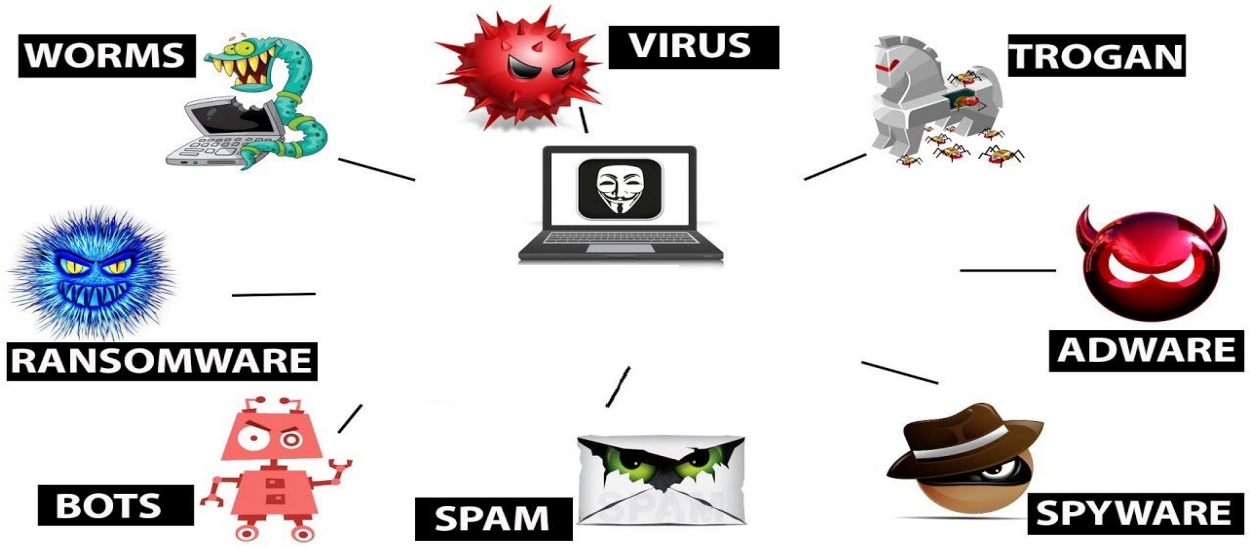
Malware:

- Malware is a term which is short for “Malicious Software” is a file or code or application.
- Malware (Malicious Software) is any program or file, that is harmful to a computer user.
- Malicious Software typically delivered over a network that infects, explores and steals.
- Malware (Malicious Software) can be conducts virtually any behavior an attacker wants.
- Malware (Malicious Software) is an inclusive term, for all types of malicious software.
- Malicious Software is terms for all as Viruses, Worms, Trojans, Rootkits, and Spyware.
- Malware is also terms for Adware, Scareware, Botnets, Logic Bombs, Key loggers etc.
- Many tools can identify Malware on the network such as Packet Captures to analyzing.
- In addition, tools Snort, NetFlow, IPS, Advanced Malware Protection, Cisco FirePOWER etc.



Virus:

- Malicious code that attached to executable files that are often regular application.
- Viruses require some type of human or any other application interaction to activate.
- Entire category of viruses is designed to damage or destroy a system or the data.

https://t.me/learningnets

Worm:

- Worms are malware that replicate themselves and spread to infect other systems.
- Think of worms as small programs that replicate themselves in a computer network.
- A worm can travel from system to system without human or application interaction.
- When worm executes, it can replicate again & infect even more systems or computer.
- Worms destroy the files and data on user's computer or system or Computer network.
- Worms usually target the operating system (OS) files to make them empty & destroy.
- Worms typically cause harm to the computer network and consuming the bandwidth.

Adware:

- Adware is computer term, which is stand for Advertising-Supported Malware.
- Adware works by executing advertisements to generate revenue for the hackers.
- Adware (Advertising-Supported Malware) is any type of advertising-supported software.
- Adware will play, display, or download advertisements automatically on a user's computer.
- Adware will play once the software has been installed or the application is in the use.

https://t.me/learningnets

Ransomware:

- Its propagate like worm but is designed to encrypt personal files on victim's hard drive.
- Ransomware works by encrypting the hard drive and all files on a system or Computer.
- Ransomware can encrypt specific files in your system or all your files or mast boot record.
- Ransomware then asks for a payment in exchange for giving the decryption key.
- Major Ransomware like Reveton, CryptoLocker, CryptoWall, Pyeta, Nyeta, Bad Rabbit.
- More recently Ransomware 2017 WannaCry attack was lunched which destroy many PCs.
- Ransomware caused no small amount of destruction, but it caused huge destruction .

Trojan:

- Trojans are malicious programs that appear like regular applications or programs.
- Trojans are malicious programs that appear like media files or other computer files.
- Trojans contain a malicious payload; the payload can be anything malicious acts etc.
- Trojans payload provide backdoor that allows attackers unauthorized access to system.
- Trojans pretend to do one thing but, when loaded, actually perform another malicious.
- Few Trojan categories are command-shell Trojans, graphical user interface (GUI) Trojans.
- HTTP/HTTPS Trojans, document Trojans, defacement Trojans, botnet Trojans, VNC Trojans.
- Remote-Access Trojans, data-hiding Trojans, banking Trojans, DoS Trojans, FTP Trojans.
- Software-Disabling Trojans, and covert-channel Trojans are few examples of trojans.
- Remote-access Trojans (RATs) allow the attacker full control over the system or PC.
- Idea behind this type of Trojan is to hide user's data sometimes known as ransomware.
- Security-software disablers Trojans are designed to attack and kill antivirus or firewalls.
- Denial of Service (DoS), These Trojans are designed to cause a DoS Denial of Service.
- They can be designed to knock out specific service or to bring an entire system offline.
- Trojans are dangerous, they represent a loss of confidentiality, integrity, and availability.
- Common targets of Trojans Credit card data & banking info have become huge targets.
- Passwords are always a big target of second common targets of trojans malware.

https://t.me/learningnets

- o P2P networks and file-sharing sites such as The Pirate Bay are generally unmonitored.
- o And allow anyone to spread any programs they want, legitimate or not like trojans.
- o Instant Messaging, Internet Relay Chat, Email attachments, and browser extension etc.

Spyware:

- o Spyware computer network term, which is common types of malware.
- o Spyware monitors the activities performed by a computer user on the PC.
- o The main intention of a spyware is to collect the private information of PC user.
- o Spyware normally come from internet while user download freeware software.
- o Spyware is another form of malicious code that is similar to a Trojan horse malware.

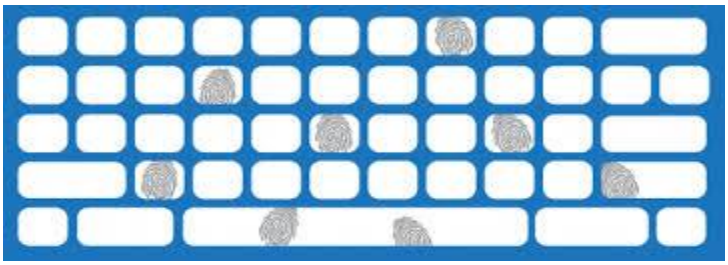
https://t.me/learningnets

Rootkits:

- A rootkit is a collection of software specifically designed to permit malware.
- Rootkits gathers information, into your system, Computer, or computer network.
- These work in the background so that a user may not notice anything suspicious.
- Rootkits in the background permit several types of malware to get into the system.
- The term rootkit is derived from the combination of two words – "root" and "kit".
- Root refers to the administrator account in Unix and Linux operating systems etc.
- Kit refers to programs allow threat actor to obtain unauthorized root/admin access.

Keyloggers:

- Keylogger is network term which is Keystroke loggers software or Hardwar.
- Software, which records all the information that is typed using a keyboard.
- Keyloggers store the gathered information and send it to the attacker.
- Attacker extract sensitive information like password or credit card details.



Scareware:

- Scareware is a type of malware, which is designed to trick victims.
- Scareware trick victims into purchasing and downloading useless software.
- Scareware trick victims into download potentially dangerous software.
- Scareware, which generates pop-ups that resemble Windows system messages.
- Scareware usually purports to be antivirus or antispyware software or malwares.
- Scareware also usually popup a firewall application or a registry cleaner.
- The messages typically say that a large number of problems such as infected files.
- The user is prompted to purchase software to fix Computer or system problems.
- In reality, no problems were detected, and the suggested software contain malware.

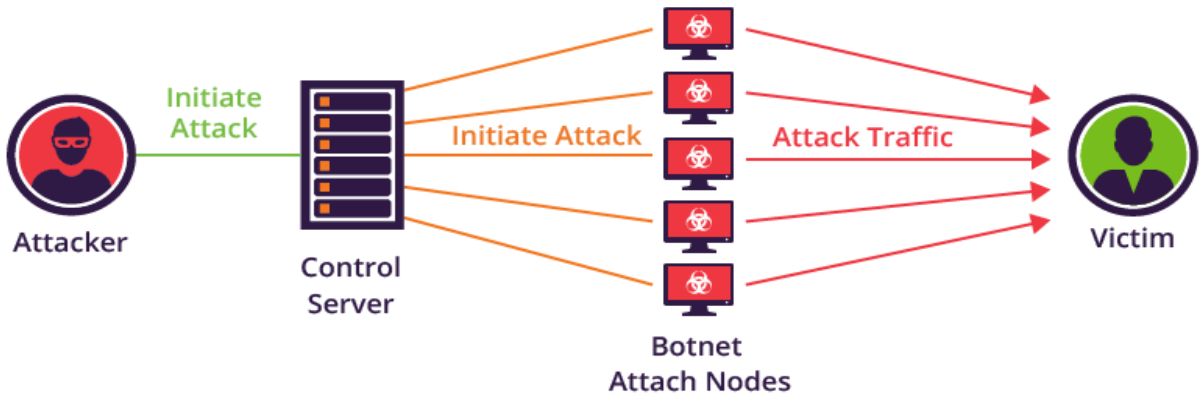
https://t.me/learningnets

Logic Bomb:

- A Logic Bomb is malware that is triggered by a response to an event.
- Such as launching an application or when a specific date/time is reached.
- Attackers can use logic bombs in a variety of ways to destroy data or system.
- They can embed arbitrary code within a fake application, or Trojan horse.
- Logic Bomb will be executed whenever you launch the fraudulent software.
- Attackers can also use a combination of spyware and logic bombs to steal identity.

Botnet:

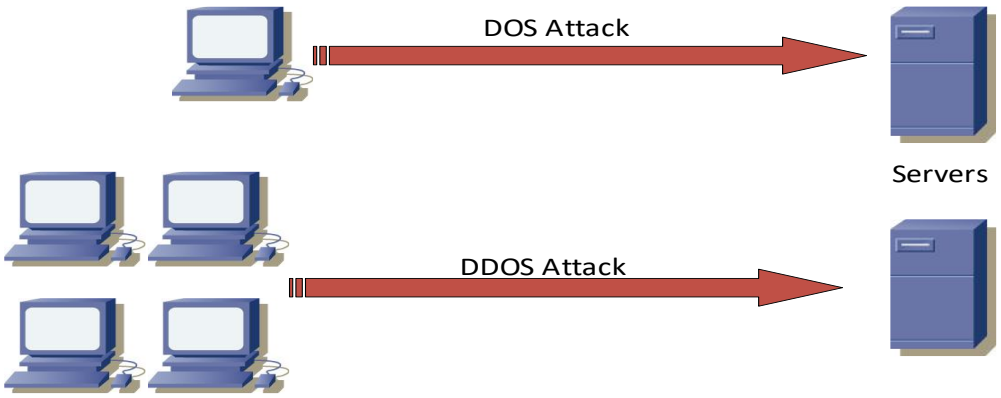
- Basically, the word botnet is made up of two words: **bot** and **net**.
- So, Bot is short for robot and Net comes from the network, Robot Network.
- People who write and operate malware cannot manually log onto every computer.
- They have infected, instead they use botnets to manage a large number of systems.
- A botnet is a network of infected computers, used by the malware to spread.
- Cybercriminals use special Trojan viruses to breach the security of several users' PCs.
- Cybercriminals take control of each computer & organize all of the infected PCs.
- Cybercriminals remotely manage and organize all infected computer bot.



https://t.me/learningnets

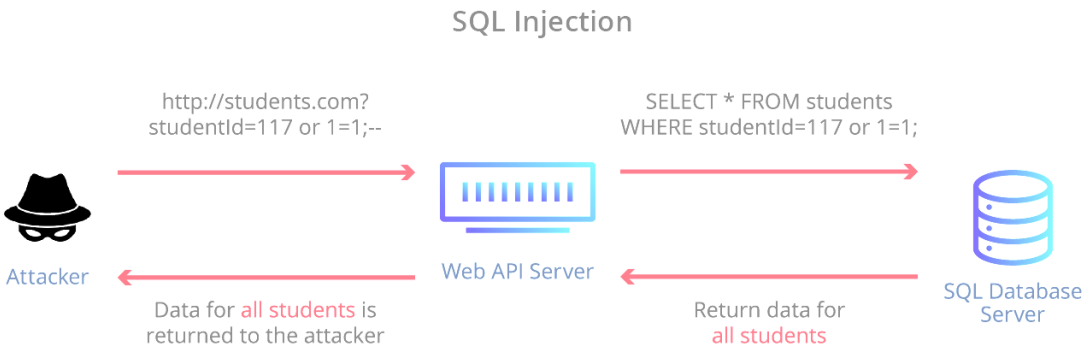
DoS (Denial of Service) Attack:

- DoS Attack is a type of attack to network server with large number of service requests.
- DoS Attack can cause server to crash the server & legitimate users are denied the service.
- DDoS stand for (Distributed Denial of Service) an Attack, which is one type of DoS attack.
- DDoS originating from many attacking computers from different geographical regions.
- Zombies and Botnets are mainly used in DDoS (Distributed Denial of Service) attacks.
- Both type of attack DoS and DDoS can cause the services to become unavailable to users.
- Such as Ping of Death, Smurf Attack, TCP SYN, CDP Flood, Buffer Overflow, ICMP Flood.
- Cloud is more vulnerable to DoS attacks because it is shared by many users & organizations.



SQL Injection:

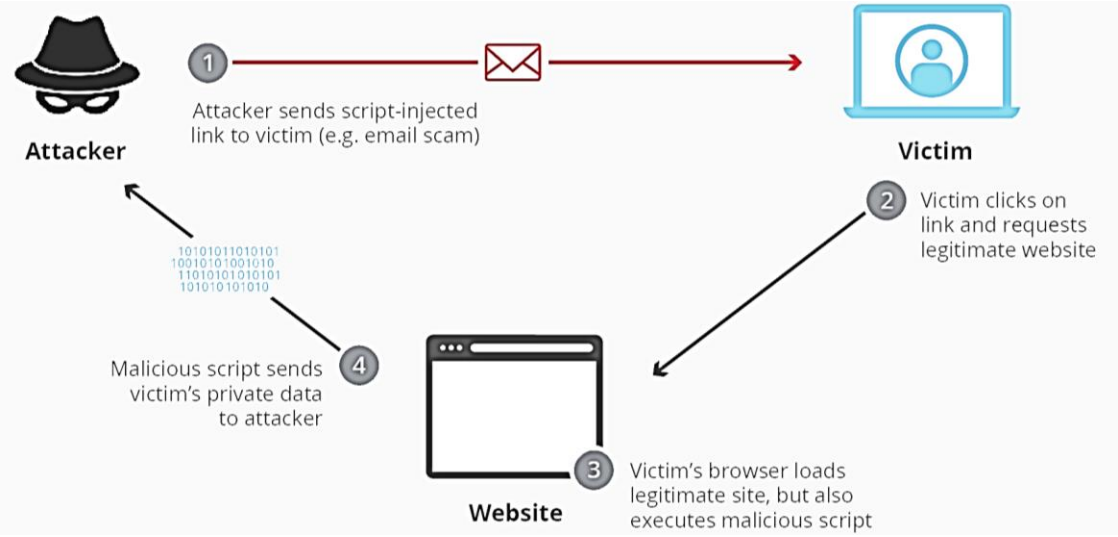
- SQL injection is a code injection technique that might destroy your database.
- SQL injection is one of the most common web hacking techniques to gain access.
- SQL injection is placement of malicious code in SQL statements, via web page input.
- SQL Injection is injection attack makes possible to execute malicious SQL statements.
- Attackers can use SQL Injection vulnerabilities to bypass application security measures.
- SQL Injection (SQLi) also used to add, modify, and delete records in the database.
- SQL injection attack exploits vulnerable cloud-based applications allow pass SQL commands.



https://t.me/learningnets

Cross Site Scripting:

- XSS is term, which stand for Cross-Site Scripting Errors, are a type of coding error.
- Where a malicious party can trigger execution of software from their browser.
- Cross-site scripting is a type of security vulnerability found in web applications.
- XSS enables attackers to inject client-side scripts into web pages viewed by other users.
- Common purpose of XSS attack is to collect cookie data such as session IDs or login info.
- XSS used to steal cookies exploited to gain access as authenticated user to a cloud-based.
- Three major categories are Reflected XSS, Stored(Persistent) XSS, and DOM-Based XSS.



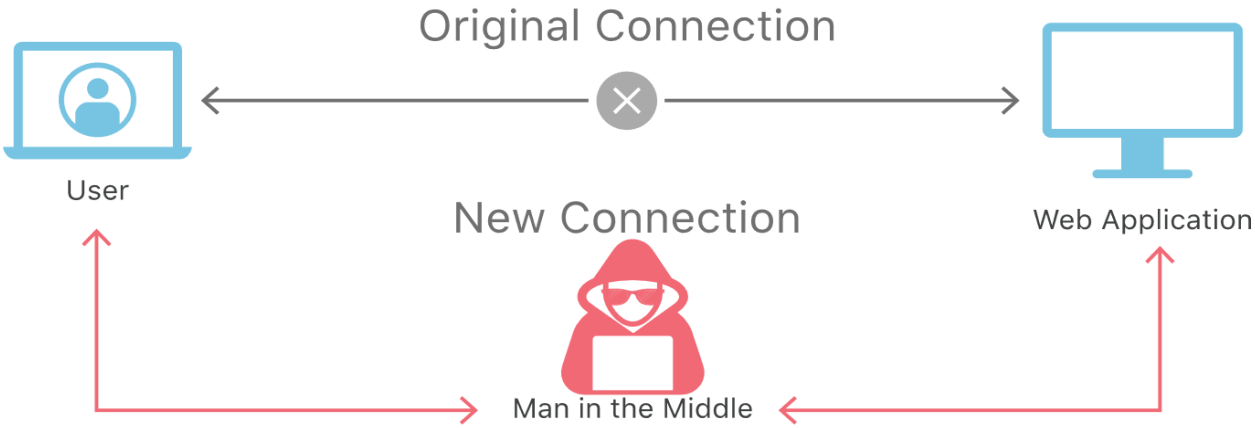
Phishing:

- Phishing is a type of social engineering attack often used to steal user data or info.
- Phishing is social engineering attack to steal login credentials & credit card numbers.
- Phishing is method of trying to gather personal info using deceptive e-mails & websites.
- Phishing is a cyber-attack that uses disguised email as a weapon to steal user data or info.

https://t.me/learningnets

Man-In-The-Middle:

- MITM (Man in The Middle) means man in the middle of your conversation.
- In a Man-in-The-Middle attack, attackers place themselves between two devices.
- MITM attack to intercept or modify communications between the two devices.
- MITM cyberattacks allow attackers to secretly intercept communications.
- MITM attack happens when hacker inserts themselves between a user & apps.
- Attackers have many different reasons and methods for using a MITM attack.
- MITM is used to steal something, like credit card numbers or user login credentials.
- MITM attacks involve interception of communication between two digital systems.



https://t.me/learningnets

Data Breach:

- Data breach can involve data that was not supposed to be released to the public.
- Which includes financial information, personal health information & trade secrets.
- Which includes. Personally, identifiable information and other intellectual property.
- Value of the organization's cloud-based data might be different for different people.
- Data Breach happen if organization lacks managing authentication & identity properly.
- The Businesses need to properly allocate access to data as per every user's job role.
- One-time passwords & phone-based authentications are the two factor authentications.
- That help securing cloud services by making it tough for the attacks to steal the credentials.

https://t.me/learningnets