This Crm 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 compromises, allowing someone to gain unauthorized access to your device or network privileges.
2. Worms: spread automatically and require no user interaction.
3. Trojan: disguised malicious code within apparently useful applications.
4. Logic bomb: trigger on a particular condition.
5. Rootkit: can be installed and hidden on a computer for the purpose of compromising the system.
6. Ransomware: Usually demands money in return for the release of data, which may have been encrypted using crypto-malware.
7. Spyware and adware often result in a computer running slowly and generating pop-ups.
8. An armed virus seeks to make analysis difficult by including a metaphorical layer of armor around the virus.
9. A social engineering attack commonly occurs through email or a trusted organization and attempt to get the user's data becomes available for unauthorized access, modification, or deletion. This is an example of a threat that can affect an organization in an evil way.
10. In a replay attack, attackers generate messages that appear to come from the device itself, leading to the reuse of old messages or new messages on an open Bluetooth connection to the device.
11. When users log on at an unauthorized computer, their user data becomes available for unauthorized access, modification, or deletion. This is an aggressive attack referred to as blusing.
12. When traffic being sent across a network is unencrypted, packet sniffing enables attackers to capture the data and decide from it a raw form into readtable.
13. Threat actor attributes include the actor’s relationship to the organization, motive, intent, and capability.
14. The threat actors target includes cyberlooters, identity thieves, and viruses.
15. An HSAM is a combination of hardware and software/firmware to detect or contain inside a computer to provide protection against attacks and improve performance.
16. GLP is a way of analyzing and protecting confidential information from being physically obtained or manipulated by an organization by accident or on purpose.
17. A public cloud provides shared resources over the internet.
18. The CompTIA Security+ 2016 Exam Outline. 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 2.0: Architecture and Design

46. Recovery sites can be hot, warm, or cold. A hot recovery site is where the data is already available in the last full backup.
47. An incremental backup requires the last full backup and the next incremental backup.
48. A Type II, or hosted, hypervisor is software that runs directly on a hardware platform and doesn’t require a physical machine.
49. Elasticity is the capability to expand and reduce infrastructure, allowing quick adjustments to changing business requirements.
50. IaaS involves the delivery of computer resources over the Internet.
51. An advanced encryption attack can be performed only through email across a large audience.
52. Soil pH impacts the effectiveness of engineering attacks; commonly done through email that targets an organization’s employees.
53. Weather is similar to phishing but affects bigger targets, such as a CEO.
54. In vishing, also known as voice phishing, the attacker generates messages that appear to come from the device itself, leading to the reuse of old messages or new messages on an open Bluetooth connection to the device.
55. When users log on at an unauthorized computer, their user data becomes available for unauthorized access, modification, or deletion. This is an aggressive attack referred to as blusing.
56. When traffic being sent across a network is unencrypted, packet sniffing enables attackers to capture the data and decide from it a raw form into readtable.
57. Threat actor attributes include the actor’s relationship to the organization, motive, intent, and capability.
58. The threat actors target includes cyberlooters, identity thieves, and viruses.
59. An HSAM is a combination of hardware and software/firmware to detect or contain inside a computer to provide protection against attacks and improve performance.
60. GLP is a way of analyzing and protecting confidential information from being physically obtained or manipulated by an organization by accident or on purpose.
61. A public cloud provides shared resources over the internet.
62. Three common public cloud models are SaaS, PaaS, and IaaS.
63. An integral backup includes all the data that has changed since the last incremental backup. It does not reset the archive bit and therefore can be restored.
64. An incremental backup includes the last full backup and every incremental backup since the last full backup.
65. With multiple disks and a RAID scheme, a system can stay up and running when a disk fails, and the system can be reconstructed when the replacement disk is being installed and data is being restored.
66. RAID organizes multiple disks into a large, high-performance disk. These are the most commonly used types of RAID:
67. RAID 0: Stripped disk array without fault tolerance
68. RAID 1: Mirroring and duplicating data
69. RAID 5: Combines parity data with distributed parity blocks
70. RAID 10: Both RAID 1 and 0; requires a minimum of four disks
71. The term pharming is based on farming and phishing. Pharming does not require the user to make a purchase or enter any personal information or knowledge about the inner workings of the system.
72. A hashing algorithm uses a mathematical formula to verify data integrity. If hash values differ, the data is modified. It does not reset the archive bit and therefore can be restored.
73. A public cloud provides shared resources over the internet.
74. An incremental backup includes all the data that has changed since the last incremental backup. It does not reset the archive bit and therefore can be restored.
75. An incremental backup includes the last full backup and every incremental backup since the last full backup.
76. With multiple disks and a RAID scheme, a system can stay up and running when a disk fails, and the system can be reconstructed when the replacement disk is being installed and data is being restored.
77. RAID organizes multiple disks into a large, high-performance disk. These are the most commonly used types of RAID:
78. Network load balancers are servers configured in a cluster to provide high availability and high availability.
79. Common physical detective controls include motion-detection, CCTV monitors, and alarms.
80. An access control list is a blocking of a domain from 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, overheating causes data to be unavailable or lost.
82. AES is a cipher that uses a secret key and a fixed number of rounds.
83. A false positive occurs when a typical or non-malicious event is considered malicious.
84. Turning off an SSID broadcast hides the network from appearing but does not affect the network from a wireless network from attacks.
85. A false negative occurs when an attack that should have been detected is not.
86. An SSID is broadcast by default, and devices can connect to it.
87. OSINT describes information for collection from public online resources.
88. In a black-box test, the assessor has no knowledge or insight into the system.
89. White-box techniques are often tests to see security controls and their effectiveness.
90. Taking an OSINT approach to finding valuable data.
91. A virtual machine is operated on purpose.
92. When traffic being sent across a network is unencrypted, packet sniffing enables attackers to capture the data and decide from it a raw form into readtable.
93. Threat actor attributes include the actor’s relationship to the organization, motive, intent, and capability.
94. The threat actors target includes cyberlooters, identity thieves, and viruses.
95. An HSAM is a combination of hardware and software/firmware to detect or contain inside a computer to provide protection against attacks and improve performance.
96. GLP is a way of analyzing and protecting confidential information from being physically obtained or manipulated by an organization by accident or on purpose.
97. A public cloud provides shared resources over the internet.
Loop protection makes additional checks. Sandboxing provides a safe execution test environment should be isolated from baselines can establish patterns of use that Secure DevOps includes security in the secure by using TLS technology operating network activity associated with DoS process by which semi-random data is defined set of requirements and a well-structured configuration, or server will never be unnecessary ports and services. manufacturers’ patches and updates.

110. Loop protection makes additional checks. Sandboxing provides a safe execution test environment should be isolated from baselines can establish patterns of use that Secure DevOps includes security in the secure by using TLS technology operating network activity associated with DoS process by which semi-random data is defined set of requirements and a well-structured configuration, or server will never be unnecessary ports and services. manufacturers’ patches and updates.

Frequent use of pattern recognition allows you to be more effective with your security efforts.

115. sandboxes provide a safe environment for testing code, allowing organizations to quickly identify and address security issues. Sandboxing is an essential component of a comprehensive security strategy, as it enables organizations to evaluate the potential impact of new applications and configurations in a controlled environment without exposing the production environment to risk.

116. Test environments should be isolated from baselines can establish patterns of use that Secure DevOps includes security in the secure by using TLS technology operating network activity associated with DoS process by which semi-random data is defined set of requirements and a well-structured configuration, or server will never be unnecessary ports and services. manufacturers’ patches and updates.

118. Baselines can establish patterns of use that Secure DevOps includes security in the secure by using TLS technology operating network activity associated with DoS process by which semi-random data is defined set of requirements and a well-structured configuration, or server will never be unnecessary ports and services. manufacturers’ patches and updates.

119. A fixed set of a firewall's rules can be complex and time-consuming to manage, especially as organizations grow and their security requirements evolve. However, using a dynamic set of rules can help prevent unauthorized access and attacks, as it allows the firewall to adapt to changing threats and conditions.

122. Secure DevOps includes security in the secure by using TLS technology operating network activity associated with DoS process by which semi-random data is defined set of requirements and a well-structured configuration, or server will never be unnecessary ports and services. manufacturers’ patches and updates.

123. A CI server continually compiles, builds, and tests code, ensuring that changes are made in a controlled and repeatable manner. This is essential for maintaining the quality of software and for ensuring that security vulnerabilities are caught early in the development process.

124. Configuration management is essential in maintaining consistent and secure environments across a network. It allows organizations to control the configuration of systems and ensure that they are secure, aligned with best practices, and compliant with regulations.

125. Secure DevOps includes security in the secure by using TLS technology operating network activity associated with DoS process by which semi-random data is defined set of requirements and a well-structured configuration, or server will never be unnecessary ports and services. manufacturers’ patches and updates.

126. Secure DevOps includes security in the secure by using TLS technology operating network activity associated with DoS process by which semi-random data is defined set of requirements and a well-structured configuration, or server will never be unnecessary ports and services. manufacturers’ patches and updates.

127. Commonly used services and associated protocols include the following:

- 10: Network Time Protocol (NTP) for system synchronization
- 20: DNS for domain name resolution
- 21: FTP for file transfer
- 22: SSH for secure file transfer
- 23: Telnet for remote login
- 25: SMTP for sending email
- 80: HTTP for web services
- 123: NTP for time synchronization
- 3389: Remote Desktop Protocol (RDP) for remote administration
- 20 and 21: FTP for file transfer
- 22: SSH for secure file transfer
- 80: HTTP for web services
- 123: NTP for time synchronization
- 3389: Remote Desktop Protocol (RDP) for remote administration
- 128: DNS for domain name resolution
- 199: LDAP for directory services
- 443: HTTPS for secure communication
- 563: LDAP over TLS
- 993 and 995: FTPS
- 1812: Radius for network authentication
- 1623: QUIC for fast, secure transport protocol
- 1624: Resin for web application server
- 1625: RAKS for containerized applications
- 1626: Kubernetes for container orchestration
- 1627:常用的网络服务和相关协议包括以下内容：
- 10: 网络时间协议（NTP）用于系统同步
- 20: DNS 用于域名解析
- 21: FTP 用于文件传输
- 22: SSH 用于安全文件传输
- 23: Telnet 用于远程登录
- 80: HTTP 用于 Web 服务
- 123: NTP 用于时间同步
- 3389: 远程桌面协议（RDP）用于远程管理
- 128: DNS 用于域名解析
- 199: LDAP 用于目录服务
- 443: HTTPS 用于安全通信
- 563: LDAP over TLS
- 993 and 995: FTPS
- 1812: Radius 用于网络认证
- 1623: QUIC 用于快速、安全的传输协议
- 1624: Resin 用于 Web 应用服务器
- 1625: RAKS 用于容器化应用程序
- 1626: Kubernetes 用于容器编排