Prof. Nilesh Parghi

CYBER SECURITY

B.C.A. 5TH SEMESTER **UNIT-1** **KSC - AMRELI**

Define:

1. Cyberspace:
   Cyberspace is that space in which users share information, interact with each other; engage in discussions or social media platforms, and many other activities. The whole Cyberspace is composed of large computer networks which have many sub networks. These follow the TCP or IP protocol.

2. Security
   Computer security is crucial to protect data and systems from threats like viruses, malware, and hackers. Antivirus software, firewalls, and encryption are common security measures.
3. Networking
   Computers can connect to each other and the internet via wired (e.g., Ethernet) or wireless (e.g., Wi-Fi) networks. Networking enables data sharing, communication, and remote access. Security
4. Cyber security
   The architecture of cyberspace includes various security measures to protect data, networks, and users. Firewalls, encryption, intrusion detection systems, and antivirus software are examples of cyber security components.
5. Internet
   The internet is the foundation of web technology. It is a global network of interconnected computers and servers that allows for the transfer of data and information across the world.
6. Confidentiality
   This principle focuses on ensuring that sensitive information is only accessible to authorized individuals or systems. It involves encryption, access controls, and data classification to prevent unauthorized access or disclosure.
7. Integrity
   Integrity in cyber security means that data and systems are accurate and trustworthy. Any unauthorized modification or tampering with data or systems should be detected and prevented. Techniques like checksums and digital signatures are used to maintain data integrity.
8. Availability
   Availability ensures that systems and data are accessible when needed. Cyber attacks can disrupt services or make them unavailable, so cyber security measures aim to prevent or mitigate such disruptions through redundancy, load balancing, and disaster recovery planning.
9. Authentication
   Authentication is the process of verifying the identity of users, devices, or systems trying to access resources. This can be achieved through passwords, biometrics, two-factor authentication (2FA), and multi-factor authentication (MFA).

10. Cyber Attacks

    A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

11. Injection attacks

    It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

12. Session Hijacking

    It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

13. Phishing

    Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

14. Denial of Service

    It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash.

15. Virus

    It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

16. Worm

    It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

17. Trojan horse

    It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

18. Cyber Threat

    A Cyber threat is any malicious act that attempts to gain access to a computer network without authorization or permission from the owners.

19. Data Breaches

    Data breaches can have severe consequences for organizations and individuals. The theft or exposure of sensitive data, such as personal information, financial records, or intellectual property, can lead to financial losses, reputational damage, and legal liabilities.

Full Forms:

1. CPU - central processing unit
2. TCP- Transmission Control Protocol
3. IP - Internet Protocol
4. HTTP - Hypertext Transfer Protocol
5. SMTP - Simple Mail Transfer Protocol
6. FTP - File Transfer Protocol
7. DNS - Domain Name System
8. IoT - Internet of Things
9. WWW - World Wide Web
10. TLS - Transport Layer Security
11. AWS - Amazon Web Services
12. W3C-Wide Web Consortium (W3C)
13. CDNs - Content Delivery Networks
14. QoS - Quality of Service
15. ISOC - Internet Society
16. 2FA - two-factor authentication

CYBER SECURITY

B.C.A. 5TH SEMESTER **UNIT-2** **KSC - AMRELI**

Define:

1. cyber crimes
   Cyber crimes are crimes that involve criminal activities done through cyberspace by devices connected to the internet. ▪ At times, cyber crimes are also called ‘computer crimes’.
2. Email spoofing
   A spoofed email is one in which the e-mail header is forged so that the mail appears to originate from one source but actually has been sent from another source.
3. Spamming
   Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.
4. Cyber Defamation
   This occurs when defamation takes place with the help of computers and/or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.
5. Harassment & Cyber stalking

Cyber Stalking Means following an individual's activity over internet. It can be done with the help of many protocols available such as e- mail, chat rooms, and user net groups.

6. Internet time theft
   This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.
7. Email Bombing
   Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.
8. Salami Attack
   When negligible amounts are removed & accumulated in to something larger. These attacks are used for the commission of financial crimes.
9. Logic Bomb
   It is an event dependent program. As soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.
10. Trojan Horse
    This is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.
11. Data diddling
    This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.
12. Forgery
    Currency notes, revenue stamps, mark sheets etc. can be forged using computers and high quality scanners and printers.
13. Cyber Terrorism
    Use of computer resources to intimidate or coerce people and carry out the activities of terrorism.
14. Web Jacking
    Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.
15. Malware Attacks
    Malicious software (malware) is designed to infect computers and mobile devices. This includes viruses, worms, Trojans, ransomware, spyware, and adware. Malware can steal data, damage systems, or hold data hostage for a ransom.
16. Phishing
    Phishing attacks involve tricking individuals into revealing sensitive information like passwords, credit card numbers, or personal details by posing as a legitimate entity through email, text messages, or fake websites.
17. Identity Theft
    Cybercriminals can steal personal information, such as Social Security numbers and financial data, to commit fraud, open accounts in victims' names, or access their financial resources.
18. Online Scams

Various online scams target individuals, such as advance-fee fraud, lottery scams, and romance scams. These scams deceive people into sending money or personal information to fraudsters.

19. DDoS Attacks
    Distributed Denial of Service (DDoS) attacks overwhelm a target's computer or network with traffic, making it unavailable to users. These attacks are often used to disrupt services or extort money.
20. Data Breaches
    Cybercriminals infiltrate organizations to steal sensitive data like customer information, trade secrets, or financial records. These breaches can result in significant financial losses and reputational damage.
21. Cyberbullying
    Cyberbullying involves the use of technology to harass, threaten, or intimidate individuals. It can take place through social media, messaging apps, or email.
22. Cyber Extortion
    Criminals may threaten to release sensitive or embarrassing information unless a victim pays a ransom. This can involve sextortion (threatening to expose explicit content) or other forms of extortion.
23. Insider Threats
    Employees or individuals with insider access to computer systems and data may misuse their privileges to steal or manipulate information.
24. Cryptojacking
    Cybercriminals use a victim's computer or mobile device to mine cryptocurrency without their consent, which can slow down the device and increase energy consumption.
25. Online Trafficking
    Human traffickers may use the internet to lure and exploit women and children, including for purposes of forced labor or sexual exploitation. Online platforms can be used to recruit victims.
26. Cyberstalking
    This involves persistent and unwanted online attention, often leading to fear or emotional distress. Women and children can be targeted by cyberstalkers who may threaten or harass them through digital means.
27. Ponzi Schemes
    Ponzi schemes lure investors with promises of unusually high returns in a short period. The fraudsters use funds from new investors to pay off earlier investors, creating a false illusion of profitability.
28. Adware
    Display ads (sometimes malicious ads) to users as they work on their computers or browse the web.
29. Keyloggers
    Capture keystrokes as users type in URLs, credentials, and personal information and send it to an attacker.
30. Zero day

Software often has security vulnerabilities that hackers can exploit to cause havoc. The term "zero-day" refers to the fact that the vendor or developer has only just learned of the flaw – which means they have “zero days” to fix it.

31. Zero click
    zero-click attacks require no action from the victim – meaning that even the most advanced users can fall prey to serious cyber hacks and spyware tools. ▪ also called interaction-less or fully remote attacks.
32. Data Encryption
    Encrypt sensitive data, both in transit and at rest, to ensure that even if it is intercepted or stolen, it remains unreadable and unusable for unauthorized individuals.
33. Cyber law
    Cyber law is a framework created to give legal recognition to all risks arising out of the usage of computers and computer networks.

Full Forms:

1. RAT - Remote access tools
2. PoS - point-of-sale
3. APWG - Anti-Phishing Working Group
4. AMTSO - Anti-Malware Testing Standards Organization
5. ISP - Internet Service Provider
6. MFA - Multi-factor Authentication
7. ITA - IT Act
8. IPC - Indian Penal Code
9. NCSC - National Cyber Security Coordinator
10. CERT-In - Computer Emergency Response Team-India
11. NCIIPC - National Critical Information Infrastructure Protection Centre
12. NIA - National Investigation Agency
13. CAT - Cyber Appellate Tribunal

CYBER SECURITY

B.C.A. 5TH SEMESTER **UNIT-3** **KSC - AMRELI**

Define:

1. Social networks
   Social networks are websites and apps that allow users and organizations to connect, communicate, share information and form relationships. People can connect with others in the same area, families, friends, and those with the same interests.

2. Social networking
   Social networking refers to using internet-based social media sites to stay connected with friends, family, colleagues, or customers. Social networking can have a social purpose, a business purpose, or both through sites like Facebook, X (formerly Twitter), Instagram, and Pinterest.
3. Hashtag
   The hashtag is used to draw attention, organize, promote, and connect. Hashtags refer to the usage of the pound or number symbol, "#," to mark a keyword or topic on social media.
4. Viral content
   To be “viral” on social media means that a piece of content, such as a post, video, or image, has become extremely popular and is being shared by a large number of people on various social media platforms.
5. Social Media Marketing
   Social media marketing is a form of digital marketing that leverages the power of popular social media networks to achieve your marketing and branding goals.
6. Hate Speech and Discrimination: Many countries have laws against hate speech, which includes content that promotes violence or discrimination against individuals or groups based on characteristics like race, religion, ethnicity, gender, sexual orientation, or disability.
7. Copyright Infringement: Using someone else's content without permission can violate copyright laws. This applies to images, videos, music, and other creative works. 4. Privacy Violations: Sharing private information, such as someone's address, personal details, or intimate media, without their consent can violate privacy laws.
8. Defamation and Libel: Posting false information that harms someone's reputation can lead to legal action for defamation or libel. This includes both written and visual content that portrays someone in a false and negative light.

CYBER SECURITY

B.C.A. 5TH SEMESTER **UNIT-4** **KSC - AMRELI**

Define:

1. E- Commerce
   E-Commerce or Electronic Commerce means buying and selling of goods, products, or services over the internet. E-commerce is also known as electronic commerce or internet commerce. Transaction of money, funds, and data are also considered as E-commerce.
2. Payment Gateway
   The payment mode through which customers shall make payments. Payment gateway represents the way e-commerce vendors collect their payments. Examples are Credit / Debit

Card Payments, Online bank payments, Vendors own payment wallet, Third Party Payment wallets, like PAYTM and Unified Payments Interface (UPI).

3. SQL Injection

   Attackers exploit vulnerabilities in the website's code to insert malicious SQL queries, allowing them to access or manipulate the database, compromising sensitive information.
4. Man-in-the-Middle (MITM) Attacks

   Hackers intercept communication between a user and an e-commerce website to eavesdrop, steal information, or manipulate data during the transmission.
5. Scalability

   If you have a physical storefront, your business can only grow so much before you have to move to a larger storefront. You also have to move inventory and equipment from one location to another, which makes it even harder to scale your store with the growth of your business. With e-commerce, your website and store can grow as your business does, and you don't have to spend a fortune moving to a new physical space.
6. Mobile Wallets

   Apps or platforms that store payment information, allowing users to make transactions through their Smartphone's. Examples include Apple Pay, Google Pay, and PayPal.
7. Card Skimming

   Card skimming involves the illegal copying of a user's credit or debit card information using a skimming device when the card is swiped for payment. The scammers then use the copied information to make fraudulent transactions.
8. Settlement Finality

   The Act provides for settlement finality, meaning that once a settlement in a payment system is deemed final, it cannot be revoked or reversed, except in certain specified circumstances.

Full Forms:

1. B2B - Business to Business
2. B2C - Business to Customer
3. C2C - Customer to Customer
4. C2B - Customer to Business
5. UPI - Unified Payments Interface
6. MITM - Man-in-the-Middle
7. SSL - Secure Sockets Layer
8. PCI DSS - Card Industry Data Security Standard
9. DDoS - Distributed Denial of Service
10. NFC - Near Field Communication
11. PSPs - Payment Service Providers

12. e-Wallets - Electronic wallets
13. USSD - Unstructured Supplementary Service Data
14. AEPS - Aadhar enabled payments system
15. RBI - The Reserve Bank of India

CYBER SECURITY

B.C.A. 5TH SEMESTER **UNIT-5** **KSC - AMRELI**

Define:

1. Password policy
   A password policy sets the rules that passwords for a service must meet, such as length and type of characters allowed and disallowed. ▪ Password policies are crucial for ensuring the security of digital accounts and systems. They typically include guidelines and requirements that dictate how passwords should be created, used, and managed.
2. Host Firewall
   A host firewall is a software or hardware component that monitors and controls incoming and outgoing network traffic on an individual device (such as a computer or server). Its primary function is to act as a barrier between your device and potentially malicious content from the internet or other networks.
3. Antivirus Software
   Antivirus software is designed to detect, prevent, and remove malicious software (malware) from a computer or device.

Full Forms:

16. VPN - Virtual Private Network
17. BYOD - Bring Your Own Device
18. MFA - Multi-Factor Authentication
19. WI-FI - Wireless Fidelity
20. WPA3 - Wi-Fi Protected Access 3
21. SSID - Service Set Identifier
22. WPS - Wi-Fi Protected Setup
23. ACL - access control lists
24. RBAC - Role-Based Access Control