Cheat Sheet for comprehensive Cisco Certified Network Associate (CCNA) - Security

Network Security Fundamentals

- **Security Threats**
  - **Malware**: Viruses, Worms, Trojans, Ransomware
  - **Phishing**: Email scams to trick users into revealing sensitive information
  - **DDoS**: Distributed Denial of Service attacks
  - **Man-in-the-Middle (MitM)**: Intercepting communication between two parties
- **Security Principles**
  - **Confidentiality**: Ensuring data is accessible only to those authorized to have access
  - **Integrity**: Ensuring data is not altered in transit
  - **Availability**: Ensuring systems and data are accessible when needed

Cisco IOS Security Features

- **Access Control Lists (ACLs)**
  - **Standard ACLs**: Filter based on source IP address

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

  - **Extended ACLs**: Filter based on source/destination IP, protocol, and port

```
access-list 101 permit tcp 192.168.1.0 0.0.0.255 host 10.0.0.1 eq 80
```

  - **Applying ACLs**:

```
interface GigabitEthernet0/1
ip access-group 101 in
```

- **Port Security**

- **Enabling Port Security**:

```
interface GigabitEthernet0/1
switchport mode access
switchport port-security
```

- **Configuring Maximum MAC Addresses**:

```
switchport port-security maximum 2
```

- **Violation Mode**:

```
switchport port-security violation restrict
```

Firewalls and Intrusion Prevention Systems (IPS)

- **Cisco Firepower**

- **Deploying Firepower**:

```
configure terminal
firewall
```

- **Creating Access Rules**:

```
access-list extended ALLOW_HTTP
permit tcp any any eq www
```

- **Applying Access Rules**:

```
interface GigabitEthernet0/1
ip access-group ALLOW_HTTP in
```

- **Intrusion Prevention System (IPS)**

- **Deploying IPS**:

```
configure terminal
ips
```

- **Configuring IPS Policies**:

```
policy-map type inspect ips_policy
class type inspect ips_class
```

- **Applying IPS Policies**:

```
service-policy ips_policy global
```

VPN and Encryption

- **IPsec VPN**

- **Configuring Site-to-Site VPN**:

```
crypto isakmp policy 10
encryption aes
hash sha
authentication pre-share
group 2
lifetime 86400
```

- **Configuring IPsec Transform Set**:

```
crypto ipsec transform-set MY_SET esp-aes esp-sha-hmac
```

- **Configuring Crypto Map**:

```
crypto map MY_MAP 10 ipsec-isakmp
set peer 10.0.0.1
set transform-set MY_SET
match address 101
```

- **SSL VPN**

- **Enabling SSL VPN**:

```
webvpn
enable outside
```

- **Configuring SSL VPN Access**:

```
tunnel-group 10.0.0.1 type remote-access
tunnel-group 10.0.0.1 general-attributes
address-pool 192.168.1.0 255.255.255.0
```

AAA (Authentication, Authorization, and Accounting)

- **Configuring AAA**

- **Setting Up Local Authentication**:

```
aaa new-model
aaa authentication login default local
```

- **Configuring TACACS+**:

```
aaa authentication login default group tacacs+ local
tacacs-server host 10.0.0.1 key mysecretkey
```

- **Configuring RADIUS**:

```
aaa authentication login default group radius local
radius-server host 10.0.0.2 key mysecretkey
```

Secure Routing Protocols

- **OSPF Authentication**

- **Configuring MD5 Authentication**:

```
interface GigabitEthernet0/1
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 mysecretkey
```

- **Configuring Simple Password Authentication**:

```
interface GigabitEthernet0/1
ip ospf authentication
ip ospf authentication-key mypassword
```

- **EIGRP Authentication**

  - **Configuring MD5 Authentication**:

```
key chain mykeychain
key 1
key-string mysecretkey
interface GigabitEthernet0/1
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 mykeychain
```

Secure Network Management

- **Secure Shell (SSH)**

  - **Configuring SSH**:

```
ip domain-name mydomain.com
crypto key generate rsa
username admin privilege 15 secret mypassword
line vty 0 4
login local
transport input ssh
```

- **SNMPv3**

  - **Configuring SNMPv3**:

```
snmp-server user admin network-admin auth md5 myauthkey priv aes
128 myprivkey
```

Security Best Practices

- **Regular Updates**

- Keep firmware and software up to date
- Apply security patches promptly

- **Strong Passwords**

- Use complex passwords
- Change default passwords immediately

- **Network Segmentation**

- Use VLANs to segment networks
- Implement firewalls between segments

- **Monitoring and Logging**

- Enable logging and review logs regularly
- Use tools like Cisco Security Manager for centralized monitoring

Troubleshooting and Maintenance

- **Common Issues**

  - **ACL Misconfigurations**: Check ACLs for correct syntax and placement

  - **Port Security Violations**: Review port security settings and violation modes

  - **VPN Connectivity Issues**: Verify IPsec and SSL VPN configurations

- **Commands for Troubleshooting**

  - **Show Commands**:

```
show running-config
show access-lists
show port-security
show crypto isakmp sa
show ipsec sa
show webvpn
show aaa
```

  - **Debug Commands**:

```
debug ip packet
debug crypto isakmp
debug aaa authentication
```

Additional Resources

- **Cisco Documentation**

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

- **Cisco Learning Network**

- [Cisco Learning Network](https://learningnetwork.cisco.com/)

- **Cisco Security Blog**

- [Cisco Security Blog](https://blogs.cisco.com/security)

This cheat sheet provides a comprehensive overview of essential security features, configurations, and best practices for the Cisco Certified Network Associate (CCNA) - Security certification. Use these tips and commands to secure your network effectively.

By Ahmed Baheeg Khorshid

ver 1.0