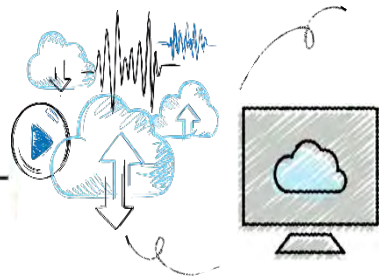
CompTIA Security+

Summary and Review



Information Security Summary

- Information security attacks have grown exponentially in recent years
- There are many reasons for the high number of successful attacks
- It is difficult to defend against today's attacks
- Information security protects the
  - **C**onfidentiality
  - **I**ntegrity
  - **A**vailability
  - of both the data and the devices that it resides on
- Regardless of the state: Being stored, manipulated, or transmitted
- Using the products, people, and procedures available

Information Security Summary

- Main goals of information security
  - Prevent data theft
  - Thwart identity theft
  - Avoid legal consequences of not securing information
  - Maintain productivity
  - Foil cyberterrorism
- Threat actors fall into several categories and exhibit different attributes
- Although multiple defenses may be necessary to withstand the steps of an attack, these defenses should be based on five security principles:
  - Layering, limiting, diversity, obscurity, and simplicity

Malware and Social Engineering Summary

- Malware is malicious software that enters a computer system without the owner's knowledge or consent
- Malware that spreads include computer viruses and worms
- Ransomware prevents a user's device from properly and fully functioning until a fee is paid
- A rootkit can hide its presence or the presence of other malware on the computer by accessing lower layers of the OS
- Different types of malware are designed to collect data from the user's computer and make it available to the attacker
  - Spyware, keylogger, and adware

Malware and Social Engineering Summary

- A logic bomb is computer code that is typically added to a legitimate program but lies dormant until triggered by a specific logical event
- A backdoor gives access to a computer, program, or service that circumvents any normal security protections
- A popular payload of malware is software that will allow the infected computer to be placed under the remote control of an attacker (known as a bot)
  - Multiple bot computers can be used to created a botnet
- Social engineering is a means of gathering information for an attack from individuals
- Types of social engineering approaches include phishing, dumpster diving, and tailgating

Basic Crypto Summary

- Cryptography is the practice of transforming information into a secure form while being transmitted or stored
- The strength of a cryptographic algorithm depends upon several factors
- Cryptography can provide confidentiality, integrity, authentication, non-repudiation, and obfuscation
- Hashing creates a unique digital fingerprint that represents contents of original material
  - Used only for comparison
- Symmetric cryptography uses a single key to encrypt and decrypt a message
  - Stream ciphers and block ciphers

Basic Crypto Summary

- Asymmetric cryptography
  - Public key cryptography
  - Uses two keys: public key and private key
- Cryptography can be applied through hardware or software
- Hardware encryption cannot be exploited like software cryptography

Advanced Crypto Summary

- Cryptography that is improperly applied can lead to vulnerabilities that will be exploited
- A digital certificate is the user's public key that has been digitally signed by a trusted third party who verifies the owner and that the public key belongs to that owner
- A certificate repository (CR) is a list of approved digital certificates
- Revoked digital certificates are listed in a Certificate Revocation List (RCL)
  - Status can also be checked through the Online Certificate Status Protocol (OCSP)
- There are several different types of digital certificates

Advanced Crypto Summary

- Domain validation digital certificates verify the identity of the entity that has control over the domain name but indicate nothing regarding the trustworthiness of the individuals behind the site
- A public key infrastructure (PKI) is a framework for all the entities involved in digital certificates to create, store, distribute, and revoke digital certificates
- An organization that uses multiple digital certificates on a regular basis needs to properly manage those digital certificates
- Cryptography is commonly used to protect data-in-transit
  - SSL and TLS are widely used protocols
- IPsec is a set of protocols developed to support the secure exchange of packets

Networking and Server Attacks Summary

- Some attacks are designed to intercept network communications
  - Man-in-the-middle and replay attacks are examples
- Some types of attacks inject “poison” into a normal network process to facilitate an attack
- Whereas some attacks are directed at the network itself, other attacks are directed at network servers
  - Denial of service, DNS amplification attack, and SYN flood attack are examples
- A cross-site scripting (XSS) attack is focused not on attacking a web application server, but on using the server to launch other attacks on computers that access it

Networking and Server Attacks Summary

- Several server attacks are the result of threat actors “commandeering” a technology and then using it for an attack
- Some attacks can target either a server or a client by “overflowing” areas of memory with instructions from the attacker
- Most websites today rely heavily upon advertising revenue
  - Several attacks attempt to use ads or manipulate the advertising system
- To provide enhanced features, virtually all websites today allow scripting code to be downloaded from the web server into the user’s web browser

Network Security Devices Summary

- Standard network security devices provide a degree of security
  - Switches, router, load balancer, and proxies
- Hardware devices specifically designed for security give higher protection level
  - Hardware-based firewall, Web application firewall
- Virtual private networks (VPNs) use an unsecured public network and encryption to provide security
- A mail gateway monitors emails for unwanted content and prevents these messages from being delivered
- An intrusion detection system (IDS) is designed to detect an attack as it occurs

Network Security Devices Summary

- A Security and Information Event Management (SIEM) product consolidates real-time monitoring and management of security information along with an analysis and reporting of security events
- Other network security hardware devices include:
  - Hardware security modules, SSL decryptors, SSL/TLS accelerators, media gateways, UTM products, Internet content filters, and web security gateways
- Methods for designing a secure network
  - Demilitarized zones
  - Virtual LANs
- Network technologies can help secure a network
  - Network access control (NAC)

Administering a Secure Network Summary

- TCP/IP is the most common protocol for LANs and the Internet
- Protocols for transferring files
  - FTP and FTPS
- The correct placement of security devices is essential for protection
  - An SSL/TLS accelerator can be a separate hardware card or a separate SSL/TLS hardware module installed as a “virtual SSL server”
- Monitoring traffic on switches can be done in two ways:
  - A managed switch that supports port mirroring
  - Install a network tap (test access point)

Administering a Secure Network Summary

- A log is a record of events that occur
  - Security logs are particularly important because they can reveal the types of attacks that are being directed at the network
- A solution to log management is to use a centralized device log analyzer
- Some applications and platforms require special security considerations
  - Virtualization
  - Cloud computing
  - Software defined network (SDN)

Wireless Network Security Summary

- Bluetooth is a wireless technology using short-range RF transmissions
- Near field communication (NFC) is a set of standards primarily for smartphones and smartcards used to communicate with devices in close proximity
- A wireless technology similar to NFC is radio frequency identification (RFID)
- A wireless local area network (WLAN) is designed to replace or supplement a wired LAN
  - The IEEE has developed standards for WLANs
- A rouge AP is an unauthorized AP that allows an attacker to bypass network security and open the network and its users to attacks

Wireless Network Security Summary

- IEEE 802.11 committee implemented several wireless security protections in the 802.11 standard
  - WEP and WPS, however, have significant design and implementation flaws
- Controlling access to the WLAN can be accomplished using MAC filtering on the AP
- Wi-Fi Protected Access (WPA) and WPA2 have become the foundations of wireless security today
- Extensible Authentication Protocol (EAP) is a framework for transporting authentication protocols by defining the format of the messages

Wireless Network Security Summary

- Other steps to protect a wireless network include:
  - Detecting rogue access points
  - Choose the best type of AP to match the needs of the network
  - Manage APs through a wireless LAN controller (WLC)
  - Use a captive portal AP
  - Access point power level adjustment
  - Antenna positioning

Client and Application Security Summary

- Secure Boot is designed to ensure that a computer boots using only software that is trusted by the computer manufacturer
- In a chain of trust each element relies on the confirmation of the previous element to know that the entire process is secure
  - Strongest starting point is hardware
- In addition to protecting hardware, the OS software that runs on the host also must be protected
- Modern OSs have hundreds of different security settings that can be manipulated to conform to the baseline

Client and Application Security Summary

- Antimalware software can help protect against these infections
  - AV software can examine a computer for any infections as well as monitor computer activity and scan new documents that might contain a virus
- Peripheral devices attached to a client computer must likewise be protected
- A multifunctional device (MFD) is a combination printer, copier, scanner, and fax machine and should also be protected
- Physical security is an often overlooked consideration when protecting a client device
- Door locks are important to protect equipment
- Hardware security is physical security that involves protecting the hardware of the host system

Client and Application Security Summary

- Applications that run on client devices need to be secure
- There are different tools and processes that can be used to test the quality of the application code

Mobile and Embedded Device Security Summary

- Tablet computers are portable computing devices smaller than portable computers, larger than smartphones, and focused on ease of use
- Portable computers are devices that closely resemble standard desktop computer
  - A laptop is designed to replicate the abilities of a desktop computer with only slightly less processing power
- Many mobile devices use Wi-Fi as the standard connectivity method to connect to remote networks
- Many organizations have adopted an enterprise deployment model as it relates to mobile devices
- BYOD allows users to use their own personal mobile devices for business purposes

Mobile and Embedded Device Security Summary

- Mobile devices can be easily lost or stolen and usually use public external networks for their Internet access
  - Attackers can eavesdrop on data transmissions and view services to identify the location of a person carrying a mobile device
- Mobile devices have the ability to access untrusted content that other types of computing devices generally do not have
- It is important to disable features and turn off those that do not support the business use of the device or that are rarely used
- A lock screen prevents the mobile device from being used until the user enters the correct passcode

Mobile and Embedded Device Security Summary

- Mobile device management (MDM) tools allow a device to be managed remotely
- Mobile application management (MAM) consists of tools and services responsible for distributing and controlling access to apps
- MDMs can support application whitelisting, which ensures that only preapproved apps can be run on the device
- An embedded system is computer hardware and software contained within a larger system that is designed for a specific function
- The Internet of Things (IoT) is connecting any device to the Internet for the purpose of sending and receiving data to be acted upon

Authentication and Account Mgmt Summary

- Authentication credentials can be classified into five categories: what you know, what you have, what you are, what you do, and where you are
- Passwords provide a weak degree of protection
  - Must rely on human memory
- Most password attacks today use offline attacks
  - Attackers steal encrypted password file
- A dictionary attack begins with the attacker creating digests of common dictionary words, which are compared with those in a stolen password file
- Securing passwords from attacks depends upon the user as well as the enterprise
  - Security experts recommend that technology be used to store and manage passwords called password managers

Authentication and Account Mgmt Summary

- Another type of authentication credential is based on the approved user having a specific item in her possession
  - A hardware token is a small device that generates a code from an algorithm once every 30 to 60 seconds
- Biometrics bases authentication on characteristics of an individual
  - Standard and cognitive biometrics are examples
- Behavioral biometrics authenticates by normal actions the user performs
- Single sign-on (SSO) allows a single username and password to gain access to all accounts
- Group Policy settings allow an administrator to set password restrictions for an entire group at once

Access Management Summary

- Access control is the process by which resources or services are denied or granted
- Five major access control models:
  - Discretionary Access Control, Mandatory Access Control, Role-Based Access Control, Rule-Based Access Control, Attribute-Based Access Control
- Configuring accounts with proper permissions is the first step in providing strong security
- Location-based policies establish the geographical boundaries of where a mobile device can and cannot be used
- Once accounts have been created, it is important that they be periodically maintained and audited to ensure they still follow all enterprise policies

Access Management Summary

- Best practices for implementing access control
  - Separation of duties, job rotation, mandatory vacations, and following a clean desk policy
- Implementing access control methods includes using access control lists (ACLs)
- Different services can be used to provide identity and access services
- A directory service is a database stored on the network itself that contains information about users and network devices
- One implementation of a directory service as an authentication is the Lightweight Directory Access Protocol (LDAP)

Vulnerability Assessment and Data Security Summary

- Vulnerability assessment
  - Methodical evaluation of exposure of assets to risk
  - Three are five steps in a vulnerability assessment
- One tool used to assist in determining potential threats is a process known as threat modeling
- Several techniques can be used in a vulnerability assessment
- Port scanners, protocol analyzers, honeypots, and honeynets are used as assessment tools
- Banner grabbing can be used to perform an inventory on the services and systems operating on a server

Vulnerability Assessment and Data Security Summary

- A vulnerability scan searches system for known security weakness and reports findings
- Penetration testing designed to exploit any discovered system weaknesses
  - Tester may have various levels of system knowledge
- Privacy is defined as the state or condition of being free from public attention to the degree that you determine
- Standard techniques used to mitigate and deter attacks
  - Healthy security posture
  - Proper configuration of controls
  - Hardening and reporting

Business Continuity Summary

- Business continuity is an organization's ability to maintain its operations after a disruptive event
- In IT contingency planning, an outline of procedures that are to be followed in the event of a major IT incident is developed
- Disaster recovery
  - Focuses on restoring information technology functions
  - Disaster recovery plan (DRP) details restoration process
- A server cluster combines two or more servers that are interconnected to appear as one
- RAID uses multiple hard disk drives for redundancy

Business Continuity Summary

- Network components can be duplicated to provide a redundant network
- Data backup
  - Copying information to a different medium and storing (preferably offsite) for use in event of a disaster
- Recovery point objective and recovery time objective help an organization determine backup frequency
- Fire suppression systems include water, dry chemical, and clean agent systems

Business Continuity Summary

- A defense for shielding an electromagnetic field is a Faraday cage
- The control and maintenance of HVAC systems are important for data centers
- Forensic science is the application of science to questions that are of interest to the legal profession
- An incident response plan (IRP) is a set of written instructions for reacting to a security incident

Risk Mitigation Summary

- A risk is a situation that involves exposure to some type of danger
- Privilege management and change management are risk management approaches
- Two approaches to risk calculation: qualitative risk calculation and quantitative risk calculation
- Several approaches are used to reduce risk
  - A security control and modifying the response to the risk instead of accepting the risk
- A policy is a document that outlines specific requirements or rules that must be met

Risk Mitigation Summary

- An acceptable use policy (AUP) defines the actions users may perform while accessing systems and networking equipment
- Other policies:
  - Personal email policy
  - Social media policy
- Different parties can reach an understanding of their relationships and responsibilities through interoperability agreements

CompTIA Security+ Exam

GOOD LUCK!