Unit – 07: System Security

- Intruders, types of attacks, protecting against Intruders honeypots, scanning and analysis tools,
- Viruses and worms, types of viruses, protection,
- Firewall architecture implementing firewalls, xml firewalls,
- Trusted systems, trusted system applications, multilevel security, trusted products.
- Security implementation, wireless security, securities in Adhoc-networks.

Questions to be discussed:

1. What do you mean by Intruder?
2. What is attack? Describe different types of attacks in network security.
3. Define the term virus. Explain various types of virus in brief.
4. Describe virus and antivirus in details.
5. Write short notes on:
    a. Firewall
    b. Virtual Private Network(VPN)
    c. Honeypot

CTH EDUCATION Name of Faith Education

What do you mean by an Intruder?

- It is an unauthorized person that tries to access a system or network without authorization.
- An intruder is anyone that tries to get access to any part of your computer system.
- An intruder is typically referred to as a hacker.
- They are very smart and know a lot about technology and security.
- They typically try to sell this information to third parties.

What is attacks in network security?

- Network attacks are unauthorized actions on the digital assets within an organizational network.
- Malicious parties usually execute network attacks to alter, destroy, or steal private data.
- There are various types of attack, some of them are given below:
  1. Unauthorized access
  2. Denial of service attack
  3. Man in the middle attack
  4. SQL injection attack
  5. Insider threats etc.

CTH EDUCATION Name of Faith Education

Unauthorized access

- Unauthorized access refers to attackers accessing a network without receiving permission.

Denial of Service (DoS) attacks

- It is a type of attack that crash a machine or network, making it inaccessible to its intended user.

Man in the middle attacks

- It is a type of attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other.
- The attack is a type of eavesdropping in which the attacker intercepts & controls the entire conversation.

Code and SQL injection attacks

- It is a common attack that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.

Insider threats

- Insider threats are cybersecurity threats that originate with authorized users—employees, contractors, business partners—who intentionally or accidentally misuse their legitimate access, or have their accounts hijacked by cybercriminals.

What is Honeypot?

- Honeypot is a network-attached system.
- It is used as a trap for cyber-attackers to detect and study the tricks used by hackers.
- Honeypots are mostly used by large companies and organizations involved in cybersecurity.
- It helps cybersecurity researchers to learn about the different type of attacks used by attackers.
- The cost of a honeypot is generally high because it requires specialized skills and resources.

What is Virus? Explain various types of viruses.

- Virus stands for Vital Information Resource Under Seize.
- It is a malicious software loaded onto a user's computer without the user's knowledge and performs malicious actions.
- It is an unwanted software programs that interfere with the functioning of the computer.
- Once it enters your system, it can replicate to produce copies of itself to spread from one program to another.
- So, we can say that it is a self-replicating computer program that interferes with the functioning of the computer by infecting files, data, programs, etc.
- There are various types of virus some of them are given below:
  - Malware
  - Trojan horse
  - Worm
  - Spyware
  - Boot sector etc.

CTH EDUCATION Name of Faith Education

Malware:

- Malware stands for malicious software.
- Malware is the name that is given to any type of software that could harm a computer system.
- It interferes with and gather a user's data, or make the computer perform actions without the owner's knowledge or permission.

Trojan horse:

- A type of malware that uses malicious code to install software that seems ok, but is hidden to create back doors into a system.
- This typically causes loss or theft of data from an external source.

Worm:

- Unlike a virus, a worm, is a standalone piece of malicious software that replicates itself in order to spread to other computers.
- It often uses a computer network to spread itself, relying on security flaws on the target system to allow access.

Spyware:

- Spyware is software that aids in gathering information about a person or organization without their knowledge.
- Spyware can monitor and log the activity that is performed on a target system, like log key strokes, or gather credit card and other information.

Boot sector virus:

- This type of virus can take control when you start — or boot — your computer.
- One way it can spread is by plugging an infected USB drive into your computer.

CTH EDUCATION Name of Faith Education

What is Anti-Virus?

- Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer.
- Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.
- Antivirus software helps protect your computer against malware and cybercriminals.
- Antivirus software looks at data — web pages, files, software, applications — traveling over the network to your devices.
- It searches for known threats and monitors the behavior of all programs, flagging suspicious behavior.
- It seeks to block or remove malware as quickly as possible

Explain how Anti-Virus is useful to prevent and detect the viruses.

- Antivirus software provides protection against these types of threats by performing key tasks:
- Pinpointing specific files for the detection of malicious software.
- Scheduling automatic scans.
- Scanning either one file or your entire computer at your discretion

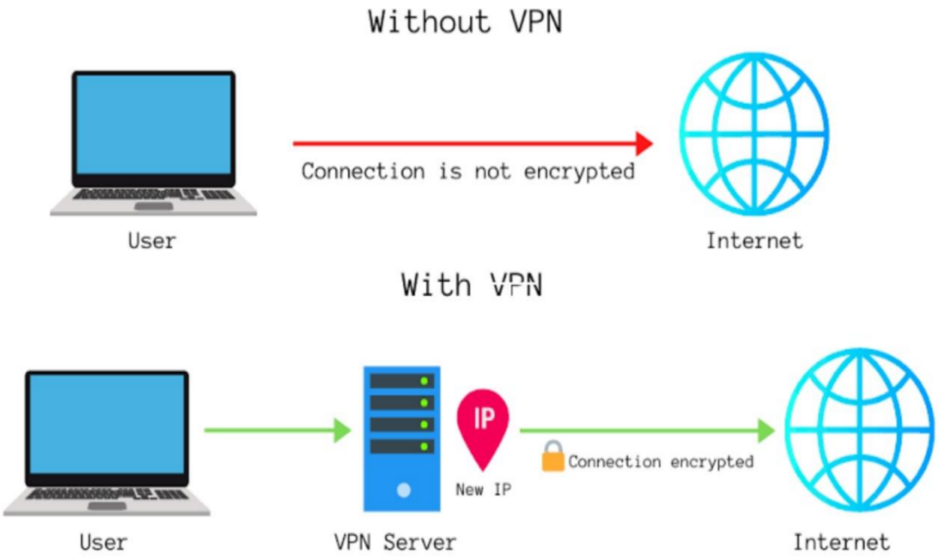
What is Firewalls?

- A firewall is a network security system that manages the network traffic based on some protocols.
- It monitors and control incoming & outgoing traffic based on pre-defined rules.
- A firewall acts like a hardware.
- Firewalls exist as software or hardware both.
- Most personal computers use software-based firewalls to secure data from threats from the internet.
- Firewalls are used in private networks or intranets to prevent unauthorized access from the internet.
- Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

CTH EDUCATION Name of Faith Education

Virtual Private Networks(VPN):

- A VPN is type of Network security.
- It hides your IP address on the internet.
- It prevents unauthorized people and allows the unauthorized user.
- A VPN is an encrypted connection over the Internet.
- The encrypted connection helps ensure that sensitive data is safely transmitted.
- VPN technology is widely used in corporate environments.
- VPN supports the user in creating a secure private connection between the networks.
- Users working from home usually connect to the company's network via a VPN.


Without VPN
Connection is not encrypted
User
Internet
With VPN
IP
New IP
Connection encrypted
User
VPN Server
Internet