

**UNIT**

**1**

**INTRODUCTION TO CYBER  
SECURITY, CYBER SECURITY  
VULNERABILITIES AND CYBER  
SECURITY SAFEGUARDS**



## Short Answer Questions:

1. What is Cyber security?
2. What is Hacktivism?
3. Explain Phishing.
4. How Ransomware can be challenging in the 21st century?
5. Explain the need of nodal agency.
6. What is Weak Authentication?
7. Explain use of Biometrics in security.
8. What is Access Control?
9. What is Denial of Service?
10. Write about Ethical Hacking.

## Multiple Choice Questions:

1. What words consist in Hacktivism?
  - (a) Hack Acknowledge
  - (b) Hack Active Acknowledge
  - (c) Hack N Activism
  - (d) Hack N Acknowledge
2. What Malware program demands Ransom from victims?
  - (a) Ransomware
  - (b) Ransom Trojan
  - (c) Virus Money
  - (d) Active Ransom
3. Which of the following refers to the violation of the principle if a computer is no more accessible?
  - (a) Access Control
  - (b) Confidentiality
  - (c) Availability
  - (d) Information of Things
4. Which of the following is not a cyber threat?
  - (a) Cyber Warfare
  - (B) CYBERCRIME
  - (c) CYBER Terrorism
  - (d) None of the above
5. Which of the following is not a vulnerable software?
  - (a) Virus
  - (b) Worm
  - (c) WinRAR
  - (d) Trojan Horse
6. Bot is short form of \_\_\_\_\_
  - (a) Battery
  - (b) Boot
  - (c) Best of Technology
  - (d) Robot
7. Firewalls are to protect against
  - (a) Virus Attacks
  - (b) Unauthorized Attacks
  - (c) Data Driven Attacks
  - (d) Fire Attacks
8. In which of the following, a person is constantly followed/chased by another person or group of several peoples?
  - (a) Phishing
  - (b) Stalking
  - (c) Bulling
  - (d) Identity theft

9. Which of the following is considered as the unsolicited commercial e-mail?  
(a) Spam (b) Virus  
(c) Malware (d) Worm
10. Which of the following refers to exploring the appropriate, ethical behaviours related to the online environment and digital media platform?  
(a) Cyber law (b) Cybersecurity  
(c) Cyber ethics (d) Cyber safety

Answers:

1. (c); 2. (a); 3. (c); 4. (d); 5. (c); 6. (d); 7. (b); 8. (b); 9. (a); 10. (c).

Fill in the Blanks:

1. \_\_\_\_\_ is the convergence of cyberspace and terrorism.
2. \_\_\_\_\_ blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
3. Which type of the following malware does not replicate or clone themselves through infection \_\_\_\_\_.
4. \_\_\_\_\_ is a self-replicating malicious software program that spread throughout the computer files without the knowledge of a user.
5. \_\_\_\_\_ is a type of independent malicious program that never requires any host program.
6. In order to ensure the security of the data/information, we need to \_\_\_\_\_ the data.
7. \_\_\_\_\_ is a type of software designed to help the user's computer detect viruses and avoid them.
8. \_\_\_\_\_ a method that bypasses the normal authentication process.
9. \_\_\_\_\_ is an intrusion that may steal sensitive data such as passwords and credit card numbers from your internal systems.
10. \_\_\_\_\_ refers to the process of proving an identity to an application or system.

Answers:

1. Cyber terrorism; 2. Firewall; 3. Trojans; 4. Virus; 5. Worm; 6. Encrypt;  
7. Antivirus; 8. Backdoors; 9. Spyware; 10. Authentication.



**UNIT**

**2**

**CYBER SECURITY**



## Short Question Answers

1. What is DNS Spoofing?
2. What do mean by Proxies and Caching in http security?
3. Write about Cross-Site Scripting and Session Hijacking.
4. What is DoS?
5. Explain Web services.
6. What challenges do web application has to face in modern security concerns?

## Multiple Choice Questions

1. What does cyber security protect?
  - (a) Cyber security protects criminals
  - (b) Cyber security protects internet-connected systems
  - (c) Cyber security protects hackers
  - (d) None of the mentioned
2. Who is the father of computer security?
  - (a) August Kerckhoff's
  - (b) Bob Thomas
  - (c) Robert
  - (d) Charles
3. Which of the following is not a cybercrime?
  - (a) Denial of Service
  - (b) Man in the Middle
  - (c) Malware
  - (d) AES
4. "Cyberspace" was coined by \_\_\_\_\_
  - (a) Richard Stallman
  - (b) William Gibson
  - (c) Andrew Tannenbaum
  - (d) Scott Fahlman
5. Where did the term "hacker" originate?
  - (a) MIT
  - (b) New York University
  - (c) Harvard University
  - (d) Bell's Lab
6. What is the existence of weakness in a system or network is known as?
  - (a) Attack
  - (b) Exploit
  - (c) Vulnerability
  - (d) Threat
7. To retain a competitive advantage and to meet basic business requirements organizations must:
  - (a) Ensure the integrity of the information stored on their computer systems
  - (b) Preserve the confidentiality of sensitive data

- (c) Ensure the continued availability of their information systems
  - (d) All of the above
8. The key components of an information systems security policy include:
- (a) Management support and commitment
  - (b) Access Authorization
  - (c) Security Awareness
  - (d) All of the above
9. A number of different mechanisms are available for raising security awareness including:
- (a) Distribution of a written security policy
  - (b) Training on a regular basis of new employees, users
  - (c) Both (a) & (b)
  - (d) None
10. Data classification as a control measure should define:
- (a) Who has access rights
  - (b) Who is responsible for determining the access rights and access levels
  - (c) What approvals are needed for access
  - (d) All of the above
11. \_\_\_\_\_ is an attack type that tries to bring down a web host by overwhelming it with requests.
- (a) DoS
  - (b) Sniffjacking
  - (c) SQL injections
  - (d) Man in the Middle attack
12. \_\_\_\_\_ is a process with which we can allow or restrict resources of a web service
- (a) Authentication
  - (b) Authorization
  - (c) Mandatory Access Control
  - (d) None of the above

**Answers:**

1. (a); 2. (a); 3. (d); 4. (b); 5. (a); 6. (c); 7. (d); 8. (d); 9. (c); 10. (d); 11. (a); 12. (b).

**Fill in the Blanks:**

1. Full form of HTTP \_\_\_\_\_.
2. Full form of SOAP \_\_\_\_\_.
3. In SOAP, XML \_\_\_\_\_ introduce malicious code into an application or database.
4. \_\_\_\_\_ attacks overwhelm web services with overly many or long messages.
5. \_\_\_\_\_ is a code injection, but happens from the web application side to the website.



6. \_\_\_\_\_ is an unauthorized user who obtains session ID, and that user gains full access to the application and/or another user's account.
7. Full form of RBAC \_\_\_\_\_.
8. Full form of ABAC \_\_\_\_\_.
9. Full form of RADAC \_\_\_\_\_.
10. Full form of PBAC \_\_\_\_\_.
11. \_\_\_\_\_ is an authorization mechanism that associates a set of access privileges with a particular role, often corresponding to a job function.
12. An \_\_\_\_\_ system defines and manages user identities and access permissions.
13. \_\_\_\_\_ is a XML-based protocol for accessing web services.
14. \_\_\_\_\_ is a system for authenticating users and storing user data.

**Answers:**

**1. Hyper text transfer protocol; 2. Simple Object Access Protocol; 3. code injections; 4. Denial of Service; 5. Cross-Site Scripting; 6. Session Hijacking; 7. Role-based access control; 8. Attribute-Based Access Control; 9. Risk adaptive access control; 10. Policy-based access control; 11. Role Based Access Control; 12. Identity and Access Management (IAM); 13. SOAP. 14. User Management.**



**UNIT**  
**3**

**INTRUSION DETECTION AND  
PREVENTION**

### Short Answer Questions:

1. What is Intrusion?
2. Write about Anti-Malware Software
3. What are the Advantages of network IPS?
4. Host-based vs. Network IPS
5. Write about System Integrity Validation

## Multiple Choice Questions:

1. What are the major components of the intrusion detection system?
  - (a) Analysis Engine
  - (b) Event provider
  - (c) Alert Database
  - (d) All of the mentioned
2. What are the different ways to classify an IDS?
  - (a) Zone-based
  - (b) Host and Network-based
  - (c) Network and Zone-based
  - (d) Level-based
3. What are the characteristics of anomaly-based IDS?
  - (a) It models the normal usage of network as a noise characterization
  - (b) It doesn't detect novel attacks



- (c) Anything distinct from the noise is not assumed to be intrusion activity  
 (d) It detects based on signature
4. What is the major drawback of anomaly detection IDS?  
 (a) These are very slow at detection (b) It generates many false alarms  
 (c) It doesn't detect novel attacks (d) None of the mentioned
5. What are the characteristics of signature-based IDS?  
 (a) Most are based on simple pattern matching algorithms  
 (b) It is programmed to interpret a certain series of packets  
 (c) It models the normal usage of network as a noise characterization  
 (d) Anything distinct from the noise is assumed to be intrusion activity
6. What are the characteristics of Host-based IDS?  
 (a) The host operating system logs in the audit information  
 (b) Logs includes logins, file opens and program executions  
 (c) Logs are analysed to detect tails of intrusion  
 (d) All of the mentioned
7. What are the drawbacks of the host-based IDS?  
 (a) Unselective logging of messages may increase the audit burdens  
 (b) Selective logging runs the risk of missed attacks  
 (c) They are very fast to detect  
 (d) They have to be programmed for new patterns
8. What are characteristics of Network based IDS?  
 (a) They look for attack signatures in network traffic  
 (b) Filter decides which traffic will not be discarded or passed  
 (c) It is programmed to interpret a certain series of packet  
 (d) It models the normal usage of network as a noise characterization
9. Where is an IPS commonly placed in a network?  
 (a) In front of the firewall (b) In line with the firewall  
 (c) Behind the firewall (d) On the end users' device
10. If it detects a threat, an IPS can:  
 (a) Record the details of the threat  
 (b) Report the threat to security admins  
 (c) Take preventative action to stop the threat  
 (d) All of the above

**Answers:**

1. (d); 2. (b); 3. (a); 4. (b); 5. (a); 6. (d); 7. (a); 8. (a); 9. (b); 10. (d).



**Fill in the Blanks:**

1. Full form of IDS is \_\_\_\_\_.
2. \_\_\_\_\_ is used to prevent, detect, and remove computer viruses, worms, Trojan horses and any other type of malware.
3. Full form of IPS is \_\_\_\_\_.
4. Full form of HIPS is \_\_\_\_\_.
5. \_\_\_\_\_ audits host log files, host file systems, and resources.
6. The features of traditional IPS are found in all of these modern systems, except \_\_\_\_\_.
7. \_\_\_\_\_ is used to keep subjects accountable for their actions while they are authenticated to a system.
8. \_\_\_\_\_ tool is the most useful in sorting through large log files when searching for intrusion-related events.
9. \_\_\_\_\_ type of IDS can be considered an expert system.
10. \_\_\_\_\_ attacks is an attempt to test every possible combination against a security feature in order to bypass it.

**Answers:**

- 1. Intrusion detection system; 2. Anti-Malware program; 3. Intrusion prevention systems; 4. Host-based Intrusion Prevention System; 5. Host-based Intrusion Prevention System; 6. Anti-Malware; 7. Monitoring; 8. IDS; 9. Behaviour-based; 10. Brute force attack.**



**UNIT**

**4**

**CRYPTOGRAPHY AND  
NETWORK SECURITY**

## Short Answer Questions:

1. Cryptography
2. Symmetric cryptography
3. Asymmetric cryptography
4. Message Authentication
5. Digital signatures
6. Digital certificate
7. Firewall
8. VPN
9. PGP
10. S/MIME
11. SSL
12. TSL
13. IPSec

## Multiple Choice Questions:

1. The process of transmitting data in a form so that only intended users can access it, is
  - (a) Cryptography
  - (b) Morphing
  - (c) Monography
  - (d) None of these
2. A software program or a hardware device that filters all data packets coming through a network is known as \_\_\_\_\_
  - (a) Antivirus
  - (b) Firewall
  - (c) Cookies
  - (d) Malware
3. To protect the computer system against the hacker, one must always keep \_\_\_\_\_ on in the computer system.
  - (a) Antivirus
  - (b) Firewall
  - (c) VLC player
  - (d) Script
4. In the computer networks, the encryption techniques are primarily used for improving the \_\_\_\_\_
  - (a) Security
  - (b) Performance
  - (c) Reliability
  - (d) Longevity
5. Which of the following statements is true about the VPN in Network security?
  - (a) It is a type of device that helps to ensure that communication between a device and a network is secure.
  - (b) It is usually based on the IPsec (IP Security) or SSL (Secure Sockets Layer)
  - (c) It typically creates a secure, encrypted virtual "tunnel" over the open internet
  - (d) All of the above
6. If the same pair of keys are used for encryption and decryption, it is called
  - (a) Asymmetric cryptography
  - (b) Symmetric cryptography
  - (c) Public cryptography
  - (d) None of these
7. VPN is abbreviated as \_\_\_\_\_
  - (a) Visual Private Network
  - (b) Virtual Protocol Network
  - (c) Virtual Private Network
  - (d) Virtual Protocol Networking
8. A \_\_\_\_\_ can hide a user's browsing activity.
  - (a) Firewall
  - (b) Antivirus
  - (c) Browser
  - (d) VPN



9. \_\_\_\_\_ are also used for hides user's physical location.
- (a) Firewall (b) Antivirus  
(c) VPN (d) Incognito mode
10. What are the protocols used for creating VPNs?
- (a) Layer 2 Tunneling Protocol (L2TP)  
(b) Secure Socket Tunneling Protocol (SSTP)  
(c) Point-to-Point Tunneling Protocol (PPTP)  
(d) All the above
11. Packet filtering firewalls are deployed on \_\_\_\_\_
- (a) Routers (b) Switches  
(c) Hubs (d) Repeaters
12. ACL stands for \_\_\_\_\_
- (a) Access Condition List (b) Anti-Control List  
(c) Access Control Logs (d) Access Control List
13. The approved general-purpose MAC algorithm is are
- (a) HMAC (b) KMAC  
(c) CMAC (d) All the above
14. \_\_\_\_\_ is a popular program used to encrypt and decrypt e-mail over the Internet
- (a) SMTP (b) FTP  
(c) PGP (c) None of these
15. The key size of Data Encryption Standard algorithm is
- (a) 56 bits (b) 64 bits  
(c) 128 bits (d) 168 bits
16. Which of the following is not a secured mail transferring methodology?
- (a) POP3 (b) SSMTP  
(c) PGP (d) S/MIME
17. HTTPS is abbreviated as \_\_\_\_\_
- (a) Hypertexts Transfer Protocol Secured  
(b) Secured Hyper Text Transfer Protocol  
(c) Hyperlinked Text Transfer Protocol Secured  
(d) Hyper Text Transfer Protocol Secure



18. SSL is abbreviated as
  - (a) Security Socket Layer
  - (b) Session Security Layer
  - (c) Security Session Layer
  - (d) Socket Security Layer
19. TLS is abbreviated as
  - (a) Transaction Level Security
  - (b) Transaction Layer Security
  - (b) Transport Layer Security
  - (d) Transaction Level Security
20. \_\_\_\_\_ is used for encrypting data at network level.
  - (a) IPsec
  - (b) HTTPS
  - (c) SMTP
  - (d) S/MIME
21. Users are able to see a pad-lock icon in the address bar of the browser when there is \_\_\_\_\_ connection.
  - (a) HTTP
  - (b) HTTPS
  - (b) SMTP
  - (c) SFTP
22. SSL provides
  - (a) Message integrity
  - (b) Confidentiality
  - (c) Compression
  - (c) All the above
23. \_\_\_\_\_ is the protocol designed by IETF to provide security for data packets at network level
  - (a) PGP
  - (b) SSL
  - (c) IPsec
  - (d) S-HTTP

Answers:

1. (a); 2. (b); 3. (b); 4. (a); 5. (d); 6. (b); 7. (c); 8. (d); 9. (c); 10. (d); 11. (a); 12. (d); 13. (d); 14. (c); 15. (b); 16. (a); 17. (d); 18. (a); 19. (c); 20. (a); 21. (b); 22. (d); 23. (c).

Fill in the Blanks:

1. A \_\_\_\_\_ cipher processes the input one block of elements at a time, producing an output block for each input block.
2. A \_\_\_\_\_ cipher processes the input elements continuously, producing output one element at a time as it goes along.
3. The \_\_\_\_\_ is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter to protect the premises network from Internet-based attacks.

4. A \_\_\_\_\_ firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.
5. A \_\_\_\_\_ uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.
6. \_\_\_\_\_ software is used to protect the company's information from external and internal threats.
7. \_\_\_\_\_ ensures that the document originated with the person signing it.
8. Conversion of data into secured format is known as \_\_\_\_\_.
9. \_\_\_\_\_ means protecting information, equipment devices, computer, computer resource, communication device and information stored.
10. A \_\_\_\_\_ serves as a barrier between a LAN and the Internet.
11. \_\_\_\_\_ is a method of converting data to a smaller fixed value known as the key, which is then used to represent the original data.
12. In \_\_\_\_\_, both encryption and decryption can be done using just one key.
13. In \_\_\_\_\_, it uses two keys to encrypt and decrypt data respectively.
14. IPSec VPNs are operated at the \_\_\_\_\_ level.
15. The privacy of the data is safeguarded in IPSec using \_\_\_\_\_ encryption.
16. TLS evolved from \_\_\_\_\_ which was originally developed by Netscape Communications Corporation.
17. Digital certificates are issued by a \_\_\_\_\_.
18. SSL enabled websites display the prefix \_\_\_\_\_ at the beginning of their URL.
19. The sender cannot deny having sent the e-mail is called \_\_\_\_\_.
20. The term \_\_\_\_\_ refers to the tasks involved in managing users for different systems and applications within an organization or network.
21. \_\_\_\_\_ define the processes and methodology to secure network data from any illegitimate attempt to extract the contents.

**Answers:**

1. Block; 2. Stream; 3. Firewall; 4. Packet Filtering; 5. VPN; 6. Firewall; 7. Digital Signature; 8. Encryption; 9. Cyber Security; 10. Firewall; 11. Hashing; 12. Symmetric Encryption; 13. Asymmetric Encryption; 14. Network; 15. public key/Asymmetric; 16. Secure Socket Layers (SSL); 17. Certificate Authority (CA); 18. HTTPS; 19. non-Repudiation; 20. User management; 21. Network security protocols.





**UNIT  
5**

**CYBERSPACE AND THE LAW,  
CYBER FORENSICS**

### **Short Answer Questions:**

1. Cyber space
2. Cyber law
3. Cyber forensics
4. Data localization
5. E-mail header
6. Memory dump
7. Elements of E-mail header

### Multiple Choice Questions:

1. \_\_\_\_\_ refers to an electronic medium that is used to facilitate online communication.  
(a) Cyber space  
(b) E-Commerce  
(c) e-Payment  
(d) None of these
2. \_\_\_\_\_ is a legal system designed to deal with the Internet, computing, Cyberspace, and related legal issues  
(a) Communication law  
(b) Cyber law  
(c) Computer law  
(d) None of these



3. Information Technology Act (IT Act) was enacted in year \_\_\_\_\_
  - (a) 1998
  - (b) 2010
  - (c) 2000
  - (d) 2005
4. CERT stands for
  - (a) Computer Emergency Response Team
  - (b) Computer Emergency Rapid Team
  - (c) Cyber Emergency Response Team
  - (d) None of the above
5. Registry in WINDOWS operating system contains the information like,
  - (a) OS installation date
  - (b) User name
  - (c) Files that are used recently
  - (d) All of the above
6. The tool which is used to extract information from non-volatile devices is called \_\_\_\_\_
  - (a) Digger
  - (b) Envelope
  - (c) Recover
  - (d) Imager
7. An E-mail contains
  - (a) Header
  - (b) Body
  - (c) (a) and (b)
  - (d) None of these
8. E-mail headers are organized \_\_\_\_\_
  - (a) Bottom-up
  - (b) Top-Bottom
  - (c) Horizontal
  - (d) Vertical
9. \_\_\_\_\_ is the technology that helps to reduce spam and phishing of e-mails
  - (a) RAM
  - (b) DKIM
  - (c) IEEE
  - (d) MIIN
10. \_\_\_\_\_ is the command to get IP address of your computer
  - (a) Ipcoan
  - (b) ipconfig
  - (c) getip
  - (d) traceip
11. IP addresses of IPv4 are \_\_\_\_\_ long
  - (a) 28 bit
  - (b) 30 bit
  - (c) 48 bit
  - (d) 32 bit
12. \_\_\_\_\_ is a special script executed to collect enough information about the user
  - (a) Chatbot
  - (b) Beacon
  - (c) Cookies
  - (d) web fingerprinting

**Answers:**

1. (a); 2. (b); 3. (c); 4. (a); 5. (d); 6. (d); 7. (c); 8. (a); 9. (b); 10. (b); 11. (d); 12. (d)

**Fill in the Blanks:**

1. A policy, which demand that certain kinds of data must be stored in servers located physically within India, termed as \_\_\_\_\_.
2. \_\_\_\_\_ is referred to as the Law of the Internet.
3. \_\_\_\_\_ is the ISO standard containing the specification for security management systems for the supply chain.
4. \_\_\_\_\_ is the ISO standard containing guidelines for the identification, collection, acquisition, and preservation of digital evidence.
5. The process of gathering and documenting proof from a computer or a computing device by applying the techniques of investigation and analysis is called \_\_\_\_\_.
6. Collecting, Preserving, Analyzing, and Presenting digital artifacts are the primary goals of \_\_\_\_\_.
7. The \_\_\_\_\_ file system for Microsoft's Windows 7 which is used to manage files present on disk.
8. \_\_\_\_\_ is a technical standard and e-mail authentication technique that helps protect e-mail senders and recipients from spam, spoofing, and phishing.
9. \_\_\_\_\_ provides an encryption key and digital signature that verifies that an e-mail message was not faked or altered.
10. An \_\_\_\_\_ is a unique address that identifies a device on the internet or a local network.
11. IP addresses of IPv6 are \_\_\_\_\_ long.
12. \_\_\_\_\_ are small text files placed on a user's computer, which are commonly used to collect personal data.
13. A \_\_\_\_\_ is a hidden, transparent graphic image that is used to read user behaviour on user's computer.
14. \_\_\_\_\_ refers to the analysis of volatile data in a computer's memory dump.
15. A snapshot capture of computer memory data from a specific instant is called a \_\_\_\_\_.

**Answers:**

- 1. Data Localization; 2. Cyber law; 3. ISO 28000; 4. ISO/IEC 27037; 5. Cyber Forensics; 6. Cyber Investigation 7. NTFS file system; 8. Sender Policy Framework, SPF; 9. DKIM, Domain Keys Identified Mail; 10. IP address; 11. 128 bit; 12. Cookies; 13. Web beacon; 14. Memory tracing; 15. memory dump.**

