Cheat Sheet for comprehensive CompTIA Secure Infrastructure Specialist

Network Security Fundamentals

Network Topologies

- **Bus Topology**: All devices connected to a single cable.
  - **Pros**: Easy to implement, cost-effective.
  - **Cons**: Single point of failure, limited cable length.
- **Star Topology**: All devices connected to a central hub or switch.
  - **Pros**: Easy to troubleshoot, centralized management.
  - **Cons**: Hub failure affects all devices.
- **Ring Topology**: Devices connected in a circular fashion.
  - **Pros**: Equal access to network, no collisions.
  - **Cons**: Single point of failure, difficult to troubleshoot.
- **Mesh Topology**: Each device connected to every other device.
  - **Pros**: High redundancy, fault tolerance.
  - **Cons**: Complex, expensive.

Network Devices

- **Router**: Connects different networks, routes data packets.
  - **Commands**: `show ip route`, `configure terminal`.
- **Switch**: Connects devices within a network, forwards data.
  - **Commands**: `show vlan`, `configure terminal`.
- **Firewall**: Controls incoming and outgoing network traffic.
  - **Commands**: `show firewall`, `configure firewall`.
- **Access Point (AP)**: Provides wireless access to a wired network.
  - **Commands**: `show wireless`, `configure wireless`.

Security Protocols

Encryption Protocols

- **SSL/TLS**: Secure data transmission over the internet.
  - **Ports**: 443 (HTTPS).
- **IPSec**: Secure IP communication.
  - **Modes**: Transport, Tunnel.
- **SSH**: Secure remote login.
  - **Ports**: 22.
- **VPN**: Secure remote access to a private network.
  - **Types**: PPTP, L2TP, OpenVPN.

Authentication Protocols

- **Kerberos**: Network authentication protocol.
  - **Components**: KDC, TGT, ST.
- **RADIUS**: Remote Authentication Dial-In User Service.
  - **Ports**: 1812 (auth), 1813 (acct).
- **TACACS+**: Terminal Access Controller Access-Control System Plus.
  - **Ports**: 49.

Security Best Practices

Password Management

- **Complexity**: Use a mix of uppercase, lowercase, numbers, and special characters.
- **Rotation**: Change passwords regularly (every 90 days).
- **MFA**: Enable Multi-Factor Authentication.

Patch Management

- **Regular Updates**: Apply patches and updates promptly.
- **Automated Tools**: Use tools like WSUS, SCCM.
- **Testing**: Test patches in a non-production environment.

Network Segmentation

- **VLANs**: Use Virtual LANs to segment network traffic.
- **DMZ**: Create a Demilitarized Zone for external-facing services.
- **Firewall Rules**: Implement strict inbound and outbound rules.

Incident Response

Phases of Incident Response

1. **Preparation**: Develop a plan, train staff.
2. **Detection & Analysis**: Identify and analyze incidents.
3. **Containment**: Limit the scope of the incident.
4. **Eradication**: Remove the threat.
5. **Recovery**: Restore systems and services.
6. **Lessons Learned**: Review and improve the response process.

Tools and Techniques

- **SIEM**: Security Information and Event Management.
  - **Examples**: Splunk, IBM QRadar.
- **Forensics**: Collect and analyze digital evidence.
  - **Tools**: EnCase, FTK.
- **Log Analysis**: Review system and application logs.
  - **Commands**: `grep`, `awk`.

Compliance and Regulations

Key Regulations

- **GDPR**: General Data Protection Regulation.
  - **Scope**: EU residents' data.
  - **Penalties**: Up to 4% of global turnover.
- **HIPAA**: Health Insurance Portability and Accountability Act.
  - **Scope**: Protected Health Information (PHI).

  - **Penalties**: Up to $1.5 million per violation.

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

  - **Scope**: Cardholder data.

  - **Penalties**: Up to $500,000 per incident.

Compliance Best Practices

- **Documentation**: Maintain detailed records of compliance activities.

- **Audits**: Conduct regular internal and external audits.

- **Training**: Train staff on compliance requirements.

Cloud Security

Cloud Models

- **IaaS**: Infrastructure as a Service.

  - **Examples**: AWS EC2, Azure VMs.

- **PaaS**: Platform as a Service.

  - **Examples**: Google App Engine, Heroku.

- **SaaS**: Software as a Service.

  - **Examples**: Office 365, Salesforce.

Security Considerations

- **Data Encryption**: Encrypt data at rest and in transit.

- **Access Control**: Implement strong authentication and authorization.

- **Monitoring**: Use cloud-native monitoring tools.

Tools and Technologies

Security Tools

- **Nessus**: Vulnerability scanner.

  - **Commands**: `nessuscli`, `nessusd`.

- **Wireshark**: Network protocol analyzer.

  - **Commands**: `wireshark`, `tshark`.

- **Metasploit**: Exploit framework.
  - **Commands**: `msfconsole`, `msfvenom`.

Automation

- **Ansible**: Configuration management and automation.
  - **Commands**: `ansible-playbook`, `ansible-vault`.
- **Puppet**: IT automation.
  - **Commands**: `puppet apply`, `puppet agent`.
- **Chef**: Infrastructure automation.
  - **Commands**: `chef-client`, `knife`.

Troubleshooting and Maintenance

Common Issues

- **Network Latency**: High ping times.
  - **Troubleshooting**: Use `ping`, `traceroute`.
- **Firewall Blocking**: Traffic not passing through.
  - **Troubleshooting**: Check firewall rules, use `telnet`.
- **Authentication Failures**: Login issues.
  - **Troubleshooting**: Verify credentials, check logs.

Maintenance Tasks

- **Backup**: Regularly back up data.
  - **Tools**: Veeam, Acronis.
- **Monitoring**: Continuously monitor network and system health.
  - **Tools**: Nagios, Zabbix.
- **Documentation**: Keep updated documentation of network and security configurations.

Conclusion

- **Continuous Learning**: Stay updated with the latest security trends and technologies.
- **Collaboration**: Work closely with other IT and security teams.

- **Best Practices**: Adopt and enforce security best practices across the organization.

By Ahmed Baheeg Khorshid

ver 1.0