Cheat Sheet for comprehensive CompTIA Security+

Security Concepts

- **CIA Triad**
  - **Confidentiality**: Protecting data from unauthorized access.
  - **Integrity**: Ensuring data is accurate and unaltered.
  - **Availability**: Ensuring data is accessible to authorized users.
- **Defense in Depth**
  - Multiple layers of security controls to protect assets.
  - Examples: Firewalls, IDS/IPS, encryption, physical security.
- **Risk Management**
  - **Risk Assessment**: Identify, analyze, and evaluate risks.
  - **Risk Mitigation**: Implement controls to reduce risk.
  - **Risk Acceptance**: Accept the risk if it is within acceptable limits.
  - **Risk Transfer**: Transfer risk to another party (e.g., insurance).
  - **Risk Avoidance**: Avoid the activity that introduces risk.

Threats and Vulnerabilities

- **Threats**
  - **Malware**: Viruses, worms, Trojans, ransomware.
  - **Phishing**: Deceptive emails to gain sensitive information.
  - **Social Engineering**: Manipulating individuals to divulge information.
  - **Denial of Service (DoS)**: Overwhelming a system to make it unavailable.
  - **Man-in-the-Middle (MitM)**: Intercepting communication between parties.
- **Vulnerabilities**
  - **Software Vulnerabilities**: Bugs, flaws in code.
  - **Configuration Issues**: Misconfigurations in systems.

- **Human Factors**: Weak passwords, lack of awareness.

Security Controls

- **Technical Controls**

  - **Firewalls**: Network security systems that monitor and control incoming and outgoing network traffic.

  - **Intrusion Detection Systems (IDS)**: Monitors network traffic for suspicious activity.

  - **Intrusion Prevention Systems (IPS)**: Acts on detected malicious activity.

  - **Encryption**: Protects data by converting it into a secure format.

- **Administrative Controls**

  - **Policies**: Written guidelines for security practices.

  - **Procedures**: Step-by-step instructions for carrying out policies.

  - **Training**: Educating users on security best practices.

- **Physical Controls**

  - **Access Control**: Restricting physical access to facilities.

  - **Surveillance**: Monitoring with cameras and alarms.

  - **Environmental Controls**: Fire suppression, HVAC for temperature control.

Cryptography

- **Symmetric Encryption**

  - **Single Key**: Same key for encryption and decryption.

  - **Examples**: AES, DES, 3DES.

- **Asymmetric Encryption**

  - **Public/Private Key Pair**: Different keys for encryption and decryption.

  - **Examples**: RSA, ECC.

- **Hashing**

  - **One-Way Function**: Converts data into a fixed-size string of bytes.

  - **Examples**: MD5, SHA-256.

- **Digital Signatures**
  - **Authentication**: Verifies the identity of the sender.
  - **Integrity**: Ensures the message has not been altered.

Identity and Access Management (IAM)

- **Authentication Methods**
  - **Something You Know**: Passwords, PINs.
  - **Something You Have**: Smart cards, tokens.
  - **Something You Are**: Biometrics (fingerprints, facial recognition).
- **Authorization**
  - **Role-Based Access Control (RBAC)**: Access based on roles within an organization.
  - **Mandatory Access Control (MAC)**: Access based on security labels.
  - **Discretionary Access Control (DAC)**: Access controlled by the owner of the resource.
- **Account Management**
  - **Account Types**: User, Service, Guest.
  - **Lifecycle Management**: Creation, modification, deactivation.
  - **Password Policies**: Complexity, expiration, history.

Security Assessment and Testing

- **Vulnerability Scanning**
  - **Automated Tools**: Nessus, OpenVAS.
  - **Purpose**: Identify vulnerabilities in systems.
- **Penetration Testing**
  - **Simulated Attacks**: Ethical hacking to test defenses.
  - **Phases**: Planning, Discovery, Attack, Reporting.
- **Security Audits**
  - **Review of Controls**: Assess compliance with policies and standards.

- **Types**: Internal, External, Compliance.

Security Operations

- **Incident Response**

- **Phases**: Preparation, Detection, Analysis, Containment, Eradication, Recovery, Lessons Learned.

- **Incident Types**: Malware, DoS, Data Breach.

- **Disaster Recovery**

- **Backup Strategies**: Full, Incremental, Differential.

- **Recovery Time Objective (RTO)**: Maximum acceptable time to restore operations.

- **Recovery Point Objective (RPO)**: Maximum acceptable data loss measured in time.

- **Business Continuity**

- **Plan Development**: Identify critical functions and resources.

- **Testing**: Tabletop exercises, simulations.

Legal, Regulations, and Compliance

- **Regulatory Requirements**

- **GDPR**: General Data Protection Regulation (EU).

- **HIPAA**: Health Insurance Portability and Accountability Act (USA).

- **PCI DSS**: Payment Card Industry Data Security Standard.

- **Standards**

- **ISO/IEC 27001**: Information Security Management System (ISMS).

- **NIST SP 800-53**: Security and Privacy Controls for Federal Information Systems.

- **Legal Considerations**

- **Data Breach Notification**: Laws requiring notification of data breaches.

- **Privacy Laws**: Protecting personal information.

Network Security

- **Network Topologies**

- **LAN**: Local Area Network.
- **WAN**: Wide Area Network.
- **VPN**: Virtual Private Network.

- **Network Devices**
  - **Routers**: Direct traffic between networks.
  - **Switches**: Connect devices within a network.
  - **Firewalls**: Control incoming and outgoing network traffic.

- **Protocols**
  - **TCP/IP**: Transmission Control Protocol/Internet Protocol.
  - **HTTPS**: Secure version of HTTP.
  - **SSH**: Secure Shell for secure remote login.

Security Tools and Technologies

- **Network Monitoring**
  - **Wireshark**: Network protocol analyzer.
  - **Nagios**: Network monitoring and alerting.

- **Endpoint Security**
  - **Antivirus**: Detects and removes malware.
  - **Endpoint Detection and Response (EDR)**: Continuous monitoring and response for endpoints.

- **Security Information and Event Management (SIEM)**
  - **Log Management**: Collects and analyzes logs.
  - **Real-Time Analysis**: Detects and responds to security incidents.

Security Best Practices

- **Patch Management**

- Regularly update software to fix vulnerabilities.

- **User Awareness**

- Train users on phishing, social engineering, and secure practices.

- **Secure Configuration**

- Follow security baselines and hardening guides.

- **Data Protection**

- Encrypt sensitive data at rest and in transit.

Examples and Scenarios

- **Scenario: Phishing Attack**

  - **Detection**: Suspicious email with a link.

  - **Response**: Block the sender, educate the user, report to IT.

- **Scenario: Data Breach**

  - **Detection**: Unusual database access.

  - **Response**: Isolate the system, change passwords, notify authorities.

- **Scenario: Malware Infection**

  - **Detection**: High CPU usage, unusual network activity.

  - **Response**: Quarantine the device, run antivirus, restore from backup.

Quick Tips

- **Password Management**

- Use strong, unique passwords.
- Enable multi-factor authentication (MFA).

- **Network Security**

- Regularly update firewall rules.
- Use VPN for remote access.

- **Incident Response**

- Document all incidents for future reference.
- Conduct regular drills to improve response times.

Summary

- **Key Takeaways**

- Understand the CIA Triad and Defense in Depth.
- Implement strong authentication and authorization controls.
- Regularly assess and test your security posture.
- Stay compliant with relevant laws and standards.

This cheat sheet provides a comprehensive overview of essential concepts, tools, and best practices for the CompTIA Security+ certification. Use it as a quick reference to reinforce your knowledge and prepare for the exam.

By Ahmed Baheeg Khorshid

ver 1.0