EXAM CRAM

The CompTIA® Security+ SY0-601 Cram Sheet

This Cram Sheet contains the distilled key facts about the CompTIA Security+ exam. Review this information as the last step before you enter the testing center, paying special attention to those areas where you think you need the most review.

Domain 1.0: Attacks, Threats, and Vulnerabilities

1. Programming errors can result in system compromise, allowing someone to gain unauthorized privileges. This is known as privilege escalation.
2. Forms of malware include the following:
   - **Viruses:** Infect systems and spread copies of themselves
   - **Worms:** Similar to viruses but do not require a host to replicate
   - **Trojans:** Disguise malicious code within apparently useful applications
   - **Logic bombs:** Trigger on a particular condition
   - **Rootkits:** Can be installed and hidden on a computer mainly for the purpose of compromising the system
   - **Ransomware:** Usually demands money in return for the release of data, which may have also been encrypted using crypto-malware
   - **Spyware:** May monitor browser activity and log keystrokes and may impact computer performance
3. Spyware and adware often result in a computer running slowly and generating pop-ups.
4. An armored virus seeks to make analysis difficult by including a metaphorical layer of armor around the virus.
5. Phishing is a social engineering attack commonly done through email across a large audience.
6. Spear phishing is a social engineering attack commonly done through email that targets an individual or an individual group.
7. Whaling is similar to spear phishing but affects big targets, such as a CEO.
8. In vishing, also known as voice phishing, the attacker often uses a fake caller ID to appear as a trusted organization and attempt to get the individual to enter account details via the phone.
9. The term pharming is based on farming and phishing. Pharming does not require the user to be tricked into clicking on a link. Instead, it redirects victims to a bogus website, even if they correctly entered the intended site.
10. DoS and DDoS attacks involve disruption of normal network services and include attacks based on the ICMP echo reply called Smurf attacks.
11. Spoofing is the process of making data look as if it came from a trusted or legitimate origin.
12. With a an on-path attack, a third system intercepts traffic between two systems by pretending to be the other system.
13. Replay attacks involve reposting captured data.
14. Zero-day vulnerabilities do not have patches yet and aren't detected by antimalware software.
15. Password guessing, brute-force, and dictionary attacks involve repeated guessing of logons and passwords.
16. DNS poisoning allows a perpetrator to redirect traffic by changing the IP record for a specific domain (thus permitting attackers to send legitimate traffic anywhere they choose).
17. ARP poisoning is a Layer 2 attack that deceives a device on a network and poisons the table associations of other devices.
18. XSRF is an attack in which the end user executes unwanted actions on a web application while currently authenticated.
19. XSS vulnerabilities can be used to hijack a user's session.
20. Injection attacks include SQL, LDAP, DLL, and XML. Such attacks insert code or malicious input to try to force unauthorized activity or access.
21. A rogue access point is an unauthorized wireless access point that is set up.
22. A rogue access point can serve as a type of on-path attack that is often referred to as an evil twin.
23. In bluejacking, attackers generate messages that appear to come from the device itself, leading users to follow obvious prompts and establish an open Bluetooth connection to the attacker's device.
24. When a user pairs with an attacker's device, the user's data becomes available for unauthorized access, modification, or deletion. This is an aggressive attack referred to as bluesnarfing.
25. When traffic being sent across a network is unencrypted, packet sniffing enables an attacker to capture the data and decode it from its raw form into readable text.
26. Threat actor attributes include the actor's relationship to the organization, motive, intent, and capability.
27. Threat actor types include script kiddies, insiders, hacktivists, organized crime, competitors, and nation-states.
28. Nation-states and organized crime are likely to have greater capabilities than other threat actors. Competitors are more likely to want to steal intellectual property to gain a competitive advantage.
29. OSINT describes information for collection from publicly available information sources, such as publications, geospatial information, and many online resources.
30. In a black-box test, the assessor has no information or knowledge about the inner workings of the system.
31. The four primary phases of a penetration test are planning, discovery, attack, and reporting.
32. White-box techniques are often tests to see whether programming constructs are placed correctly and to carry out the required actions. The assessor has knowledge about the inner workings of the system or knowledge of the source code.
33. Gray-box testing uses a combination of both white- and black-box techniques. The tester has some understanding of or limited knowledge of the inner workings.
34. Initial exploitation, escalation of privilege, pivot, and persistence occur (in this order) during the attack phase of a penetration test.
35. A vulnerability scan identifies vulnerabilities, misconfigurations, and lacking security controls.
36. A credentialed vulnerability scan helps reduce false positives.
37. A race condition can result in system malfunction and unexpected results. Resulting errors can cause crashes and may allow attackers to escalate their privileges.
38. Default accounts and passwords provide a simple means for an attacker to gain access.
39. Proper input handling prevents input that can impact data flow, allowing an attacker to gain control of a system or remotely execute commands.
40. Turning off an SSID broadcast hides the network from appearing but does not effectively protect a wireless network from attack.
41. A false positive occurs when a typical or expected behavior is identified as being irregular or malicious.
42. A false negative occurs when an alert that should have been generated did not occur.
43. SIEM tools collect, correlate, and display data feeds that support response activities.
44. SOAR combines security orchestration and automation with threat intelligence platforms and incident response platforms.
45. Threat hunting is a proactive approach to finding an attacker before alerts are triggered.

Domain 2.0: Architecture and Design

46. Recovery sites can be hot, warm, or cold. A hot site is an operational ready-to-go data center; it has the fastest recovery time and highest cost. A cold backup site is the opposite; it has a longer recovery window with a lower cost. A warm site is a compromise between the two.
47. Honeypots and honeynets are used to study the actions of hackers and distract them from more valuable data.
48. An HSM is a combination of hardware and software/firmware that is attached to or contained inside a computer to provide cryptographic functions for tamper protection and increased performance.
49. DLP is a way of detecting and preventing confidential data from being exfiltrated physically or logically from an organization by accident or on purpose.
50. A public cloud provides shared resources over the Internet.
51. Three common public cloud models are SaaS, PaaS, and IaaS:
   - SaaS involves the delivery of a licensed application to customers over the Internet for use as a service on demand.
   - PaaS involves the delivery of a computing platform, often an operating system with associated services, over the Internet without downloads or installation.
   - IaaS involves the delivery of computer infrastructure in a hosted service model over the Internet.
52. A hypervisor is a software- or hardware-layer program that permits the use of many instances of an operating system or instances of different operating systems on the same machine, independent of each other.
53. A Type I native or bare-metal hypervisor is software that runs directly on a hardware platform.
54. A Type II, or hosted, hypervisor is software that runs within an operating system environment.
55. Scalability is based on the capability to handle the changing needs of a system within the confines of the current resources.
56. Elasticity is the capability to expand and reduce resources as needed at any given point in time.
57. SDN is a method for organizations to manage network services through a decoupled underlying infrastructure, allowing quick adjustments to changing business requirements.
58. IAAS clouds consist of workloads deployed across subnets within one or more isolated availability zones that make up the VPC deployed within a geographic region.
59. An IaaS transit gateway allows for the connection of on-premise networks to cloud-hosted networks.
60. A HIDS is implemented to monitor event and application logs, port access, and other running processes.
61. Authentication factors are something you are, something you have, something you know, somewhere you are, and something you do.
62. Biometrics, such as iris scans and fingerprints, are examples of physical access controls.
63. Identification is presenting credentials or keys; authentication is verifying presented credentials.
64. The TOTP algorithm relies on a shared secret and a moving factor or counter, which is the current time.
65. The HOTP algorithm relies on a shared secret and a moving factor or counter.
66. Username and password combinations are the most common form of authentication.
67. Token-based authentication is a strong form requiring possession of the token item.
68. Biometric authentication uses parts of the human body for authentication.
69. Password lockout prevents brute-force attacks.
70. Formal backup types include full, incremental, and differential. In addition, snapshots and copies meet requirements for certain backup use cases.
71. A differential backup includes all data that has changed since the last full backup, regardless of whether or when the last differential backup was made. It does not reset the archive bit
72. A differential backup never requires more than two backups for restore operations (the last full backup and the latest differential backup).
73. An incremental backup includes all the data that has changed since the last incremental backup. It does reset the archive bit.
74. An incremental backup requires the last full backup and every incremental backup since the last full backup.
75. With multiple disks and a RAID scheme, a system can stay up and running when a disk fails, as well as during the time the replacement disk is being installed and data is being restored.
76. RAID organizes multiple disks into a large, high-performance logical disk. These are the most commonly used types of RAID:
   - **RAID 0:** Striped disk array without fault tolerance
   - **RAID 1:** Mirroring and duplexing
   - **RAID 5:** Independent data disks with distributed parity blocks
   - **RAID 10:** RAID 1 and RAID 0; requires a minimum of four disks
77. CASB solutions address security requirements such as visibility, data protection, threat protection, and compliance across public cloud services.
78. Network load balancers are servers configured in a cluster to provide scalability and high availability.
79. Common physical detective controls include motion detectors, CCTV monitors, and alarms.
80. An access control vestibule is a holding area between two entry points in which one door cannot be unlocked and opened until the other door has been closed and locked.
81. With HVAC systems, overcooling causes condensation on equipment, and too-dry environments lead to excessive static.
82. A wet-pipe fire-suppression system is the system most people think of when discussing indoor sprinkler systems. Dry-pipe systems work in exactly the same way as wet-pipe systems, except that the pipes are filled with pressurized air instead of water.
83. The following are fire classes and suppression remedies:
   - For Class A fires (trash, wood, and paper), water decreases the fire's temperature and extinguishes its flames.
   - Foam is usually used to extinguish Class B fires, which are fueled by flammable liquids, gases, and grease.
   - Class C fires (energized electrical equipment, electrical fires, and burning wires) are put out using extinguishers based on carbon dioxide.
   - Class D fires involve combustible metals. The extinguishing agents for Class D fires are sodium chloride and a copper-based dry powder.
84. The purpose of a PDS is to make physical access difficult by enclosing equipment and to make electronic access difficult by using different cables and patch panels.
85. Data centers and server farms make use of alternating rows facing opposing directions. Fan intakes draw in cool air vented to racks facing the cold aisle, and then fan output of hot air is vented to the alternating hot aisles for removal from the data center.
86. EMI shielding seeks to reduce electronic signals that "leak" from computer and electronic equipment. The shielding can be local, can cover an entire room, or can cover a whole building. The two types are TEMPEST shielding and Faraday cages.
87. Cryptographic technology provides for confidentiality, integrity, nonrepudiation, and authentication.
88. Exchanging keys often happens securely "in band" during the need to establish a secure session. Any type of out-of-band key exchange relies on having been shared in advance.
89. Encryption can be applied to data state, which includes data at rest, in transit, and in use.
90. Confusion refers to the level of change from the plaintext input to the ciphertext output, which should be significant.
91. Diffusion ensures that any change, even minor, to the plaintext input results in significant change to the ciphertext output.
92. Symmetric key algorithms depend on a shared single key for encryption and decryption. Examples include DES, 3DES, RC5, and AES.
93. Asymmetric key algorithms use a public key for encryption and a private key for decryption. Examples include the RSA, Diffie-Hellman, El Gamal, and elliptic curve cryptography standards.
94. Nonrepudiation ensures proof or origin, submission, delivery, and receipt.
95. Block ciphers are not as fast, but they encrypt on blocks of a fixed length and have a higher level of diffusion compared to stream ciphers, in which encryption is performed bit by bit.
96. Elliptic curve cryptography is most common in mobile and wireless use cases.
97. A hashing algorithm uses a mathematical formula to verify data integrity. If hash values are different, the file has been modified.
98. Proven, well-known cryptographic technologies should be used in implementations.
99. ROT13 is a substitution cipher. The first half of the Roman alphabet corresponds to the second half, and it is inverse in nature.
100. After a session is complete, when both sides in the communication process destroy the keys, this is known as perfect forward secrecy or just forward secrecy.
101. Ephemeral key agreement protocols such as DHE and ECDHE provide perfect forward secrecy.
102. Bcrypt and PBKDF2 are key derivation functions (KDFs) that are primarily used for key stretching, which provides a means to "stretch" a key or password, making an existing key or password stronger.
103. Blockchains are digital ledgers with transactions grouped into cryptographically linked blocks.
104. Adding a salt prevents a rainbow table attack on password hashes.

Domain 3.0: Implementation

105. You can make LDAP traffic confidential and secure by using TLS technology operating over port 636.
106. Web traffic is unencrypted over HTTP and occurs by default over port 80.
107. Encrypted web traffic over HTTPS occurs by default over port 443.
108. FTP SSH uses TCP port 22 by default.
109. Port security is a Layer 2 traffic control feature that enables individual switch ports to be configured to allow only a specified number of source MAC addresses coming in through the port.
110. Loop protection makes additional checks in Layer 2 switched networks.
111. A flood guard is a firewall feature to control network activity associated with DoS attacks.
112. Static code analysis is a white-box software testing process for detecting bugs early in the program development.
113. Dynamic code analysis is based on observing how the code behaves during execution.
114. Fuzzing is a black-box software testing process by which semi-random data is injected into a program or protocol stack to detect bugs.
115. Sandboxing provides a safe execution environment for untrusted programs.
116. Test environments should be isolated from development environments.
117. Staging environments reduce the risk of introducing issues before solutions are deployed in production.
118. Baselines can establish patterns of use that later can help identify variations that identify unauthorized access attempts.
119. Smart cards use embedded systems with an operating system on the included chip.
120. The Waterfall SDLC model starts with a defined set of requirements and a well-developed plan, and adjustments are confined to the current development stage.
121. The Agile SDLC model starts with less rigorous guidelines and allows for adjustments during the process.
122. Secure DevOps includes security in the SDLC, ensuring that security is built in during the development process.
123. A CI server continually compiles, builds, and tests each new version of code committed to the central repository without user interaction.
124. Immutability means that a valuable program, configuration, or server will never be modified in place.
125. System hardening involves disabling unnecessary ports and services.
126. To keep an attacker from exploiting software bugs, an organization must continually apply manufacturers' patches and updates.
127. Commonly used services and associated ports include the following:
    - 15: Netstat
    - 20 and 21: FTP
    - 22: SSH/SFTP/SCP
    - 23: Telnet
    - 25: SMTP
    - 53: DNS
    - 80: HTTP
    - 123: NTP
    - 389: LDAP
    - 443: HTTPS
    - 636: LDAPS
    - 989 and 990: FTPS
    - 1812: RADIUS
    - 3389: RDP
128. TPM chips are secure cryptoprocessors used to authenticate hardware devices.
129. A file integrity checker tool computes a cryptographic hash and compares the result to known good values to ensure that the file has not been modified.
130. Signature-based methods detect known signatures or patterns.
131. A VPN concentrator is used to allow multiple external users to access internal network resources using secure features that are built in to the device. They are deployed when a single device needs to handle a very large number of VPN tunnels.
132. NAC offers a method of enforcement which helps ensure that computers are properly configured.
133. Zero trust is a model that provides granular and dynamic access control, regardless of where the user or application resides, and doesn't place trust in the entire network.
134. A screened subnet is a small network between the internal network and the Internet that provides a layer of security and privacy.
135. NAT acts as a liaison between an internal network and the Internet across a routing device. It allows multiple computers to connect to the Internet using one IP address.
136. Network segregation, isolation, and segmentation are effective controls an organization can implement to mitigate the effect of a network intrusion.
137. Air gaps are physically isolated machines or networks.
138. Network taps, SPAN, and mirror ports are the primary methods used to get network traffic to network monitoring tools.
139. The purpose of a VLAN is to unite network nodes logically into the same broadcast domain, regardless of their physical attachment to the network.
140. Intrusion detection is managed by two basic methods: knowledge-based and behavior-based detection.
141. An IDS monitors packet data by using behavior-based (to identify anomalies) or knowledge-based methods, operating in network-based or host-based configurations.
142. NIDSs and NIPSs are designed to catch attacks in progress within a network, not just on individual machines or the boundary between private and public networks.
143. Proxy servers can be placed between the private network and the Internet for Internet connectivity or can be placed internally for web content caching.
144. Firewalls separate external and internal networks and include the following types:
    - Packet-filtering firewalls (network layer, Layer 3)
    - Proxy-service firewalls, including circuit level (session layer, Layer 5) and application level (application layer, Layer 7) gateways
    - Stateful inspection firewalls (application layer, Layer 7)
145. A stateless firewall works as a basic access control list filter.
146. Stateful firewalls are a deeper inspection firewall type that analyze traffic patterns and data flows, often combining layered security and known as next-gen firewalls.
147. Wireless access methods, from the least secure to the most secure, include open authentication, shared authentication, and EAP.
148. WPA-Personal requires a password shared by all devices on the network.
149. WPA-Enterprise requires certificates and uses an authentication server from which keys are distributed.
150. WPA2 and WPA3 favor CCMP over TKIP common to WPA. TKIP should still be used for systems that are unable to support 802.1i.
151. EAP authentication protocols include EAP-TLS, PEAP, EAP-TTLS, and EAP-FAST. Only EAP-TLS requires a client certificate, and only EAP-FAST does not require a server certificate.
152. EAP is an authentication framework and is used by WPA, WPA2, and WPA3 for authentication.
153. PEAP encapsulates EAP in a TLS tunnel and only requires a certificate on the server.
154. Jailbreaking and rooting mobile devices removes restrictions imposed by the manufacturer and can introduce risk.
155. Employees who leave an organization should have their accounts disabled but not deleted.
156. Generic accounts used by multiple users must be prohibited.
157. When working with logical controls, two models exist for the assignment of permissions and rights: user based and role or group based.
158. Too many failed authentication attempts should incur a penalty, such as account lockout.
159. Enforcing password history prevents users from reusing old passwords.
160. Auditing user permissions is a common method for identifying access violations and issues.
161. A federation system allows accessibility from each domain. Accounts in one area can be granted access rights to any other resource, whether local or remote within the domains.
162. Remote access authentication includes RADIUS or TACACS+.
163. RADIUS provides authentication and authorization functions in addition to network access accounting functions, but it does not provide further access control.
164. Kerberos supports mutual authentication, protecting against on-path attacks.
165. Using PAP is strongly discouraged because user passwords are easily readable.
166. OAuth provides authorization services and does not provide authentication such as OpenID and SAML.
167. SAML offers single sign-on capabilities.
168. The IdP is the source of a username and password and authenticates the user. The SP provides service to the user.
169. Access controls includes MAC, DAC, ABAC, and RBAC.
170. CACs and PIV cards provide smart card functions for identity and authentication.
171. Implicit deny is an access control practice in which resource availability is restricted to only logins that are explicitly granted access.
172. PKI relies on asymmetric key cryptography using certificates, which are digitally signed blocks of data issued by a CA.
173. A CSR is generated and submitted before a CA signs a certificate.
174. A root CA should be taken offline to reduce the risk of key compromise because this would compromise the entire chain or system.
175. The three types of validated certificates are DV, OV, and EV certificates.
176. EV certificates provide the highest level of trust and require the most effort for a CA to validate.
177. DER and PFX certificates are binary encoded; PEM and P7B certificates are ASCII encoded, and the contents can easily be cut and pasted.
178. Ensuring a certificate's validity is accomplished through a CRL or OCSP.
179. OCSP stapling puts the responsibility of OCSP requests on the web server instead of on the issuing CA.
180. Key escrow stores the private key with a trusted third party.

Domain 4.0: Operations and Incident Response

181. ping is a command-line tool that tests network connectivity. It is a good troubleshooting tool for determining whether a route is available to a host.
182. nmap is a network scanning tool that is often used in security auditing.
183. netstat shows network statistics, including the protocol, local address, foreign address, and connection state.
184. netcat is a network utility for gathering information from transport layer network connections.
185. dig and nslookup are troubleshooting tools that query DNS servers.
186. head, tail and cat are common command line tools for file display and manipulation.
187. Python is a general-purpose programming.
188. tcpdump is a packet analyzer tool to capture TCP/IP packets.
189. PowerShell is a command-line shell and scripting interface for Microsoft Windows environments.
190. dd, Memdump, WinHex, FTK Imager and Autopsy are forensics tools.
191. Protocol analyzers can be placed inline or in between the devices from which you want to capture traffic.
192. Some of the most common firewall configuration errors include permissions for traffic to run from any source to any destination, unnecessary services running, weak authentication, and log file negligence.
193. A misconfigured web content filter can either prevent legitimate content or allow prohibited content.
194. Written authorization should be required before conducting vulnerability or penetration tests.
195. Incident response plans should include details related to incident categorization, preparation, roles, responsibilities, reporting requirements, escalation procedures, and details on cyber incident response teams and training exercises.
196. The incident response process includes preparation, identification, containment, eradication, recovery, and post-incident events such as lessons learned.
197. Order of volatility describes the order in which evidence should be collected, from the most volatile systems to the least volatile.
198. Data in RAM and swap or paging files is considered the most volatile.
199. Chain of custody ensures that evidence is properly handled.
200. Data acquisition during and after an incident includes capturing system images, traffic logs, video, time offset, hashes, screenshots, and witness interviews.
201. When computers are examined, their date and time settings are recorded and compared with the current time. This can be used to calculate the difference between the two. This difference is then used as an offset and applied to all the time evidence on the computer.
202. MITRE ATT&CK is a framework similar to a kill chain and provides a reference for incident response.
203. The Diamond Model of Intrusion Analysis places the basic components of malicious activity at one of four points: adversary, infrastructure, capability, and victim.
204. Incident responses exercises can be discussion oriented or simulated.
205. BCP and COOP ensure the restoration of organizational functions in the shortest possible time, even if services resume at a reduced level of effectiveness or availability

Domain 5.0: Governance, Risk, and Compliance

206. Generally, controls deter, prevent, detect, or correct. Some controls, such as anti-malware, provide more than one of those functions.
207. A computer login notification is an example of a common preventive control.
208. Compensating controls are used when a business or technological constraint exists and an alternate control is effective in the current security threat landscape.
209. SLA, BPA, MOU, and ISA are types of interoperability agreements that help mitigate risk when dealing with third parties.
210. User types require unique training and awareness. The user types include general users, privileged users, system administrators, executive users, data owners, and system owners. The latter three are in positions that are responsible for creating or managing security policies.
211. Users must be given training in the proper use of their various personal applications, including email and social media networks. This training should address any limitations or expectations regarding their use.
212. RPO designates the amount of data that will be lost or will have to be reentered due to network downtime.
213. RTO designates the amount of time that can pass before a disruption begins to seriously impede normal business operations.
214. MTBF is the average time before a product requires repair.
215. MTTF is the average time before a product fails and cannot be repaired.
216. A privacy threshold assessment determines whether systems contain personal information. A privacy impact assessment is needed for any organization that collects, uses, stores, or processes such information.
217. Risk assessment is largely a function of threat, vulnerability, and impact. It can be considered with this formula:

    Risk = Threat x Vulnerability x Impact
218. Risk identification includes asset identification, risk assessment, threat identification and classification, and identification of vulnerabilities.
219. Regarding risk, qualitative measures are based on subjective values; they are less precise than quantitative measures, which rely on numbers.
220. An identified risk can be accepted, mitigated, transferred, or avoided. Purchasing insurance is a common example of transferring risk.
221. ALE equals the SLE times the ARO.
222. Change management is important because change introduces risk that can impact systems and services.
223. A DRP details considerations for backup and restoration, including secure recovery methods.
224. To be considered PII, information must be specifically associated with an individual person.
225. Data owners determine data's classification level. Data custodians implement the controls for the data.
226. Degaussing is a data disposal method that involves using a tool to reduce or remove the magnetic field of storage media.
227. Benchmarks provide guidance for creating a secure configuration posture.