Quizlet

Cybersecurity 1a: Foundations Course Vocab

Study online at quizlet.com/_8nx7s1

1.	**access control**	a security technique used to regulate who or what can utilize the resources of a computer system
2.	**accountability**	making sure every individual working with an information system has specific responsibilities for information assurance
3.	**accounting**	measures how much information has been accessed or the amount of time spent on a session
4.	**adware**	software that displays unwanted advertising while running an application on your computer
5.	**AIC triad**	a three-pronged system of cybersecurity
6.	**air gap network**	keeps a system secure by physically isolating it from all unsecured networks
7.	**air-gapped system**	one that is physically isolated from the internet and only able to pass data along via removable media
8.	**algorithm**	process or set of rules
9.	**application lifecycle management (ALM)**	the governance, development, and maintenance of computer programs
10.	**application program**	the governance, development, and maintenance of computer programs
11.	**application security**	the use of software and hardware in combination with certain procedural methods to protect applications from external threats
12.	**authentication**	identifies a user by asking them to enter some kind of valid information, like a password or user name
13.	**authenticity**	guarantee that the message, transaction, or other exchange of information has shown its proof of identity
14.	**authorization**	gives a user permission to do certain things
15.	**availability**	guarantee of reliable access to information
16.	**biometric input**	relies on human characteristics to distinctly identify individuals as themselves
17.	**boot sequence**	an orderly search for nonvolatile data storage to load the OS
18.	**bridge forwarding table**	a table of addressable memory used by a switch during transmission
19.	**bridge**	helps join two separate computer networks together to allow for communication
20.	**broadband**	a high-capacity transmission technique with a lot of frequencies and messaging capabilities
21.	**bus network**	each station is connected to a main cable running down the center, like a bus
22.	**byte**	a unit of data used to represent a character, such as a letter, number, or symbol, consisting of eight binary digits
23.	**central processing unit (CPU)**	the electronic circuitry within the computer
24.	**checksum**	part of an encryption protocol that calculates and compares data on either end of a network to see if it matches
25.	**cipher**	an algorithm for performing encryption
26.	**client operating system (COS)**	supports the functions of both desktop and portable computers
27.	**cloud computing security**	a broad set of policies, technologies, and controls used to protect information, applications, and related infrastructure
28.	**cloud computing**	the use of a remote network on the internet for the delivery of paid, on-demand computing services
29.	**coaxial cable (coax)**	the medium used to transmit video, audio, and other communications, with a single copper conductor at the center
30.	**computer patch**	a piece of software designed to update a computer program by fixing bugs or improving overall function
31.	**confidentiality**	a set of rules limiting access to certain information, much like privacy
32.	**configuration**	arrangement of setup of hardware and software
33.	**counterterrorism**	efforts to prevent attacks of terrorism, in both the real and digital world
34.	**critical infrastructure**	government term describing assets that keep society and the economy functioning (including national and economic security, public health and safety, communication, transportation, and electricity generation)
35.	**crosstalk**	unwanted transfer of signals between communication channels
36.	**cyber assets**	items or people of value online
37.	**cybersecurity regulations**	directives created to teach companies and organizations how to protect their own IT systems

38. **cybersecurity**	the state of being protected against criminal or unauthorized online activity
39. **cyberspace**	the virtual, online world
40. **cyberterrorism**	the use of computers and information technology to spread fear in pursuit of a political agenda
41. **decryption key**	the piece of information able to turn text into code and vice versa
42. **degaussing**	a method to destroy data in which the magnetic field of a storage drive is removed or reduced, and the data is irrecoverable
43. **demilitarized zone (DMZ)**	a special configuration designed to improve security in home and business settings through isolating computer connections on either side of a firewall
44. **Denial of Service (DoS)**	an attack that overwhelms a network resource with fake visitors and crowds out legitimate traffic, so the server becomes overloaded
45. **digital arms race**	the neck-and-neck competition between hackers and security experts
46. **digital citizenship**	how someone uses information technology to engage with society, organizations, the government, and other outside entities
47. **digital industrial control system**	a general term for managing systems associated with highly-mechanized and automated processes
48. **digital network**	a group of computer systems and computing hardware devices linked together through a variety of communication channels
49. **directory files**	keeps track of all the other files through cataloging
50. **eavesdrop**	listen in on the transmissions between people without being detected
51. **e-commerce**	goods and services available for online purchase
52. **electromagnetic (EM) shielding**	practice of surrounding electronics and cables with magnetic or conductive materials to create a barrier from outside frequencies
53. **encryption**	the process of encoding messages or information in such a way that only authorized people can easily access it
54. **end user error**	when someone involved in the complex computer system makes a human mistake of trusting where they shouldn't
55. **endpoint security**	a method to protect a network when remote access is requested by a device
56. **extranet**	an extension of the intranet that allows companies to share some information and communications with the outside world of vendors, partners, and customers
57. **fiber optic cable**	connective network material that uses both glass and copper fibers
58. **firewall**	a security appliance designed to block unauthorized access while still allowing outward communication
59. **firmware**	software embedded in the router to offer network security and control
60. **frame**	a unit of digital data transmitted in a network
61. **hacker**	a person who gains unauthorized access to a computer
62. **hard disk drive (HDD)**	stores critical things like the operating system, software titles, and other files
63. **hardening**	the process of securing a computer system by reducing its vulnerabilities
64. **hardware**	any physical aspect of your computer, like the keyboard, mouse, motherboard, or cables
65. **hashing**	the transformation of characters into a shorter key that represents the original string
66. **honeypot**	a security measure to divert hackers from the live network
67. **hotfix**	a collective, single package of information (usually in the form of files) that handles a software problem
68. **hub**	the central connection point, where multiple ports exist, and all of the associated data of packets and frames come and go
69. **information assurance**	the practice of protecting digital and non-digital information
70. **information security certifications**	programs developed to teach candidates the skills to excel in cybersecurity
71. **information security**	preventing unauthorized access to information and actively detecting, documenting, and counteracting such threats
72. **infrastructure**	the basic physical and organizational structures and facilities the world depends on
73. **integrity**	assures online information is trustworthy and accurate

74. **Internet Control Message Protocol (ICMP)** the protocol that sends error messages and other operational information indicating issues like unavailable service or an unreachable router

75. **Internet of Things (IoT)** the network of devices, appliances, and other items that are embedded with software to transfer data without human interaction

76. **intranet** a private network used by one organization

77. **Intrusion Detection System (IDS)** monitors fishy activity or policy violations on a network

78. **Intrusion Prevention System (IPS)** looks for possible threats on the network and responds quickly

79. **IP address** Internet Protocol, the unique address (phone number) of a device

80. **kernel** software responsible for running the programs and providing secure access to the machine’s hardware

81. **key size** the number of bits a key uses to create a cipher

82. **keyloggers** software that records your every keystroke, allowing intruders to gain access to passwords and other confidential information

83. **kill switch** a countermeasure that offers a single point of control to shut down a system

84. **Local Area Network (LAN)** connects devices over a short distance

85. **logical address** the address at which an item, such as a memory cell, appears to reside

86. **Logical Link Control (LLC)** a part of the OSI Model that controls frame synchronization, flow control, and error investigation

87. **loop** when a transmission pathway is repeated on the network

88. **macros** a rule or pattern that specifies the mapping of an input sequence

89. **macroviruses** infect programs or applications by triggering a series of actions not started by the user

90. **mainframe** a high-performance computer, primarily used by large organizations, that possesses the capacity to handle large-scale computing, such as processing bulk data

91. **malware** software designed to damage or disable computer systems

92. **Man-In-The-Middle (MITM)** a manipulation attack that involves eavesdropping and/or manipulation

93. **Media Access Control (MAC)** maintains all the physical addresses for devices on the network

94. **memory management** the superpower that oversees the primary memory in a computer and keeps track of all its locations

95. **mesh network** a network that directly connects some or all workstations to one another so that data can be distributed among workstations

96. **Metropolitan Area Network (MAN)** connects devices over a longer distance but shorter than a WAN

97. **mobile device** a portable computer

98. **mobile malware** malicious software that targets mobile phones or wireless devices

99. **modem** a device or program enabling a computer to transmit data over certain channels

100. **monetized** how something can be financially profited from

101. **motherboard** connects all the computer parts together via cables

102. **network access control (NAC)** an approach to computer security that restricts the availability of network resources through the enforcement of a defined security policy

103. **network address translation (NAT)** assigns a public address to one or more computers inside a private network

104. **network operating systems (NOS)** supports the functions of a network to enable the sharing of data, users, security, applications, and other functions

105. **network security appliance** a server-related piece of equipment designed to protect computer networks from unwanted traffic

106. **network security** the use of both software and hardware to safeguard the usability and integrity of a network

107. **network topology** the arrangement of workstations, both physically and logically

108. **node** a point in a larger network capable of redistributing data

109. **nonrepudiation** provides a way for denial to be impossible

110. **open source software** software that can be publicly accessed, shared, and modified

111. **Open System Interconnection (OSI) Model** a conceptual model depicting the communications functions of a computing system

112. **operating system (OS)** software that supports a computer's basic functions

113. **packets** a formatted unit of data routed between an origin and a destination on the internet

114. **peer-to-peer network (P2P)** a network of computers that facilitates sharing of files among computers on the network without the use of a central server

115. **phishing** methods, like email, used to entice you into clicking things you normally wouldn't

116. **port blocking** the action of closing vulnerable points of entry on a network

117. **port number** a point through which information flows from a program to a computer on a network, ensuring that data packets make it to the proper destination

118. **port** a connection point where cables, routers, modems or other peripheral devices can be plugged into a computer

119. **ports and services** the main mechanism in managing network traffic

120. **primary memory** memory that functions internally and is considered volatile because it can't hold on to data forever

121. **proof-of-concept (PoC) attack** small in scale and performed only to prove that it can be done

122. **protocols** a set of rules for exchanging messages on the internet

123. **ransomware** malware that holds information "hostage" until the recipient pays for its return

124. **regular files** store text, binary, or executable data

125. **Remote Access Trojan (RAT)** a more advanced form of malware, known as a Trojan Horse, which is able to bypass a computer's security for administrative control

126. **remote access** the ability to use data and information regardless of physical location

127. **removable media** a storage device that can be removed from a computer while the system is running and used elsewhere

128. **restore brain** a saved "snapshot" of your computer's data at a specific time

129. **reverse engineering** the duplication of another person's product in an attempt to disassemble it, and thereby master its composition

130. **ring network** in a ring network, workstations are all linked in a closed loop-like configuration, like a ring

131. **risk management** the process of identifying, assessing, and controlling threats to corporate data

132. **root** the first or top-most directory of a file system

133. **rootkits** allow unauthorized users to gain control over a computer system without being detected

134. **router** a device that forwards data packets between computer networks

135. **routing table** a data table that stores network locations and how they can be reached

136. **security controls** technical or administrative safeguards to countermeasure or lessen the possibility of threats

137. **security policy** a plan to protect a company's physical and digital assets

138. **security zones** areas with increased trust, accountability, and safety

139. **server** a computer program or computer that provides data and functionality to other programs or computers, which are known as clients

140. **service set identifier (SSID)** a unique set of alphanumeric characters set at the header of the data packets being sent out over the wireless network

141. **social engineering** a cyberattack using deception as a way to manipulate users into revealing personal information

142. **software** the set of instructions used to tell the hardware what it should do and how

143. **special files** help with communication and process efficiency happening in the computer

144. **spoofing attack** one that gains advantage over a system by masquerading as a familiar person or program

145. **spyware** software that can steal sensitive information and is installed without your knowledge or permission

146. **star network** a network in which a central computer or server "hub" sits at the center of all the workstations and indirectly connects them all

147. **switch** a network device used to connect computers together on a network

148. **systems utilities** a core software function that instructs the hardware and manages computer functions

149. **thin client** a lightweight computer that has been optimized to function remotely in a server-based environment

150. **third party apps** applications provided by a vendor who is not the device manufacturer

151. **token ring network** similar design to a ring network, but it uses "token passing," which means only the computer with the token can pass data along to the next one

152. **tokenization** a process allowing sensitive information to be replaced with unique identification symbols that retain all the essential characteristics of the data without compromising its security

153. **trend** general movement towards a certain way of thinking or living

154. **Trojan Horse** programs that breach security by relying on a user to interact with them

155. **tunneling protocol** allows for data from a private network to travel safely across a public network

156. **two-factor authentication (2FA)** when two separate pieces of evidence are required to gain access

157. **unsecured network** an open, public internet connection offered without the need for a password or login credential

158. **Virtual Machine (VM) escape** an exploit that gives an attacker access to the host OS and all those running on the VMs

159. **virtual private network (VPN)** technology that provides a safe connection over a network like the internet to provide remote users with access to resources on a network

160. **virtual** where something exists without a physical state

161. **virtualization** the process where a device or resource is created to provide more than one framework for the resource

162. **viruses** pieces of code with the ability to corrupt a system and/or destroy data

163. **vulnerability** a weakness or gap in our effort to protect ourselves

164. **wardriving** the act of searching for Wi-Fi wireless networks while on the move

165. **Wide Area Network (WAN)** connects devices over a vast distance, like the whole world

166. **Wireless Local Area Network** connects two or more devices using high-frequency radio waves

167. **worms** standalone software that penetrates an OS to spread malicious code, similar to viruses but spread faster because they don't need to be opened to become active