Cheat Sheet for comprehensive CompTIA Secure Network Professional

Network Security Fundamentals

- **Security Zones**

  - **Demilitarized Zone (DMZ)**: Public-facing servers (e.g., web, email) isolated from internal network.

  - **Internal Network**: Protected network segment for sensitive data and resources.

  - **External Network**: Public internet.

- **Security Models**

  - **Defense in Depth**: Layered security approach (e.g., firewalls, IDS/IPS, encryption).

  - **Zero Trust**: "Never trust, always verify" principle; continuous authentication and authorization.

- **Security Controls**

  - **Preventive**: Firewalls, antivirus, access controls.

  - **Detective**: IDS/IPS, SIEM, log analysis.

  - **Corrective**: Patch management, incident response.

Firewalls and Access Control

- **Types of Firewalls**

  - **Packet Filtering**: Filters packets based on source/destination IP, port, protocol.

  - **Stateful Inspection**: Tracks connection state; more secure than packet filtering.

  - **Next-Generation Firewalls (NGFW)**: Includes deep packet inspection, application awareness, intrusion prevention.

- **Access Control Lists (ACLs)**

  - **Standard ACL**: Filters based on source IP address.

  - **Extended ACL**: Filters based on source/destination IP, port, protocol.

  - **Named ACL**: Uses names instead of numbers for easier management.

- **Firewall Rules**

- **Permit/Deny**: Allow or block traffic based on criteria.
- **Logging**: Enable logging for permitted and denied traffic.
- **NAT**: Network Address Translation for IP address hiding.

Intrusion Detection and Prevention Systems (IDS/IPS)

- **Types of IDS/IPS**
  - **Network-Based**: Monitors network traffic for suspicious activity.
  - **Host-Based**: Monitors individual host activity.
- **Detection Methods**
  - **Signature-Based**: Matches known attack patterns.
  - **Anomaly-Based**: Detects deviations from normal behavior.
- **Response Actions**
  - **Alert**: Notify security personnel.
  - **Block**: Automatically block suspicious traffic.
  - **Quarantine**: Isolate affected systems.

Secure Network Design

- **Network Segmentation**
  - **VLANs**: Virtual LANs for logical network segmentation.
  - **Subnets**: IP subnets for physical network segmentation.
- **Redundancy and High Availability**
  - **Load Balancers**: Distribute traffic across multiple servers.
  - **Failover Clustering**: Automatic switchover to backup systems.
- **Secure Protocols**
  - **SSH**: Secure remote access.
  - **HTTPS**: Secure web traffic.
  - **IPsec**: Secure VPN connections.

Wireless Security

- **Encryption Protocols**
  - **WPA3**: Latest standard; stronger encryption and improved security.
  - **WPA2**: AES encryption; widely used.
  - **WEP**: Weak encryption; avoid if possible.
- **Authentication Methods**
  - **Pre-Shared Key (PSK)**: Simple password-based authentication.
  - **802.1X**: Enterprise-level authentication using RADIUS.
- **Wireless Security Best Practices**
  - **Change Default SSID**: Customize network name.
  - **Disable SSID Broadcast**: Hide network from public view.
  - **Enable MAC Filtering**: Restrict access by device MAC address.

Network Monitoring and Logging

- **Key Metrics**
  - **Bandwidth Utilization**: Monitor network traffic volume.
  - **Latency**: Measure network response time.
  - **Packet Loss**: Track lost data packets.
- **Logging Tools**
  - **Syslog**: Centralized logging for network devices.
  - **SNMP**: Simple Network Management Protocol for monitoring devices.
  - **ELK Stack**: Elasticsearch, Logstash, Kibana for log analysis.
- **Log Retention**
  - **Regulatory Compliance**: Retain logs for required periods (e.g., PCI DSS, HIPAA).
  - **Backup**: Regularly back up logs to secure storage.

Incident Response and Disaster Recovery

- **Incident Response Phases**

- **Preparation**: Develop response plan, train personnel.
- **Detection and Analysis**: Identify and analyze incidents.
- **Containment**: Limit damage and prevent spread.
- **Eradication**: Remove threat and restore systems.
- **Recovery**: Restore normal operations.
- **Post-Incident Activity**: Lessons learned, updates to policies.

- **Disaster Recovery Plan**
  - **Backup Strategies**: Full, incremental, differential backups.
  - **Recovery Time Objective (RTO)**: Maximum acceptable downtime.
  - **Recovery Point Objective (RPO)**: Maximum acceptable data loss.

Security Policies and Compliance

- **Key Policies**
  - **Acceptable Use Policy (AUP)**: Defines permitted and prohibited activities.
  - **Password Policy**: Guidelines for creating strong passwords.
  - **BYOD Policy**: Rules for using personal devices in the workplace.
- **Regulatory Compliance**
  - **GDPR**: General Data Protection Regulation for EU data protection.
  - **HIPAA**: Health Insurance Portability and Accountability Act for healthcare data.
  - **PCI DSS**: Payment Card Industry Data Security Standard for credit card data.

Tools and Techniques

- **Network Scanning**
  - **Nmap**: Network mapper for scanning open ports and services.
  - **Wireshark**: Packet analyzer for network troubleshooting.
- **Vulnerability Assessment**
  - **Nessus**: Vulnerability scanner for identifying security weaknesses.
  - **OpenVAS**: Open-source vulnerability assessment tool.

- **Penetration Testing**
  - **Metasploit**: Framework for penetration testing and exploit development.
  - **Kali Linux**: Distro with tools for penetration testing and security auditing.

Best Practices

- **Regular Updates**
  - **Patch Management**: Regularly update software and firmware.
  - **Security Patches**: Apply critical security updates promptly.
- **User Training**
  - **Security Awareness**: Regular training on security best practices.
  - **Phishing Simulations**: Practice recognizing and responding to phishing attempts.
- **Physical Security**
  - **Access Controls**: Restrict physical access to critical infrastructure.
  - **Surveillance**: Use cameras and monitoring systems.

Examples

- **Firewall Rule Example**

```
Permit TCP 192.168.1.0/24 80 10.0.0.0/24 80
Deny All
```

- **VLAN Configuration Example**

```
interface vlan 10
ip address 192.168.10.1 255.255.255.0
```

- **SSH Command Example**

```
ssh user@192.168.1.100
```

Summary

- **Key Takeaways**

- Implement layered security controls.
- Regularly update and patch systems.
- Monitor and log network activity.
- Train users on security best practices.
- Develop and test incident response and disaster recovery plans.

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

By Ahmed Baheeg Khorshid

ver 1.0