Cheat Sheet for comprehensive Cisco Cybersecurity Certifications - CyberOps Professional

Network Security Fundamentals

Key Concepts

- **CIA Triad**: Confidentiality, Integrity, Availability
- **Threats**: Malware, Phishing, DDoS, Man-in-the-Middle
- **Vulnerabilities**: Software bugs, misconfigurations, human error
- **Controls**: Firewalls, IDS/IPS, Encryption, Access Control

Security Protocols

- **SSL/TLS**: Secure communication over networks
- **IPsec**: VPN encryption
- **SSH**: Secure remote login
- **HTTPS**: Secure HTTP traffic

Incident Response

Phases of Incident Response

1. **Preparation**
   - Develop IR plan, train staff, maintain backups
2. **Detection & Analysis**
   - Monitor logs, use SIEM, analyze alerts
3. **Containment**
   - Short-term vs. long-term containment strategies
4. **Eradication**
   - Remove malware, fix vulnerabilities
5. **Recovery**
   - Restore systems, verify functionality

6. **Lessons Learned**

- Document findings, update policies

Tools & Techniques

- **SIEM**: Splunk, ArcSight
- **Forensics**: Autopsy, FTK
- **Patch Management**: WSUS, SCCM

Threat Hunting

Techniques

- **Proactive Search**: Look for indicators of compromise (IOCs)
- **Data Analysis**: Correlate logs, identify anomalies
- **Behavioral Analysis**: Monitor user and system behavior

Tools

- **Threat Intelligence Platforms**: MISP, ThreatConnect
- **Network Monitoring**: Wireshark, tcpdump
- **Endpoint Detection & Response (EDR)**: Carbon Black, CrowdStrike

Security Operations Center (SOC)

Roles & Responsibilities

- **SOC Analyst**: Monitor, detect, respond to incidents
- **SOC Manager**: Oversee operations, manage teams
- **Incident Handler**: Contain, eradicate, recover from incidents

Best Practices

- **24/7 Monitoring**: Continuous surveillance
- **Alert Prioritization**: Triage based on severity
- **Collaboration**: Work with other teams (e.g., IT, Legal)

Network Traffic Analysis

Key Metrics

- **Throughput**: Data transfer rate

- **Latency**: Time delay in data transfer
- **Jitter**: Variation in latency
- **Packet Loss**: Percentage of lost packets

Tools

- **Wireshark**: Packet analysis
- **PRTG**: Network monitoring
- **Nagios**: Infrastructure monitoring

Log Management & Analysis

Log Sources

- **Firewalls**: Cisco ASA, Palo Alto
- **Servers**: Windows, Linux
- **Applications**: Web servers, databases

Tools

- **ELK Stack**: Elasticsearch, Logstash, Kibana
- **Splunk**: Log aggregation and analysis
- **Graylog**: Centralized log management

Automation & Orchestration

Benefits

- **Efficiency**: Automate repetitive tasks
- **Consistency**: Ensure uniform execution
- **Scalability**: Handle large-scale operations

Tools

- **Ansible**: Configuration management
- **Puppet**: IT automation
- **Terraform**: Infrastructure as code

Compliance & Governance

Regulatory Requirements

- **GDPR**: EU data protection
- **HIPAA**: US healthcare data
- **PCI DSS**: Payment card industry

Best Practices

- **Policy Development**: Create clear security policies
- **Audit & Review**: Regular compliance audits
- **Documentation**: Maintain detailed records

Cyber Threat Intelligence

Types of Intelligence

- **Strategic**: High-level, long-term trends
- **Tactical**: Specific threats, attack methods
- **Operational**: Immediate actions, incident response
- **Technical**: Detailed technical data, IOCs

Sources

- **Open Source**: Publicly available data
- **Commercial**: Paid services, threat feeds
- **Government**: National security agencies
- **Community**: Security forums, mailing lists

Practical Tips & Tricks

Network Troubleshooting

- **Ping**: Test connectivity
- **Traceroute**: Trace path to destination
- **Telnet**: Test port connectivity

Security Best Practices

- **Regular Updates**: Patch systems regularly

- **Strong Passwords**: Use complex, unique passwords
- **Multi-Factor Authentication**: Add an extra layer of security

Incident Response Checklist

- **Isolate Affected Systems**: Contain the breach
- **Gather Evidence**: Collect logs, network captures
- **Notify Stakeholders**: Inform relevant parties
- **Document Everything**: Maintain detailed records

Example Scenarios

Scenario 1: Phishing Attack

- **Detection**: Email flagged by spam filter
- **Response**: Quarantine email, notify users, reset compromised accounts

Scenario 2: DDoS Attack

- **Detection**: High traffic, network latency
- **Response**: Activate DDoS mitigation, block malicious IPs, notify ISP

Scenario 3: Ransomware

- **Detection**: Unusual encryption activity
- **Response**: Isolate affected systems, restore from backup, notify law enforcement

Summary

- **Understand Fundamentals**: CIA Triad, Threats, Vulnerabilities
- **Master Incident Response**: Phases, Tools, Techniques
- **Leverage Threat Hunting**: Proactive search, data analysis
- **Optimize SOC Operations**: Roles, Best Practices
- **Analyze Network Traffic**: Key metrics, tools
- **Manage Logs**: Sources, tools, analysis
- **Automate & Orchestrate**: Benefits, tools
- **Ensure Compliance**: Regulatory requirements, best practices
- **Utilize Threat Intelligence**: Types, sources

- **Apply Practical Tips**: Troubleshooting, security best practices
- **Respond to Scenarios**: Phishing, DDoS, Ransomware

By Ahmed Baheeg Khorshid

ver 1.0