# Chapter 4 - QUIZ – Network Security

1. Match the term on the left to the associated description on the right.

| | | | |
|---|---|---|---|
| A. | Operating system weakness. | ➔ | Technological Weakness |
| B. | Unsecured user accounts. | ➔ | Configuration Weakness |
| C. | Network equipment weaknesses. | ➔ | Technological Weakness |
| D. | Unsecured default settings. | ➔ | Configuration Weakness |
| E. | Lack of consistency and continuity. | ➔ | Security Policy Weakness |
| F. | TCP/IP and ICMP weaknesses. | ➔ | Technological Weakness |
| G. | Lack of disaster recovery plan. | ➔ | Security Policy Weakness |

2. Which two pieces of information can be determined from opening the Cisco SDM homepage of a router? (Choose two.)
   A. Routing table.
   B. CDP neighbors.
   C. Snapshot of the router configuration.
   D. Interface status.
   E. Features supported by the Cisco I O S software.

3. A technician has been asked to perform a Cisco SDM one-step lockdown test. Which location should be used to initiate the test?
   A. Diagnostic mode on the Firewall page.
   B. Configure mode on the Security Audit page.
   C. Test mode on the Security Audit page.
   D. Test mode on the Firewall page.

4. Match the term on the left to the associated description on the right.

| | | | |
|---|---|---|---|
| A. | Reconnaissance attack | ➔ | Using ping sweeps, port scans, and packet sniffers to gain information about a network. |
| B. | Password attack | ➔ | Dictionary cracking and brute force attack. |
| C. | Port redirection | ➔ | Using a compromised host to pass traffic through a firewall that would otherwise be dropped. |
| D. | Worm, virus, Trojan horse | ➔ | Malicious software designed to damage a system, replicate itself, or deny services or access to networks, systems, or services. |
| E. | DoS attack | ➔ | Flooding a network device with traffic in an attempt to render it unusable for legitimate traffic. |

5. What is a major advantage of HIPS over HIDS?
   A. HIPS does not require host-based client software.
   B. HIPS consumes fewer system resources.
   C. HIPS can prevent intrusions.
   D. HIPS prevents the need to update signature files as often.

6. What is the core or hub component of the Security Wheel?
   A. secure
   B. monitor
   C. improve
   D. test
   E. security policy

7. As part of a network security plan, where does Cisco recommend that administrators send events captured by syslog?
   A. flash
   B. NV RAM
   C. designated log hosts
   D. designated TFTP clients
   E. designated SNMP clients

8. Which protocol should be used when strong privacy and session integrity are needed for remote router administration?
   A. HTTP
   B. SNMP
   C. SSH
   D. Telnet
   E. TFTP

9. Match the policy on the left to its associated description on the right. Not all options are used.

| | | | |
|---|---|---|---|
| A. | Account access request policy | ➔ | Formalizes the process of how users request access to systems. |
| B. | Remote access policy | ➔ | Defines the standards for connecting to the internal network from outside the organization. |
| C. | Risk assessment policy | x | |
| D. | Audit policy | ➔ | Specifies procedures to investigate incidents, ensure conformance to security policies, and monitor user and system activity. |
| E. | Acceptable use policy. | ➔ | Defines how network resources may and may not be employed. |

10. Match the three items required to configure SDM to the steps in the proper sequence. Not all options are used.

| | | | |
|---|---|---|---|
| A. | Use the **auto secure** command to configure router security. | x | |
| B. | Enable the HTTP and HTTP S servers on the router. | ➔ | Step 2 |
| C. | Create a user account defined with privilege level 15. | ➔ | Step 3 |
| D. | Create a user account defined with privilege level 0. | x | |
| E. | Create an ACL to allow HTTP traffic into the router and apply it to the vty's. | x | |
| F. | Configure SSH and Telnet for local login and privilege level 15. | ➔ | Step 1 |
| G. | Configure SSH and Telnet for local login and privilege level 0. | x | |

11. Which three services should be disabled on a router to prevent security vulnerabilities? (Choose three.)
   A. Network Time Protocol (NTP)
   B. Domain Name System (DNS)
   C. Secure Socket Layer (SSL)
   D. Cisco Express Forwarding (CEF)
   E. Simple Network Management Protocol (SNMP)
   F. Secure Shell (SSH)

12. Which feature provides a straightforward one-touch device lockdown for configuring the security posture of routers?
   A. SSH
   B. SDM
   C. AutoSecure
   D. SNMP

13. Match the descriptions on the left to the appropriate protocol on the right. Not all descriptions are used.

| | | | |
|---|---|---|---|
| A. | Application Layer protocol that provides a facility for retrieving and posting data for monitoring and management of devices in a network using TCP for 161. | ➔ | Simple Network Management Protocol (SNMP). |
| B. | Protocol designed to synchronize the time on a network of machines and runs over UDP using port 123. | ➔ | Network Time Protocol (NTP) |
| C. | Distributed database that maps hostnames to IP addresses using services | ➔ | Domain Name System (DNS). |

14. Which feature is a web-based-management tool for Cisco I O S software-based routers?

A. SSH
B. SDM
C. AutoSecure
D. SNMP

15. Which three SDM wizards are available to configure a router? (Choose three.)

A. Security audit
B. Firewall
C. DHCP
D. NAT
E. Routing
F. Access list