CCNA4 v 4.0 Exam chapter 4 Network Security

1. Which two statements are true regarding network security? (Choose two.)

Securing a network against internal threats is a lower priority because company employees represent a low security risk.
Both experienced hackers who are capable of writing their own exploit code and inexperienced individuals who download exploits from the Internet pose a serious threat to network security.
Assuming a company locates its web server outside the firewall and has adequate backups of the web server, no further security measures are needed to protect the web server because no harm can come from it being hacked.
Established network operating systems like UNIX and network protocols like TCP/IP can be used with their default settings because they have no inherent security weaknesses.
Protecting network devices from physical damage caused by water or electricity is a necessary part of the security policy.

2. Which two statements are true about network attacks? (Choose two.)

Strong network passwords mitigate most DoS attacks.
Worms require human interaction to spread, viruses do not.
Reconnaissance attacks are always electronic in nature, such as ping sweeps or port scans.
A brute-force attack searches to try every possible password from a combination of characters.
Devices in the DMZ should not be fully trusted by internal devices, and communication between the DMZ and internal devices should be authenticated to prevent attacks such as port redirection.

3. Users are unable to access a company server. The system logs show that the server is operating slowly because it is receiving a high level of fake requests for service. Which type of attack is occurring?

reconnaissance
access
DoS
worm
virus
Trojan horse

4. An IT director has begun a campaign to remind users to avoid opening e-mail messages from suspicious sources. Which type of attack is the IT director trying to protect users from?

DoS
DDoS
virus
access
reconnaissance

5. Which two statements regarding preventing network attacks are true? (Choose two.)

The default security settings for modern server and PC operating systems can be trusted to have secure default security settings.
Intrusion prevention systems can log suspicious network activity, but there is no way to counter an attack in progress without user intervention.
Physical security threat mitigation consists of controlling access to device console ports, labeling critical cable runs, installing UPS systems, and providing climate control.
Phishing attacks are best prevented by firewall devices.
Changing default usernames and passwords and disabling or uninstalling unnecessary services are aspects of device hardening.

6. Intrusion detection occurs at which stage of the Security Wheel?

securing
monitoring
testing
improvement
reconnaissance

7. Which two objectives must a security policy accomplish? (Choose two.)

provide a checklist for the installation of secure servers
describe how the firewall must be configured
document the resources to be protected
identify the security objectives of the organization
identify the specific tasks involved in hardening a router

8. What are three characteristics of a good security policy? (Choose three.)

It defines acceptable and unacceptable use of network resources.
It communicates consensus and defines roles.
It is developed by end users.
It is developed after all security devices have been fully tested.
It defines how to handle security incidents.
It should be encrypted as it contains backups of all important passwords and keys.

9. Which two statements define the security risk when DNS services are enabled on the network? (Choose two.)

By default, name queries are sent to the broadcast address 255.255.255.255.
DNS name queries require the **ip directed-broadcast** command to be enabled on the Ethernet interfaces of all routers.
Using the global configuration command **ip name-server** on one router enables the DNS services on all routers in the network.
The basic DNS protocol does not provide authentication or integrity assurance.
The router configuration does not provide an option to set up main and backup DNS servers.

10. What are two benefits of using Cisco AutoSecure? (Choose two.)

It gives the administrator detailed control over which services are enabled or disabled.
It offers the ability to instantly disable non-essential system processes and services.
It automatically configures the router to work with SDM.
It ensures the greatest compatibility with other devices in your network.
It allows the administrator to configure security policies without having to understand all of the Cisco IOS software features.

11. Refer to the exhibit. A network administrator is trying to configure a router to use SDM, but it is not functioning correctly. What could be the problem?

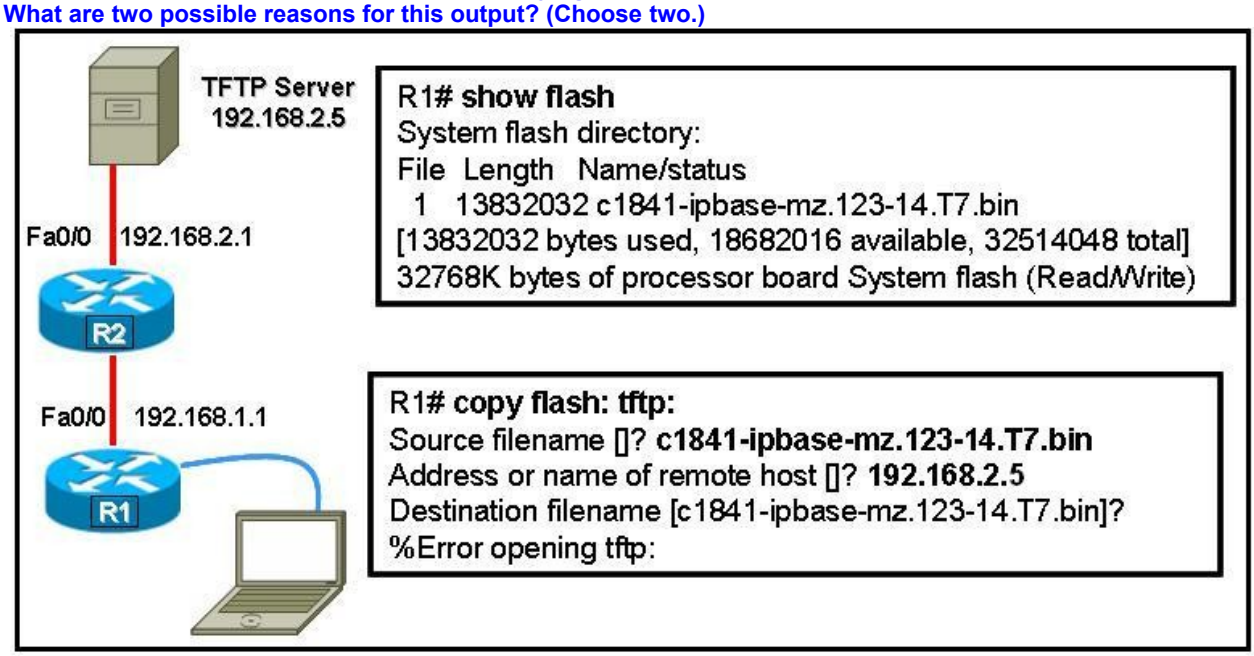
```
<output omitted>
!
username sdm privilege 5 password 0 sdm
!
ip http server
ip http authentication local
ip http secure-server
ip http timeout-policy idle 600 life 86400 requests 10000
!
<output omitted>
!
line con 0
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
```

The privilege level of the user is not configured correctly.
The authentication method is not configured correctly.
The HTTP server is not configured correctly.
The HTTP timeout policy is not configured correctly.

12. The Cisco IOS image naming convention allows identification of different versions and capabilities of the IOS. What information can be gained from the filename c2600-d-mz.121-4? (Choose two.)

The "mz" in the filename represents the special capabilities and features of the IOS.
The file is uncompressed and requires 2.6 MB of RAM to run.
The software is version 12.1, 4th revision.
The file is downloadable and 121.4MB in size.
The IOS is for the Cisco 2600 series hardware platform.

13. Refer to the exhibit. The network administrator is trying to back up the Cisco IOS router software and receives the output shown. What are two possible reasons for this output? (Choose two.)



The Cisco IOS file has an invalid checksum.
The TFTP client on the router is corrupt.
The router cannot connect to the TFTP server.
The TFTP server software has not been started.
There is not enough room on the TFTP server for the software.

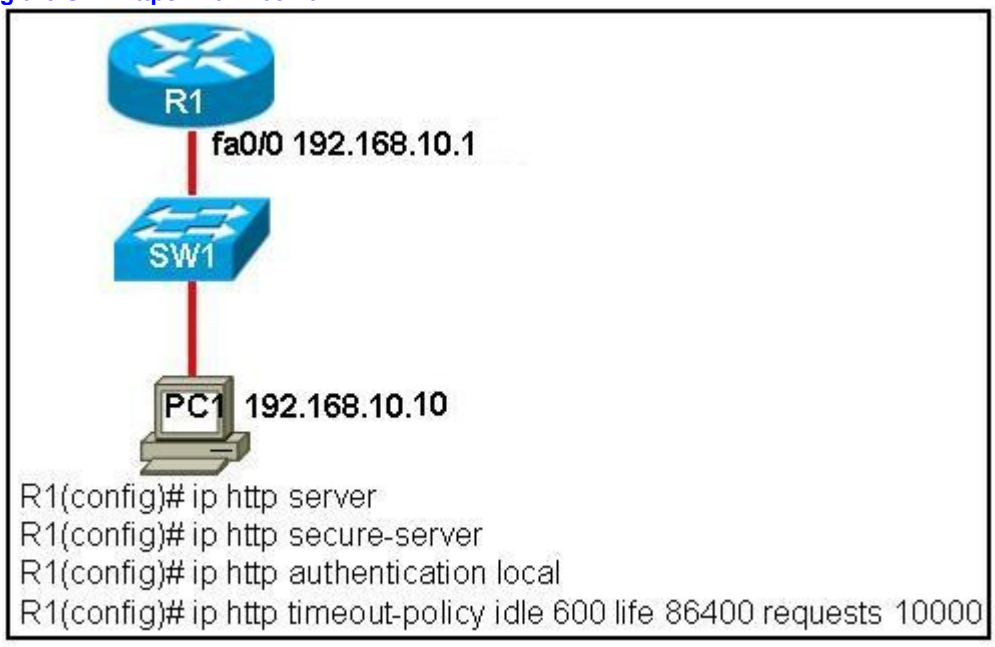
14. Which two conditions should the network administrator verify before attempting to upgrade a Cisco IOS image using a TFTP server? (Choose two.)

Verify the name of the TFTP server using the **show hosts** command.
Verify that the TFTP server is running using the **tftpdnld** command.
Verify that the checksum for the image is valid using the **show version** command.

Verify connectivity between the router and TFTP server using the ping command.
Verify that there is enough flash memory for the new Cisco IOS image using the show flash command.

15. The password recovery process begins in which operating mode and using what type of connection? (Choose two.)
ROM monitor
boot ROM
Cisco IOS
direct connection through the console port
network connection through the Ethernet port
network connection through the serial port

16. Refer to the exhibit. Security Device Manager (SDM) is installed on router R1. What is the result of opening a web browser on PC1 and entering the URL https://192.168.10.1?



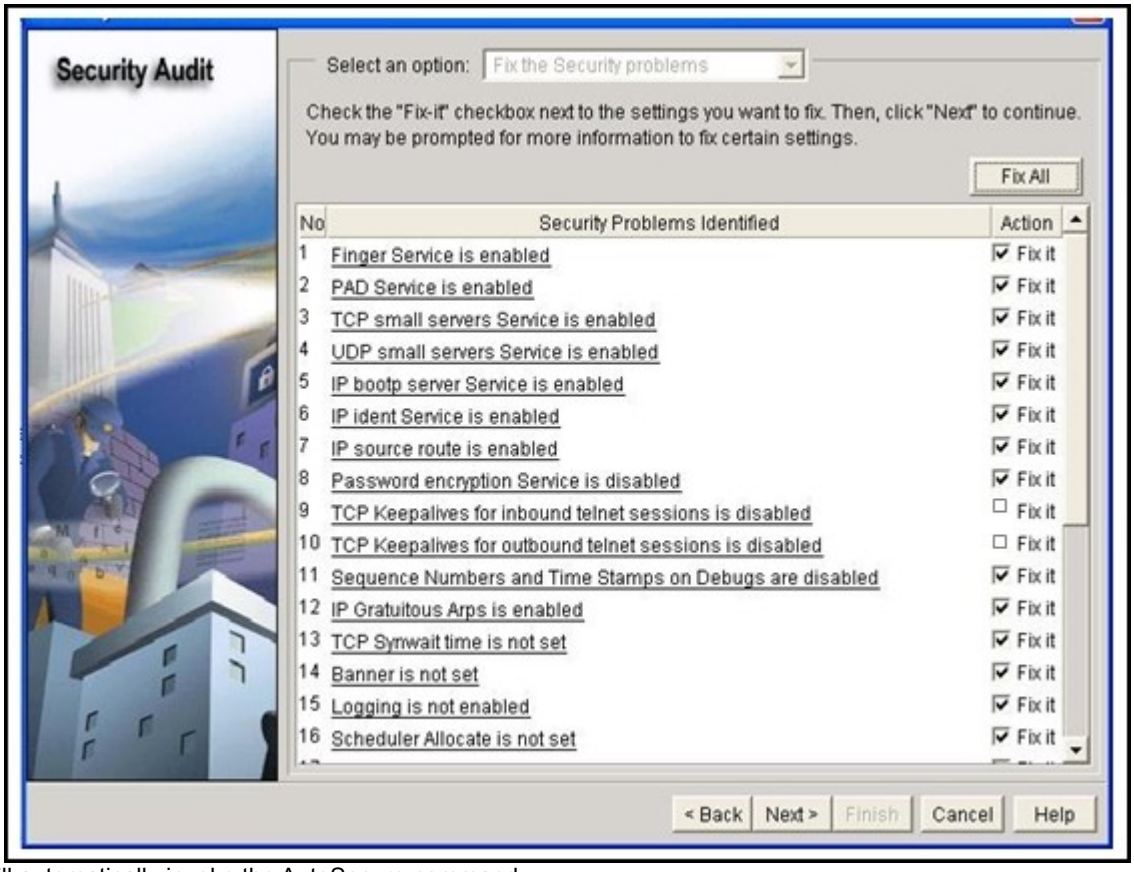
The password is sent in plain text.
A Telnet session is established with R1.
The SDM page of R1 appears with a dialog box that requests a username and password.
The R1 home page is displayed and allows the user to download Cisco IOS images and configuration files.

17. Which statement is true about Cisco Security Device Manager (SDM)?
SDM can run only on Cisco 7000 series routers.
SDM can be run from router memory or from a PC.
SDM should be used for complex router configurations.
SDM is supported by every version of the Cisco IOS software.

18. Which step is required to recover a lost enable password for a router?
Set the configuration register to bypass the startup configuration.
Copy the running configuration to the startup configuration.
Reload the IOS from a TFTP server from ROMMON.
Reconfigure the router using setup mode.

19. What is the best defense for protecting a network from phishing exploits?
Schedule antivirus scans.
Schedule antispyware scans .
Schedule training for all users.
Schedule operating systems updates.

20. Refer to the exhibit. Security Device Manager (SDM) has been used to configure a required level of security on the router. What would be accomplished when the SDM applies the next step on the security problems that are identified on the router?



SDM will automatically invoke the AutoSecure command.
SDM will generate a report that will outline the proper configuration actions to alleviate the security issues.
SDM will create a configuration file that can be copy and pasted into the router to reconfigure the services.
SDM will reconfigure the services that are marked in the exhibit as "fix it" to apply the suggested security changes.

21. Refer to the exhibit. What is the purpose of the "ip ospf message-digest-key 1 md5 cisco" statement in the configuration?

```
R3# show running-config
<output omitted>
interface serial0/0/0
ip ospf  message-digest-key 1 md5 cisco
<output omitted>
```

to specify a key that is used to authenticate routing updates
to save bandwidth by compressing the traffic
to enable SSH encryption of traffic
to create an IPsec tunnel

22. Refer to the exhibit. What is accomplished when both commands are configured on the router?

```
R1(config)# no service tcp-small-servers
R1(config)# no service udp-small-servers
```

The commands filter UDP and TCP traffic coming to the router.
The commands disable any TCP or UDP request sent by the routing protocols.
The commands disable the services such as echo, discard, and chargen on the router to prevent security vulnerabilities.
The commands disable the BOOTP and TFTP server services to prevent security vulnerabilities.