BASIC TERMINOLOGIES IN INFORMATION SECURITY

1. Unauthorized access − An unauthorized access is when someone gains access to a server, website, or other sensitive data using someone else's account details.

2. Hacker − Is a Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc.

3. Threat − Is an action or event that might compromise the security.

4. Vulnerability − It is a weakness, a design problem or implementation error in a system that can lead to an unexpected and undesirable event regarding security system.

5. Attack − Is an assault on the system security that is delivered by a person or a machine to a system. It violates security.

6. Antivirus or Antimalware − Is a software that operates on different OS which is used to prevent from malicious software.

7. Social Engineering − Is a technique that a hacker uses to stole data by a person for different for purposes by psychological manipulation combined with social scenes.

8. Virus − It is a malicious software that installs on your computer without your consent for a bad purpose.

9. Firewall − It is a software or hardware which is used to filter network traffic based on rules.

10. Adware – Adware refers to any piece of software or application that displays advertisements on your computer.

11. Advanced Persistent Threat (APT) – An advanced persistent threat is an attack in which an unauthorised user gains access to a system or network without being detected.

12. Anti-Virus Software – Anti-virus software is a computer program used to prevent, detect, and remove malware.

13. Artificial Intelligence – Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions.

14. Attachment – An attachment is a computer file sent with an email message.

15. Authentication – Authentication is a process that ensures and confirms a user's identity.

16. Back door – A backdoor is used to describe a hidden method of bypassing security to gain access to a restricted part of a computer system.

17. Backup – To make a copy of data stored on a computer or server to reduce the potential impact of failure or loss.

18. Baiting – Online baiting involves enticing a victim with an incentive.

19. Bluetooth – Bluetooth is a wireless technology for exchanging data over short distances.

20. Blackhat – Black hat hacker refers to a hacker that violates computer security for personal gain or malice.

21. Botnet – A botnet is a collection of internet-connected devices, which may include PCs, servers and mobile devices that are infected and controlled by a common type of malware.

22. Broadband – High-speed data transmission system where the communications circuit is shared between multiple users.

23. Browser – A browser is software that is used to access the internet. The most popular web browsers are Chrome, Firefox, Safari, Internet Explorer, and Edge.

24. Brute Force Attack – Brute force attack is an activity which involves repetitive successive attempts of trying various password combinations to break into any website.

25. Bug – A bug refers to an error, fault or flaw in a computer program that may cause it to unexpectedly quit or behave in an unintended manner.

26. BYOD – Bring your own device (BYOD) refers to employees using personal devices to connect to their organisational networks.

27. Clickjacking – Clickjacking, also known as a UI redress attack, is a common hacking technique in which an attacker creates an invisible page or an HTML element that overlays the legitimate page.

28. Cloud Computing – The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

29. Cookie – Cookies are small files which are stored on a user's computer. Cookies provide a way for the website to recognize you and keep track of your preferences.

30. Critical Update – A fix for a specific problem that addresses a critical, non-security-related bug in computer software.

31. Cyber Warfare – Cyber warfare typically refers to cyber-attacks perpetrated by one nation-state against another.

32. Data Breach – A data breach is a confirmed incident where information has been stolen or taken from a system without the knowledge or authorization of the system's owner.

33. Data Server – Data server is the phrase used to describe computer software and hardware that delivers database services.

34. DDoS Attack – A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

35. Deepfake – Deepfake refers to any video in which faces have been either swapped or digitally altered, with the help of AI.

36. Domain name – The part of a network address which identifies it as belonging to a particular domain.

37. Domain Name Server – A server that converts recognisable domain names into their unique IP address

38. Download – To copy (data) from one computer system to another, typically over the Internet.

39. Exploit – A malicious application or script that can be used to take advantage of a computer's vulnerability.

40. Firewall – A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.

41. Hacking – Hacking refers to an unauthorised intrusion into a computer or a network.

42. Honeypot – A decoy system or network that serves to attract potential attackers.

43. HTML – Hypertext Markup Language (HTML) is the standard markup language for creating web pages and web applications.

44. Identity theft – Identity theft is a crime in which someone uses personally identifiable information in order to impersonate someone else.

45. Incident Response Plan – An incident response policy is a plan outlying organisation's response to an information security incident.

46. Internet of things (IoT) – The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, collecting and sharing data.

47. IP Address – An IP address is an identifying number for a piece of network hardware. Having an IP address allows a device to communicate with other devices over an IP-based network like the internet.

48. IOS – An operating system used for mobile devices manufactured by Apple.

49. Keystroke logger – A keystroke logger is software that tracks or logs the keys struck on your keyboard, typically in a covert manner so that you are unaware actions are being monitored.

50. Malware – Malware is shorthand for malicious software and is designed to cause damage to a computer, server, or computer network.

51. Malvertising – The use of online advertising to deliver malware.

52. Memory stick – A memory stick is a small device that connects to a computer and allows you to store and copy information.

53. MP3 – MP3 is a means of compressing a sound sequence into a very small file, to enable digital storage and transmission.

54. Multi-Factor Authentication – Multi-Factor Authentication (MFA) provides a method to verify a user's identity by requiring them to provide more than one piece of identifying information.

55. Packet Sniffer – Software designed to monitor and record network traffic.

56. Padlock – A padlock icon displayed in a web browser indicates a secure mode where communications between browser and web server are encrypted.

57. Patch – A patch is a piece of software code that can be applied after the software program has been installed to correct an issue with that program.

58. Penetration testing – Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

59. Phishing – Phishing is a method of trying to gather personal information using deceptive e-mails and websites.

60. Policy Management – Policy Management is the process of creating, communicating, and maintaining policies and procedures within an organisation.

61. Proxy Server – A proxy server is another computer system which serves as a hub through which internet requests are processed.

62. Pre-texting – Pre-texting is the act of creating a fictional narrative or pretext to manipulate a victim into disclosing sensitive information.

63. Ransomware – A type of malicious software designed to block access to a computer system until a sum of money is paid.

64. Rootkit – Rootkits are a type of malware designed to remain hidden on your computer.

65. Router – A router is a piece of network hardware that allows communication between your local home network and the Internet.

66. Scam – A scam is a term used to describe any fraudulent business or scheme that takes money or other goods from an unsuspecting person.

67. Scareware – Scareware is a type of malware designed to trick victims into purchasing and downloading potentially dangerous software.

68. Security Awareness Training – Security awareness training is a training program aimed at heightening security awareness within an organisation.

69. Security Operations Centre (SOC) – A SOC monitors an organisation's security operations to prevent, detect and respond to any potential threats.

70. Server – A server is a computer program that provides a service to another computer programs (and its user).

71. Smishing – Smishing is any kind of phishing that involves a text message.

72. Spam – Spam is slang commonly used to describe junk e-mail on the Internet.

73. Social Engineering – Social engineering is the art of manipulating people, so they disclose confidential information.

74. Software – Software is the name given to the programs you will use to perform tasks with your computer.

75. Spear Phishing – Spear phishing is an email-spoofing attack that targets a specific organization or individual, seeking unauthorized access to sensitive information.

76. Spyware – Spyware is a type of software that installs itself on a device and secretly monitors a victim's online activity.

77. Tailgating – Tailgating involves someone who lacks the proper authentication following an employee into a restricted area.

78. Tablet – A tablet is a wireless, portable personal computer with a touchscreen interface.

79. Traffic – Web traffic is the amount of data sent and received by visitors to a website.

80. Trojan – A Trojan is also known as Trojan horse. It is a type of malicious software developed by hackers to disguise as legitimate software to gain access to target users' systems.

81. Two-Factor Authentication – Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are.

82. USB – USB (Universal Serial Bus) is the most popular connection used to connect a computer to devices such as digital cameras, printers, scanners, and external hard drives.

83. Username – A username is a name that uniquely identifies someone on a computer system.

84. Virus – A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions.

85. VPN (Virtual Private Network) – A virtual private network gives you online privacy and anonymity by creating a private network from a public Internet connection. VPNs mask your Internet protocol (IP) address so your online actions are virtually untraceable.

86. Vulnerability – A vulnerability refers to a flaw in a system that can leave it open to attack.

87. Vishing – Vishing is the telephone equivalent of phishing. It is an attempt to scam someone over the phone into surrendering private information that will be used for identity theft.

88. Whaling – Whaling is a specific form of phishing that's targeted at high-profile business executives and managers.

89. Whitehat – White hat hackers perform penetration testing, test in-place security systems and perform vulnerability assessments for companies.

90. Worm – A computer worm is a malware computer program that replicates itself in order to spread to other computers.

91. Wi-Fi – Wi-Fi is a facility that allows computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

92. Zero-Day – Zero-Day refers to a recently discovered vulnerability that hackers can use to attack systems.