

**Academic Year 2018-19**



SHRIDEVI  
EDUCATION

Sri Shridevi Charitable Trust (R.)

**SHRIDEVI INSTITUTE OF ENGINEERING & TECHNOLOGY**

(Recognised by Govt. of Karnataka, Affiliated to VTU, Belagavi and Approved by AICTE, New Delhi)

Sira Road, Tumakuru - 572 106, Karnataka.

Phone: 0816-2212629 | Fax: 0816-2212628 | Email: info@shrideviengineering.org | Web: <http://www.shrideviengineering.org>




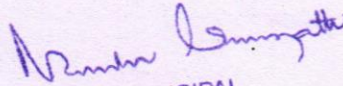
DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

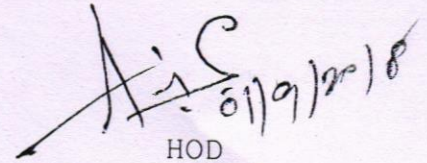
Date: 01/9/2018

## Circular

It is hereby informed to all 7th semester students that the "ANTENNA DESIGN training course from "8th September 2018 to 30th September 2018" will be conducted all students are informed to attend the training course with full attention to avoid any fail.

  
Coordinator

  
PRINCIPAL  
SIET., TUMAKURU.

  
HOD

Dept. of ECE  
SIET, TUMAKURU

HOD  
Dept of E&C  
SIET, Tumkur-6

Ref: SIET/EC/2018-19/01

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

**APPROVAL LETTER**

To,  
The Principal,  
SIET, Tumakuru

Respected Sir,

Sub: - Approval for Organizing Students Training Program on "ANTENNA DESIGN"-Reg.

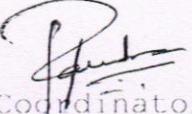
With reference to the subject cited above, I would like to bring to your kind notice that, the Department is planned to organize Student Training Program on "ANTENNA DESIGN" from "8th September 2018 to 30th September 2018" for 7th semester Electronics & communication engineering students.

Kindly consider the above request and approve the same for further proceedings.

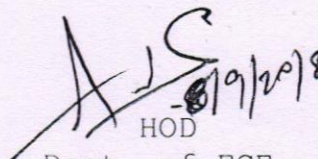
Thanking you

Date: 01/9/2018

Place: SIET, Tumakuru.

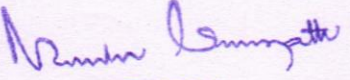


Coordinator



HOD  
Dept. of ECE  
SIET, TUMAKURU

HOD  
Dept of E&C  
SIET, Tumkur-6



PRINCIPAL  
SIET, TUMAKURU



Sri Shridevi Charitable Trust (R.)

# SHRIDEVI INSTITUTE OF ENGINEERING & TECHNOLOGY

(Recognised by Govt. of Karnataka, Affiliated to VTU, Belagavi and Approved by AICTE, New Delhi)

Sira Road, Tumakuru - 572 106. Karnataka.



An ISO 9001:2015 Certified Institution

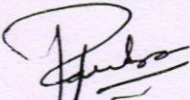
Phone: 0816-2212629 | Fax: 0816-2212628 | Email: info@shrideviengineering.org | Web: http://www.shrideviengineering.org

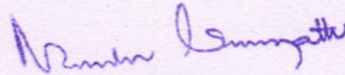
## DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING


Date: 12/11/2018

### Circular

It is hereby informed to all 7th semester students that the Real Time operating Systems training course from "19/11/2018 to 25/05/2018" will be conducted all students are informed to attend the training course without fail.

  
Coordinator

  
PRINCIPAL  
SIET., TUMAKURU.

  
HOD  
Dept. of ECE  
SIET, TUMAKURU  
  
HOD  
Dept of E&C  
SIET, Tumkur-6



Sri Shridevi Charitable Trust (R.)  
**SHRIDEVI INSTITUTE OF ENGINEERING & TECHNOLOGY**

(Recognised by Govt. of Karnataka, Affiliated to VTU, Belagavi and Approved by AICTE, New Delhi)

Sira Road, Tumakuru - 572 106. Karnataka.

Phone: 0816-2212629 | Fax: 0816-2212628 | Email: info@shrideviengineering.org | Web: http://www.shrideviengineering.org



Ref: SIET/EC/2018-19/01

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

**APPROVAL LETTER**

To,  
The Principal,  
SIET, Tumakuru

Respected Sir,

Subject: - Approval for Organizing Students Training Program on "Real Time operating Systems"-Reg.

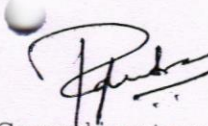
With reference to the subject cited above, I would like to bring to your kind notice that, the Department is planned to organize Student Training Program on "Real Time operating Systems" from "19/11/2018 to 25/05/2018" for 7th semester Electronics & communication engineering students.

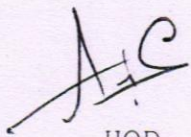
Kindly consider the above request and approve the same for further proceedings.

Thanking you

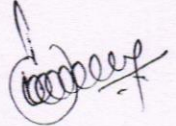
Date: 10/11/2018

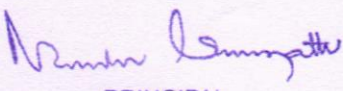
Place: SIET, Tumakuru.

  
Coordinator

  
HOD  
Dept. of ECE  
SIET, TUMAKURU

HOD  
Dept of E&C  
SIET, Tumkur-6

  
PRINCIPAL  
SIET, TUMAKURU

  
PRINCIPAL  
SIET, TUMAKURU.

Date: 11-02-2019

**CIRCULAR**

Department of Civil Engineering, SIET in association with CASD DESK, Tumkur is conducting software programmes related to Civil Engineering.

All students of Civil Engineering are hereby informed to attend the as per the schedule below:

Sem	Software Name	Duration
IV	Google Sketchup	15 <sup>th</sup> Feb 2019 to 15 <sup>th</sup> March 2019
VI	Revit Architecture and Structure	15 <sup>th</sup> Feb 2019 to 15 <sup>th</sup> March 2019
VIII	SAFE	15 <sup>th</sup> Feb 2019 to 15 <sup>th</sup> March 2019

**Venue:**

IV SEM: CivilCAD LAB, Time: 4:30pm to 6:00pm

VI SEM: MechanicalCAD LAB, Time: 4:30pm to 6:00pm

IV SEM: CS LAB, Time: 4:30pm to 6:00pm

*N. Srinivas*  
PRINCIPAL  
SIET., TUMAKURU.

*G. Mahesh Kumar*  
Dr. G Mahesh Kumar  
(HOD)  
HOD  
Dept. of Civil Engineering  
SIET, TUMKUR - 6.



# SHRIDEVI INSTITUTE OF ENGINEERING & TECHNOLOGY

(Recognised by Govt. of Karnataka, Affiliated to VTU, Belagavi and Approved by AICTE, New Delhi)

Sira Road, Tumakuru - 572 106. Karnataka.



## Ethical hacking MCQ test quiz question and answer

### 1. What is Ethical Hacking?

- A. Hacking to steal sensitive information
- B. Hacking to identify vulnerabilities in a system
- C. Hacking to disrupt a system's functionality
- D. Hacking to cause damage to a system

**Answer: B**

**Explanation:** Ethical hacking involves finding vulnerabilities in a system, network or web application and reporting them to the system owner so that they can be fixed before malicious hackers can exploit them.

### 2. What is the main goal of ethical hacking?

- A. To cause damage to a system
- B. To gain unauthorized access to a system
- C. To identify and fix security vulnerabilities
- D. To steal sensitive information

**Answer: C**

*Nanda Lakshmi*  
PRINCIPAL  
SIET, TUMKUR.



# SHRIDEVI INSTITUTE OF ENGINEERING & TECHNOLOGY

(Recognised by Govt. of Karnataka, Affiliated to VTU, Belagavi and Approved by AICTE, New Delhi)

Sira Road, Tumakuru - 572 106. Karnataka.



**Explanation:** The main goal of ethical hacking is to identify security vulnerabilities in a system or network and to help fix them before malicious hackers can exploit them.

### 3. What is the difference between ethical hacking and malicious hacking?

- A. Ethical hacking is legal and sanctioned, while malicious hacking is illegal and unsanctioned.
- B. Ethical hacking only involves finding vulnerabilities, while malicious hacking involves exploiting them.
- C. Ethical hacking is done with the permission of the system owner, while malicious hacking is done without permission.
- D. There is no difference between ethical hacking and malicious hacking.

**Answer: A**

**Explanation:** Ethical hacking is legal and sanctioned, while malicious hacking is illegal and unsanctioned. Ethical hacking is done with the permission of the system owner, while malicious hacking is done without permission. Ethical hacking only involves finding vulnerabilities, while malicious hacking involves exploiting them.

### 4. What is a vulnerability assessment?

- A. A process to identify vulnerabilities in a system or network
- B. A process to exploit vulnerabilities in a system or network

*Nanda Kumar*  
PRINCIPAL  
SIET, TUMKUR.





# SHRIDEVI INSTITUTE OF ENGINEERING & TECHNOLOGY

(Recognised by Govt. of Karnataka, Affiliated to VTU, Belagavi and Approved by AICTE, New Delhi)

Sira Road, Tumakuru - 572 106. Karnataka.



- C. A process to fix vulnerabilities in a system or network
- D. A process to steal sensitive information from a system or network

**Answer: A**

**Explanation:** A vulnerability assessment is the process of identifying vulnerabilities in a system or network. It involves using various tools and techniques to scan the system or network for potential vulnerabilities.

**5. Which of the following is not a common method used in ethical hacking?**

- A. Social engineering
- B. Penetration testing
- C. SQL injection
- D. Denial of service attack

**Answer: D**

**Explanation:** Denial of service attack is not a common method used in ethical hacking. It is an attack designed to disrupt the normal functioning of a system or network by overwhelming it with traffic.

**6. What is social engineering?**

- A. A technique to identify vulnerabilities in a system or network
- B. A technique to exploit vulnerabilities in a system or network

*Nandha Kumar*  
PRINCIPAL  
SIET. TUMKUR.



# SHRIDEVI INSTITUTE OF ENGINEERING & TECHNOLOGY

(Recognised by Govt. of Karnataka, Affiliated to VTU, Belagavi and Approved by AICTE, New Delhi)

Sira Road, Tumakuru - 572 106. Karnataka.



- C. A technique to manipulate people into giving up sensitive information
- D. A technique to fix vulnerabilities in a system or network

**Answer: C**

**Explanation:** Social engineering is the use of psychological manipulation to trick people into divulging confidential information. It is a common method used in ethical hacking to gain access to sensitive information.

## 7. What is the purpose of a penetration test?

- A. To identify vulnerabilities in a system or network
- B. To exploit vulnerabilities in a system or network
- C. To fix vulnerabilities in a system or network
- D. To steal sensitive information from a system or network

**Answer: B**

**Explanation:** The purpose of a penetration test is to exploit vulnerabilities in a system or network to demonstrate the potential impact of a successful attack. It is used to identify weaknesses that need to be fixed.

## 8. What is SQL injection?

- A. A technique to identify vulnerabilities in a system or network
- B. A technique to exploit vulnerabilities in a system or network

*Nimisha Suresh*  
PRINCIPAL  
SIET, TUMKUR.



# SHRIDEVI INSTITUTE OF ENGINEERING & TECHNOLOGY

(Recognised by Govt. of Karnataka, Affiliated to VTU, Belagavi and Approved by AICTE, New Delhi)

Sira Road, Tumakuru - 572 106. Karnataka.



- C. A technique to fix vulnerabilities in a system or network
- D. A technique to steal sensitive information from a system or network

**Answer: B**

**Explanation:** SQL injection is a common method used by malicious hackers to exploit vulnerabilities in a web application. It involves inserting malicious SQL code into a form field or URL parameter in order to gain access to sensitive information or execute unauthorized commands on a database.

## 9. What is the difference between a vulnerability and an exploit?

- A. A vulnerability is a weakness in a system or network, while an exploit is a tool or technique used to take advantage of that weakness.
- B. A vulnerability is a tool or technique used to identify weaknesses in a system or network, while an exploit is a weakness that has already been identified.
- C. A vulnerability is a type of malware that can infect a system or network, while an exploit is a method of spreading that malware.
- D. There is no difference between a vulnerability and an exploit.

**Answer: A**

**Explanation:** A vulnerability is a weakness in a system or network that can be exploited by attackers. An exploit is a tool or technique used to take advantage of that weakness.

*N. Srinivas*  
PRINCIPAL  
SIET, TUMKUR.



**10. What is a firewall?**

- A. A device used to prevent unauthorized access to a network
- B. A device used to monitor network traffic
- C. A device used to encrypt network traffic
- D. A device used to block email spam

**Answer: A**

**Explanation:** A firewall is a device used to prevent unauthorized access to a network. It can be a hardware device or software program that monitors incoming and outgoing network traffic and blocks any traffic that does not meet the specified security criteria.

**11. What is a honeypot?**

- A. A device used to lure attackers into a trap
- B. A type of malware that spreads through a network
- C. A tool used to test network performance
- D. A device used to monitor network traffic

**Answer: A**

**Explanation:** A honeypot is a device or system designed to attract attackers and monitor their behavior. It is used to gather information about new or emerging threats and to learn about the tactics and techniques used by attackers.

*Nandhu Kumar*  
PRINCIPAL  
SIET, TUMKUR.



**12. What is the difference between a virus and a worm?**

- A. A virus spreads by attaching itself to a host file, while a worm spreads by exploiting network vulnerabilities.
- B. A virus is a type of malware that can replicate itself and spread to other systems, while a worm is a standalone program that can replicate itself and spread to other systems.
- C. A virus requires human interaction to spread, while a worm can spread automatically without user intervention.
- D. There is no difference between a virus and a worm.

**Answer: B**

**Explanation:** A virus is a type of malware that can replicate itself and spread to other systems by attaching itself to a host file. A worm is a standalone program that can replicate itself and spread to other systems by exploiting network vulnerabilities.

**13. What is a zero-day vulnerability?**

- A. A vulnerability that has been identified and patched
- B. A vulnerability that has been identified but not yet patched
- C. A vulnerability that has never been identified
- D. A vulnerability that does not exist

**Answer: B**

*N. Srinivas*  
PRINCIPAL  
SIET, TUMKUR.



**Explanation:** A zero-day vulnerability is a vulnerability that has been identified by hackers but not yet patched by the software vendor. It is called “zero-day” because the vendor has zero days to fix the vulnerability before it can be exploited by attackers.

**14. What is a man-in-the-middle attack?**

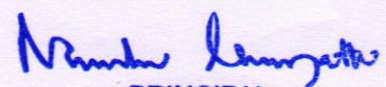
- A. An attack that intercepts communication between two parties
- B. An attack that infects a system with malware
- C. An attack that exploits a software vulnerability
- D. An attack that floods a network with traffic

**Answer: A**

**Explanation:** A man-in-the-middle attack is an attack that intercepts communication between two parties in order to eavesdrop on or alter the communication. It is commonly used to steal sensitive information such as login credentials, credit card numbers, and other personal data.

**15. What is a denial-of-service attack?**

- A. An attack that floods a network with traffic to make it unavailable
- B. An attack that steals sensitive information from a system
- C. An attack that exploits a software vulnerability
- D. An attack that intercepts communication between two parties

  
PRINCIPAL  
SIET, TUMKUR.



**Answer: A**

**Explanation:** A denial-of-service attack is an attack that floods a network with traffic to make it unavailable to users. This can be accomplished through various methods, such as flooding the network with packets or overwhelming a server with requests.

**16. What is a password cracker?**

- A. A tool used to guess passwords through trial and error
- B. A tool used to encrypt passwords for storage
- C. A tool used to decrypt passwords for storage
- D. A tool used to block password guessing attempts

**Answer: A**

**Explanation:** A password cracker is a tool used to guess passwords through trial and error. It works by using various methods such as brute force attacks, dictionary attacks, and rainbow table attacks to guess passwords.

**17. What is a vulnerability scanner?**

- A. A tool used to identify weaknesses in a system or network
- B. A tool used to exploit vulnerabilities in a system or network
- C. A tool used to monitor network traffic
- D. A tool used to block email spam

*Nanda Lakshmi*  
PRINCIPAL  
SIET, TUMKUR.



**Answer: A**

**Explanation:** A vulnerability scanner is a tool used to identify weaknesses in a system or network. It works by scanning the system or network for known vulnerabilities and reporting the results to the user.

**18. What is a packet sniffer?**

- A. A tool used to capture and analyze network traffic
- B. A tool used to block network traffic
- C. A type of malware that spreads through a network
- D. A tool used to encrypt network traffic

**Answer: A**

**Explanation:** A packet sniffer is a tool used to capture and analyze network traffic. It works by intercepting packets of data as they travel across the network and decoding their contents.

**19. What is a proxy server?**

- A. A server that acts as an intermediary between a client and a server
- B. A server that stores and retrieves files over a network
- C. A server that provides email services
- D. A server that provides web hosting services

*Nanda Kumar*  
PRINCIPAL  
SIET, TUMKUR.





**Answer: A**

**Explanation:** A proxy server is a server that acts as an intermediary between a client and a server. It is commonly used to improve security, filter content, or provide anonymity for users.

**20. What is a rootkit?**

- A. A type of malware that encrypts files on a system
- B. A type of software used to monitor network traffic
- C. A type of software used to hide malicious activity on a system
- D. A type of software used to perform brute force attacks

**Answer: C**

**Explanation:** A rootkit is a type of software used to hide malicious activity on a system. It works by modifying the operating system or other software to conceal its presence and prevent detection.

**21. What is encryption?**

- A. A technique used to hide the contents of a message
- B. A technique used to hide the identity of a sender
- C. A technique used to hide the location of a sender
- D. A technique used to hide the existence of a message

*Nimisha Lakshmi*  
PRINCIPAL  
SIET, TUMKUR.



**Answer: A**

**Explanation:** Encryption is a technique used to hide the contents of a message. It works by transforming the original message, or plaintext, into an unreadable form, or ciphertext, using a mathematical algorithm and a secret key.

**22. What is steganography?**

- A. A technique used to hide a message in plain sight
- B. A technique used to encrypt a message
- C. A technique used to decrypt a message
- D. A technique used to hide the existence of a message

**Answer: A**

**Explanation:** Steganography is a technique used to hide a message in plain sight. It works by embedding the message in a carrier, such as an image or audio file, in a way that is not easily detectable.

**23. What is a backdoor?**

- A. A hidden entry point into a system or network
- B. A tool used to remove malware from a system
- C. A type of malware that spreads through email attachments
- D. A tool used to scan a network for vulnerabilities

*N. Srinivasan*  
PRINCIPAL  
SIET, TUMKUR.



**Answer: A**

**Explanation:** A backdoor is a hidden entry point into a system or network that is used to bypass normal authentication procedures. It can be used for legitimate purposes, such as system maintenance, but can also be used by attackers to gain unauthorized access.

**24. What is a Trojan horse?**

- A. A type of malware that spreads through social media
- B. A type of malware that disguises itself as legitimate software
- C. A type of attack that exploits a software vulnerability
- D. A type of attack that floods a network with traffic

**Answer: B**

**Explanation:** A Trojan horse is a type of malware that disguises itself as legitimate software in order to trick users into downloading and installing it. Once installed, it can perform a variety of malicious activities, such as stealing sensitive information or giving an attacker remote access to the system.

**25. What is a botnet?**

- A. A network of compromised computers used for malicious purposes
- B. A type of malware that steals sensitive information

*Namha Ramgatta*  
PRINCIPAL  
SIET, TUMKUR.



# SHRIDEVI INSTITUTE OF ENGINEERING & TECHNOLOGY

(Recognised by Govt. of Karnataka, Affiliated to VTU, Belagavi and Approved by AICTE, New Delhi)

Sira Road, Tumakuru - 572 106. Karnataka.



- C. A type of malware that encrypts files on a system
- D. A type of attack that floods a network with traffic

**Answer: A**

**Explanation:** A botnet is a network of compromised computers, or bots, that are controlled by a central command-and-control server. It can be used for various malicious purposes, such as sending spam email or launching distributed denial-of-service attacks.

## 26. What is a sandbox?

- A. A virtual environment used to isolate and execute untrusted software
- B. A physical device used to block network traffic
- C. A device used to analyze network traffic
- D. A tool used to analyze system logs

**Answer: A**

**Explanation:** A sandbox is a virtual environment used to isolate and execute untrusted software. It provides a safe and controlled environment for testing and analyzing software, without risking damage to the underlying system.

## 27. What is a phishing attack?

*Murthy Srinivas*  
PRINCIPAL  
SIET, TUMKUR.



# SHRIDEVI INSTITUTE OF ENGINEERING & TECHNOLOGY

(Recognised by Govt. of Karnataka, Affiliated to VTU, Belagavi and Approved by AICTE, New Delhi)

Sira Road, Tumakuru - 572 106. Karnataka.



- A. An attack that exploits a software vulnerability
- B. An attack that floods a network with traffic
- C. An attack that steals sensitive information by tricking users into providing it
- D. An attack that intercepts communication between two parties

**Answer: C**

**Explanation:** A phishing attack is an attack that steals sensitive information by tricking users into providing it. It typically involves sending an email or message that appears to be from a trusted source, such as a bank or social media site, and asking the user to provide their login credentials or other personal information.

## 28. What is vulnerability scanning?

- A. The process of identifying security vulnerabilities in a system or network
- B. The process of encrypting sensitive information
- C. The process of hiding malicious activity on a system
- D. The process of monitoring network traffic

**Answer: A**

**Explanation:** Vulnerability scanning is the process of identifying security vulnerabilities in a system or network. It involves scanning the system or network for known vulnerabilities and producing a report that details the findings.

*Nanda Lakshmi*  
PRINCIPAL  
SIET, TUMKUR.



**29. What is network mapping?**

- A. The process of identifying the devices and topology of a network
- B. The process of encrypting network traffic
- C. The process of hiding malicious activity on a network
- D. The process of monitoring network traffic

**Answer: A**

**Explanation:** Network mapping is the process of identifying the devices and topology of a network. It involves scanning the network and producing a map or diagram that shows the devices and how they are connected.

**30. What is a buffer overflow?**

- A. A type of malware that spreads through email attachments
- B. A type of attack that exploits a software vulnerability
- C. A type of attack that floods a network with traffic
- D. A tool used to remove malware from a system

**Answer: B**

**Explanation:** A buffer overflow is a type of attack that exploits a software vulnerability in which an application accepts more input than it is designed to handle. This can allow an attacker to overwrite adjacent memory and execute arbitrary code.

*Nanda Kumar*  
PRINCIPAL  
SIET, TUMKUR.



**31. What is a virtual private network (VPN)?**

- A. A device used to encrypt network traffic
- B. A device used to monitor network traffic
- C. A device used to block network traffic
- D. A device used to analyze system logs

**Answer: A**

**Explanation:** A virtual private network (VPN) is a technology used to encrypt network traffic between two endpoints, providing a secure and private connection over an otherwise insecure network. It can be used to protect sensitive information and allow remote access to a network.

**32. What is an exploit?**

- A. A type of malware that spreads through email attachments
- B. A type of attack that takes advantage of a software vulnerability
- C. A tool used to scan a network for vulnerabilities
- D. A type of attack that floods a network with traffic

**Answer: B**

**Explanation:** An exploit is a type of attack that takes advantage of a software vulnerability to gain unauthorized access to a system, steal information, or perform other malicious activities.

  
PRINCIPAL  
SIET, TUMKUR.



**33. What is a brute-force attack?**

- A. An attack that intercepts communication between two parties
- B. An attack that floods a network with traffic to make it unavailable
- C. An attack that attempts every possible combination of characters to guess a password
- D. A type of malware that disguises itself as legitimate software

**Answer: C**

**Explanation:** A brute-force attack is an attack that attempts every possible combination of characters to guess a password or encryption key. It can be a slow and resource-intensive process, but can be effective against weak or simple passwords.

**34. What is session hijacking?**

- A. An attack that exploits a software vulnerability to gain unauthorized access to a system
- B. An attack that floods a network with traffic to make it unavailable
- C. An attack that intercepts communication between two parties
- D. A type of malware that spreads through social media

**Answer: C**

  
PRINCIPAL  
SIET, TUMKUR.





# SHRIDEVI INSTITUTE OF ENGINEERING & TECHNOLOGY

(Recognised by Govt. of Karnataka, Affiliated to VTU, Belagavi and Approved by AICTE, New Delhi)

Sira Road, Tumakuru - 572 106. Karnataka.



**Explanation:** Session hijacking is an attack that intercepts communication between two parties in order to steal information or perform other malicious activities. It typically involves stealing a session ID or other authentication token to gain unauthorized access to a system.

### 35. What is a payload?

- A. The encrypted data transmitted over a network
- B. The malicious code executed during an attack
- C. The traffic generated by a botnet
- D. The log files generated by a system

**Answer: B**

**Explanation:** A payload is the malicious code executed during an attack, such as a virus, Trojan horse, or backdoor. It can be used to perform a variety of malicious activities, such as stealing sensitive information, providing unauthorized access to a system, or causing damage to the system itself.

*N. Srinivas*  
PRINCIPAL  
SIET, TUMKUR.