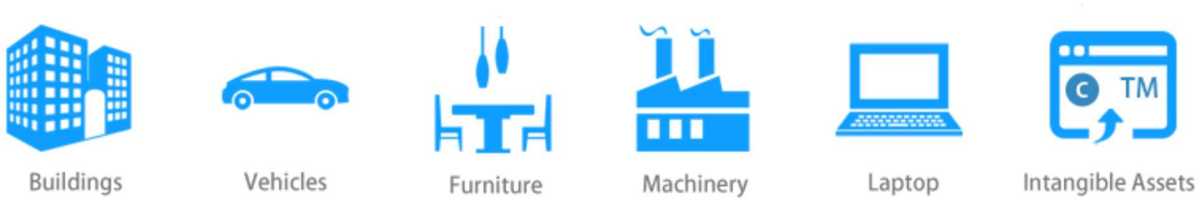
CHAPTER – 1

Common Network Security Terms:

Key Network Security technical terms are Asset, Vulnerability, Exploit, Threat, Attack, Risk and Countermeasures.

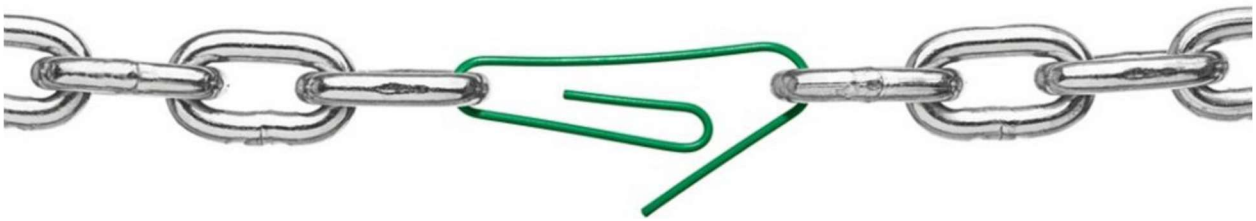
Asset:

Asset is anything, which the organization is invested, and which is valuable to the organization. Examples: Properties, Vehicles, Heavy Equipment, Plants, Buildings, Employees, Computers, Data, Intellectual Properties etc. Protecting the organization's assets is the prime function of security (Physical Security or Network Security).



Vulnerability:

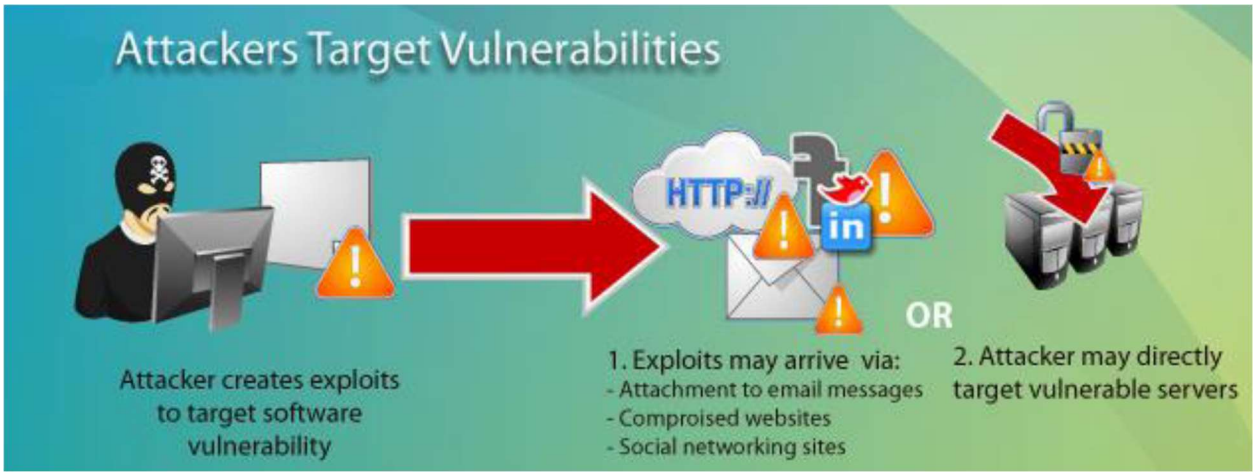
Vulnerability can be defined a weakness in a system or its design. Every system is human created. Chances for errors, mistakes are always there in every human created system. Vulnerabilities are always there in Applications, Network Protocols, and Operating Systems etc. An attacker to gain access to an organization's network can exploit vulnerability.



Email: info@tgmacad.com
Contact: 8319893647 | 9828507227 | 7742483008

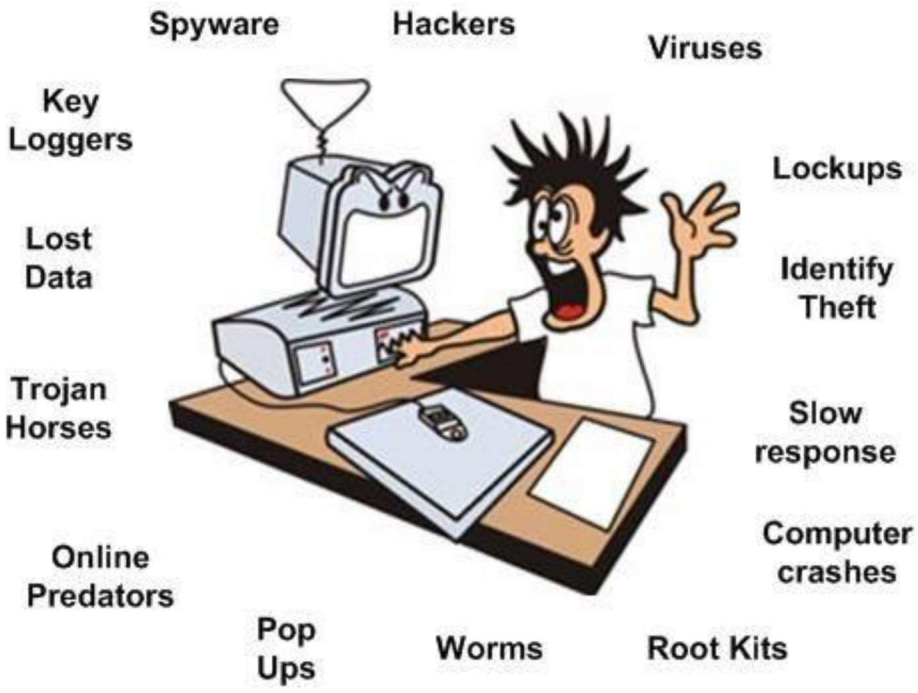
Exploit:

An Exploit can be defined as a way, method or tool which is used by an attacker, on a vulnerability, to cause damage to the target network or system. The exploit can be software that may cause a buffer overflow or a method of social engineering to hack a password.



Threat:

Threat can be defined as anything danger to an Asset. Threats can be accidentally triggered or intentionally exploited.



Email: info@tgmacad.com
Contact: 8319893647 | 9828507227 | 7742483008

Attack:

Attack can be defined as action taken by an attacker to harm an asset.

Risk:

The term "Risk" can be defined as potential for loss, compromise, damage, destruction or other negative consequence of an organization's Asset. Risk arises from a threat, multiple threats, and exploiting vulnerability. Risk forms an adverse negative affect an organization's Asset.

Risk = Asset + Threat + Vulnerability

Email: info@tgmacad.com
Contact: 8319893647 | 9828507227 | 7742483008

Countermeasure:

Countermeasure is an action initiated by the organization typically security professionals to mitigate a threat.

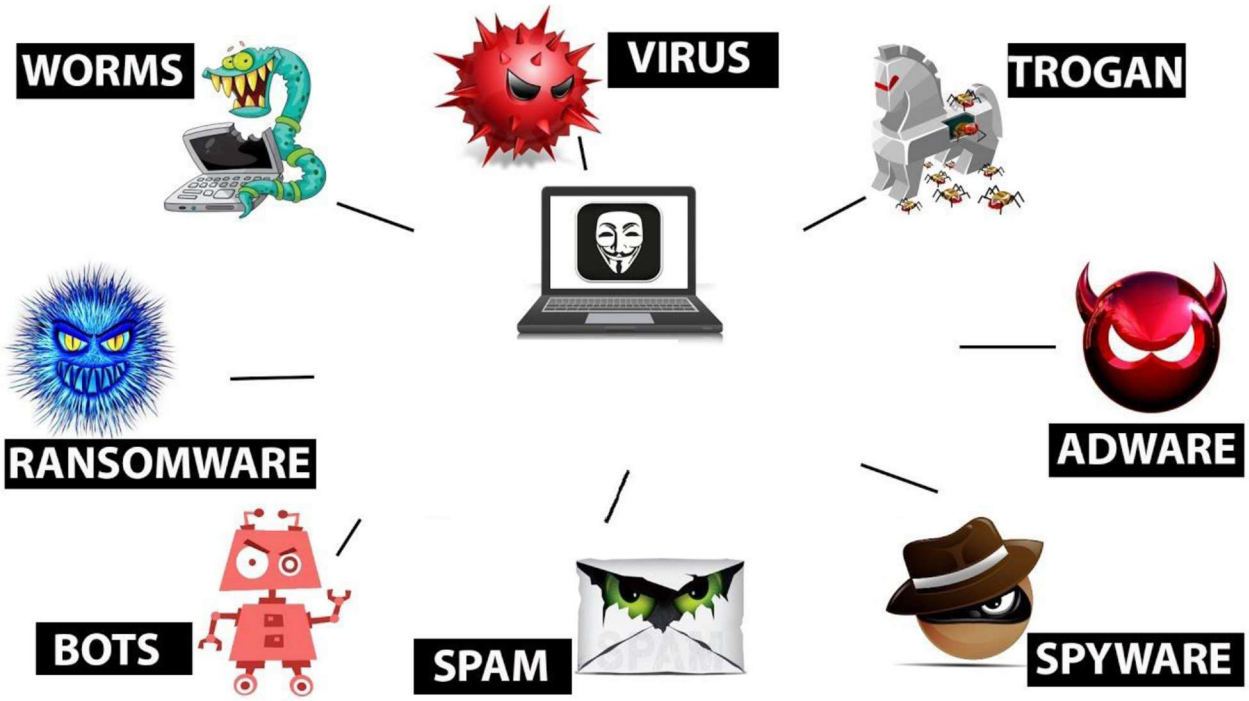
Common Security Terms:

Key Network Security technical terms are Asset, Vulnerability, Exploit, Threat, Attack, Risk and Countermeasures.

Email: info@tgmacad.com
Contact: 8319893647 | 9828507227 | 7742483008

Identify Malware:

- Malware short for “Malicious Software” is a file, program or code.
- Malware is any program or file that is harmful to a computer user.
- Typically delivered over a network that infects, explores and steals.
- Can be conducts virtually any behavior an attacker wants.
- Malware is an inclusive term for all types of malicious software.
- Malware 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 Fire POWER etc.



Virus:

- Malicious code that attached to executable files that are often a regular application.
- Most virus require end-user activation to damage the system or device.

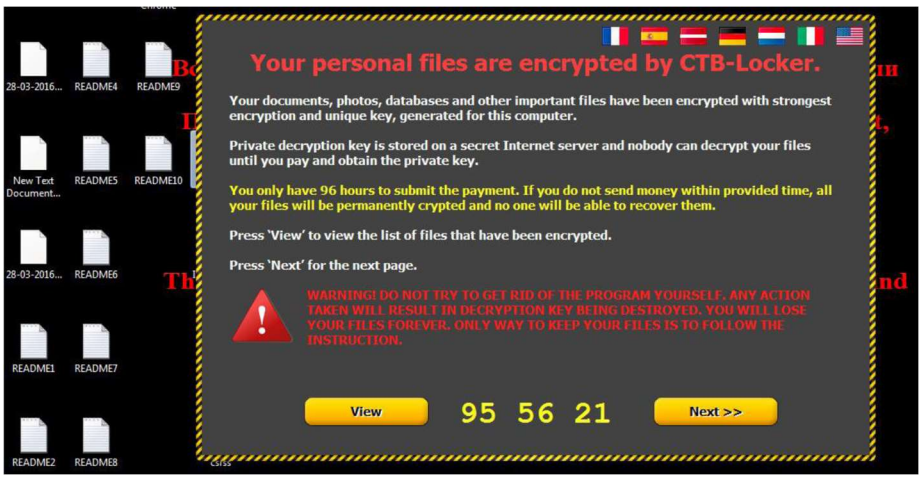
Email: info@tgmacad.com
Contact: 8319893647 | 9828507227 | 7742483008

Adware:

- Adware stand for Advertising-Supported Malware.
- Adware works by executing advertisements to generate revenue for the hackers.
- Adware 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 use.

Ransomware:

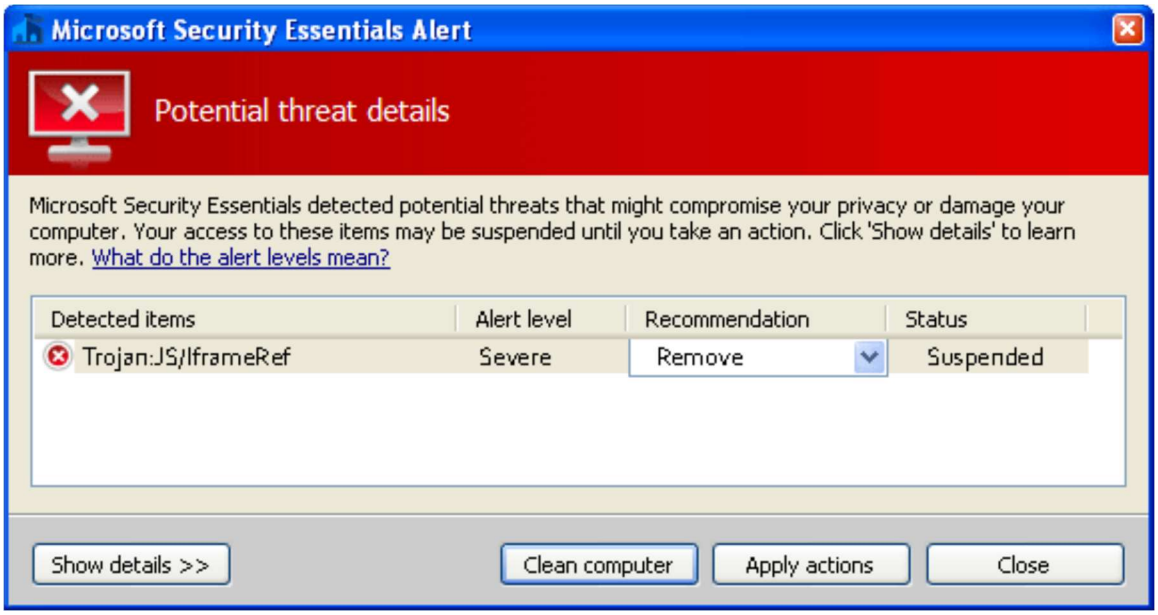
- Ransomware works by encrypting the hard drive and all files on a system.
- Ransomware then asks for a payment in exchange for giving the decryption key.
- Major Ransomware like Reveton, CryptoLocker, CryptoWall.
- More recently ransomware 2017 WannaCry attack.
- Ransomware caused no small amount of destruction.



Email: info@tgmacad.com
Contact: 8319893647 | 9828507227 | 7742483008

Trojan:

- Trojans are malicious programs that appear like regular applications.
- Trojans are malicious programs that appear like media files or other files.
- Trojans contain a malicious payload. The payload can be anything.
- Trojans payload provide backdoor that allows attackers unauthorized access.



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.
- Worms destroy the files and data on user's computer or system.
- They usually target the operating system files to make them empty.
- Worms typically cause harm to the network and consuming bandwidth.

Email: info@tgmacad.com
Contact: 8319893647 | 9828507227 | 7742483008

Spyware:

- Spyware is common types of malware.
- Spyware monitors the activities performed by a computer user on PC.
- The main intention of a spyware is to collect the private information of PC user.
- Spyware normally come from internet while user downloads free software.

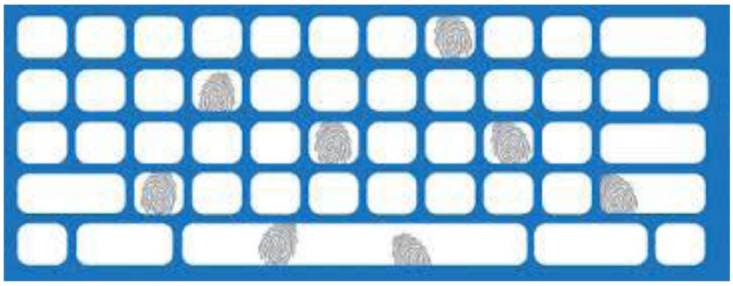
Rootkits:

- A rootkit is a collection of software specifically designed to permit malware.
- Rootkits gathers information, into your system.
- 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.

Email: info@tgmacad.com
Contact: 8319893647 | 9828507227 | 7742483008

Keyloggers:

- 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 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.
- 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 the problems.
- In reality, no problems were detected, and the suggested software contain malware.

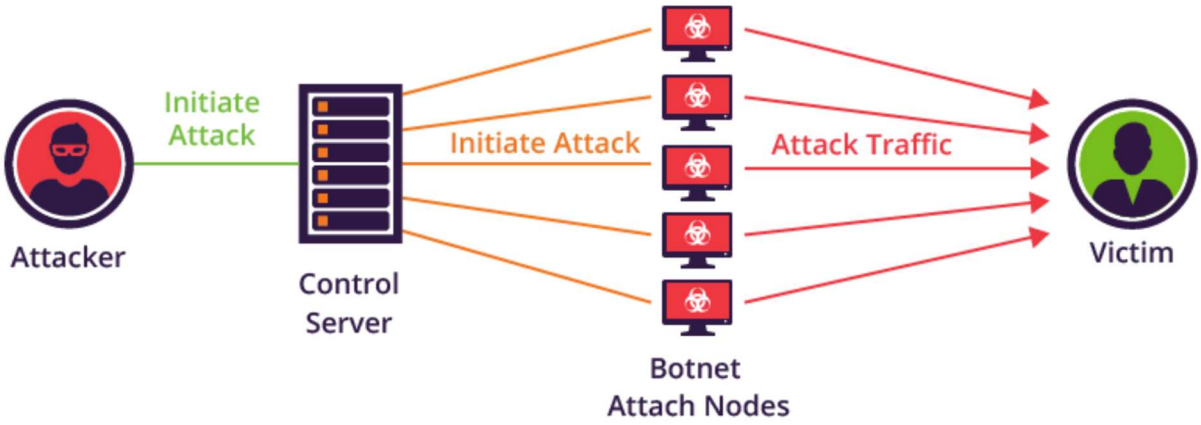
Email: info@tgmacad.com
Contact: 8319893647 | 9828507227 | 7742483008

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.
- 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:

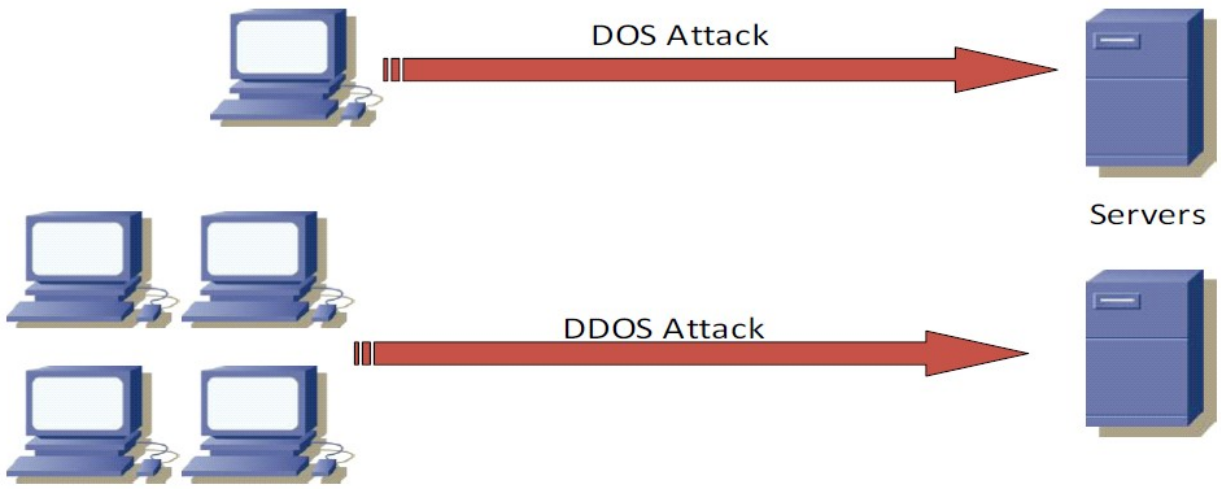
- The word botnet is made up of two words: **bot** and **net**.
- Bot is short for robot. Net comes from network.
- People who write and operate malware cannot manually log onto every computer.
- They have infected, instead they use botnets to manage a large number of systems.
- A botnet is a network 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 all infected computer bot.



Email: info@tgmacad.com
Contact: 8319893647 | 9828507227 | 7742483008

DoS (Denial of Service) Attack:

DOS Attack is a type of attack to a network server with large number or service requests with it cannot handle. Denial of Service Attack can causes the server to crash the server and legitimate users are denied the service. DDoS (Distributed Denial of Service) Attack is a type of DoS attack, originating from many attacking computers from different geographical regions. Zombies and Botnets are used in DDoS attacks. Both attack types can cause services to become unavailable. Such as Ping of Death, Smurf Attack, TCP SYN Flood, CDP Flood, Buffer Overflow, ICMP Flood.



Email: info@tgmacad.com
Contact: 8319893647 | 9828507227 | 7742483008