CEH Definition Flashcards

1.	**Acceptable Use Policy (AUP)**	A policy that states what users of a system can and cannot do with the organization's assets.
2.	**Access Control List (ACL)**	A method of defining what rights and permissions an entity has to a given resource. In networking, access control lists are commonly associated with Firewall and Router traffic filtering rules.
3.	**Access Creep**	This occurs when authorized users accumulate excess privileges on a system because of moving from one position to another. The privileges accidentally remain with the account from position to position.
4.	**Access Point (AP)**	A wireless LAN device that acts as a central point for all wireless traffic. The AP is connected to both the wireless LAN and the wired LAN, providing wireless clients access to network resources.
5.	**Accountability**	The ability to trace actions performed on a system to a specific user or system entity.
6.	**Acknowledgment (ACK)**	This is a TCP flag notifying an originating station that the proceeding packet (or packets) has been received. The ACK is part of the 3-way TCP handshake.
7.	**Active attack**	An attack that is direct in nature, usually where the attacker injects something into or otherwise alters the network or system target.
8.	**Active Directory (AD)**	The directory service created by Microsoft for use on its networks. It provides a variety of network services using Lightweight Directory Access Protocol (LDAP), Kerberos-based authentication, and single sign-on for user access to network based resources.
9.	**Active fingerprinting**	Injecting traffic into the network to identify the operating system of a device.
10.	**Address Resolution Protocol (ARP)**	A protocol used to map a known IP address to a physical (MAC) address. It is defined in RFC 826. The ARP Table is a list of IP addresses and corresponding MAC addresses on a local computer.
11.	**ad hoc mode**	A mode of operation in a wireless LAN in which clients send data directly to one another without utilizing a wireless access point (WAP), much like a point to point wired connection.
12.	**Adware**	Software that has advertisements embedded within it. It normally displays ads in the form of pop-ups.
13.	**Algorithm**	A step-by-step method of solving a problem. In computer security, an algorithm is a set of mathematical rules (logic) for the process of encryption and decryption.
14.	**Annualized Loss Expectancy (ALE)**	A measurement of the cost of an asset's value to the organization and the monetary loss that can be expected for an asset due to risk over a one year period. ALE is the product of the Annual Rate of Occurrence (ARO) and the Single Loss Expectancy (SLE). The formula is: ALE = ARO x SLE.
15.	**Annualized Rate of Occurrence (ARO)**	An estimate of the number of times during a year that a particular asset would be lost or experience downtime.
16.	**Anonymizer**	A device or service designed to obfuscate traffic between a client and the Internet. It is generally used to make activity on the Internet as untraceable as possible.
17.	**Antivirus (AV) software**	An application that monitors a computer or network to identify and prevent malware. Antivirus is usually signature based and can take multiple actions on the defined malware files/activity.
18.	**Application Layer**	Layer 7 of the OSI Model. The Application layer provides services to applications, which allows them to access the network. Protocols such as FTP and SMTP reside here.
19.	**Application-level attacks**	Attacks on the actual programming code of an application.
20.	**Archive**	A collection of historical records or the place where they are kept. In computing, an archive normally refers to backup copies of logs and/or data.
21.	**Assessment**	Activities to determine the extent to which a security control is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
22.	**Asset**	Any item of value or worth to an organization, whether physical or virtual.

23.	**Asymmetric**	In computing, asymmetric refers to a difference in networking speeds upstream to downstream. In cryptography, it's the use of more than one key for encryption or authentication purposes. Think Public and Private Key.
24.	**Asymmetric Algorithm**	In computer security, an algorithm that uses separate keys for encryption and decryption.
25.	**Asynchronous**	The lack of cloking (imposed time ordering) on a bit stream. It is also an industry term that refers to an implant or malware that does not require active interaction from the attacker.
26.	**Asynchronous Transmission**	The transmission of digital signals without precise clocking or synchronization.
27.	**Audit**	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes.
28.	**Audit Data**	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
29.	**Auditing**	The process of recording activity on a system for monitoring and later review.
30.	**Audit Trail**	A record showing which user has accessed a given resource and what operations the user performed during a given period.
31.	**Authentication**	The process of determining whether a network entity (user or a service) is legitimate. This is usually accomplished through a User ID and Password. Authentication measures are categorized by Something you Know (User ID/Password), Something You Have (smartcard or token), and Something You Are (biometric, like a fingerprint).
32.	**Authentication, Authorization, and Accounting (AAA)**	Authentication confirms the identity of the user or device. Authorization determines the privileges (or rights) of the user or device. Accounting records the access attempts, both successful and unsuccessful.
33.	**Authentication Header (AH)**	An Internet Protocol Security (IPSec) header used to verify that the contents of a packet have not been modified while the packet was in transit.
34.	**Authenticity**	Sometimes included as a security element. It refers to the characteristic of data that ensures it is genuine.
35.	**Authorization**	The conveying of official access or legal power to a person or entity.
36.	**Availability**	The condition of a resource being ready for use and accessible by authorized users.
37.	**Backdoor**	A hidden capability in a system or program for bypassing normal computer authentication systems. A backdoor can be purposeful or the result of malware or other attack.
38.	**Banner Grabbing**	An enumeration technique used to provide information about a computer system. It is generally used for operating system identification (also is known as fingerprinting).
39.	**Baseline**	A point of reference used to mark an initial state in order to manage change.
40.	**Bastion host**	A computer placed outside a firewall to provide public services to other Internet sites and hardened to resist external attacks.
41.	**Biometrics**	A measurable, physical characteristic used to recognize the identify, or verify the claimed identity of an applicant. Things like Facial images, fingerprints, retina measurements, and handwriting are examples.
42.	**bit flipping**	A cryptographic attack, where bits are manipulated in the cipher text to generate a predictable outcome in the plain text once it is decrypted.
43.	**Black-Box testing**	A method of Penetration testing, where the security of a system or subnet is tested, without any previous knowledge of the device or network. It is designed to simulate an attack by an outside intruder (usually from the Internet).
44.	**Black Hat**	An attacker who breaks into a computer system with malicious intent, without the owner's knowledge or permission.
45.	**Block Cipher**	A Symmetric key cryptographic algorithm that transforms a block of information at a time using a cryptographic key. For a block cipher algorithm, the length of the input block is the same as the length of the output block.
46.	**Blowfish**	A symmetric block-cipher data-encryption standard that uses a variable key length that ranges from 32 bits to 448 bits.
47.	**Bluejacking**	Sending unsolicited messages over Bluetooth to Bluetooth-enabled devices, like mobile phones, PDAs, and laptops.

48. **Bluesnarfing** Unauthorized access to information such as a calendar, contact list, emails, and text messages on a wireless device through a Bluetooth connection.

49. **Bluetooth** A proprietary, open, wireless technology used for transferring data from fixed and mobile devices over short distances.

50. **Boot sector virus** A virus that plants itself in a system's boot sector and infects the master boot record.

51. **Brute-force password attack** A method of password cracking where all possible options are systematically attempted until a match is found. These attacks try every password (or authentication option), one after the other, until successful. Brute force attacks take a long time to work and are easy to detect.

52. **Buffer** A portion of memory used to temporarily store output or input data.

53. **Buffer overflow** A condition that occurs when more data is written to a buffer than it has space to store, which results in data corruption or other system errors. This is normally because of insufficient bounds checking, a bug, or improper configuration in the program's code.

54. **Bug** In computers, this is a software or hardware defect that often results in system vulnerabilities.

55. **Business Continuity Plan (BCP)** A set of plans and procedures to follow in the event of a failure or disaster, security related or not, to get business services back up and running. BCPs include a disaster recovery plan (DRP) that addresses exactly what to do to recover any lost data or services due to a natural (or other) disaster.

56. **Business Impact Analysis (BIA)** An organized process to gauge the potential effects of an interruption to critical business operations as a result of a disaster, accident, or emergency.

57. **Cache** A storage buffer that transparently stores data, so future requests for the same data can be served faster.

58. **CAM Table** Content Addressable Memory table. A CAM table holds all of the MAC address-to-port mappings on a switch.

59. **Certificate** In computers, it is an electronic file used to verify a user's identity, providing non-repudiation throughout the system. It is also known as a Digital Certificate. It is also a set of data that uniquely identifies an entity. Certificates contain the entity's public key, serial number, version, subject, algorithm type, issuer, valid dates, and key usage details.

60. **Certificate Authority (CA)** A trusted entity that issues and revoke public key certificates. In a network, a CA is a trusted entiry that issues, manages, and revokes security credentials and public keys for message encryption and/or authentication. Within a public key infrastructure (PKI), the CA works with registration authorities (RA) to verify information provided by the requester of a digital certificate.

61. **Challenge Handshake Authentication Protocol (CHAP)** An authentication method on point-to-point links, using a three-way handshake and a mutually agreed upon key.

62. **CIA Triad** Confidentiality, Integrity, and Availability. These are the three aspects of security and they make up the CIA Triad. This is also sometimes called the CIA Triangle.

63. **Cipher text** Text or data in its encrypted form; the result of plain text being input into a cryptographic algorithm.

64. **Client** In computers, it is a computer process that requests a service from another computer and accepts the server's responses.

65. **Cloning** A cell phone attack in which the serial number from one cell phone is copied to another in an effort to copy the cell phone.

66. **CNAME record** A Canonical Name Record within DNS that is used to provide an alias for a domain name.

67. **Cold site** A backup facility with the electrical and physical components of a computer facility, but with no computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event the user has to move from their main computing location to an alternate site.

68. **Collision** In regard to hashing algorithms, it occurs when two or more distinct inputs produce the same output.

69. **Collision Domain** A domain that is composed of all the systems sharing any given physical transport media. Systems within a collision domain may collide with each other during the transmission of data. Collisions can be managed by CSMA/CD (collision detection) or CSMA/CA (collision avoidance).

70. **Community Cloud** A cloud model, where the infrastructure is shared by several organizations, usually with the same policy and compliance considerations.

71.	**Community string**	A string that is used for authentication in SNMP. The public community string is used for Read-Only searches and the private community string is used for Read-Write. Community strings are transmitted in clear text in SNMPv1. SNMPv3 provides encryption for the strings as well as other improvements.
72.	**Competitive Intelligence**	Freely and readily available information on an organization that can be gathered by a business entity about its competitor's customers, products, and marketing. It can be used by an attacker to build useful information about targets for attack (i.e.- obtaining intellectual property).
73.	**Computer-based attack**	A social engineering attack that uses computer resources such as IRC or email.
74.	**Computer Emergency Response Team (CERT)**	The name given to expert groups that handle computer security incidents. US-CERT is probably the most well-known.
75.	**Confidentiality**	A security objective that ensures a resource can be accessed only by authorized users. This is also the security principle that stipulates sensitive information is not disclosed to unauthorized individuals, entities, or processes.
76.	**Console Port**	Physical socket provided on routers and switches for cable connections between a computer and the router or switch. This connection enables the computer to configure, query, and troubleshoot the router/switch by use of a terminal emulator and a command-line interface.
77.	**Contingency Plan**	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of a disaster, system failure, or other emergency.
78.	**Cookie**	In computers, it is a text file stored within the browser, by a Web server, that maintains the information about a connection. Cookies are used to store information to maintain a unique, but consistent Web surfing experience, but can also contain authentication parameters. Cookies can be encrypted and have defined expiration dates.
79.	**Copyright**	A set of exclusive rights granted by the law of a jurisdiction to the author or creator or an original work. This includes the right to copy, distribute, and adapt the work.
80.	**Corrective Controls**	Controls internal to a system designed to resolve vulnerabilities and errors soon after they arise.
81.	**Countermeasures**	Actions, devices, procedures, techniques, and/or other measures intended to reduce the vulnerability of an information system.
82.	**Covert channel**	A communications channel that is being used for a purpose it was not intended for, usually to transfer information secretly.
83.	**Cracker**	A cyber attacker who acts without permission from, and gives no prior notice to, the resource owner. Also known as a malicious hacker.
84.	**Cross-site Scripting (XSS)**	An attack where the hacker injects code into an otherwise legitimate web page, which is then clicked by other users or is exploited via Java or some other script method. The embedded code within the link is submitted as part of the client's web request and can execute on the user's computer.
85.	**Crypter**	A software tool that uses a combination of encryption and code manipulation to render malware undetectable to antivirus and other security monitoring products.
86.	**Cryptographic key**	A value used to control cryptographic operations, such as decryption, encryption, signature generation, and signature verification.
87.	**Cryptography**	The science or study of protecting information, whether in transit or at rest, by using techniques to render the information unusable to anyone who does not possess the means to decrypt it.
88.	**Daisy Chaining**	A method of external testing where several systems or resources are used together to make an attack.
89.	**Data Encryption Standard (DES)**	An outdated symmetric cipher encryption algorithm, previously approved for U.S. government use, and used by business and civilian government agencies. In modern computing, it is easy to attempt the entire keyspace of DES for cracking, so it is no longer considered secure.

90.	**Data Link Layer**	Layer 2 of the OSI Model. The Data Link Layer provides reliable transit of data across a physical link. This layer is concerned with things like physical addressing, network topology, access to the network medium, error detection, sequential delivery of frames, and flow control. Think of the MAC (physical) address at this layer and of switches.
91.	**Decryption**	The process of transforming cipher text into plain text through the use of a cryptographic algorithm.
92.	**Defense in Depth**	An information assurance strategy in which multiple layers of defense are placed throughout an information technology system. Note: You will likely get sick of hearing about defense in depth, if you work in the security industry.
93.	**Demilitarized Zone (DMZ)**	A partially protected zone on a network that acts as an intermediary between the Internet and your internal network. DMZs are commonly used for things like Web servers that must remain open to the public (Internet), but still access protected resources (like your database).
94.	**Denial of Service (DoS)**	An attack with the goal of preventing authorized users from accessing services and preventing the normal operation of computers and networks. DDoS (Distributed Denial of Service) attacks fall into this category, with the main difference being DDoS attacks are higher in scale. Many DDoS attacks these days use botnets taking advantage of cloud services.
95.	**Detective controls**	Controls to detect anomalies or undesirable events occurring on a system.
96.	**Digital Certificate**	Also known as a Public Key Certificate, a digital certificate is an electronic file that is used to verify a user's identity. It provides non-repudiation throughout the system. Certificates contain the entity's Public Key, Serial Number, Version, Subject, Algorithm type, Issuer, Valid Dates, and Key Usage details.
97.	**Digital Signature**	The result of using a private key to encrypt a hash value for identification purposes within a PKI (Public Key Infrastructure) system. The signature can be decoded by the originator's public key, verifying their identity, and providing non-repudiation. A valid digital signature gives a recipient verification that a message was created by a known sender.
98.	**Directory Traversal Attack**	An attacker attempts to access restricted directories and execute commands outside of the intended Web server directories by using the URL to redirect to an unintended folder location. This attack is also known as the "dot-dot-slash" attack.
99.	**Disaster Recovery Plan (DRP)**	A documented set of procedures to recover business infrastructures in the event of a disaster.
100.	**Domain Name**	A unique hostname that is used to identofy resources on the Internet. Domain names start with a root (.) and then add a top-level (i.e.- .com, .gov, .org) and a given namespace. Example: Microsoft.com
101.	**Domain Name System (DNS)**	A network system of servers that translates numeric IP addresses (i.e.- 192.168.1.1) into more human-friendly addresses (i.e.- Microsoft.com) and vice-versa.
102.	**Domain Name System (DNS) Cache Poisoning**	An attack technique that tricks your DNS server into believing it has received authentic information, when in reality it has been provided false information. DNS cache poisoning affects user traffic by sending it to erroneous or malicious end points, instead of its intended destination.
103.	**Domain Name System (DNS) Lookup**	The process where a system provides a Fully Qualified Domain Name (FQDN) to a local name server, for resolution to its corresponding IP address.
104.	**Doxing**	The process of searching for and publishing private information about a target (usually an individual) on the Internet, typically with malicious intent.
105.	**Droppers**	Malware designed to install some sort of virus, backdoor, etc... onto a target system.
106.	**Dumpster Diving**	This is where an attacker sifts through garbage bins for information that might be useful in an attack. EC-Council considers this a "passive" activity; however, common sense dictates that you will likely be arrested if you jump into a dumpster at a business. For the exam, just focus on dumpster diving being Passive.
107.	**Eavesdropping**	The act of secretly listening to the private conversations of others without their consent. This can be done over telephone lines (wiretapping), email, instant messaging, and other methods of communication that are considered private.

108.	**ECHO reply**	A type 0 ICMP message that is used to reply to ECHO requests. It is used with ping to verify network layer connectivity between hosts.
109.	**EDGAR Database**	A system used by the SEC for businesses and companies to transmit required filings and information. The database is publicly available and potentially a source of information for malicious hackers.
110.	**Encapsulation**	The process of attaching a particular protocol header and trailer to a unit of data before transmission on the network. It occurs at Layer 2 of the OSI model.
111.	**Encryption**	Conversion of plain text to cipher text through the use of a cryptographic algorithm.
112.	**Enumeration**	In penetration testing, enumeration is the act of querying a device or network segment thoroughly and systematically for information.
113.	**Ethical Hacker**	A computer security expert who performs security audits and penetration tests against systems or network segments, with the owner's full knowledge and permission.
114.	**False Negative**	A situation in which an IDS does not trigger on an event that was an intrusion attempt. False negatives are considered more dangerous than false positives.
115.	**False Positive**	A situation in which an IDS or other sensor triggers on an event as an intrusion attempt, when it was actually legitimate traffic.
116.	**Firewalking**	The process of systematically testing each port on a firewall to map rules and determine accessible ports.
117.	**Footprinting**	All measures and techniques taken to gather information about an intended target. This can be passive or active.
118.	**Fragmentation**	The process of breaking a packet into smaller units when it is being transmitted over a network medium that is unable to support a transmission unit the original size of the packet.
119.	**GET**	GET is a command used in HTTP and FTP to retrieve a file from a server.
120.	**Government Access to Keys (GAK)**	An attempt through key disclosure laws to have software companies provided copies of all keys to the government, which will be used only when a warrant is provided during law enforcement efforts.
121.	**honeynet**	A network deployed as a trap to detect, deflect, or deter unauthorized use of information systems.
122.	**honeypot**	A host designed to collect data on suspicious activity.
123.	**HTTP tunneling**	A firewall-evasion technique whereby packets are wrapped in HTTP (port 80) as a covert channel to the target.
124.	**IaaS**	Infrastructure as a Service. IaaS provides virtualized computing resources over the Internet.
125.	**Impersonation**	A social engineering effort in which the attacker pretends to be an employee, a valid user, or even an executive to try and obtain information or access.
126.	**Insider affiliate**	A spouse, friend, or client of an employee who uses the employee's credentials to gain physical or logical access to organizational resources.
127.	**Insider associate**	A person with limited authorized access to the organization, like contractors, guards, and cleaning crews.
128.	**Integrity**	In computer security, it is validating that data is not modified in an unauthorized and undetected manner. Integrity is making sure that the data received is in the same state as when it was sent.
129.	**Interior Gateway Protocol (IGP)**	IGP is an Internet routing protocol that is used to exchange routing information within an autonomous system.
130.	**International Organization for Standardization (ISO)**	An international organization composed of national standards bodies from over 75 countries. ISO standards include 27001 and 27002.
131.	**Internet Control Message Protocol (ICMP)**	A protocol used to pass control and error messages between nodes on the Internet.
132.	**Internet Service Provider (ISP)**	A business, government agency, or educational institution that provides access to the Internet.

133. **Intrusion Detection System (IDS)** A security tool designed to protect a system or network against attacks by comparing traffic patterns against a list of both known attack signatures and general characteristics of how attacks may be carried out. Threats are rated and reported. HIDS (Host-based Intrusion Detection System) and NIDS (Network-based Intrusion Detection System) are two types. Think monitoring or logs.

134. **Intrusion Prevention System (IPS)** A security tool designed to protect a system or network against attacks by comparing traffic patterns against a list of both known attack signatures and general characteristics of how attacks may be carried out. Threats are rated and proactive measures are taken to prevent more significant threats. The main difference by just an IDS and IPS is the IPS is designed to respond to the threat (i.e.- block an IP address) and not to just monitor the threat. In the "real world," you normally just see a combination IDS/IPS device in use.

135. **IpSec (Internet Protocol Security) Architecture** A suite of protocols that are used for securing IP communications by authenticating and encrypting each IP packet of a communication session. This suite includes protocols for establishing mutual authentication between agents at session establishment and for negotiating the cryptographic keys to be used throughout the session.

136. **iris scanner** A biometric device that uses pattern-recognition techniques based on the image of the irises of a person's eyes.

137. **ISO 17799** A standard that provides best-practice recommendations on initiating, implementing, and/or maintaining Information Security Management Systems (ISMS).

138. **Kerberos** An authentication protocol developed at MIT that uses tickets, a ticket granting service (TGS), and a key distribution center.

139. **keylogger** A software or hardware application or device that captures user keystrokes.

140. **LDAP (Lightweight Directory Access Protocol)** LDAP is an industry standard protocol used for accessing and managing information within a directory service; an application protocol for querying and modifying data using directory services running over TCP/IP.

141. **MAC filtering** A method of permitting only MAC addresses in a pre-approved list of network access. Addresses not matching are blocked.

142. **macro virus** A virus written in a macro language and embedded in document (Microsoft Word) or spreadsheet (Excel) files. Most later versions of Microsoft Office automatically disable Macros to protect you from this.

143. **malware** A program or piece of code inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, and/or the availability of the victim's data, applications, or operating system. Malware consists of viruses, worms, and other types of malicious code.

144. **man-in-the-middle (MitM) attack** An attack, where the malicious hacker positions themselves between the client and the server to intercept (and potentially alter) data traveling between the two.

145. **mantrap** A small space having two sets of interlocking doors; the first set of doors must close before the second set opens. Typically authentication is required for each door and normally these use different factor types (i.e.- biometric, keycard, etc...). Note: A mantrap is not something your wife puts out to catch you and make you mow the lawn. That is called love and marriage.

146. **Maximum tolerable downtime** A measurement of the potential cost due to a particular asset being unavailable. This is used primarily as a means to prioritize the recovery of assets should the worst occur.

147. **MD5** A hashing algorithm that results in a 128-bit output.

148. **Multipartite Virus** A computer virus that infects and spreads in multiple ways.

149. **NetBIOS (Network Basic Input/Output System)** An API that provides services related to the OSI model's Session Layer, allowing applications on separate computers to communicate over a LAN.

150. **Network Address Translation (NAT)** A technology, where you advertise one IP address externally and data packets are rerouted to the appropriate IP address inside your network by a device providing translation services. In this way, the IP addresses of machines on your internal network are hidden from external users.

151. **node** A device on a network.

152. **Nonrepudiation** The means by which a recipient of a message can ensure the identity of the sender and that neither party can deny having sent or received the message. The most common method of this is through the use of digital certificates.

153. **nslookup** A network administration command-line tool available for many operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mappings, or any other specific DNS record.

154. **NTLM (NT LAN Manager)** The default network authentication suite of protocols for Windows NT 4.0 that has been retained in later versions of Windows for backward compatibility. NTLM is considered insecure.

155. **PaaS (Platform as a Service)** A cloud computing type geared toward software development, providing a platform that allows subscribers to develop applications without building the infrastructure it would normally take to develop and launch the software.

156. **Packer** A crypter that uses compression to pack malware executables into smaller sizes to avoid detection.

157. **Packet Filtering** Controlling access the a network by analyzing the headers of incoming and outgoing packets and letting them pass or discarding them, based on rule sets created by a network administrator. A packet filter allows or denies packets based on destination, source, and/or/port.

158. **PCI-DSS (Payment Card Industry Data Security Standard)** A security standard for organizations handling credit cards, ATM, and other point-of-sales cards. The standards apply to all groups and organizations involved in the entirety of the payment process (i.e.- from card issuers, to merchants, to those storing/transmitting card information).

159. **PGP (Pretty Good Privacy)** A data encryption/decryption program often used for email and file storage.

160. **piggybacking** When an authorized person allows (intentionally or unintentionally) someone to pass through a secure door, despite the intruder not having a badge.

161. **Polymorphic Virus** Malicious code that uses a polymorphic engine to mutate, while keeping the original algorithm intact; the code changes itself each time it runs, but the function of the code will not change.

162. **POP 3 (Post Office Protocol)** An Application layer protocol used by local e-mail clients to retrieve email from a remote sever over a TCP/IP connection.

163. **POST** AN HTTP command to transmit text to a web server for processing. This is the opposite of an HTTP GET command.

164. **PPTP (Point-to-Point Tunneling Protocol)** A VPN tunneling protocol, with encryption. PPTP connects two nodes in a VPN by using one TCP port for negotiation and authentication, and one IP protocol for data transfer.

165. **private cloud** A cloud model operated solely for a single organization.

166. **private key** The secret portion of an asymmetric key pair, typically used to decrypt or digitally sign data. The private key is never shared and is always used for decryption, with one notable exception; the private key is used to encrypt the digital signature.

167. **proxy server** A device set up to send a response on behalf of an end node to the requesting host. Proxies are generally used to obfuscate the host from the Internet.

168. **public cloud** A cloud model, where service are provided over a network that is open for public use (i.e.- Internet).

169. **public key** The public portion of an asymmetric key pair, typically used to encrypt data or verify signatures. Public keys are shared and are used to encrypt messages.

170. **public key infrastructure (PKI)** A set of hardware, software, people , policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

171. **pure insider** An employee, with all of the rights and access associated with being employed by the company.

172. **Replay Attack** An attack where the hacker repeats a portion of a cryptographic exchange in hopes of fooling the system into setting up a communications channel.

173. **RID (Resource Identifier)** This is the last portion of the SID that identifies the user to the system in Windows. A RID of 500 identifies the administrator account.

174. **rogue access point** A wireless access point that either has been installed on a secure company network without explicit authorization from a local network administrator or has been created to allow a hacker to conduct man-in-the-middle attacks.

175.	**rootkit**	A set of tools (applications or code) that enables administrator-level access to a computer or computer network and is designed to obscure the fact that the system has been compromised. Rootkits are dangerous malware entities that provide administrator control of machines to attackers and are difficult to detect and remove.
176.	**SaaS (Software as a Service)**	A type of cloud computing used as a software distribution model.
177.	**SAM (Security Accounts Manager)**	The SAM file in Windows stores all of the password hashes for the system.
178.	**Sarbanes-Oxley Act (SOX)**	This was created to make corporate disclosures more accurate and reliable in order to protect the public and investors from shady behavior.
179.	**script kiddie**	A derogatory term used to describe an attacker who simply uses easy-to-follow scripts or programs developed by others to attack computer systems and networks, and deface websites.
180.	**Smurf Attack**	A DoS attack, where the attacker sends a ping to the network's broadcast address from the spoofed IP address of the target. All systems in the subnet then respond to the spoofed address, eventually flooding the device.
181.	**SOAP (Simple Object Access Protocol)**	Used for exchanging structured information, such as XML-based messages, in the implementation of web services.
182.	**steganography**	The art and science of creating covert messages or images within another message, image, audio, or video file.
183.	**TKIP (Temporal Key Integrity Protocol)**	A security protocol used in IEEE 802.11i to replace WEP without the requirement to replace legacy hardware.
184.	**tunneling virus**	A self-replicating malicious program that attempts installation beneath antivirus software by directly intercepting the interrupt handlers or the operating system to avoid network.
185.	**Zenmap**	This is just a Windows-based GUI version of nmap.