Cheat Sheet for comprehensive Cisco Cybersecurity Certifications - CyberOps Associate

Network Fundamentals

- **OSI Model Layers**
  - **Layer 7: Application** (HTTP, FTP)
  - **Layer 6: Presentation** (Encryption, Compression)
  - **Layer 5: Session** (Session Management)
  - **Layer 4: Transport** (TCP, UDP)
  - **Layer 3: Network** (IP, Routing)
  - **Layer 2: Data Link** (MAC, Switching)
  - **Layer 1: Physical** (Cables, Signals)
- **TCP/IP Model**
  - **Application Layer** (HTTP, FTP, DNS)
  - **Transport Layer** (TCP, UDP)
  - **Internet Layer** (IP, ICMP)
  - **Network Access Layer** (Ethernet, ARP)

Network Security Concepts

- **Threats and Vulnerabilities**
  - **Malware**: Viruses, Worms, Trojans
  - **Phishing**: Email scams, social engineering
  - **DDoS**: Distributed Denial of Service
  - **Man-in-the-Middle (MitM)**: Intercepting communications
- **Security Controls**
  - **Firewalls**: Packet filtering, stateful inspection
  - **IDS/IPS**: Intrusion Detection/Prevention Systems

- **Encryption**: SSL/TLS, VPNs
- **Access Control**: ACLs, RBAC

Network Traffic Analysis

- **Tools**
  - **Wireshark**: Packet capture and analysis
  - **tcpdump**: Command-line packet analyzer
  - **NetFlow**: Traffic analysis and reporting
- **Protocols**
  - **HTTP/HTTPS**: Web traffic
  - **DNS**: Domain Name System
  - **SMTP/POP3/IMAP**: Email protocols
  - **SSH/Telnet**: Remote access

Incident Response

- **Phases**
  - **Preparation**: Policies, procedures, tools
  - **Detection & Analysis**: Alerts, logs, indicators
  - **Containment**: Isolate affected systems
  - **Eradication**: Remove threat, clean systems
  - **Recovery**: Restore services, verify integrity
  - **Lessons Learned**: Review, update policies
- **Tools**
  - **SIEM**: Security Information and Event Management
  - **Log Management**: Centralized logging
  - **Forensics Tools**: Disk imaging, memory analysis

Security Monitoring

- **Key Metrics**

- **Availability**: Uptime, downtime
- **Performance**: Latency, throughput
- **Compliance**: Policy adherence
- **Threat Detection**: Alerts, anomalies

- **Logs and Alerts**
  - **Syslog**: Standard for logging
  - **SNMP**: Network monitoring
  - **Sysmon**: Windows system monitoring

Automation and Orchestration

- **Tools**
  - **Ansible**: Configuration management
  - **Puppet**: IT automation
  - **Chef**: Infrastructure automation
- **Use Cases**
  - **Patch Management**: Automated updates
  - **Compliance Audits**: Automated checks
  - **Incident Response**: Automated scripts

Cloud Security

- **Key Concepts**
  - **Shared Responsibility Model**: Cloud provider vs. customer
  - **IAM**: Identity and Access Management
  - **Data Encryption**: At rest and in transit
- **Best Practices**
  - **Least Privilege**: Minimal access rights
  - **Multi-Factor Authentication (MFA)**
  - **Regular Audits**: Compliance checks

Practical Tips and Tricks

- **Wireshark Shortcuts**

- `Ctrl+Shift+N`: Next packet
- `Ctrl+Shift+B`: Previous packet
- `Ctrl+Shift+R`: Follow TCP stream

- **tcpdump Commands**

- `tcpdump -i eth0`: Capture on interface eth0
- `tcpdump -w capture.pcap`: Write to file
- `tcpdump -r capture.pcap`: Read from file

- **NetFlow Commands**

- `show flow exporter`: Display flow exporter settings
- `show flow monitor`: Display flow monitor settings

- **SIEM Queries**

  - **Suspicious Login**: `eventType="login" AND status="failed"`

  - **High Traffic**: `protocol="HTTP" AND bytes > 1000000`

Example Scenarios

- **DDoS Attack Detection**

  - **Symptoms**: High CPU, network congestion

  - **Response**: Block suspicious IPs, enable scrubbing

- **Phishing Email Analysis**

  - **Indicators**: Suspicious links, attachments

  - **Response**: Quarantine, user education

- **Unauthorized Access**

  - **Detection**: Failed login attempts

  - **Response**: Lock account, investigate logs

Resources and References

- **Cisco Documentation**

- [Cisco Security](https://www.cisco.com/c/en/us/products/security/index.html)

- [Cisco CyberOps Associate](https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/cyberops-associate.html)

- Books

- *Network Security Essentials* by William Stallings
- *Incident Response & Computer Forensics* by Jason Luttgens

- Online Courses

- [Cisco Networking Academy](https://www.netacad.com/)
- [Udemy Cybersecurity Courses](https://www.udemy.com/topic/cyber-security/)

Summary

- Key Takeaways

- Understand network fundamentals and security concepts.
- Master network traffic analysis and incident response.
- Utilize security monitoring and automation tools.
- Apply cloud security best practices.
- Practice with real-world scenarios and tools.

This cheat sheet provides a comprehensive overview of essential topics for the Cisco CyberOps Associate certification, ensuring you are well-prepared for the exam and real-world cybersecurity operations.

By Ahmed Baheeg Khorshid

ver 1.0