| | |
|---|---|
| 1. at is Add-N-Edit | Cookie Editor that allows you add and edit "session" and saved cookies; Cookies |
| 2. Inspection | A. Slow; requires Stateful tracking of data; inspects all fields, including variable length. |
| 3. Q. What is Application/Protocol Analysis - NIDS | A. Protocol Analysis works by carefully examining the entirety of protocols and how they operate; IDS has understanding of the logic for a specific application or protocol; any protocol activity that is not known as normal flagged; difficult to implement (few protocol implementations are "standard') (pg 156 - 157) |
| 4. Q. What is Application Proxy | A. Interacts with the application to determine which network services will be required. When a program requires access to the network, the Application Layer will manage requests from the program to the other layers down the stack. |
| 5. Q. What is AppLocker | A. Permits admins to define which exe's can and cannot be run. (Win7/2008R2 and later) |
| 6. Q. What is AppLocker audit only mode | A. Can be used to test out new rules without actually blocking any programs and triggering user complaints. |
| 7. Q. What is Approaches to DiD | A. Deploy measures to reduce, accept, or transfer risk. •4 approaches to DiD: 1.)Uniform protection 2.)Protected enclaves, 3.)Information centric 4.)Threat vector analysis |
| 8. Q. What is APT | A. Update tool (APT-GET) for Debian-based systems, including Kali and, Knoppix and Ubuntu; • Will go out and research the package , see libraries and other programs that the package might need (dependencies), download from Internet, install, present configuration choices to user, and then check its work (Ubuntu) |
| 9. Q. What is APT Information Warfare | A. EXAMPLES: highly sophisticated adversaries who can bypass virtually all of today's "best practice" security controls; primary goal is long term persistent occupation for data theft, intelligence espionage, and other malicious activities; MATURITY: sophisticated, planned over long periods, complex, and targeted; ATTACKERS: nation states, sophisticated adversaries; |
| 10. Q. What is Arbitrary Substitution | A. exchanging one character for the other; easy to break using character frequency analysis |
| 11. Q. What is ARO | A. The estimated frequency at which a threat is expected to occur. Value ranges from 0 to a large number. |
| 12. Q. What is ARP | A. Layer 2 broadcast; Given an IP, determine MAC. Broadcast IP to get physical MAC address; • The scheme used by one host on a LAN to determine the MAC address of another host on the same LAN; allows a host to find the MAC address of another host based upon the IP address. |
| 13. Q. What is Asset Identification and Valuation | A. Step 2 in Risk Management Steps |
| 14. Q. What is Asset Identification and Valuation (Step 2) | A. ID the value of your assets you want to protect, and validate the need to protect them |
| 15. Q. What is Asymmetric Key Cryptosystems | A. uses two keys for encryption: one for encryption, one for decryption. Used for key exchange, authentication, and non repudiation. Ex: RSA, El Gamal, ECC |
| 16. Q. What is Asymmetric Key Exchange | A. Uses public-key technology to encrypt messages. Used for key exchange; dual key pair (public and private); expensive and slow |
| 17. Q. What is Asymmetry | A. essentially is where a fairly small investment or input has a very large effect. |
| 18. Q. What is at.exe | A. to schedule tasks to run automatically on the system (at, schtasks (.exe), Taskschd.msc) Obsolete - should not be used. |
| 19. A. Virtual circuit connections between devices with cell switching through a specialized ATM device. Can be run in ATM | Permanent (PVC) or Switched (SVC) virtual circuit mode; Expensive; good for low-latency traffic such as video; connection-oriented; high-speed backbones that interconnect smaller networks over large distances, must establish a virtual circuit between each other; considered virtual because its communication channel traverse a shared medium; provide QoS/ 53 byes, 5 header, 48 data |

| | | |
|---|---|---|
| | Q. What is | |
| 20. | Q. What is ATM Cell | A. A unit of data transported over an ATM network. Constant in size to facilitate QoS. Always 53 Bytes (48 Bytes of Payload). |
| 21. | Q. What is Attacker Activities | A. Actions include initially compromising a machine to establish a foothold by exploiting one or more vulnerabilities. |
| 22. | Q. What is Attack History | A. A chart showing a brief chronology of attack techniques. |
| 23. | Q. What is Attack Lifecycle | A. 8 step process for attacks created by Mandiant (now FireEye) |
| 24. | Q. What is Attack Lifecycle Model | A. 1.Initial recon, 2.Initial compromise, 3.Establish Foothold, 4.Escalate privileges, 5.Internal recon, 6.Move laterlly, 7.Maintain presence, 8.Complete mission |
| 25. | Q. What is Audit | A. verifying measures are being actually followed by examine the logs and machines. |
| 26. | Q. What is Audit Object Access | A. Used to monitor access to objects in Windows. Works in conjunction with SACLs. |
| 27. | Q. What is AUDITPOL.EXE | A. used to manage local security policy |
| 28. | Q. What is Audit Policy Compliance | A. Maintain & check written change logs. Examine machines themselves. Use Change Control Board (CCB) |
| 29. | Q. What is Authentication | A. process by which you prove you are who you say you are: something you have (SMARTCARD), something you know (PASSWORD), something you are (FINGERPRINT), some place you are (GPS-location) |
| 30. | Q. What is Authentication | A. validate the authenticity of the person they are communicating |
| 31. | Q. What is Authentication - Attacks | A. password guessing, brute force, bypassing authentication mechanisms. |
| 32. | Q. What is Authentication - Forms Based | A. Uses HTML form fields to request the user's authentication credentials |
| 33. | Q. What is Authentication - HTTP | A. User's authentication credentials are sent within the HTTP headers. Basic mode (base-64) and Digest mode (MD5 hash). |
| 34. | Q. What is Authentication - Multifactor | A. The use of more than one "factor" to verify a user's identity. |
| 35. | Q. What is Authentication protocols | A. SAT, Kerberos, NTLM • (SAT-Sec Access Token) One job is to connect both the SID for the user's domain account and the SIDs for the domain groups of which the user is a member to the target server. |
| 36. | A. http authentication, credentials sent in HTTP header; 2 modes: basic mode where credentials sent in clear text or Authentication base 64 encoded or digest mode where credentials send MD5 hash of password; - Web Application | |
| 37. | Q. What is Authorization | A. Should be based on a principle of least privilege; determining what someone has access to or is allowed to do after authentication |

| | |
|---|---|
| Q. What is | |
| 38. Q. What is Automation | A. how to get your work done more quickly and easily with the use of scripts, command line tools, and task scheduler (95%); Vast amount of auditing data can be extracted via command line & scripts |
| 39. Q. What is Automountd (Linux) | A. Mounts and unmounts NFS resources only when needed |
| 40. Q. What is Availability | A. availability=destruction; Accessibility of the data for employees and customers. |
| 41. Q. What is Azure Single Sign-On | A. Windows 8 and later. Link your user account to a Microsoft Account. Planetary roaming profile in OneDrive can sync some settings across all machines. |
| 42. Q. What is Background Intelligent Transfer | A. WSUS Clients download updates using this service. "Drizzles" files down to the client in the background. |
| 43. Q. What is Backup Importance | A. needed for forensics analysis, performing audits against a baseline, disaster recovery, accidental data deletion, compliance with regulations |
| 44. Q. What is Back-up Solutions, Third Party | A. (See list) ARCserve(www.ca.com),Backup Exec and Netbackup(www.symantec.com),Ultrabac(www.ultrabac.com),EMC Networker(www.emc.com),Backup Express(www.syncsort.com),Archive(www.commvault.com),OmniBackII and Data Protector(www.hp.com) |
| 45. Q. What is Baseline | A. more specific implementation of a standard; gets into specific technical details of how a system should be configured from a software and hardware standpoint; baselines are compulsory when adopted by an organization |
| 46. Q. What is Baseline - Documentation | A. A foundation for evaluating policy; made up of several components including Acceptable Use Policy (AUP), checklists, procedures, management directives, etc; survey the organization for everything that is written down; key documents: all applicable policies at all levels, checklists, procedures, management directives, AUP, and system specific hardening documents |
| 47. Q. What is Basic Information Warfare | A. EXAMPLES: generic phishing scams, attacks again organizations with little to no security, weakest in the heard opportunistic approach, cyber techniques available on internet or open source; ATTACKERS: amateur hackers, scam artists; MATURITY: simple, easily accessed tools and not particularly targeted |
| 48. Q. What is Basic methods of encryption | A. Substitution and Permutation. Also, hybrid. |
| 49. Q. What is Basic Mode | A. Basic Mode = base-64; Digest Mode = MD5 hash, used in the users authentication credentials through the HTTP header |
| 50. Q. What is Basics of Secure Coding | A. Initialize all variables before use (pg 71); Validate All user input before use (pg 71); Don't make your app require admin permissions on the server or database (pg 71); Handle Errors, and Don't display errors to end users (pg 71); Employ least privileges/limit access (pg 72); Use Tested, Reliable Libraries or Modules for Common Functions (Authentication, Encryption, Session Tracking) (pg 72); Watch for Vulnerability Notifications in Any Open-source Libraries or Web Parts (Bulletin Board, Shopping Cart, etc.) Utilized (pg 72) |
| 51. Q. What is Bastille (linux) | A. hardening program (reports on how secure system is; shows security issues in order to educate admin; optionally fixes issues but changes can be reverted); works on Linux, HP-UX, Mac OSX |
| 52. A. in IIS a specially hardened box that will withstand tomorrow's new batch of exploits and attack tools bastion host | |
| 53. Q. What is Battista Cipher Disk | A. Each disc (2 total- one slightly smaller) had alphabet around it periphery; Attached in the center, rotate the disks and each letter gives a different value for 'x' in the rotation cipher |

| | |
|---|---|
| Q. What is | |
| 54. Q. What is BCP | A. Defined as a plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency; overarching plan that details recovery from a disaster and business resumption planning, as well as a compilation of other plans (ex. Disaster, End-User recovery plan, Contingency, Emergency response, Crisis Management plan; Last line of defense against Risk that cannot be controlled or avoided by other risk management practices; it also define how a business will restore 100% of the operation including the ability to continue to meet business goals |
| 55. Q. What is BCP-DRP planning mistakes | A. LACK OF: BCP testing, prioritization, plan updates, plan ownership, communication, security controls; limited scope; inadequate evaluation of vendor suppliers and insurance |
| 56. Q. What is BCP-DRP planning process lifecycle | A. •project initiation, (mgmt approval to start the project); •risk analysis; •BIA; •build the plan; •test and validate the plan; •modify and update the plan; •approve and implement the plan |
| 57. Q. What is BCP Key Components | A. PLANNING-Assess, Evaluate; BCP - Prepare, Mitigate; DRP - Respond, Recover |
| 58. Q. What is BCP vs. DRP | A. BCP (Recovery) covers restoration of business processes; DRP (Response to Disruption) cover restoration of critical IT sys |
| 59. Q. What is BCP vs DRP | A. BCP covers restoration of business processes; DRP cover restoration of critical IT sys |
| 60. Q. What is Be Careful patching | A. Any new patch may impact the way your current system/apps function. Test in production lab first |
| 61. Q. What is Bell-LaPadula | A. deals with the control of information flow. It is a linear non-discretionary model. This model of protection consists of the following components: A set of subjects; a set of objects; and an access control matrix. •Focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model; AKA - the multilevel model |
| 62. Q. What is best evidence | A. Refers to a requirement to produce the original of a piece of evidence rather than a mere copy (ex. Snapshot or Mirror Image) |
| 63. Q. What is BIA | A. Primary goal is to determine the Maximum allowable downtime for any given system or MAXIMUM TOLERABLE DOWNTIME (MTD); Prioritizes functions versus risks to identify the criticality of functions and the timeframe for which they must recover; what impact disruptive events might have on business prioritizes, function vs. risk, max allowable downtime |
| 64. Q. What is Big-O notation | A. Used to give a general idea of how many operations a problem takes relative to the input size n; indicates a problems complexity |
| 65. Q. What is Binary Disk Images | A. a special type of backup involves creating a binary image of the desired disk or partition. Image contains complete snapshot of the entire volume, including boot sector. can be searched, edited, updated; • Recent version of Symantec Ghost and Acronis Recovery can be used to backup and restore folders and files without a reboot, deploy software or OS upgrades, create a virtual machine image file, and the image of a drive can be searched and edited. |
| 66. Binding - Network Adapter | A. connection between physical NIC and protocols; path of communication between a network component (like a service or protocol) |

| | | |
|---|---|---|
| | Q. What is | |
| 67. | Q. What is Bindings | A. A binding is an internal communications pathway between networking components Each interface has its own separate binding. |
| 68. | Q. What is Biometrics | A. •Hand: Fingerprint, hand geometry; •Eye: Retina, iris; •Face: thermograms, photo; •Voice print; •Mannerisms: Keystroke, tread, handwriting; •Key factors in selecting biometrics: Reliability, user friendliness, cost for implementation, maintenance |
| 69. | Q. What is Birthday Attack | A. Exploiting the fact that two completely different inputs of plaintext can have the same output in a hash function. Hash collisons related to this probability |
| 70. | Q. What is BitLocker | A. On the fly, or full disk, encryption made by Microsoft. Bundled in pro or business versions of Windows Vista or later; 128/256bit AES HDD sector encryption; transparent to user |
| 71. | Q. What is BitLocker Backup to AD | A. Using GP, the plaintext BitLocker key can be stored in the Active Directory database as well as an encrypted copy of the FVEK key itself. |
| 72. | Q. What is BitLocker Benefits | A. -verification of integrity of boot up files and other start up data structures to prevent rootkits; -sector level encryption of entire hard drive volumes to prevent exposure of confidential data on stolen or lost hard drives |
| 73. | Q. What is BitLocker Emergency Recovery | A. Recovery password can be saved to another (non-encrypted) hard drive volume or USB drive, or printed out for manual re-entry. You can also print to an .xps file. Recall that the recovery password is used when one of the TPM options doesn't work. For example the USB token is lost or the PIN forgotten. |
| 74. | Q. What is BitLocker Requirements | A. Does not require 2 hard drives, but it must have at least 2 NTFS volumes. The system volume cannot be encrypted but the boot volume can. |
| 75. | Q. What is BitLocker TPM options | A. With or without a TPM chip |
| 76. | Q. What is BITS | A. WSUS Clients download updates using this service. "Drizzles" files down to the client in the background. |
| 77. | Q. What is Blended Threat | A. single piece of malware that exploits several methods of propagating. Common for malware specimens particularly WORMS, to possess multiple propagation vectors; increases the number of targets that the worm can infect; EXAMPLE: Nimda |
| 78. | Q. What is Block Cipher | A. Obtained by segregating plaintext into blocks of n character or bits and applying the identical encryption algorithm and key to each block. |
| 79. | Q. What is Bluesnarf Attacks | A. exploit Bluetooth weaknesses at the Application Layer, connecting to a discoverable device without providing security credentials and remotely accessing the device |
| 80. | Q. What is Bluetooth Protecting | A. Configure in non-discover mode, strong PIN (12+ char), pair in trusted environment, encourage vendor to use SIG 2.0 spec / PKI support |
| 81. | Q. What is Bluetooth [Protocol] | A. Used to connect disparate devices (PAN networks); up to 7 simultaneous connections; no LOS requirement |
| 82. | Q. What is Bluetooth Security | A. 4-16 char pin; pin and MAC Address to create encryption; some required fixed pins |
| 83. | A. Sniffing risk when device first pairs; easy to eavesdrop; encryption shown weak; Bluetooth Security Issues | |
| 84. | Q. What is Bluetooth Specification | A. Classes 1-3: (1m, 10m, 100m range); NOT designed for high speed network capability; Max Bandwidth 2.1Mbs (EDR); |

| | |
|---|---|
| Q. What is | |
| 85. Q. What is BNEP | A. The Bluetooth Network Encapsulation Protocol (BNEP) provides this encapsulation by replacing the networking header, such as an Ethernet header, with a BNEP headers. (REF: msdn.microsoft.com); • Bluetooth PANs support up to 7 devices in a single network and can be used for proprietary protocols or standards-based protocols including internet access over IP and the BNEP. (A form of PAN) |
| 86. Q. What is Book or Running Cipher | A. Uses text form a source (books) with a modula 26 addition; text is matched character for character with the plaintext. |
| 87. Q. What is Boolean Exclusive OR | A. (See examples) |
| 88. Q. What is Boot Loader | A. prepares the system to begin executing kernel code. Types: lilo, grub. |
| 89. Q. What is Boot Record Infector/Virus | A. Malware that places malicious code into the boot sector of a device; most often a virus. |
| 90. Q. What is Border Router | A. Placed between ISP and our firewall. Used to filter out certain types of network traffic that are unwanted. |
| 91. Q. What is bridge | A. A network device that connections two network segments or dissimilar networks together; Connects 2 physical segments of a network; maintains track of network addresses, segments traffic, breaks up collision domains; used to connect two physical segments of a network |
| 92. Q. What is Bridged Network | A. Used for: ( Data Center Mode) As if you are all on the same network |
| 93. Q. What is Broadcast Address | A. A broadcast packet is a single packet that is processed by every IP stack on the LAN. The address in a subnet in which all devices within that subnet can receive broadcast messages. |
| 94. Q. What is Broadcast Address, Limited | A. Contain a destination address composed entirely of 1s, which is 255.255.255.255. Its referred to as limited because routers or gateways never pass on these sorts of packets. |
| 95. Q. What is Broadcast Address, Net Directed | A. A fancy way to say that the network number bits in the broadcast address are the same as those in the host's address. They are intended for all hosts with a specific network numer. |
| 96. Q. What is Browsing (attack) | A. The simplest attack you do, you look at the large amounts of data to find compromising information. Open-source searching can reveal sensitive information useful for attacks. |
| 97. Q. What is BRP | A. Is a generic term used to refer to the actionable plan that coordinates efforts to restore an organization to normal working order |

| | |
|---|---|
| 98. Q. What is Brute Force | Q. What is Brute Force |
| 99. Q. What is Brute Force Attack | A. Password crack technique that is very powerful and will always recover the password, it is merely a matter of time. Requires a cracking tool. tools: Jack the Ripper / CAIN |
| 100. Q. What is Brutus | A. A Windows-only tool that allows you to easily import lists of common usernames and passwords and try them out against website and other internet services. •Password Cracker |
| 101. Q. What is Buffer Overflow | A. Can overwrite the return pointer with the pointer of our choice, we can execute the payload that we have inserted. |
| 102. Q. What is Buffer Overflow Defenses | A. Best defense is to patch all vulnerabilities, regularly |
| 103. Q. What is Buffer Overflows | A. If no error checking is performed, buffers can be "overfilled" by inserting extra code, which can be used to execute system commands and overwrite the return pointer. |
| 104. Q. What is Bulletin Board Monitoring | A. Automated and manual monitoring and blocking of offensive keywords, metacharacters, or script language. |
| 105. Q. What is Business Case Application | A. should always map back to risk; if you can't provide proof that systems are at risk, it will be harder to get additional funds for the countermeasures you recommend |
| 106. Q. What is Business Case: Applications | A. Business case should always map back to risk, and document proof to get additional funds for the countermeasures you recommend |
| 107. Q. What is Business Case (Risk Management) | A. Uses qualitative, quantitative, or best practice/checklist risk measurement to define the gap between our current risk status and where we want to be. Used to provide proof to get funds for the countermeasures you need. |
| 108. Q. What is bypassing firewall protection controls | A. audit for wireless and modem connection; application proxy for browsers; commercial tools, IDS/IPS can scan for HTTP tunneling; educate users on social engineering |
| 109. Q. What is CA | A. A certificate authority which everyone within a given operating domain has agreed to trust. |
| 110. Q. What is Cable Modem | A. Broadband internet service over your existing cable TV networks; Competing with DSL; Uses Data Over Cable Interface Specification (DOCSIS), which was the International Telecommunications Union (ITU). Most prevalent for residential users, with some adoption for businesses where available. |
| 111. Q. What is Caesar Cipher | A. A type of ROT-3 invented by Julius Caesar; key space of 25 possible keys |
| 112. Q. What is Cain | A. A powerful password auditing and cracking tool for Windows systems. Normally uses rainbow tables. Supports multiple password-cracking techniques: •Dictionary attack •Brute-force attack •Cryptanalysis attack |
| 113. Q. What is Cain | A. Tool used to dump password hasshes. |
| 114. Q. What is Caligula Virus | A. Located and transmitted victim's PGP key file to creator of the virus via FTP. |
| 115. Q. What is Carrier Sense Multiple Access / Collision Detection protocol | A. Steps taken to communicate: Listen before transmitting, Make sure only one station is transmitting at a time, Monitor transmissions to check for collisions, everyone can speak at the same time, but wont transmit data at the same time. |
| 116. Q. What is Categories of Sub-Controls | A. Quick Wins (QW); Improved Visibility and Attribution (Vis/Attrib); Hardened Configuration and Improved Information Security Hygiene (Config/Hygiene); Advanced (Adv) |
| 117. Q. What is Cathode | A. The output side of a diode. Has a bar on the diode indicating it. |
| 118. Q. What is cat (Linux Cmd) | A. Used to concatenate or display files |
| 119. Q. What is CBC | A. Authorized mode in DES by the NIST |
| 120. Q. What is CCMP | A. more secure protection options for organizations to deploy WLANS; strong encryption, replay and integrity protection |
| 121. Q. What is cd (linux cmd) | A. change directory command linux |

| | | |
|---|---|---|
| 122. | Q. What is Centralized Logging (linux) | A. Protects against log wiping. DOS possibility. Easy to search & scan |
| 123. | Q. What is Certificate Authority | A. Third-party authority who issues and verifys certificates. |
| 124. | Q. What is Certificate-Based Web Authentication | ... |
| 125. | Q. What is Certificate Lifecycles | A. Registration and initialazation, Certifications, Storage, Escrow |
| 126. | Q. What is Certificate Policies Document | A. Specifies how certain certificates are used |
| 127. | Q. What is Certificate Revocation List | A. A list of the certificate serial numbers for all of the certificates that have been revoked by the CA. |
| 128. | Q. What is Certificates | A. •An essential part of PKI; • a digital document attesting the binding of an entity to a public key; •Unique to each entity, equivalent to a passport or driver's license; •mitigates impersonation |
| 129. | Q. What is CFB | A. Authorized mode in DES by the NIST |
| 130. | Q. What is CGI | A. a standard method used to generate dynamic content on Web pages and applications. |
| 131. | Q. What is chage (Linux Cmd) | A. provides an administrator a quick look at the current value for password aging |
| 132. | Q. What is Chain of Custody | A. A concept in jurisprudence that applies to the handling of evidence and its integrity; also refers to the document or paper train showing seizure, custody, control, storage, transfer, and analysis of physical and electronic evidence. |
| 133. | Q. What is Challenges - NIDS | A. Cant analyze encrypted traffic, signature quality is an issue costly for management/monitoring topology limitations |
| 134. | Q. What is Challenges - NIPS | A. must not have false positives, must be able to keep up with network traffic despite deep packet examination; tend to have less extensive rule base with more false negatives that IDS tools |
| 135. | Q. What is Change Control | A. A method of detecting change when it occurs to the baseline outlined in your Configuration Management solution. |
| 136. | Q. What is Change/Defacement Monitoring | A. A mechanism to know if someone has defaced or made other unauthorized changes to parts of the web application. |
| 137. | Q. What is Change Detection and Analysis | A. Use the snapshot file as a baseline for comparison w/ logs to detect changes. |
| 138. | Q. What is chgrp (Linux Cmd) | A. changes group ownership |
| 139. | Q. What is chkconfig (Linux Cmd) | A. Provides an overview of what services are started and what gets started at each run level. #chkconfig -level 2 network off <-- example |
| 140. | Q. What is CHKDSK.EXE | A. Runs automatically after a failure or BSOD. Used to ensure the hard dis is in a consistent state. Can be scheduled upon a reboot. |
| 141. | Q. What is chkrootkit (Linux Cmd) | A. A free unix equivalent of antivirus. Looks for rootkits, sniffers, deleted logs, trojans, etc. chkrootkit -q \| less (Runs in quiet mode and allows you to scroll through the results.) |
| 142. | Q. What is chmod (Linux Cmd) | A. The Linux cmd to change file and directory permissions. |
| 143. | Q. What is Choosing a Passphrase in PGP | A. most critical part; use strong password with many characters with mixed characters; easy to remember and hard to guess |
| 144. | A. change file ownership chown (Linux | |

| | |
|---|---|
| Q. What is<br><br>Cmd) | |
| 145. Q. What is chroot (Linux Cmd) | A. Application isolation (Sandbox) feature that must be enabled on an app-by-app basis. sandbox |
| 146. Q. What is CIA | A. Confidentiality, Integrity, Availability; the three factors in which information can be exploited and which are the goal for security professionals to protect. |
| 147. Q. What is CIA - Availability | A. •Availability vs. destruction; •Accessibility of the data for employees and customers. |
| 148. Q. What is CIA - Confidentiality | A. •Confidentiality vs. disclosure; •Only shared among authorized persons or organizations |
| 149. Q. What is CIA - Integrity | A. •Integrity vs. alteration; •Accuracy of the data; Ensuring an encrypted message has not been altered |
| 150. Q. What is CIA - Prioritizing | A. While all 3 areas of CIA are important to an organization, there is always one area that is more critical than others. Each organization must determine their own priorities: •C: Pharmaceuticals, government •I: Financial Institutions • A: E-commerce-based organization |
| 151. Q. What is CIDR | A. Shorthand notation used to express subnet masks; abbreviation for classless inter-domain routing. Uses variable length sub net mask to allocate ip add to subsets; • Shorthand way of specifying which portion of the address is the network and which portion is the host. ( /8 \| /16 \| /24 \| /32) |
| 152. Q. What is CIFS | A. Similar to SMB with a few enhancements. One of those is not needing NetBIOS. |
| 153. Q. What is CIH | A. Virus programmed to activate every April 26 and overwrite data on infected computer's hard drive; attempted to overwrite system's flash-BIOS, rendering computer unusable. |
| 154. Q. What is Cipher (Encryption Algorithm) | A. A cryptographic transformation that operates on characters or bits; Mathematical formula |
| 155. Q. What is Ciphertext | A. An unintelligible message of a plain-text message. |
| 156. Q. What is CIS | A. A location that has security templates available, and configuration guides to go with them. |
| 157. Q. What is CIS hardening guides | A. Guides created by industry leaders to harden system (scoring tools) |
| 158. Q. What is Civil Law | A. Comprises codified, or written laws, which are supplemented by additional written laws and legislation (Most famous "Code" is the Code Napoleon (the French civil code of 1804) |
| 159. Q. What is Civil Law | A. Deals with adjudicating private disputes between parties; (The Law of Negligence; must owe a duty of care, must be breach, and damage cause by breach); Damage or lose to an individual or business; no jail time; financial restitution; Preponderance of evidence (O.J. Simpson) |
| 160. Q. What is Class A network | A. range of 1.0.0.0 through 127.255.255.255 First bit starts with zero 8 bits only 126 on internet 255.0.0.0 |
| 161. Q. What is Class B network | A. range of 128.0.0.0 to 191.255.255.255 first bit of network is 10 subnet is 255.255.0.0 10 bits over 16,000 on internet |
| 162. Q. What is Class C network | A. range of 192.0.0.0 - 223.255.255.255 first 3 bits 110 subnet 255.255.255.255.0 21 bits 8 bits for host over 2,000,000 on net |
| 163. Q. What is Client Certificate | A. A digital file with a cryptographic signature that is provided to the user either by the website owner or a trusted third party. |

| | |
|---|---|
| 164. Q. What is Client editions | A. Each client OS is normallyreleased in multiple editions, and it's important for security, manageability, and licensing to install the correct one. |
| 165. Q. What is Client Hyper-V | A. A version of Microsoft's Hyper-V hypervisor that is able to be run on top of Windows instead of running on bare metal. |
| 166. Q. What is Client OS | A. Intended for devices such as phones, tablets, laptops, and PC workstations. |
| 167. Q. What is Client Ports | A. are normally session source ports that are only selected for a particular connection and are then made available to be reused after the connection is freed. Ephemeral ports are usually numbered higher than 1023; the largest possible ephemeral port is 65535. |
| 168. Q. What is Client to Site / Transport Remote Access - VPN | A. Provides remote access from a remote client back to corporate network; Established between client computer and a gateway devices located at border of corporate network |
| 169. Q. What is Client / Transport Remote Access - VPN | A. Provides remote access from a remote client back to corporate network; Established between client computer and a gateway devices located at border of corporate network |
| 170. Q. What is CLOSED | A. No connection between the two hosts. |
| 171. Q. What is Clustering | A. Situation in which a plaintext message generates identical ciphertext messages using the same transformation algorithm, but with different cryptovariables or keys. |
| 172. Q. What is cmdlet | A. A tool run within PowerShell. |
| 173. Q. What is Code Napoleon | A. The French Civil Code of 1804 named after its creator, Napoleon Bonaparte, that significantly influenced Civil Law all over the world. |
| 174. Q. What is Codes | A. A cryptographic transformation that operates at the level of words or phrases. |
| 175. Q. What is Collisions | A. Multiple devices using the same access media at the same time. Mitigated with CSMA. |
| 176. Q. What isCombining NTFS and Share DACLs | A. breakdown of what permissions will trump others |
| 177. Q. What is Commercial Classification Levels | A. •Public Releasable; •Business proprietary, contracts, financials; • Trade secrets, manufacturing proprietary; •HR and management sensitive |
| 178. Q. What is Computational Complexity | A. Deals with time and space requirements for the execution of algorithms, helps to classify the problem as either tractable (EASY) or intractable (HARD) |
| 179. Q. What is Computer Attacker Activities these Controls are Designed to Help Thwart | A. 1)Initial Compromise "Getting In"; Maintain Long-Term Access to Compromised Systems: "Staying In"; Cause Damage: "Acting" |
| 180. Q. What is Computer-based Social Engineering | A. uses computer interface to trick into giving up info ex pop up asking to re enter user name and password |
| 181. Q. What is Confidentiality | A. confidentiality = disclosure ; only shared among authorized persons or organizations |
| 182. Q. What is Confidentiality Attacks | A. Attacks for intelligence, theft software, fraud, perception management. Increase value to the Offense. |
| 183. Q. What is Configuration Management | A. discipline of establishing a known baseline condition, and then managing that condition; 2 change categories: repairs and improvements (new construction); need 2 things for config management: an accurate baseline document and a way to detect when a change occurs to that baseline |
| 184. Q. What is Confirming a Signed Email | vA. Choose to verify the signature |
| 185. Q. What is Conflicker Worm | A. Infected millions though three methods: vulnerability in MS Server Service, brute force of admin passwords through network shares, removable devices given an malicious auto run script. |
| 186. Q. What is Constant Time | A. take the same number of operations to solve regardless of the input size |
| 187. A. Step 3 of the Six Step Incident Handling Process. The goal of this process is to stabilize the environment; Containment Stabilize, Backup, secure area, change passwords locally 3 - Incident Handling | |

Q. What is

| | |
|---|---|
| 188. Q. What is Contents Scrambling System (CSS) | A. DVD encryption standard; 40-bit key length (inadequate even then) |
| 189. Q. What is Controlling Access | A. •Least Privilege, •Need to Know, •Separation of Duties, •Rotation of Duties |
| 190. Q. What is Controls Types | A. 1.Detection 2.Corrective(Response) 3.Prevention |
| 191. Q. What is Controls Why are they important (1) | A. Cyber security is complex and becoming even more complicated everyday, Organizations are being compromised, even after spending large portions of their budget on infosec, CIOs and CISOs need prioritized controls to get the most return from their investment; More controls rarely hurt; It's critical to have priorities!! |
| 192. Q. What is Controls Why are they important (2) | A. We need agreement among: (IG's-auditors), Operations (sys-admins), Security engineers; Need metrics and measurements that everyone can agree to use; Need to stop people from violating systems and compromising the confidentiality and integrity of our data. |
| 193. Q. What is Cookies | A. A named piece of data created by a Web server and stored at the Web browser; name and contents of a cookie are determined by the application; 2 Types of cookies; Persistent and Session (non-Persistent); • Persistent cookies have a expiration dates, after which time the browser will delete them. Session cookies are good only during the current browser session; • Cookies defined (pg 64 par 4); Explains how a Cookie works (pg 64 par 5); Types of Cookies persistent cookie and session cookie (pg 65 par 1-2); Cookie Concerns (pg 65-66) |
| 194. Q. What is Cookie Server side | A. After a cookie is set on a system browsing the web, the cookie is designated to be sent to the server from which it originated. (A cookie is designated to be sent only to the server from which it originated, or to other servers in the domain in which the server resides. It is not just for client use as the server uses it to maintain state. Other servers that are trusted by the browser, but that were not the originating server/domain will not be sent the cookie.) |
| 195. Q. What is Cookies, NonPersistent | A. Session cookies; cookies that are only good during the current browser session and are lost forever when the user exits the browser. |
| 196. Q. What is Cost Benefit Analysis | A. •Cost of the safeguard versus the actual value of the asset; •Comparison of the cost of implementing countermeasures with the value of the sset |
| 197. Q. What is Cost Benefit Analysis Final report | A. Includes the interim report, safeguard selection, risk mitigation analysis, cost benefit analysis, and recommendations. |
| 198. Q. What is Council on CyberSecurity | A. Non-Profit group is the Official home of the Critical Security Controls; • Independent, global organization committed to an open and secure internet.; sustain the adoption of cybersecurity best practice; This group manages the actual documentation and updates to the controls themselves. |
| 199. Q. What is cp (Linux Cmd) | A. used to copy a file from one location to another. |
| 200. Q. What is Cracking Attack Protection | A. protect encrypted passwords, strong passwords, one time passwords, disable LANMAN, |
| 201. Q. What A. States the issue, ID the players, find all relevant docs, define policy, identify penalties for non-compliance, make is enforceable, submit for review and approval Creating the Security Policy | |

| | | |
|---|---|---|
| 202. | Q. What is CREATOR OWNER Group | A. Special group that acts as a stand-in for anyone as the current owner. You can grant permissions to the CREATOR GROUP once, and, even if the owner of a folder or file changes, the permissions you granted still applies to the new owner. |
| 203. | Q. What is Criminal Law | A. victim is society; purpose of prosecution is punishment; deterrent effect of punishment; burden of proof is reasonable doubt; felonies jail for greater than one year; misdemeanors jail for less than one year |
| 204. | Q. What is Critical Controls Versus Other Standards | A. The focus of the controls is assurance, not compliance |
| 205. | Q. What is Critical Security Controls | A. Consensus document of 20 crucial controls; • See Chart; • Securing our nation against cyber attacks; |
| 206. | Q. What is Critical Security Controls (Sub Controls ) | A. •The intent of Identifying Quick Wins areas is to highlight where security can be improved rapidly. Labled as (QW) •Attribution is associated with determining which computer system, and pottentially which users, are generating specific events. Improve visibility and attribution support organiizations in detecting attack attempts, locating the points of entry for successful attacks. This control help to increase an organizations situational awareness of it enviroment. These items are lable as (Vis/Attrib); •Improve the information security stance of an organization by reducing the number and magnitude of potential security vul. As well as improving the operations of networked computer systems. Control focuse on protecting against poor sec. practice by system admins. and end users. labled as (Config/Hygiene) •These items are designed to further improve the security of an organization beyond the other three cat. Orgs. Already following all of the other controls should focus on this category. Lable called (Advance) |
| 207. | Q. What is Critical Security Controls Versus Intrusion Kill Chain | A. Regardless of which model you choose the effects are the same |
| 208. | Q. What is Critical Security Controls Versus NIST | A. The Critical Security Controls are technical controls , not operational controls. A sub-set of the NIST |
| 209. | Q. What is Critical Security Controls: What is the Point | A. Monitor, detect, analyze, protect, report, and respond against known vulnerabilities, attacks, and exploitations and continuously test and evaluate information security controls and techniques to ensure that they are effectively implemented. |
| 210. | A. A list of the certificate serial numbers for all of the certificates that have been revoked by the CA. CRL | |
| 211. | Q. What is Cron | A. Task scheduler for Linux; works in total sync with system clock |

Q. What is

| | |
|---|---|
| 212. Q. What is Cross Error Rate | A. The rate at which the FAR and FRR (also: Equal Error Rate (EER) are equal; and is the generally accepted measure for a biometric system accuracy |
| 213. Q. What is Cross Forest Trust | A. Creates a trust between two forests, all domains in both forests will trust each other. Can be one way or two way. Are transitive. Can be 1 or 2 way. Do not replicate across domains. |
| 214. Q. What is Cross Site Scripting | A. Problem resulting from poor input validataion includes JavaScript, images,inline frames. |
| 215. Q. What is Cross-Site Scripting | A. Cross-Site Scripting (XSS) problem resulting from poor input validation; if user input is echoed back to users, HTML can be inserted into a page (includes JavaScript, images, inline frames) (dangerous for multi-user apps, rendering actions on behalf of other users) (pg 93); Can be leveraged to steal cookies, session data; crafted links can manipulate trust of target site; affects HTTP and HTTPS (pg 94); Cross-Site Scripting Defenses avoid reflecting user input back to the web site; filter (i.e. delete problem characters, especially <>()' " # and &); Translate/Encode convert to URLEncoding: < > ... ; Validate i.e. error out if unsafe data is found (pg 95) Ref: http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/cross-site-malicious-content.html |
| 216. Q. What is Cross Site Scripting - Defenses | A. avoid reflecting user input back to the web site; filter; translate and encode; validate |
| 217. Q. What is Cross-Site Scripting Input Attacks | A. If user input is echoed back to the users, HTML may be inserted into a page; includes JavaScript, images; can be used to steal cookies, session data. Effects HTTP & HTTPS; results from poor input validation |
| 218. Q. What is Cryptanalysis | A. Act of obtaining the plaintext or key from ciphertext that is used to obtain valuable information and to pass on altered or fake messages to deceive the original intended recipient |
| 219. Q. What is Cryptanalysis (Analytic) | A. Uses algorithms and mathematics to deduce key or reduce key space to be searched |
| 220. Q. What is Cryptanalysis, Analytic | A. Using algorithms and mathematics to deduce key or reduce key space to be searched. |
| 221. Q. What is Cryptanalysis (Differential) | A. Applies differential analysis with linear analysis, you can see the difference but can't control the input/output |
| 222. Q. What is Cryptanalysis, Differential | A. Analyze resultant differences as related plaintexts are encrypted using a crypto key. |
| 223. Q. What is Cryptanalysis (Differential Linear) | A. Analyzes resultant dirrerences as related plaintests are encrypted using a crytographic key |
| 224. Q. What is Cryptanalysis, A. Applying differential analysis Differential Linear | |
| 225. Q. What is Cryptanalysis (Linear) | A. Linear analysis of pairs of plaintext and ciphertext, control input and output |
| 226. Q. What is Cryptanalysis , Linear | A. Linear analysis of pairs of plaintext and ciphertext |
| 227. Q. What is Cryptanalysis (Statistical) | A. Uses statistical characteristics of language or weaknesses in keys |

| | | |
|---|---|---|
| 228. | Q. What is Cryptanalysis, Statistical | A. Using statistical characteristics of language or weaknesses in keys. |
| 229. | Q. What is Cryptanalysis Types | A. Analytic Statistical Differential (Definitions in Index) |
| 230. | Q. What is Cryptanalysts | A. Dedicate their lives to breaking ciphers |
| 231. | Q. What is Cryptanalytic compromise | A. capturing key strokes; faulty cipher; humans fail to protect their keys-(Soc Eng) |
| 232. | Q. What is Cryptogram | A. An unintelligible message. |
| 233. | Q. What is Cryptographers | A. Computer scientists that creates encryption algorithms |
| 234. | Q. What is Cryptographic Algorithm | A. A step-by-step procedure used to encipher plaintext and decipher ciphertext. |
| 235. | Q. What is Cryptography | A. The art / science of hiding the meaning of communications from unintended recipients. "Hidden Writing"; a main goal is to help fend off eavesdroppers. |
| 236. | Q. What is Cryptography, Applying it at different levels | A. Application layer; Transport Layer |
| 237. | Q. What is Cryptography Goals | A. confidentiality, integrity, authentication, and non-repudiation |
| 238. | Q. What is Cryptology | A. generic term for the study of both cryptography and cryptanalysis; encompasses both |
| 239. | Q. What is Crypto vs. Stego | A. crypto provides confidentiality; stego provides secrecy |
| 240. | Q. What is Crytosystem | A. The collection of all possible inputs and all possible output, in addition to the algorithm and keys; 3 types Symmetric, Asymmetric, and Hashing; Goals are C-I-A-N |
| 241. | Q. What is Crytptanalysis | A. The study of crypto systems and trying to break them. |
| 242. | A. These controls are NOT meant to supersede NIST (800-53 or others); CSC are a subset of the Priority 1 items in CSC vs. NIST NIST 800-53; CSC are technical only in nature, they don't address personnel and physical security controls; These are technical "high water mark"; Implementation and auditing priorities... audit CSC first, then audit remaining 800-53 controls next | |
| 243. | Q. What is CSC vs. Other Standards | A. NIST SP 800-53rev3 comprehensive SEC program covers almost all info sec; The same theory of mapping the SCS to other regulations could be applied; The goal is same, regardless of the standard, prioritize tech controls for protecting systems; These controls are just applicable to both public and private sector organizations; The focus of the control is assurance, not compliance. |
| 244. | Q. What is CSMA/CD protocol | A. Steps taken to communicate: Listen before transmitting, Make sure only one station is transmitting at a time, Monitor transmissions to check for collisions, everyone can speak at the same time, but wont transmit data at the same time. |
| 245. | Q. What is Cubic time | ... |
| 246. | Q. What is CUPS | A. Service that enables printing |
| 247. | Q. What is CWR | A. associated with a protocol known as ECN |
| 248. | Q. What is Cyber Kill Chain | A. 7 step lifecycle for attacks created by Lockheed Martin |
| 249. | Q. What is Cyber kill Chain | A. 1.Reconnaissance, 2.Weaponization, 3.Delivery, 4.Exploitation, 5.Installation, 6.Command and Control, 7.Actions on Objectives |
| 250. | Q. What is Cycle Time | A. Time between something being considered secure and being considered insecure; also refers to time between vulnerability announcement, patch availability, and release of malware to exploit vulnerability. |
| 251. | Q. What is Cygwin | A. A Windows program that allows you to compile Linux based tools for Windows machines. NOT a Linux emulator. |

Q. What is

| | | |
|---|---|---|
| 252. | Q. What is DAC | A. tag files, Group Policies |
| 253. | Q. What is DAC Access Control | A. Access managed by users. (Used by most Linux Variants "book 6, pg 211"); Consists of something a user can manage(ex. Username and password); least restrictive |
| 254. | Q. What is DACL | A. A set of NTFS permissions on a folder or file. |
| 255. | Q. What is DACL evaluated | A. Note that the MIC is independent from and enforced prior to any DACL permissions that might otherwise have allowed the edit or deletion. |
| 256. | Q. What is Danger | A. Anything that would negatively affect the confidentiality, integrity, or availability of your systems or services. |
| 257. | Q. What is Data Classification | A. 2 Primary categories: information cleared for release to public and private information; classification is the responsibility of the data owner; no organization has sufficient resources to protect all info to the highest level so it is often classified into differing levels so that appropriate protections can be applied based on the sensitivity of the info and the potential impact of loss |
| 258. | Q. What is Data Diodes | A. a Diode is a semiconductor device with two terminals, allowing the flow of current in one direction only.a Data Diode typically references military technology that moves data into classified networks without the risk of leaking classified information; little to no electrical resistance to current in one direction. |

| | | |
|---|---|---|
| | Q. What is | |
| 259. | A. Connects the physical part of the network (cables and electrical signals) with the abstract part (packets and data Data Link streams). Layer | |
| 260. | Q. What is Data Normalization | A. IDS uses Data normalization to take data and baseline it before analysis; attackers try to denormalize traffic to evade detection (numerous opportunities are available to do this); IDSs normalize data for understood protocols; gives the analyst a consistent basis for traffic analysis and rule generation (pg 160) |
| 261. | Q. What is dd (Linux Cmd) | A. A Linux cmd that can backup a partition of a hard drive as a means to ensure a mitigation or recovery step is offered. |
| 262. | Q. What is DDoS attacks | A. An attacker recruits zombie systems ahead of time to simultaneously release a flood of traffic at a specific target. Several common tool for accomplishing this: TFN, Trinoo, Stacheldracht and TFN2K. |
| 263. | Q. What is DEA (and DES) | A. Based on the Lucifer cipher developed by IBM it was adopted as the national standard for encryption of unclassified data in 1975, then later became the most commonly used encryption algorithm in the world. Not considered secure anymore; 56bit fixed key length; Only owrks if the cipher algorithm is not a group; • DES is NOT a group. LANMAN uses DES. |
| 264. | Q. What is Debugger | A. Application that allows you to examine and control a running program or OS to troubleshoot or reverse engineer it. • The Debug Programs privilege permist a user to attach a debugger to any process, even if that user did not launch the process being debugged. This is dangerous because a process might contain sensitive information in cleartext or the integrity of the process could be undermined. A DDL Injection attack requires the Debug Programs privilege to work beacuse this attack modifies a running process by injecting a new thread into the address space of the target process. |
| 265. | Q. What is Decoding an IP Header | A. Byte order 0-19; Byte 0=version, (IHL #x4); Byte 1=Type of Service; Byte 2-3=Packet Length, Byte 4-5=IPID, Byte 6=Flags(must convert to Binary; top 3 bits most is reserved, middle is DON'T Frag, least MORE Frags), byte 7 + last 3 bits of 6= Fragment offset, Byte 8=TTL, Byte 9=Embedded Protocol, Byte 10-11=Checksum, Byte 12-15=Source IP, Byte 16-19= Destination IP |
| 266. | Q. What is Decrease Availability | A. Theft, DoS, sabotage; Decreases value to the Defense |
| 267. | Q. What is Decrease Integrity | A. Tamper, penetrate, fabricate; Decreases value to the Defense |
| 268. | Q. What is Decrypting Inbound email | A. Copy it to clipboard or double-click the attachment, PGP window opens, enter your passphrase, the net of two actoins, the encryption with the public key and decryption with the private key, results in the clearest image. |
| 269. | Q. What is Decryption | A. The process of transforming an encrypted message back into its original plaintext form |
| 270. | Q. What is DeCSS 1.2b | A. Program that pulls encryption info off a DVD and stores it. |
| 271. | Q. What is Dedicated Lines | A. A leased line between sites that is physically private and isolated from other traffic. Commonly used are T1, T3, E1, and E3 lines. Predictable availability of bandwidth, reliability of the connection, and confidentiality of the transported data. Primary disadvantage: Very costly |
| 272. | Q. What is Deep Vs Shallow Packet Inspection | A. Two different mechanisms for examining packets on the network; Shallow packet inspection: fast, but provides little fidelity; examines header information, limited payload data; Deep packet inspection: SLOW, requires stateful tracking of data; inspects all fields, including variable-length fields; in practice, both are used together (pg 158 - 159) |
| 273. | Default Domain vs OU GPOs | A. default domain applies to everyone in the domain when GPO assigned to OU GPO only for computers users in that OU |

| | | |
|---|---|---|
| | Q. What is | |
| 274. | Q. What is Defense-inDepth | A. one of our most important tools as a defender. Learn to think like the attacker, see through their eyes. |
| 275. | Q. What is Defense - Social Engineering | A. develop appropriate security policies; train your users on how to detect social engineering; establish procedures for granting access and reporting violations; educate users about vulnerabilities and how to report suspicious activity |
| 276. | Q. What is Define Risk | A. Risk=Vulnerability x Threat. Vulnerability: A weakness in a system that can be exploited. Threat: Any event that can cause an undesirable outcome |
| 277. | Q. What is Delegation of Authority in AD | A. Each OU should have its own 'OU Admins' group that manages that OU |
| 278. | Q. What is Denial of Service | A. A DoS attack occurs when a user is deprived of the use of some data, computing resource or service due to malicious actions on the part of an attacker. Smurf, SYN floods and DDoS attacks are some of the different types of DoS attacks. |
| 279. | Q. What is DES (and DEA) | A. Based on the Lucifer cipher developed by IBM it was adopted as the national standard for encryption of unclassified data in 1975, then later became the most commonly used encryption algorithm in the world. Not considered secure anymore; 56bit fixed key length; Only owrks if the cipher algorithm is not a group. DES is NOT a group. LANMAN uses DES. |
| 280. | Q. What is Desktop / Personal Firewalls | A. Stateful packet filter; application and OS control; endpoint security suites focus on desktop lockdown which includes personal firewalls; packet filter approach looks at packets coming from the network to the PC and tend to treat the PC as the trusted domain. |
| 281. | Q. What is DES weaknesses | A. non-secure; crackable in short period of time; key length of 56 bits |
| 282. | Q. What is Detection and Techniques | A. Goal is to fix the problem not addressing the symptom. |
| 283. | Q. What is Developing Secure Web Applications | A. Security Training for Developers explains best practices (pg 69); Peer Review examination of source code (pg 69); Formal Testing testing program or software for errors (pg 69); Performance Testing testing functionality, application performance, or load testing (pg 70); Configuration Management and Version Control (pg 70); Staging and Development best practices for development, testing and production (pg 70) |
| 284. | Q. What is Developments in NIDS | A. Developments: reduction of false-positive reporting through target OS identification; integrated vulnerability assessment for threat profiling/alert prioritization; NIDS integration in networking devices; IDS for wireless networks (pg 180 - 181) |
| 285. | Q. What is device driver rollback | A. related to system restore enables you to roll a driver back to the previous version |
| 286. | Q. What is df (Linux Cmd) | A. A Linux cmd that displays the currently mounted partitions. |
| 287. | Q. What is Dictionary Attack | A. Password crack technique that tests all the words in a dictionary or word file against the password hashes. The fastest method for cracking passwords is a dictionary attack. |
| 288. | | A. The use of multiple layers of protection to guard against failure of a single security component. One element of DiD DiD is the principle of resource separation, which we will use when dividing the internal network into several sections. |

| | | |
|---|---|---|
| | Q. What is | |
| 289. | Q. What is DiD | A. a comprehensive, integrated approach in which multiple solutions are tiered together to accomplish a goal; any layer of protection might fail so multiple levels of protection must be deployed; measures must be across a wide range of controls; integrated defense in depth; prevention is ideal but detection is a must, but detection w/o response has minimal value; 4 approaches: uniform protection, protected enclaves, information centric, threat vector analysis •Multiple levels of protection; •There is no magic solution when it comes to network security; •Any layer of protection might fail; •Measures must be across a wide range of controls; "Prevention is ideal but detection is a must; however, detection without response has minimal value." |
| 290. | Q. What is DiD - Approaches to | A. Deploy measures to reduce, accept, or transfer risk. •4 approaches to DiD: 1.)Uniform protection 2.)Protected enclaves, 3.)Information centric 4.)Threat vector analysis |
| 291. | Q. What is DiD Information Centric | A. Starts with an awareness of the value of information within an organization; Identify critical assets and provide layered protection, Data accessed by apps, apps on host, host on network |
| 292. | Q. What is DiD Protected Enclaves | A. Segmenting your network by implementing multiple VPNs, VLAN segmentation of switches, or firewalls over a single network; •Work groups that require additional protection are segmented from the rest of the internal organization; •Restrict access to critical segments; •Internal firewalls; •VLANs and ACLs |
| 293. | Q. What is DiD Uniform Protection | A. •Most common approach to DiD; •Firewall, VPN, Intrusion Detection, Antivirus, Patching, etc; •All parts of the organization receive equal protection; •Treats all of the systems the same; - no special consideration or protection is given to the critical intellectual property of an organization; more vulnerable to malicious insiders because systems are not separated or categorized within the network; WEAKEST APPROCH |
| 294. | Q. What is DiD VectorOriented | A. Involves identifying various vectors by which threats can become manifested and providing security mechanisms to shut down the vector; •threat requires a vector to cross the vulnerability; •Stop the capability of the threat to use the vector: -USB thumb drives: Disable USB; -Auto-answer modems: Digital phone PBX |
| 295. | Q. What is Differential Cryptanalysis | A. Analyze resultant differences as related plaintexts are encrypted using a crypto key. |
| 296. | Q. What is Differential Linear - Cryptanalysis | A. Applying differential analysis |
| 297. | Q. What is Diffie-Hellman key exchange | A. USES PUBLIC KEY TECHNOLOGY TO EXCHANGE A SYMMETRIC KEY AND USE A SYMMETRIC ALGORITHM TO ENCRPYT ALL MESSAGES; key exchange method that uses asymmetric encryption to establish a symmetric session; key exchange mechanism to ensure that two parties can determine the SAME secret keying the presence of an adversary over a nonsecure network; |
| 298. | Q. What is Digest Mode | A. Digest Mode = MD5 hash; Basic Mode = base -64, used in the users authentication credentials through the HTTP header |
| 299. | Q. What is Digital Certificates | A. Standard for digital certificates is the x.509 certificate, each one contains: demographic data, validity period, supported encryption algorithm, public/private key, signature by issuing CA; credential used to help someone decide whether a key is genuine; X.509 is standard |
| 300. | Q. What is Digital Signature | A. Form of Asymmetric Encryption where you encrypt the hash output of something with your private key so it can be freely decrypted with your public key to verify the integrity of the contents and to authenticate the sender; Use public-key cryptography to "sign" a document; signatures are provably authentic and nonrepudiable |
| 301. | A. (Encrypt apply Plaintext (in binary format) with Key (in binary format) then Boolean XOR.) (DECRYPT is apply Digital the XOR to Key for the Plaintext result) Substitution | |

| | |
|---|---|
| Q. What is | |
| 302. Q. What is Direct Access | A. Provides dynamically built IPSec tunnels to VPN back into a corporate network when a domain workstation attempts to connect to a domain resource while not on the corporate network. |
| 303. Q. What is Direct Evidence | A. Evidence gathered from an eye witness or the person who watched or logged an incidence as it occurred. |
| 304. Q. What is Disable Services | A. Service Control Manager = "SC.EXE"; services tool; security template; group policy object. disable any and all services that are not essential to the systems function |
| 305. Q. What is DISA STIG | A. Directive 8500.1 requires that all DoD computers be configured using security configuration guidelines developed by DISA and the NSA. |
| 306. Q. What is Discrete Logarithm problem for finite fields | ... |
| 307. Q. What is Distribution Groups | A. groups can only be created in native mode or better domains |
| 308. Q. What is DNS | A. Static host tables; Converting IPs to hostnames; DNS hierarchy; Types of DNS queries; UDP/TCP 53 |
| 309. Q. What is DNS Cache Poisoning | A. The ability to put false data into a DNS cache on a DNS server. |
| 310. Q. What is DNS DoS | A. Involve flooding legitimate DNS servers with large number of queries |
| 311. Q. What is DNS Footprinting | A. Involves using DNS data to learn about servers in a network; done by requesting zone transfers against improperly configured DNS servers |
| 312. Q. What is DNS forward lookup | A. forward lookup - maps fully qualified domain name (FQDN) to IP |
| 313. Q. What is DNS (linux) | A. Significant security issues: spoofing, DoS, buffer overflow, ect |
| 314. Q. What is DNS maps Domain Name Sever (DNS) | A. DNS maps domain names (Application Layer) to IP addresses (Network Layer). We also use ARP to map IP addresses (Network Layer) to MAC addresses (the Data Link Layer hardware address). This diagram sows how all of those pieces fit together. |
| 315. Q. What is DNS Queries | A. Gethostbyname: forward lookup, Gethostbyaddr: reverse lookup; • Use a DNS client utility like nslookup |
| 316. Q. What is DNS Record Type | ... |
| 317. Q. What is DNS reverse lookup | A. reverse lookup - maps IP to FQDN (Fully Qualified Domain Name) |
| 318. Q. What is DNS security | A. Keep DNS software up too date; distribute authoritative DNS servers; Limit zone transfers; limit recursive lookups; register with reputable registrars; split DNS |
| 319. Q. What is Documentation Baseline | A. A foundation for evaluating policy; made up of several components including Acceptable Use Policy (AUP), checklists, procedures, management directives, etc; survey the organization for everything that is written down; key documents: all applicable policies at all levels, checklists, procedures, management directives, AUP, and system specific hardening documents |

| | | |
|---|---|---|
| 320. | Q. What is Document controls | A. numerous entities working together to proved feedback into the attacks that they are seeing and the Contributors that they have found, which are helpful in truly combating these threats |
| 321. | Q. What is DoD / federal classification levels | A. list of classifications: TS, Secret, Confidential, Sensitive but Unclassified, Unclassified |
| 322. | Q. What is Domain controllers | A. a server which helps manage AD database |
| 323. | Q. What is Domain Group Policy Objects | A. auto downloads at startup, shutdown, logon, & logoff |
| 324. | Q. What is Domain Hierarchy | A. •two types of top level domains: Generic (.aero, .biz, .com, .coom, .edu, .gov, .info, .int, .mil & etc) and Country Code(: .uk, .de, .jp, .us, and so on) •Plus a special top-level domain (.arpa) for Internet infrastructure. Country Code: .uk, .de, .jp, .us, and so on) |
| 325. | Q. What is DoS | A. resource exhaustion; when a user is deprived of the use of some data, computing resource, or service due to malicious actions on the part of an attacker EXAMPLE: smurf, SYN flood, DDoS |
| 326. | Q. What is DoS Attack | A. shutdown of network through flooded data sent to device (overload of info resulting in shutdown) |
| 327. | Q. What is DoS Attack Mitigation | A. IDS, response strategies; understand impact of DoS attack |
| 328. | Q. What is TCP Options - Calculating Variable Length Fields | A. TCP options and the length of payload are variable width fields. •We calculate some field length using other header information and fixed lengths: TCP options length = (TCP header length - Min. TCP header length) Length of packet payload = IP total length - (IP header length + TCP header length) |
| 329. | What is ./ | CLI for beginning to run an executable command in the current directory |
| 330. | What is / | Root file system top of the directory hierarchy |
| 331. | What is > | Creating output files |
| 332. | What is \| | Piping use; Piping command output into another command as input. |
| 333. | What is $ | Hidden and admin share |
| 334. | What is 3DES | used to overcome the weakness of short key length of DES and meet in the middle attack of double DES; executes 48 rounds 168 bit key length (168 bit - 3 keys) |
| 335. | What is3 roles of SSL | •Encryption, •Server ID Verification, •Data Integrity; (SSL uses port 443) |
| 336. | What is 5 Vulnerability Axioms(General Truths) | •1.) Vulnerabilities are the gateways through which threats are manifested. •2.) Scans without remediation have little value. •3.) Little scanning and remediation is better than a lot scanning and no remediation. •4.) Prioritizing is critical. •5.) Stay on track. |
| 337. | What is 6 Step Process for Incident Handling | •1.) Preparation •2.) Identification •3.) Containment •4.) Eradication •5.) Recovery •6.) Lessons Learned |
| 338. | What is 802.1x | A method for controlling access to your network to only authenticated devices or users; Used with VLANs. 802.1x = authentication; provides network-level authentication |
| 339. | What is Absinthe | Tool that can be used effectively for blind SQL injection |
| 340. | What is Absolute File Modes | Linux file permissions written in number format instead of rwx format; rwx\|rwx\|rwx; (r=4, w=2, x=1) 111\|111\|111 =777 |
| 341. | What is Acceptable Risk | method of mitigating this is with awareness method of mitigating this is with awareness •Who decides what the organization can afford to risk |
| 342. | What is Access | Typical users follow the past you anticipated through the site. Attackers poke, prod, and guess their way into every nook and |

| | | |
|---|---|---|
| | Control | crann. Keep users out of parts of the server you don't intend them to be in ex. default pages, sample sites; unnecessary programming languages; code library pages and configuration files; disable directory browsing; URL directory traversal |
| 343. | What is Access Control - DAC | Access managed by users. (Used by most Linux Variants "book 6, pg 211"); Consists of something a user can manage(ex. Username and password); least restrictive |
| 344. | What is Access Control - List Based | list of users and their privileges with each object; Associates a list of users and their privileges with each object; each object has a default set of privileges that applies to unlisted users |
| 345. | What is Access Control - MAC | Controls are set by the system and cannot be overwritten by administrator; Lot of work to maintain because all data has classification and all users have clearance (SELinux) |
| 346. | What is Access Control - RBAC | Access based on rules for a specific object; Target actions based on rules for subjects(entities) operating on objects (data/other resources); implemented in a variety of software programs and OS's (ex. Firewalls) |
| 347. | What is Access Control Techniques | Discretionary (DAC), Mandatory (MAC), Role-based (RBAC), Ruleset-based (RSBAC), List-based, Token-based |
| 348. | What is Access Control - Token Based | Associate a list of objects and their privileges (called capabilities) with each user; opposite of List-based |
| 349. | What is access management | 4 tasks: account administration, maintenance, monitoring, and revocation |
| 350. | What is Accountability | Ensures individuals are held accountable for their actions and you can trace back what occurred on a system through detailed auditing; Deals with knowing who did what and when |
| 351. | What is ACE | Individual permissions in the Discretionary Access Control List (DACL). |
| 352. | What is Achilles | A powerful but basic tool for identifying vulnerabilities in Web applications. HTTP Proxy |
| 353. | What is ACK | used to acknowledge the receipt of data |
| 354. | What is acldiag.exe | displays permissions on Active Directory objects and can be used to calculate effective permissions. |
| 355. | What is Acronis | Binary Disk Imager |
| 356. | What is Actions (syslog.conf) | Specify how specific messages should be handled by syslog |
| 357. | What is Active Directory | With AD you can make a change to the AD database on any domain controller in an AD domain, and this change will then be replicated to all other domain controllers automatically. With Windows 2008, Microsoft introduced an important exception to multi-master replication when a domain controller is running Windows Server 2008 or later and the administrator has decided to install that controller as a read-only domain controller (RODC). |
| 358. | What is Active Directory Domain | active directory is the name of the shared database that is installed on all windows servers when it is promoted to a domain controller; Central management for SIDs and SATs |

| | | |
|---|---|---|
| 359. | What is Active | Are the basis for delegation of authority in the domain. An AD domain controller authenticates and authorizes all Directory users and computers in a Windows domain type network—assigning and enforcing security policies for all Permissions computers and installing or updating software. Every object in AD has it's own DACL and SACL. |
| 360. | What is Active Directory Users & Computers | Main tool for managing accounts in Active Directory |
| 361. | What is ActiveX | Used by Windows Update to scan your system for hot fixes |
| 362. | What is Activity Monitors | aka Behavior Blockers; prevent infection by monitoring for malicious activity and blocking such activity when possible. |
| 363. | What is Additional Protocols | SMB: tcp/139/445 RCP:TCP/135 LDAP:TCP/389/636/3268/3269 Kerberos: TCP/UDP/88 DNS:UDP/TCP 53 RDP TCP/3389 PPTP: TCP/1723 protocol 47 for GRE SQL server: TCP/udp/1433/1434 NetBIOS: TCP/udp/137 UDP/138, TCP/139 TCP/UDP/1512 TCP/42 IPSEC: UDP/500/4500 for IKE, Protocols 50 and 51 for ESP and AH |
| 364. | What is Administrative accounts | ce strong passphrase policy, require smart card authentication, require Kerberos and NTLMv2; forbid LanManager and NTLMv1, rename the admin account, create a honey pot admin account,give your admin two user accounts (1. regular account 2. admin account, limit local account use of blank passwords to console logon only, audit all access to administrative users and groups in AD |
| 365. | What is Administrative Shares | root level folders (C$, D$); $ is the symbol used for this |
| 366. | What is Administrative Templates | user friendly registry editor; hundreds of settings; can import ADM templates; can edit to configure any registry value desired. ADM/ADMX templates, not INF. |
| 367. | What is Advanced Application Shielding | Locks an application into a sandbox where it is not permitted to communicate with other applications (part of HIPS). |
| 368. | What is Advanced Information Warfare | EXAMPLES: DDoS, targeted private data extraction, extortion as motive, customized tools, developed techniques; ATTACKERS: extortionists, mature cyber criminals; MATURITY: technical mature, developed by advanced attackers |
| 369. | What is Advanced Security Settings for ACEs | special permissions are a collection of individual permissions ACEs. Individual permissions are the low-level, detailed, atomic ACEs that actually make up the DACL. Deny overrides allow. Grey checked area are inherited permission, whereas the solid-checked ACEs have been assigned explicitly to that folder or file. |
| 370. | What is Advanced Snort Rules | Rule looks like the following:<br>alert tcp any any -> 192.168.1.0/24 80 (content: "/cgi-bin/test, cgi"; msg: "Attempted CGI-BIN Access!!"; sid: 2012033;) Output looks like the following:<br>[*] [1:0:0] Attempted CGI-BIN Access!! [*] 09/02-13:18:30.550445 192.168.1.104:1472 -> 192.168.1.103:80 TCP TTL:128 TOS:0x0 ID:29951 IpLen:20 DgmLen:466 DF<br>**AP** Seq: 0x32D8E9C1 Ack: 0xB427699E Win:0x4470 TcpLen: 20 pg 177<br>has explanation of Advanced Snort Rules |
| 371. | What is AES | The successor to DES and 3DES. (Rijndael). Symmetric encryption algorithm; approved 2001; 128 bit; Up to 256 bit key size. |

| | | |
|---|---|---|
| 372. | What is AES Basic functions | addroundkey, subbytes (Sbox), shiftrows, mixcolumns |
| 373. | What is AFS | Secure replacement for NFS |
| 374. | What is AGULP | model on how permissions should be applied Accounts, Global groups, Universal groups, Local groups, Permission and Rights |
| 375. | What is AH | Provides IPSec with message integrity, anti-replay, and source authentication. No confidentiality/ No encryption provided. Identifies where data originated. Seq number is 32 bits. |
| 376. | What is ALE | The annual expected loss, based on a threat; SLE (Single Loss Expectancy) x ARO (Annualized Rate Occurrence) = ALE (Annual Loss Expectancy / Multi-Hits) |
| 377. | What is Alterations of Code | When someone has compromised the integrity of your program or data. It allows attackers to create backdoors and cover their tracks. It emphasizes the importance of change control and source code versioning. |
| 378. | What is Analytic Cryptanalysis | Using algorithms and mathematics to deduce key or reduce key space to be searched. |
| 379. | What is Analyzing Encrypted Traffic - NIDS | encrypted traffic precludes many signature based detection methods; decrypt traffic when possible increasing overhead on Nods; use anomaly analysis on encrypted traffic will increase false negatives |
| 380. | What is Annualized Loss Expectancy | The annual expected loss, based on a threat; SLE (Single Loss Expectancy) x ARO (Annualized Rate Occurrence) = ALE (Annual Loss Expectancy / Multi-Hits) |
| 381. | What is Annual Loss | The frequency the threat is expected to occur. |
| 382. | What is Anode | The input side of a diode |
| 383. | What is Anomaly Analysis | Anomaly Analysis a technique IDS uses to identify EOIs on the network; baseline of network must be performed (requires an understanding of what "normal" is); flags anomalous conditions in traffic on the network (unexpected conditions are identified as suspicious); catch zero-day exploits (pg 155) |
| 384. | What is Anomaly Analysis - NIDS | Baseline of network. Flagging of anomalous conditions in traffic deviating from base; can catch zero day exploits |
| 385. | What is Anonymous Access | null session manually entered as net use \\ipaddr\IPC$ "" /user:"" |
| 386. | What is Anti-Virus Software | 3 Types of defensive techniques Scanners, Activity Monitors, Integrity Checkers |
| 387. | What is APOP | Secure POP |
| 388. | What is AppArmor | alternative to Selinux, has support for MAC, SUSE, UBUNTU. Its typically easier. |
| 389. | What is Application Behavior Monitoring | A feature of HIPS software; vendor identifies intended behavior in applications; HIPS software monitors how the application interacts with the host; only works for supported applications (pg 209) |

| | |
|---|---|
| 390. What is Application Layer | Interacts with the application to determine which network services will be required. When a program requires access to the network, the Application Layer will manage requests from the program to the other layers down the stack. |
| 391. What is /bin | location of executable programs, some SUID/SGID |
| 392. What is /bin, /usr/bin, | location of executable programs, some SUID/SGID /usr/local, /opt |
| 393. What is ./ configure | This is the new makefile usually have to type ./configure as most people don't have the current directory in their search path |
| 394. What is ./ configure &&make&&make install | •make = make would be executed, it would look for the first target in Makefile and do what the instructions said. The expected end result would be to build an executable program. •make install = This again invokes make, make finds the target install in Makefile and files the directions to install the program. |
| 395. What is /dev/hda | HDA is first IDE HDD. SDA1 is 1st partition on that drive. 0-15 |
| 396. What is /dev or /devices | location that contains devices files that programs running on the system use to communicate with the physical hardware devices controlled by the OS kernel; directory containing "files" used to talk to system devices |
| 397. What is /dev/sda | Sda is the first SCSI HDD. SDA1 is the first partition. 0-15 |
| 398. What is /etc/aliases | file is used to contain mail aliases. |
| 399. What is /etc/default/useradd | Config file for password aging |
| 400. What is /etc/fstab | File is used in most Linux/Windows to hold the static name-to-address maps \| Linux = /etc/hosts \| Windows = %\systemroot%\system32\drivers\etc\hosts and lmhosts |
| 401. What is /etc/hosts | File is used in most Linux/Windows to hold the static name-to-address maps \| Linux = /etc/hosts \| Windows = %\systemroot%\system32\drivers\etc\hosts and lmhosts |
| 402. What is /etc/init.d | directory where control scripts are stored; The initialization scripts used during system startup can also be used to startup services individually. These are located in the /etc/init.d directories, and can be used to (re)launch services using the following syntax: # /etc/init.d/<script name> start |
| 403. What is /etc/inittab | Lists each of the init processes the system should start at boot and stop at shutdown |
| 404. What is /etc/login.defs | Config files for password aging |
| 405. What is /etc/logrotate.conf | moves log files to keep from over filling log space |
| 406. What is /etc/named.conf | (if it exists) is the configuration file for the local name service cache |
| 407. What is /etc/pam.d | Location of all PAM configuration files |
| 408. What is /etc/pam.d/systemauth | used to enforce passwords strength and reuse restrictions |
| 409. What is /etc/passwd | Today's Linux environment uses a two file system - /etc/passwd and /etc/shadow; passwords are not stored in /etc/shadow/; shadow file only accessible by root |
| 410. What is /etc/resolv.conf | tells the host in which order to attempt to resolve names |
| 411. What is /etc/security/opasswd | file created to restrict use of previous passwords |
| 412. What is /etc/services | Mapping of services to port. Works with inetd.conf |
| 413. What is /etc/shadow | Today's Linux environment uses a two file system - /etc/passwd and /etc/shadow; passwords are not stored in /etc/shadow/; shadow file only accessible by root |

| | | |
|---|---|---|
| 414. | What is /etc/xinetd.conf | Global xinetd configuratio file. Read-only once the xinet service is started. |
| 415. | What is /export/home, /home | user home directories. |
| 416. | What is /home | user home directories |
| 417. | What is /opt | executable programs, some SUID/SGID |
| 418. | What is /sbin | Contains system binary files |
| 419. | What is /usr | Most of the critical components of the OS live, including system binaries, programming libraries and tools, and on-line documentation; Ready-Only unless OS is upgraded or patches installed. Files should be protected. |
| 420. | What is /usr/bin | executable programs, some SUID/SGID |
| 421. | What is /usr/local | executable programs, some SUID/SGID |
| 422. | What is /usr/sbin | Contains system binary files. |
| 423. | What is /var | Systems keeps frequent changing data, such as log files and temp queues for system services like email |
| 424. | What is /var/log/secure | Activities related to the use of the su command are authentication types of activities, where the user must authenticate themselves to the system before being allowed to switch users. Authentication activities are logged under the rules associated with the "auth" and "authpriv" facilities in the syslog.conf file. Based on this syslog.conf file, the "authpriv" facility messages are supposed to be sent to /var/log/secure. |