Opportunities

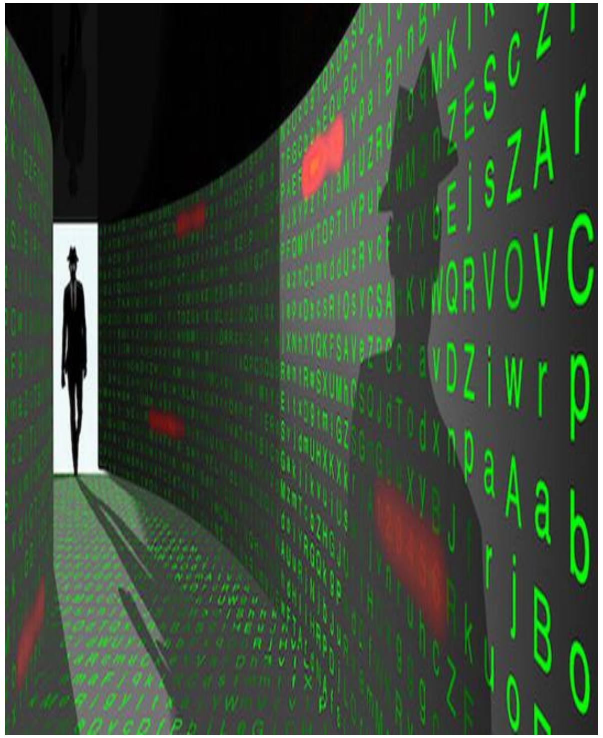


Part 2_Malicious Software



Part 2_Backdoor or Trapdoor

- Secret entry point into a program
- Allows those who know access bypassing usual security procedures
- Have been commonly used by developers
- Requires good s/w development & update
- Can’t be removed or scanned and the only way is to uninstall sw or format the system



Part 2_Viruses

- A virus is malicious software that is attached to another program to execute a particular unwanted function on a user's workstation.

- Both propagates itself & carries a payload
  - Carries code to make copies of itself
  - As well as code to perform some covert task

Part 2_Trojan Horse

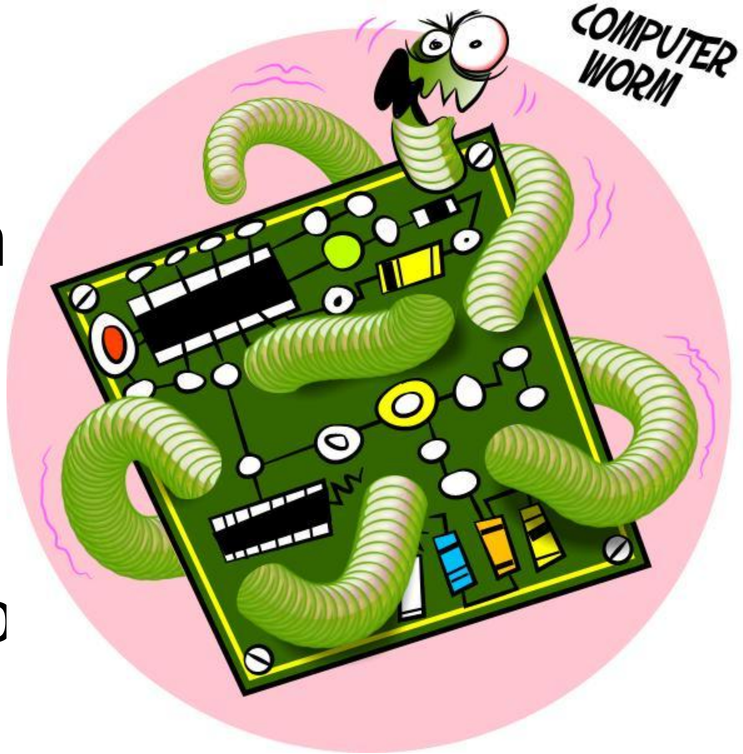
- program with hidden side-effects
- which is usually superficially attractive
  - eg game, software upgrade etc
- when run performs some additional tasks
  - allows attacker to indirectly gain access they do not have directly
- often used to propagate a virus/worm or install a backdoor or simply to destroy data
- Open some ports or pass some malicious files

Part 2_ Independent malware

- Worms
- Zombie
- Man in the middle
- DOS
- DDOS
- Spyware and Tracking Cookies

Part 2_Worms

- Replicating but **not infecting** program
- Typically spreads over a network
- Using users distributed privileges or by exploitin vulnerabilities
- Widely used by hackers to create **zombie pc's**, used for further attacks, especially dos
- Major issue is lack of security of permanently co systems



Lab

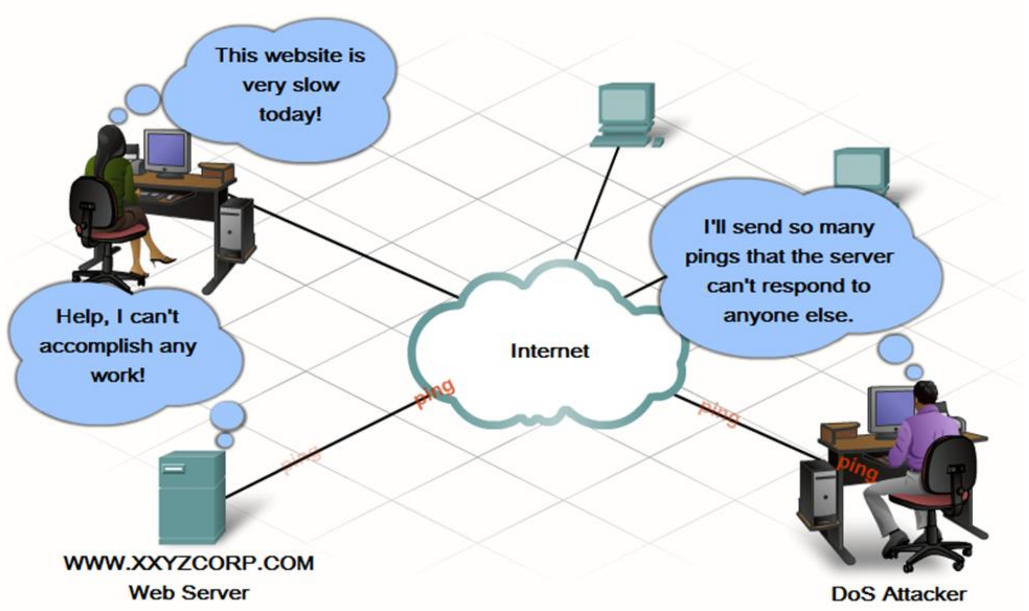
- Check you downloaded software at
  - https://www.virustotal.com/gui/home/upload

Part 2_Zombie

- Program which secretly takes over another networked computer then uses it to indirectly launch attacks
- Often used to launch distributed denial of service (DDoS attacks

Part 2_DoS Attack

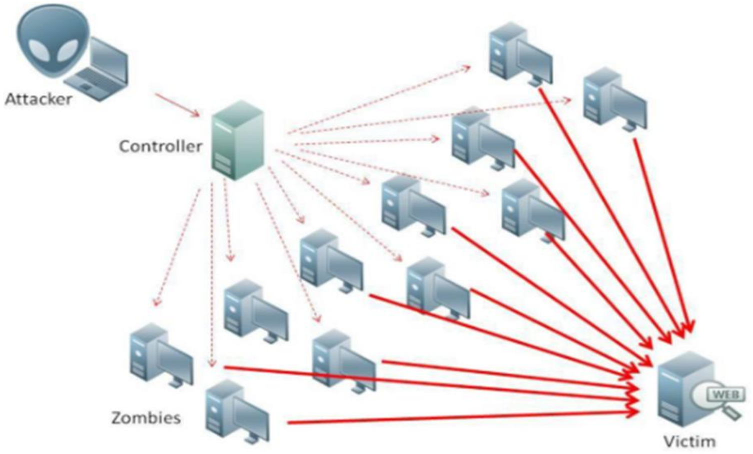
- Denial of service is about without permission knocking off services, for example through crashing the whole system.
- This kind of attacks are easy to launch and it is hard to protect a system against them.
- Consume host resources
  - Memory
  - Processor cycles
- Consume network resources
  - Bandwidth

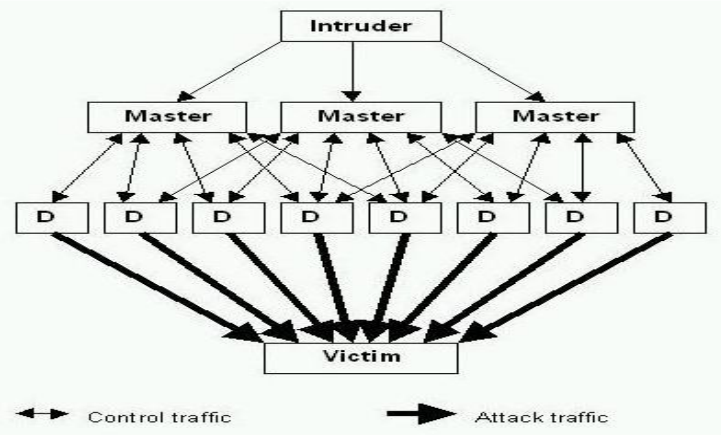

This website is very slow today!
Help, I can't accomplish any work!
Internet
I'll send so many pings that the server can't respond to anyone else.
ping
ping
ping
ping
WWW.XXYZCORP.COM
Web Server
DoS Attacker

Part 2_DDoS Attack

- DDoS – A distributed denial of service attack uses multiple machines to prevent the legitimate use of a service.

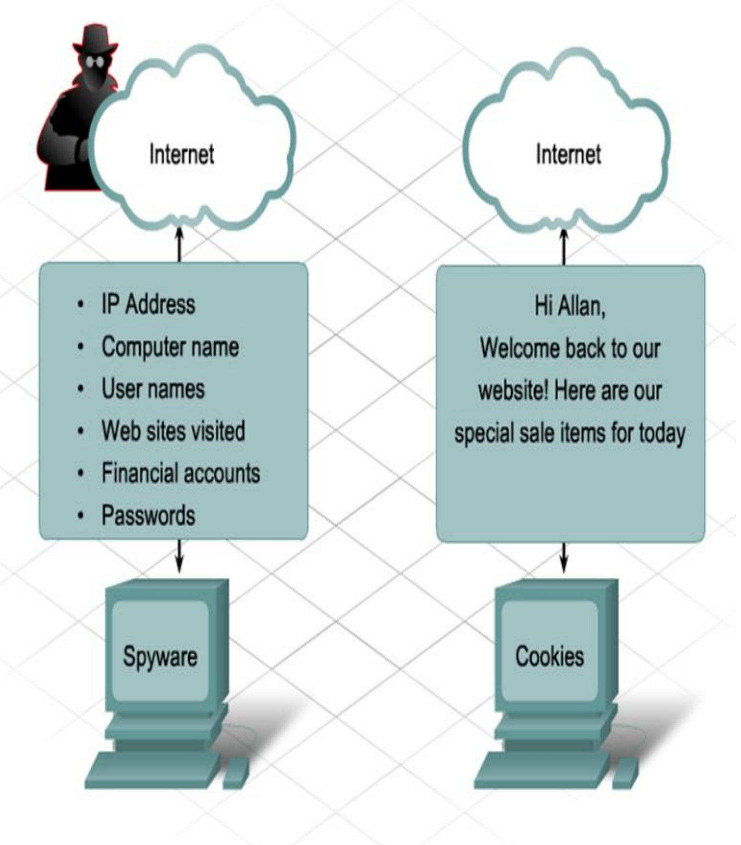
- Making networked systems unavailable by flooding with useless traffic using large numbers of "zombies" growing sophistication of attacks





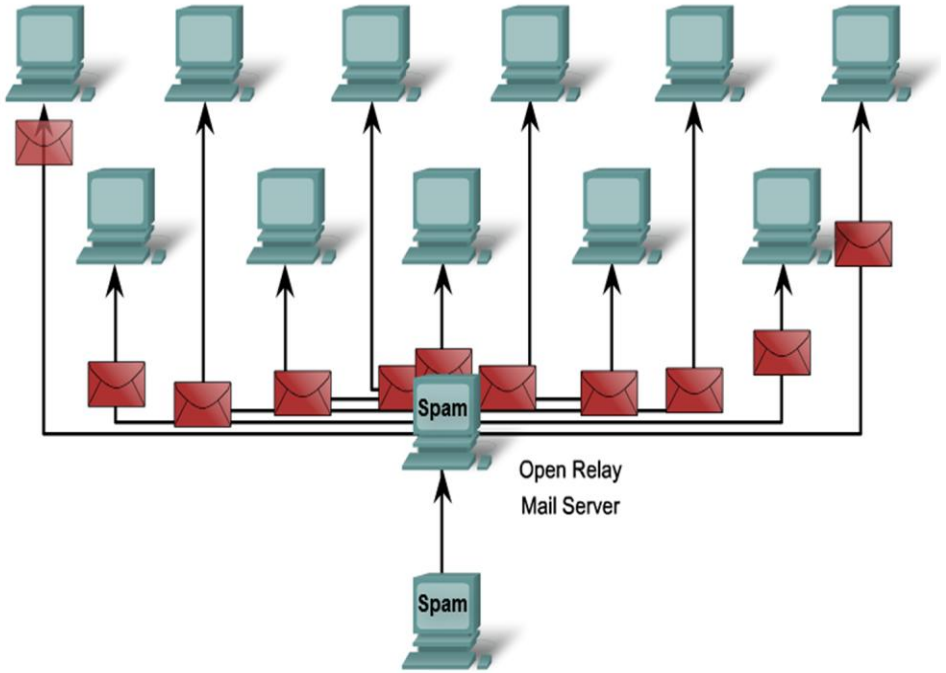
Part 2_Spyware and Tracking Cookies

- **Spyware**
  - Spyware is any program that gathers personal information from your computer **without your permission or knowledge**. This information is **sent to advertisers or others** on the Internet and can include passwords and account numbers.
- **Tracking Cookies**
  - Cookies are a **form of spyware** but are **not always bad.** They are used to record information about an Internet user when they visit websites.



Part 2_Spam

- **Spam**
- is a serious network threat that can overload ISPs, email servers and individual end-user systems.
- A person or organization responsible for sending spam is called a spammer.
- Spammers often make use of unsecured email servers to forward email.
- Spammers can use hacking techniques, such as viruses, worms and Trojan horses to take control of home computers.



Thank You