Unit

Q. What is Computer Worm?

A computer worm is a type of harmful software that copy itself and spread from one computer to another without requiring any user intervention.

A computer worm operates by finding vulnerabilities in computer systems and networks. Once it infects one computer, it searches for other computers connected to the same network and spreads to them.

Q. What is Computer virus?

A virus is a malicious executable code attached to another executable file that can be harmless or can modify or delete data.

A computer virus is a type of malicious software program ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its code.

Q. Is a computer worm a virus ? give your opinion.

A computer worm is different from a virus.

A Worm is a form of malware that replicates itself and can spread to different computers via Network. Worms can be controlled by remote.

A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data. But Worms can't be controlled by remote.

Q. Difference between computer worm and computer virus.

Computer worm	Computer virus
1. A Worm is a form of malware that replicates itself and can spread to different computers via Network	1. A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data.
2. The main objective of worms is to eat the system resources. It consumes system resources such as memory and bandwidth and made the system slow in speed to such an extent that it stops responding.	2. The main objective of viruses is to modify the information.
3. It is less harmful as compared.	3. It is more harmful.
4. Worms can be controlled by remote.	4. Viruses can't be controlled by remote.
5. Worms are executed via weaknesses in the system.	5. Viruses are executed via executable files.
6. Worms can be detected and removed by the Antivirus and firewall.	6. Antivirus software is used for protection against viruses.

Q. What do you mean by Denial of service attack (DoS)

A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning.

Their purpose is to disrupt an organization's network operations by denying access to its users. Denial of service is typically accomplished by flooding the targeted machine or resource with surplus requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

Q. How Do DoS Attacks Work?

DoS attacks typically exploit vulnerabilities in a target's network or computer systems. Attackers can use a variety of methods to generate overwhelming traffic or requests, including:

- Flooding the target with a massive amount of data
- Sending repeated requests to a specific part of the system
- Exploiting software vulnerabilities to crash the system.

Q. What is Trace route: What Does It Do & How Does It Work?

A trace route provides a map of how data on the internet travels from its source to its destination. Traceroute is a network diagnostic tool designed to trace the path that packets of information take from a source to a destination across an IP network.

- A trace route works by sending Internet Control Message Protocol (ICMP) packets, and every router involved in transferring the data gets these packets. The ICMP packets provide information about whether the routers used in the transmission are able to effectively transfer the data.
- Trace route works with the help of ICMP(Internet Control Message Protocol) echo packets consisting of variable TTL (Time To Live) and to get accurate values each hop is queried multiple times and each hop's response time is calculated.

Q. What do you mean by ethical hacking?

Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization.

An ethical hacker finds the weak points or loopholes in a computer, web application or network and reports them to the organization.

Q. **Write the Advantages of Ethical Hacking.**

Following are the advantages of Ethical Hacking as follows.

1. This helps to fight against cyber terrorism and to fight against national security breaches.
2. This helps to take preventive action against hackers.
3. This helps to build a system that prevents any kinds of penetration by hackers.
4. This offers security to banking and financial establishments.
5. This helps to identify and close the open holes in a computer system or network.

Q. Write the disadvantages of Ethical Hacking

Following are the disadvantages of Ethical Hacking as follows.

1. This may corrupt the files or data of an organization.
2. They might use information gained for malicious use. Subsequently, trustful programmers are
4. By hiring such professionals will increase costs to the company.
5. This technique can harm someone's privacy.
6. This system is illegal.
7. It hampers system operation

Q. What do you mean by phishing and spoofing ?

Phishing: Phishing is a type of attack on a computer device where the attacker tries to find the sensitive information of users in a fraud manner through electronic communication by intending to be from a related trusted organization in an automated manner.

Example: Sometimes hackers through communication ask for OTP or secret PIN of bank transactions by acting as an employee of the bank which is a fraud manner.

Spoofing: Spoofing is a type of attack on a computer device in which the attacker tries to steal the identity of the legitimate user and act as another person. This kind of attack is done to breach the security of the system or to steal the information of the users.

Example: Hackers normally change their IP addresses to hack a website so that the hacker can't be traced.

Q. What is a malicious software? How did they get into a system?

Malware is a software that gets into the system without user consent with an intention to steal private and confidential data of the user that includes bank details and password. They also generates annoying pop up ads and makes changes in system settings.

They get into the system through various means:

1. Along with free downloads.
2. Clicking on suspicious link.
3. Opening mails from malicious source.
4. Visiting malicious websites.
5. Not installing an updated version of antivirus in the system.

Q.What are the properties of computer virus?

Key Characteristics of Computer Viruses:

Replication: The defining feature of a virus is its ability to copy itself onto other programs, files, or systems.

Stealth: Many viruses are designed to evade detection by hiding from or disabling antivirus software.

Polymorphism: Polymorphic viruses can change their code or signature to avoid detection by antivirus software, making them particularly difficult to eradicate.

Triggers: Viruses may be triggered by specific events or conditions, such as a particular date or time, the presence of certain files.

UNIT 5 Networking and security

1. In which of the following, a person is constantly followed/chased by another person or group of several peoples?
    a) Phishing
    b) Bulling
    c) **Stalking**
    d) Identity theft

2. Which of the following port and IP address scanner famous among the users?
    a) Cain and Abel
    b) **Angry IP Scanner**
    c) Snort
    d) Ettercap

3. In ethical hacking and cyber security, there are _____ types of scanning:
    a) 1
    b) 2
    c) **3**
    d) 4

4. Which of the following is not a type of scanning?
    a) Xmas Tree Scan
    b) **Cloud scan**
    c) Null Scan
    d) SYN Stealth

5. Which of the following are the types of scanning?
    a) **Network, vulnerability, and port scanning**
    b) Port, network, and services
    c) Client, Server, and network
    d) None of the above

6. To protect the computer system against the hacker and different kind of viruses, one must always keep _____ on in the computer system.
    a) Antivirus
    b) **Firewall**
    c) VLC player
    d) Script

7. Which of the following can be considered as the elements of cyber security?
    a) Application Security
    b) Operational Security
    c) Network Security
    d) **All of the above**

8. Hackers usually used the computer virus for _____ purpose.
    a) To log, monitor each and every user's stroke
    b) To gain access the sensitive information like user's Id and Passwords
    c) To corrupt the user's data stored in the computer system
    d) **All of the above**

9. The term "TCP/IP" stands for_____
    a) Transmission Contribution protocol/ internet protocol
    b) Transmission Control Protocol/ internet protocol
    c) Transaction Control protocol/ internet protocol

10. Which type of the following malware does not replicate or clone them self's through infection?
    a) Rootkits
    b) Trojans
    c) Worms
    d) Viruses

11. Which of the following transmission directions listed is not a legitimate channel?
    a) Simplex
    b) Half Duplex
    c) Full Duplex
    d) **Double Duplex**

12. Which software prevents the external access to a system?
    a) **Firewall**
    b) Gateway
    c) Router
    d) Virus checker

13. The term FTP stands for?

a) File transfer program
b) File transmission protocol
c) **File transfer protocol**
d) File transfer protection

14. The length of an IPv6 address is?

a) 32 bits
b) 64 bits
c) **128 bits**
d) 256 bits

15. The maximum length (in bytes) of an IPv4 datagram is?

a) 32
b) 1024
c) **65535**
d) 512

16. When bogus reconfiguration commands are used to affect routers and switches to degrade network performance." Which type of Wireless network threat would you classify this under?

a) **Network Injection**
b) Malicious Association
c) Man in the middle attack
d) Denial Of Service

17. When there is a lack of a central point of control." Which type of Wireless network threat would you classify this under?

a) Man in the middle attack
b) Identity Theft
c) **Ad Hoc Networks**
d) Non-Traditional Networks