Take Assessment - EWAN Chapter 4 - CCNA Exploration: Accessing the WAN (Version 4.0)

1 What are two valid methods for upgrading an IOS image? (Choose two.)

- [ ] copy-and-paste through a console connection
- [ ] copy-and-paste through a network connection
- [ ] TFTP through a console connection
- [ ] TFTP through a network connection
- [ ] Xmodem through a console connection
- [ ] Xmodem through a network connection

---

2 A company has a web server on the company DMZ to provide external web services. While reviewing firewall log files, an administrator notices that a connection has been made from the web server to an internal e-mail server. Upon further investigation, the administrator discovers that an unauthorized account has been created on the internal server. Which type of attack was successfully carried out?

- ● phishing
- ● port redirection
- ● trust exploitation
- ● man-in-the-middle

---

3 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.

4

```
Router1(config)# access-list 1 permit 192.168.0.1 0.0.0.255
Router1(config)# line vty 0 4
Router1(config-line)# transport input ssh
Router1(config-line)# password cisco
Router1(config-line)# access-class 1 in
```

Refer to the exhibit. Which two statements are true about the configuration shown? (Choose two.)

- The remote session is encrypted.
- Telnet is permitted in vty lines 0 and 4.
- Passwords are sent in clear text.
- Host 192.168.0.15 is permitted on vty lines 0 through 4.
- Traffic from networks other than 192.168.0.0 is blocked from traversing Router1.

---

5 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.

6 When a user establishes an SDM connection with a Cisco router and is examining the Configuration Overview area of the home page, which three pieces of information are available? (Choose three.)

- [ ] MAC address of all DHCP clients
- [ ] total number of Cisco SDM-supported WAN interfaces on the router
- [ ] type of compression enabled on WAN interfaces
- [ ] total number of DMZ interfaces
- [ ] status of the DNS server
- [ ] number of site-to-site VPN connections

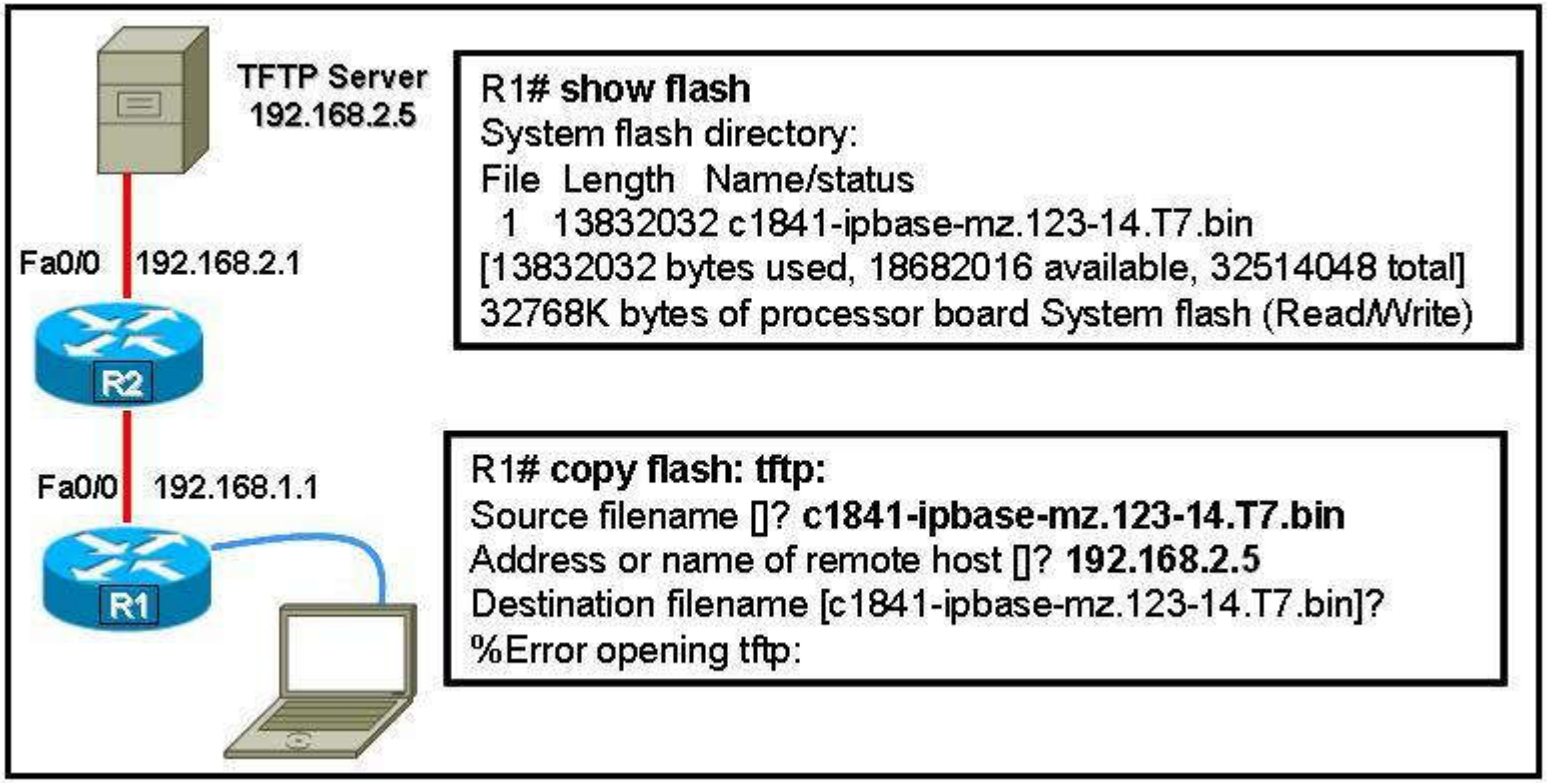
7 An IT director has begun a campaign to remind users to avoid opening e-mail messages from suspicious sources. Which type of attack is the IT director trying to protect users from?

- DoS
- DDoS
- virus
- access
- reconnaissance

8 Intrusion detection occurs at which stage of the Security Wheel?

- securing
- monitoring
- testing
- improvement
- reconnaissance

9



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.

---

10 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

---

11 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.

12

```
<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
```

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?

- 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.

---

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

- [ ] Reconnaissance attacks are always electronic in nature, such as ping sweeps or port scans.
- [ ] 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.
- [ ] Worms require human interaction to spread, viruses do not.
- [ ] Strong network passwords mitigate most DoS attacks.
- [ ] Given time, a brute force attack always yields the password, as long as the password is made up of the characters selected to test.

---

14 Which two statements define the security risk that is presented by SNMPv1 or SNMPv2 when either is enabled on the network? (Choose two.)

- [ ] SNMP uses authentication strings called community strings, which are stored and sent across the network in plain text.
- [ ] Only the station that acts as a SNMP manager can encrypt the request and respond messages. All other machines that act as SNMP agents send the messages in plain text.
- [ ] A SNMP agent can encrypt the inform requests but not the trap requests.
- [ ] No access list can be defined for the SNMP messages that are sent by the SNMP agents.
- [ ] SNMP is an easily spoofed, datagram-based transaction protocol.

15

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

Refer to the exhibit. Which two statements about the configuration shown are true? (Choose two.)

- [ ] access granted with password "local"
- [ ] SSH server function is enabled on R1
- [ ] SSH client function is enabled on R1
- [ ] remote access connection will fail with no local username database
- [ ] remote access connection will be made on secure shell port 443

---

16 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.

---

17 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.

---

18 When a user completes the Cisco SDM VPN wizard, what is done with the information that has been entered?

- ● The information is saved to a text file that can be used to configure clients.
- ● After user confirmation, the Cisco SDM-generated CLI commands are sent to the router.
- ● SDM generates traffic to test the configuration before it is applied to the router.
- ● A dialog box prompts the user for username and password information.

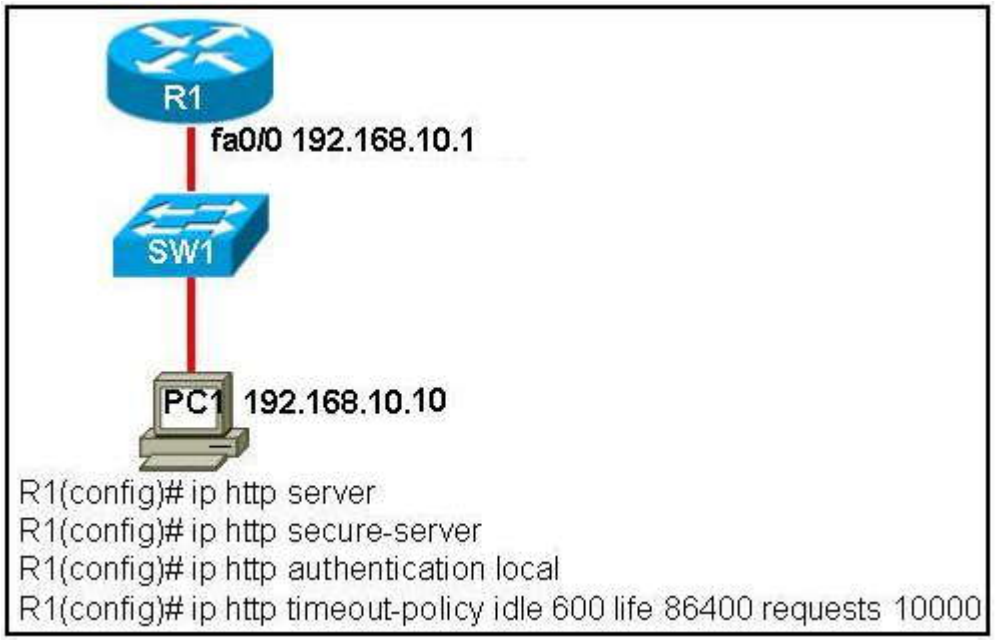
---

19 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

---

20



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.

---

21 Which statement is true about Cisco Security Device Manager (SDM)?

- SDM interrupts network communications when configuration changes are entered into router memory.
- SDM can run only on Cisco 7000 series routers.
- SDM is supported by every version of the Cisco IOS software.
- SDM can be run from router memory or from a PC.

---

22 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

23 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.

24 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.