

Cybersecurity Fundamentals

Lecture 5: Attacks Type

CYB 670
Cybersecurity Fundamentals

Presented by
Dr. Mohammad Alkhatib



Outline

This lecture covers the following topics:

- Cyber-Attacks:
- Browser Hijacker, Rootkit, Scareware , Keylogger
- Brute Force Attack, Backdoors, Cross-site scripting (XSS), Denial of service (DoS) attack and Distributed Denial of service (DDoS) attack.
- Man-in-the-middle attack , Social engineering , Phishing
- Spoofing, Structure Query language (SQL) injection, Zero-day exploit, Botnets
- Vulnerabilities.

Browser Hijacker

- You might have been in the situation when the default settings of your browser were changed. For example, your default search engine was changes to a new one without getting permission from you.
- As we know that the **browser** is one of the core software tools that are used to connect to a wide range of computer programs, web applications, websites, and many other digital resources located on the internet or even on the local networks.
- If any breach in the browser is established, all of your digital resources including the security passwords are at stake. So, hackers try to attack the browsers more frequently to establish a way to attack computers and networks.



Browser Hijacker

- When you observe this situation, be sure that your computer's browser has been hijacked by the malicious program, which is altering the settings of your browser and creating a way for the malicious programs to intrude in.
- In some cases, you might have seen that some **unknown plugins** have been installed and activated on your browser. Although you have not downloaded or installed on your browser, but still they are there and active.



Browser Hijacker

- **Browser Hijacker** malware is a **certain malicious code**.
- This code is used to pave the way for different kinds of cyberattacks on your computer or to the other computers on your network.
- Browser hijacker normally downloaded on your computer via some free software applications.
- The **main objective of browser hijacker** software is to force the users to visit certain websites for improving the volume of traffic on that particular website.
- When the traffic of a website is improved, the website gets higher revenue of online advertisement.



Browser Hijacker

- ❖ The browser hijacker malware can also be used for stealing personal information, user accounts, and other information for financial benefits.
- ❖ The **symptoms** and impact of browser hijack malware may include:
 - Slow browsing speed
 - Multiple tool bars on the browser
 - Redirecting your search queries to websites that you have not set as default
 - A large number of popup windows and ads appear on your browser



Browser Hijacker

You can **save your browser from being hijacked** by the browser hijacker malware by taking the following measures:

- Avoid free downloads as much as possible
- Disable unwanted tool bars
- Remove or disable unwanted plugins
- Set your default search engine
- Install antimalware erasers
- Use common sense while downloading and internet browsing



Rootkit

❖ There are several types of malware, the most important are as follows:

- **Rootkit:-** A class of malware that hides the existence of other malware by modifying the underlying operating system.
- **Rootkit** is a type of malware that gets the administrator level privileges on the operating system of the computer without showing its presence on the computer.
- The **main feature of rootkit** is that it hides from being detected easily but maintains the control over the operating system to perform its designated tasks on the system.
- The normal behavior of the operating system is subverted by the rootkit malware on the system.



Rootkit

- As we know all applications on the computer including the antivirus, anti-malware, and other security related applications use the application programming interfaces or APIs provided by the operating system.
- A powerful rootkit gets control on those APIs and establishes the full control on the system.
- **For instance**, windows browser program sends a request to the operating system API to find a certain file on the computer. The operating system responds to the browser through API about that file.
- The rootkit malware subverts the request sent to the operating system from reaching to the desired API and responds with fake responses.



Rootkit

- Moreover, you request the operating system to start the antivirus or anti-malware application to scan your computer; the request is interrupted from reaching to the operating system. The rootkit interrupts the request and sends you a fake response that the program you requested for is not working at this time.
- **Rootkit** is considered as one of the nastiest forms of malware that is not easily detected and removed from your computer once it has established the privileges to access and control the operating system through available vulnerabilities in the OS and other applications.



Rootkit

There are **three main goals of a rootkit** on a computer as mentioned below:

- Running freely without any restrictions of having been caught and deleted
- Hiding from the system applications and the user of the computer
- Stealing personal information, passwords, and installing other malicious programs on the computer so that the compromised computer can be used for attacking the other computers on the network



Rootkit

- There are numerous types of rootkits based on the objective and point of attack on the systems.
- A few **very well-known and important rootkits** are listed below:
 - Memory rootkits
 - Kernel rootkits
 - Bootkit rootkits
 - Firmware rootkits
 - Library rootkits
 - Application rootkits



Rootkit

- For a **normal user** of the computer, it may be very difficult to recognize that the computer has been infected by the rootkits.
- If the computer shows the following **symptoms**, then you should suspect that the computer has been infected by the rootkit attack.
 - Modifications in the dates and time of computer
 - Slowdown of the computer
 - Unexpected system error messages
 - Many programs, especially computer security related programs fail to start
 - Substantial redirects on browsers
 - Appearance of blue screen of death



Rootkit

- Rootkits travel through the standard ways of the propagation of viruses, worms and other malware programs. Those include:
 - Infected downloads
 - Peer to peer file sharing
 - Unknown emails
 - Short text messages (SMS)



Rootkit

- It is very difficult to detect and remove the rootkit from your computer, once it has established the control over the operating system APIs.
- Normally, the rootkit remains unnoticed on the machine and keeps doing its job.
- For remaining many days on the computer, the system becomes a rogue machine, and many malicious programs start running on the machine. Those programs will be used for different malicious activities.
- You will find the behavior of operating system very irritating with the passage of time. One day you will see a cryptic blue screen of death and your computer will never load again normal.
- Now, you will have to re-install and configure your computer from the scratch.

Rootkit

But you can still take the following steps to **avert from getting rootkits** control of your computer.

- Always visit the legitimate and secure websites
- Don't download free and compromised products
- Open emails and their attachments from known people only
- Never open attachments in SMS and other messages
- Activate firewall on your system
- Activate intrusion prevention system IPS
- Activate access control lists ACL on the system and network



Rootkit

- Scan and clean flash or other data traveling devices before opening the files
- Use the latest anti-rootkit tools with Security Technology and Response (STAR) technology
- Keep your anti-malware up to date
- Keep operating system up to date



Rootkit

- Many new software tools have also been created by the major computer security software providers like Norton, Avast, Panda, Kaspersky, and others.
- All those tools are able to detect the rootkits if present on your computer. They are also able to remove the nastiest forms of the rootkits on your computer easily.



Scareware

- **Scareware** is a type of malware, which pops up in window with a serious warning about any virus threat on your computer.
- **But**, in reality there is no threat or virus on your computer excepting that **hoax**, which appeared on your screen.
- The **alert looks** very genuine from certain reputable websites, but they are not genuine websites.
- This message normally prompts the users to download or call some numbers to get help.
- The **main objective behind the Scareware** is sale fake and bogus products.
- The use of scareware has been also found in the entertainment pranks.



Scareware

❑ Use of the Scareware:

(1) The hackers trick the users to input the credit card, personal, and bank information on their website. Once you provide that information, your data has been compromised for malicious financial uses.

(2) To force the user to download some free antivirus software to clean your computer from those viruses that the website has detected. But, that free antivirus is itself a dangerous software program, which can control your computer and start damaging your system or stealing your data.

- So, the **scareware** can be the foundation of many dangerous cyberattacks.



Scareware

The **main objectives of spreading scare** may include the following:

- Selling fake products
- Stealing personal and bank information
- Installing viruses and other malicious codes for cyber crimes
- Blackmailing for some ransom
- Prank for fun



Scareware

You can **avoid the impact of scareware** by taking the following steps:

- Don't panic at all
- Check if your antivirus is working well
- **Keep** your antivirus up to date
- Search about the legitimacy of that website, which alerts you of virus on your computer
- Search for the legitimacy of the message you see on your computer
- Never rely on free software in such conditions
- Purchase a genuine antivirus and install if you have none installed on your computer



Scareware

- The hackers use the social engineering tactics to force you follow the instructions they give you.
- So, always use your common sense and remain calm and cool to deal with the situation.



Other Attacks Types

- In addition to malware, there are many other types of attacks. The MITRE Corporation publishes a catalogue of attack patterns known as Common Attack Pattern Enumeration and Classification (CAPEC) as “an abstraction mechanism for helping describe how an attack against vulnerable systems or networks is executed.”
- Some of the most common attack patterns are listed below.

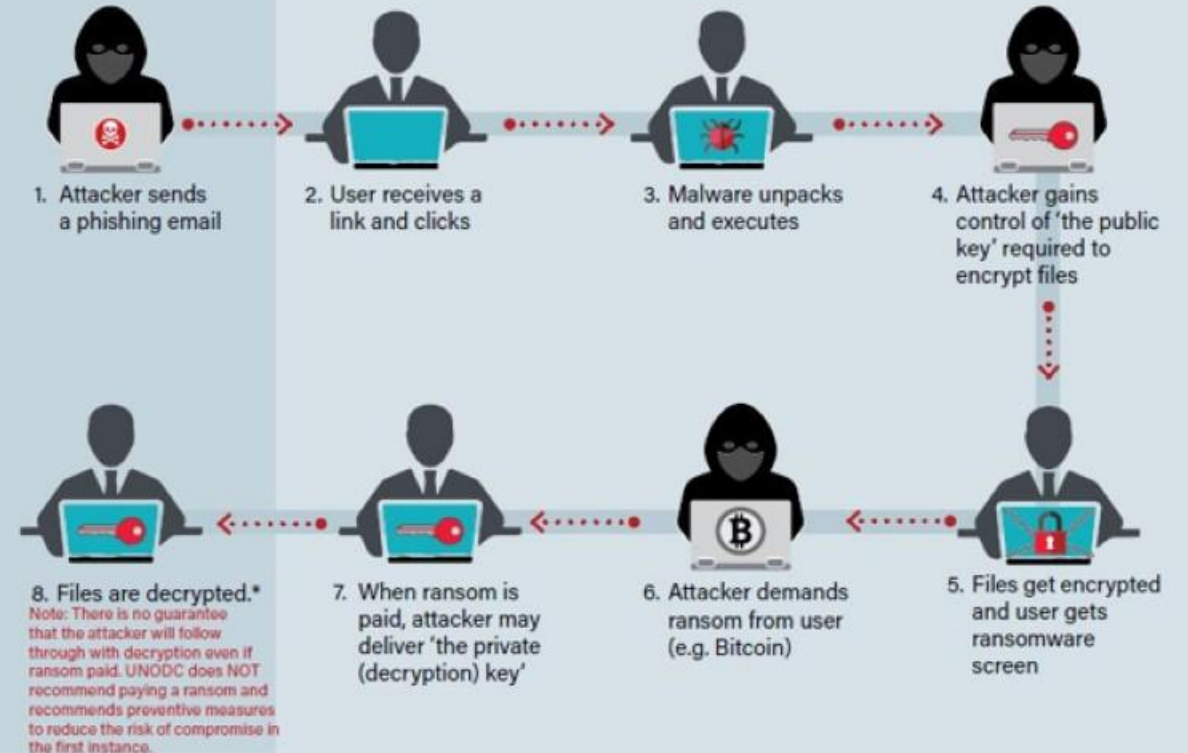
Malwares and

❖ There are several types of malware, the most important are as fellows:

➤ A number of further terms are also used to describe more specific types of malware, characterized by their purposes. They include:

- **Ransomware:-** A class of extortive malware that locks or encrypts data or functions and demands a payment to unlock them.
- operating system.

Anatomy of a ransomware attack



Keylogger

- **Keylogger:-** A class of malware that secretly records user keystrokes and, in some cases, screen content.
- A recent example of malware's ability to function as a tool for cyberespionage is Flame, also known as Flamer and Skywiper. Discovered in 2012, it can record keyboard activity and network traffic as well as screenshots, audio and video communications such as Skype.
- Once collected, the recorded information is sent to various control servers, and a "kill command" is launched to wipe all traces of the malware from the computer.



Backdoor

- **Advanced persistent threats:-** Complex and coordinated attacks directed at a specific entity or organization. They require an enormous amount of research and time, often taking months or even years to fully execute.
- **Backdoor:-** A means of regaining access to a compromised system by installing software or configuring existing software to enable remote access under attacker-defined conditions.



Brute Force Attack

- **Brute Force Attack:-** An attack made by trying all possible combinations of passwords or encryption keys until the correct one is found.
- **Buffer Overflow:-** Occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information—which has to go somewhere—can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. In buffer overflow attacks, the extra data may contain codes type of security attack on data integrity.

HOW A BASIC BRUTE FORCE ATTACK WORKS



Attacker



Guess List Of
Username &
Password
Combination



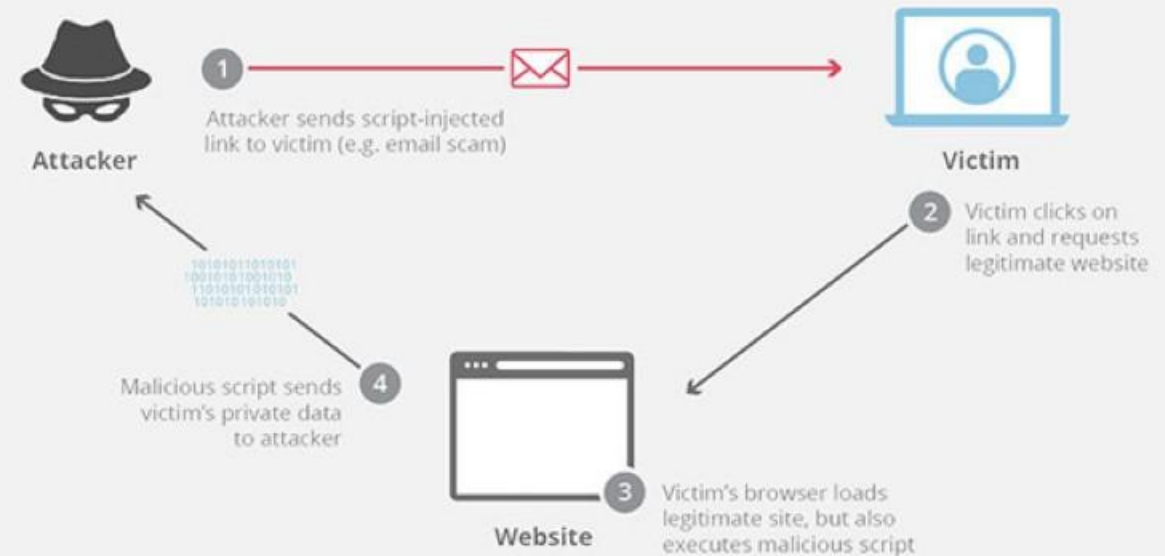
Repeats Login
Attempts Until
One Is Successful



Successful
Credential Validation

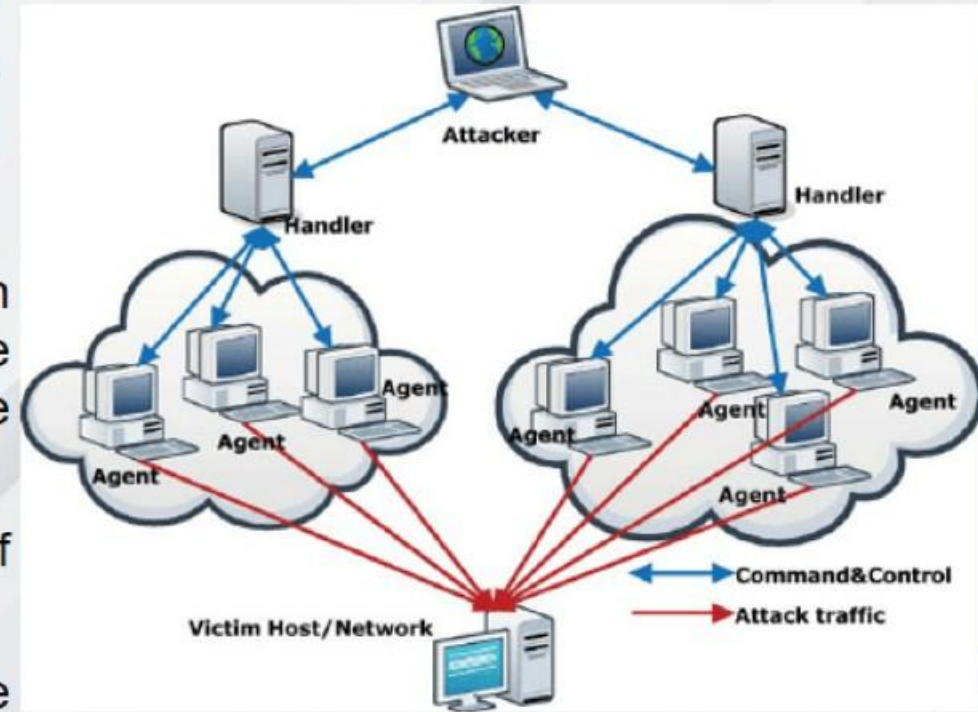
Cross-site scripting (XSS)

- **Cross-site scripting (XSS):-** A type of injection in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.



Denial-of-service (DoS) attack

- **Denial-of-service (DoS) attack:-** An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.
- **Denial of service** or **DoS** is an internet security related event in which the hackers attack a particular server running some internet services to prevent it from working normal or stop the services.
- In this case the servers are overwhelmed with the flooding of superfluous messages.
- The hacker exploits the server vulnerability and sends the bombardment of automated requests and messages to that particular server to respond.



Denial-of-service (DoS) attack

- In **certain cases**, the service stops working any more due to overloaded server.
- These kinds of malicious attacks prevent the legitimate users from accessing the online services by either disrupting the services or stopping the services completely.
- The **major symptoms** of having become the victim of DoS attacks include the following:
 - Inability in accessing a website
 - Delay in accessing online service
 - Huge delays in file opening on the websites
 - Increased volume of spam emails
 - Degradation of performance of services

Signs of a DoS attack



DEGRADATION IN NETWORK PERFORMANCE

Especially when attempting to open files stored on the network or when accessing websites.



SPECIFIC WEBSITE UNAVAILABLE

A particular site does not open or cannot be found.



INABILITY TO ACCESS ANY WEBSITE

All websites are inaccessible on the network.



HIGH VOLUME OF EMAIL SPAM

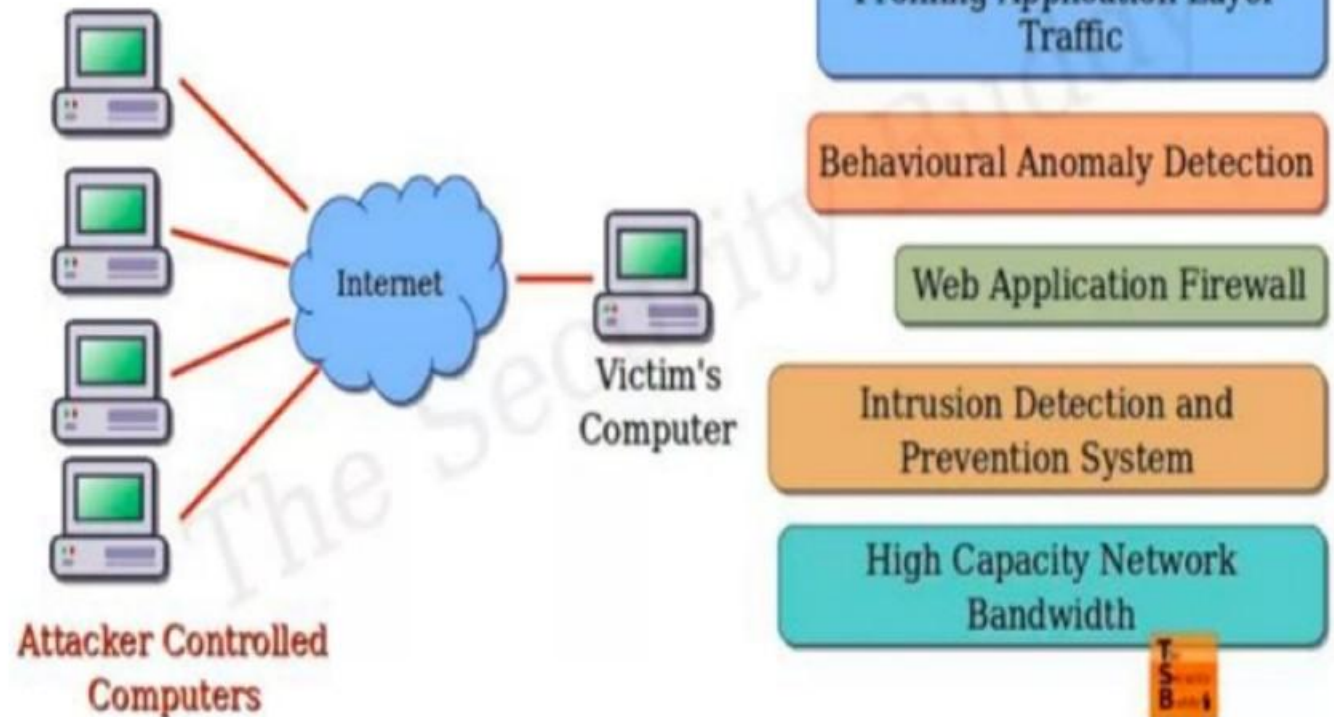
A higher than usual volume of spam email.

Denial-of-service (DoS) attack

The impact of the DoS attack can be *mitigated* by taking the following steps:

- Routing the malicious traffic.
- Using load balancers to avoid heavy malicious traffic.
- Using intrusion detection systems (IDS)
- Using intrusion prevention systems (IPS)
- Using security firewalls

Denial of Service Attacks and Prevention



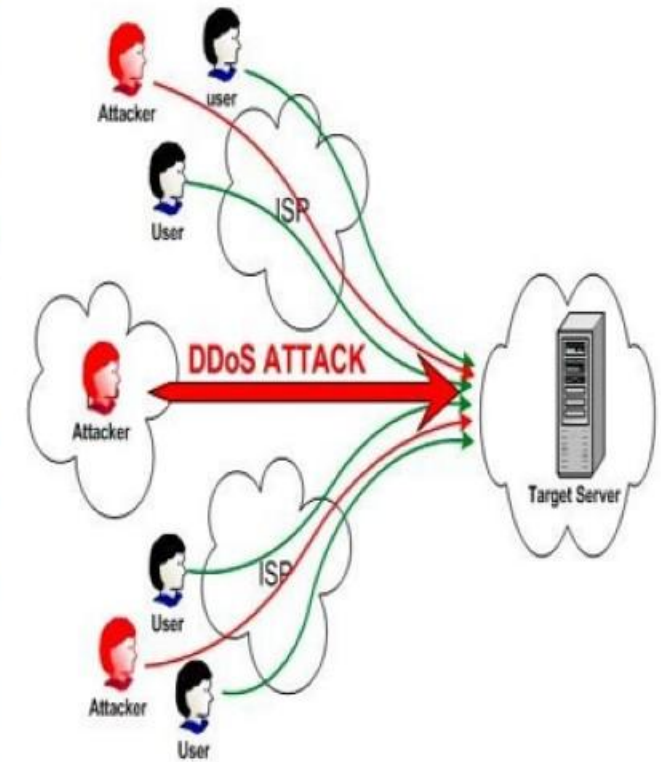
Denial-of-service (DoS) attack

Main types of DoS attacks include the following:

- DNS server attack
- HTTP server attack
- ICMP protocol flooding
- Network attack or buffer overflow attack
- Large name files attack on the network or server
- Ping of death attack
- SYN flood attack on TCP handshake protocol

Distributed Denial of Services)DDoS(

- Distributed Denial of Service or precisely DDoS is also a type of DoS attacks.
- In which the servers are jammed or overwhelmed with the malicious traffic to prevent the legitimate users from accessing their accounts or legitimate online services.
- **Main different between DoS and DDoS attacks** is that the DoS attack is targeted from a specific origination of traffic to attack the victim server, while in the DDoS attacks multiple sources of traffic are used to attack the victim server.
- DDoS is more lethal than the DoS attacks. The prevention of DDoS attacks is very difficult as compared to the normal DoS attacks.



Distributed Denial of Services)DDoS(

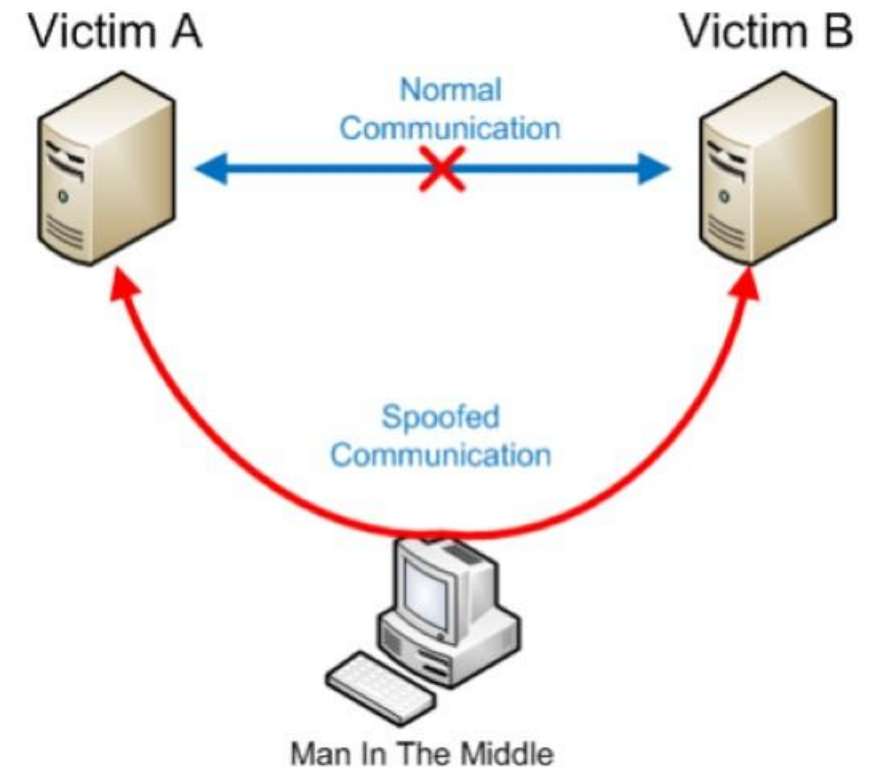
- In the distributed DoS attack, the hacker uses **controller machine** to hack multiple vulnerable machines around the globe.
- Then all those infected machines will be controlled by the software program running on the attacker's server.
- That controller sends instructions to the infected machine on which the hacker has already established the control to send automated requests (traffic) to the targeted victim machine.
- Then all those zombies start attacking the target from multiple IP sources to bring the server to almost halt.
- In this attack many computers from different parts become the part of this deadly attack without any approval and knowledge of the owner of the computer.

Man-in-the-middle attack

- **Man-in-the-middle attack:-** An attack strategy in which the attacker intercepts the communication stream between two parts of the victim system and then replaces the traffic between the two components with the intruder's own, eventually assuming control of the communication.

MITM attack consists of three major steps.

1. The hacker scans the vulnerabilities of the system and network.
2. Once the vulnerabilities are known, the phishing emails are sent to users; those emails contain the wrong addresses of your services or bank accounts.
3. Decrypt your information for stealing purpose.



Man-in-the-middle attack

Example MITM attacks:

- Sometimes, you get an email that looks like it was sent from your bank or your other financial institute.
- That is phishing email, which asks you to click certain link for the verification of your account, phone number or any other information.
- Once you click that link, the link takes you to the web server, which looks like your bank website but in real, that is not your bank website.
- You insert your credentials to login.
- Thus, you provide your bank information to the hacker.
- Finally, the hacker decodes your password and uses that password to take some from your account.
- This entire process is known as the man in the middle or MITM cyberattack.

Man-in-the-middle attack

The major types of MITM attacks

- ❖ DNS Spoofing
- ❖ HTTP Spoofing
- ❖ IP Spoofing
- ❖ Email Hijacking
- ❖ SSL Hijacking
- ❖ Wi-Fi network Eavesdropping
- ❖ Stealing the cookies set on the browsers

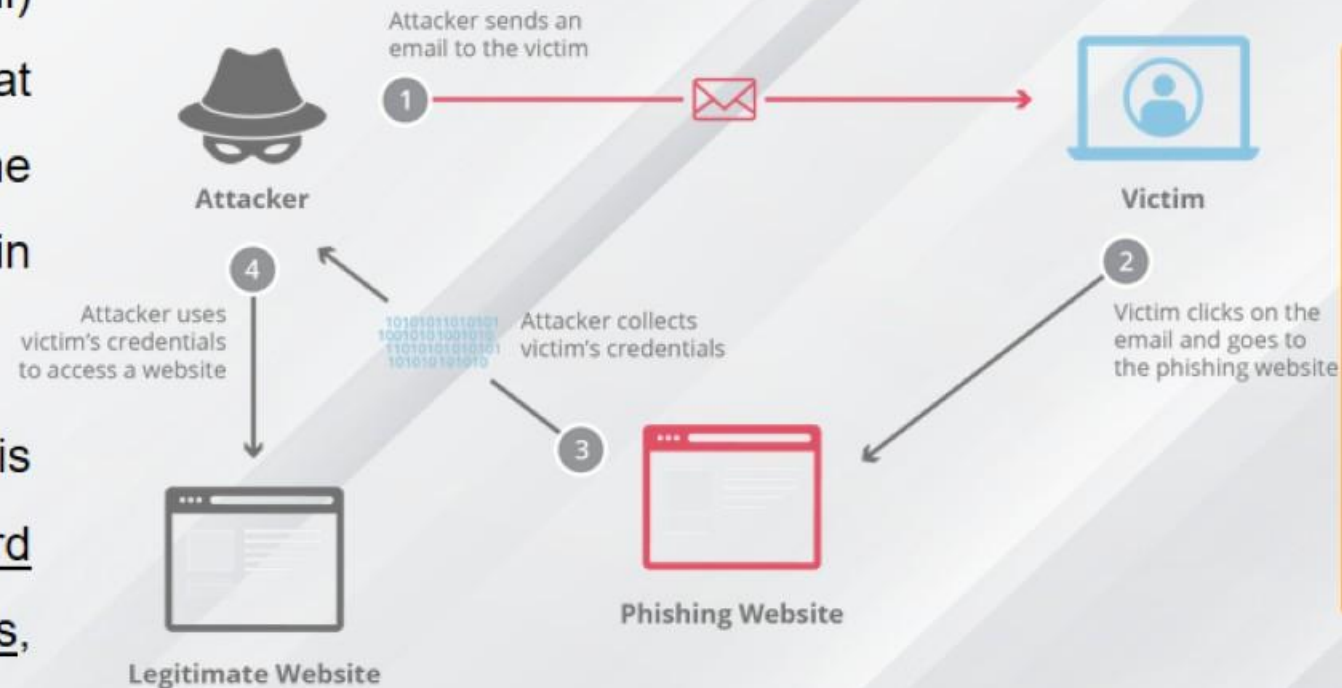
Social engineering

- **Social engineering:-** Any attempt to exploit social vulnerabilities to gain access to information and/or systems. It involves a “con game” that tricks others into divulging information or opening malicious software or programs.



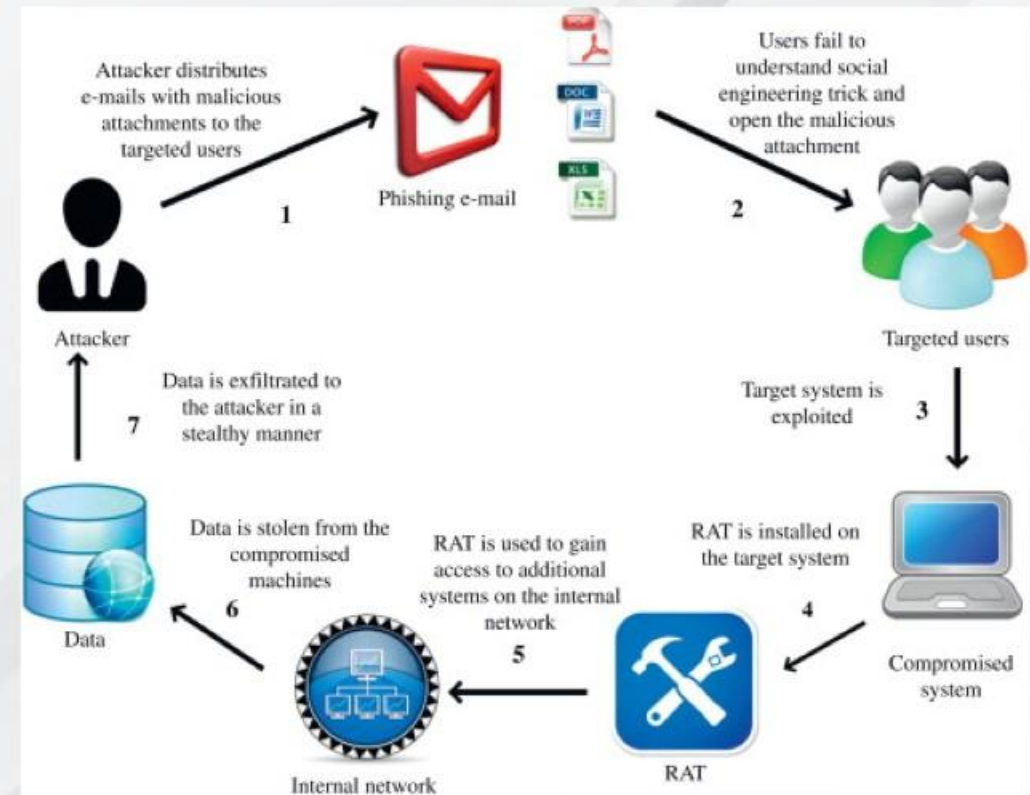
Phishing

- **Phishing:-** A type of electronic mail (email) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering.
- **The main target of the phishing attack** is to get the information about the credit card number, ATM pin codes, passwords, username, and the related information.



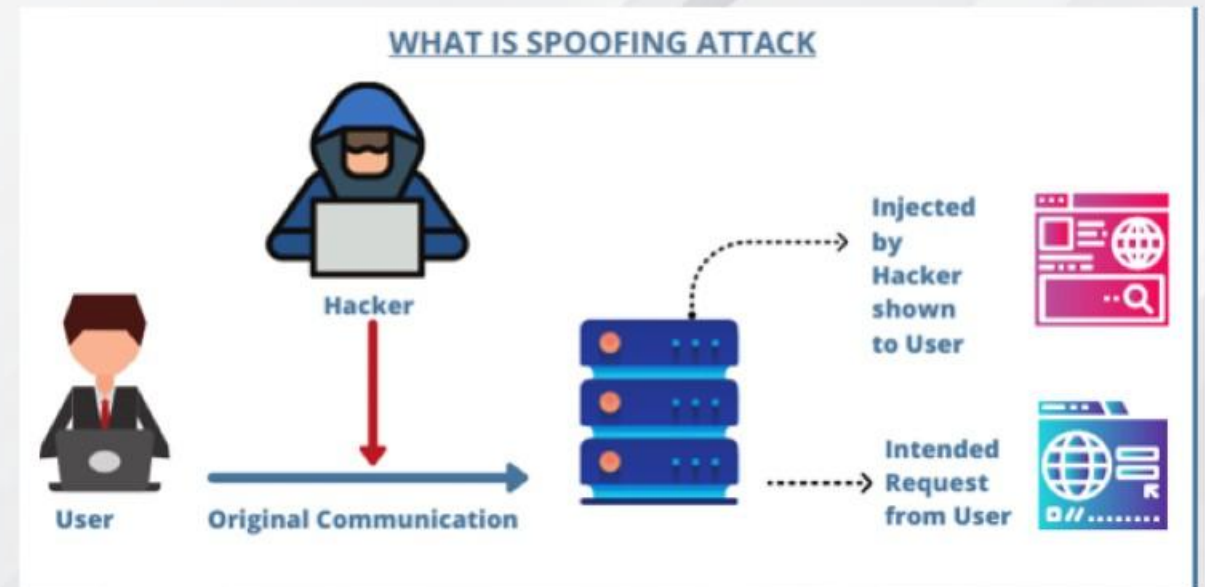
Spear phishing

- **Spear phishing:-** An attack where social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim.



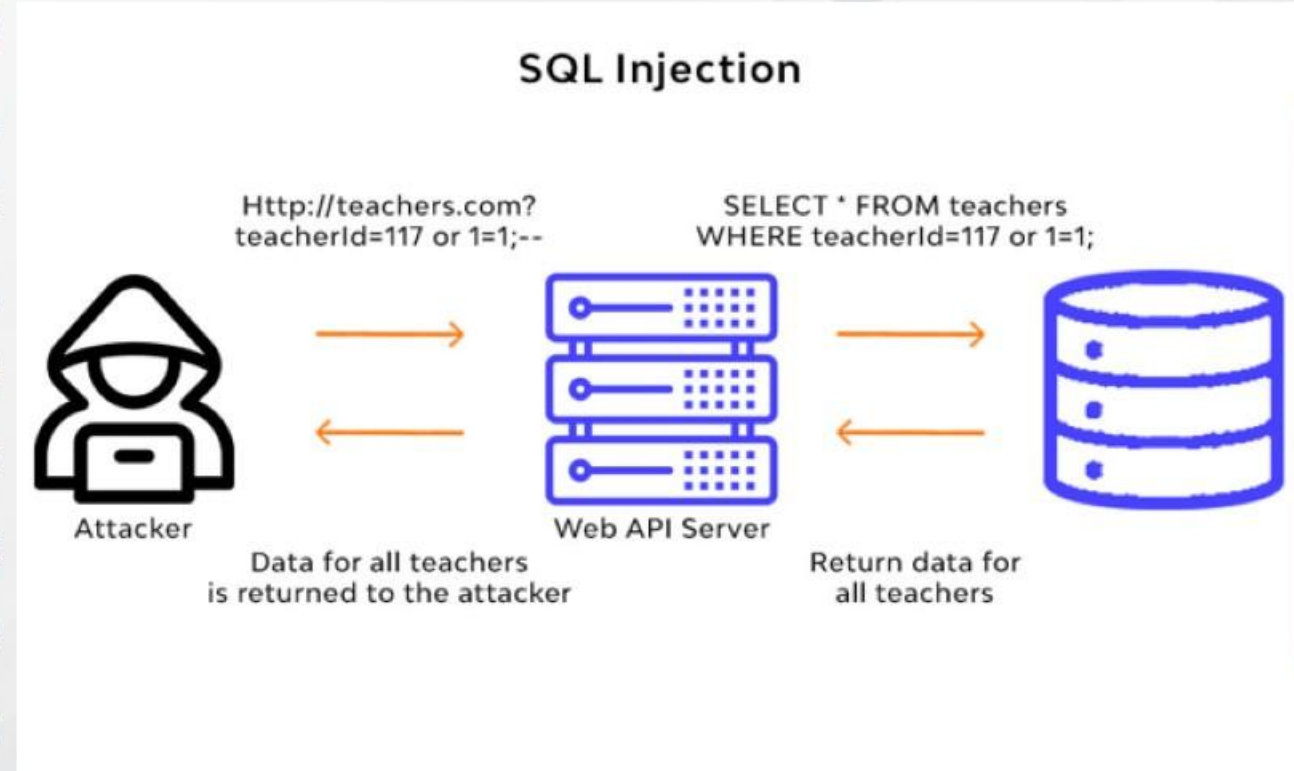
Spoofing

- **Spoofing:-** Faking the sending address of a transmission in order to gain illegal entry into a secure system.



Structure Query language(SQL)injection

- **Structure Query language (SQL) injection:-** According to MITRE, SQL injection results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design.



Zero-day exploit

- **Zero-day exploit:-** A vulnerability that is exploited before the software creator/vendor is even aware of its existence.
- Zero Day Exploitation commonly known as Zero-Day or 0-Day is a vulnerability in the computer software system that is known exactly on the same day when the malicious attacks exploit that vulnerability.
- In this attack, there is almost no time to patch up the vulnerability of the software because it was known at the same time when the attack occurred, and no time was available for the software engineers to tackle this issue.

Zero-Day Attacks Explained



1

A security flaw exists but is unbeknown to developers, making it vulnerable to attacks.

2

A hacker discovers the vulnerability and exploits it by malware injection.

3

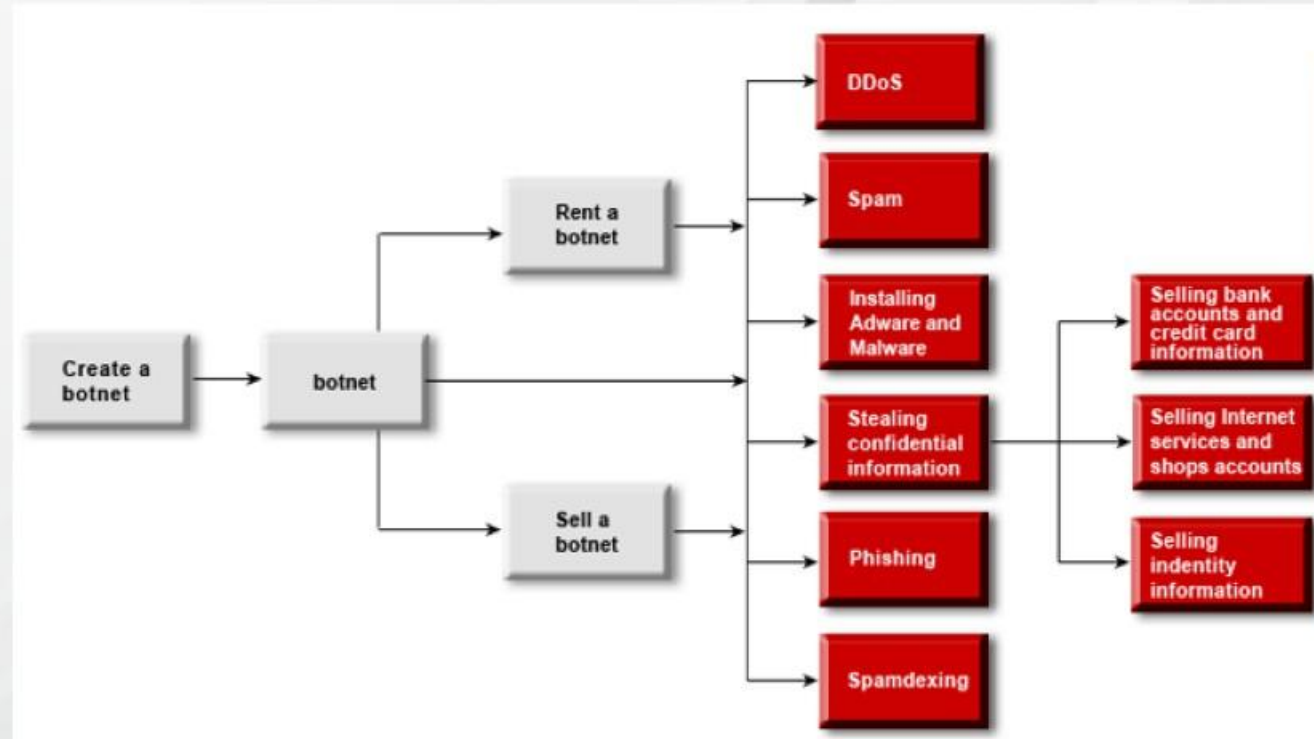
A cyberattack ensues from the malware, potentially resulting in data loss.

4

Developers detect the attack and have zero days to mitigate it.

Botnets

- **Botnets:-** A botnet (a term derived from “robot network”) is a large, automated and distributed network of previously compromised computers that can be simultaneously controlled to launch large-scale attacks such as denial-of-service (DoS).



Vulnerabilities

Vulnerabilities are the gaps or weaknesses in a system that make threats possible and tempt threat actors to exploit them.

Types of vulnerabilities in network security include but are not limited to

- SQL injections,
- server misconfigurations,
- cross-site scripting,
- and transmitting sensitive data in a non-encrypted plain text format.

Some of the most common network vulnerabilities include the following gaps in your application security: when applications are not kept up-to-date, tested, and patched, the doors are open to code injection, cross-site scripting, insecure direct object references, and much more.

Assignment

- Crypto-jacking
- Spamming
- Digital Property Misappropriation
- Digital Vandalism
- Cyberstalking
- Cyber Frauds & Forgery

Quiz, ex.

1. In, the digitally stored documents are forged to form the counterfeit documents. This crime is increased during the recent years due to the availability of high-tech devices like computer software, printers, scanners, cameras, and other tools.
 - A. cyber frauds and forgery
 - B. digital property misappropriation
 - C. zero-day exploitation
 - D. spamming

2. The impact ofin Asian countries is very high due to the traditional social structures.
 - A. cyber terrorism
 - B. digital property misappropriation
 - C. cyberstalking
 - D. Spamming

Quiz, ex.

3. Cyberstalking is a systematic approach ofdone through email, phones, SMS, chats, and other forms of communication. The main components used in the communication to threaten the targeted entity include defaming, false allegations, slandering, and other forms of blackmailing.
- A. cyber terrorism
 - B. digital property misappropriation
 - C. zero-day exploitation
 - D. harassing
4. In the attack the malware either remove the useful data from the websites or manipulate the information in such a way that the meaning of the information is reversed.
- A. cyber terrorism
 - B. digital property misappropriation
 - C. zero-day exploitation
 - D. digital vandalism



Thank You