Exam : **640-553**

Title : IINS Implementing Cisco IOS Network Security

Version : DEMO

1.As a network engineer at Cisco.com, you are responsible for Cisco network. Which will be necessarily taken into consideration when implementing Syslogging in your network?
A. Log all messages to the system buffer so that they can be displayed when accessing the router.
B. Use SSH to access your Syslog information.
C. Enable the highest level of Syslogging available to ensure you log all possible event messages.
D. Syncronize clocks on the network with a protocol such as Network Time Protocol.
Answer: D

2.Which classes does the U.S. government place classified data into.? (Choose three.)
A. SBU
B. Confidential
C. Secret
D. Top-secret
Answer: BCD

3.You are a network technician at Cisco.com. Which description is correct when you have generated RSA keys on your Cisco router to prepare for secure device management?
A. All vty ports are automatically enabled for SSH to provide secure management.
B. The SSH protocol is automatically enabled.
C. You must then zeroize the keys to reset secure shell before configuring other parameters.
D. You must then specify the general-purpose key size used for authentication with the crypto key generate rsa general-keys modulus command.
Answer: B

4.Which method is of gaining access to a system that bypasses normal security measures?
A. Creating a back door
B. Starting a Smurf attack
C. Conducting social engineering
D. Launching a DoS attack
Answer: A

5.As a candidate for CCNA examination, when you are familiar with the basic commands, if you input the command "enable secret level 5 password" in the global mode , what does it indicate?
A. Set the enable secret command to privilege level 5.
B. The enable secret password is hashed using SHA.
C. The enable secret password is hashed using MD5.
D. The enable secret password is encrypted using Cisco proprietary level 5 encryption.
E. The enable secret password is for accessing exec privilege level 5.
Answer: E

6.Which statement is true about a Smurf attack?
A. It sends ping requests to a subnet, requesting that devices on that subnet send ping replies to a target system.
B. It intercepts the third step in a TCP three-way handshake to hijack a session.

C. It uses Trojan horse applications to create a distributed collection of "zombie" computers, which can be used to launch a coordinated DDoS attack.
D. It sends ping requests in segments of an invalid size.
Answer: A

7.Which three items are Cisco best-practice recommendations for securing a network? (Choose three.)
A. Deploy HIPS software on all end-user workstations.
B. Routinely apply patches to operating systems and applications.
C. Disable unneeded services and ports on hosts.
D. Require strong passwords, and enable password expiration.
Answer: BCD

8.For the following attempts, which one is to ensure that no one employee becomes a pervasive security threat, that data can be recovered from backups, and that information system changes do not compromise a system's security?
A. Disaster recovery
B. Strategic security planning
C. Implementation security
D. Operations security
Answer: D

9.For the following options ,which one accurately matches the CLI command(s) to the equivalent SDM wizard that performs similar configuration functions?
A. setup exec command and the SDM Security Audit wizard
B. auto secure exec command and the SDM One-Step Lockdown wizard
C. aaa configuration commands and the SDM Basic Firewall wizard
D. Cisco Common Classification Policy Language configuration commands and the SDM Site-to-Site VPN wizard
Answer: B

10.Which three options are network evaluation techniques? (Choose three.)
A. Scanning a network for active IP addresses and open ports on those IP addresses
B. Using password-cracking utilities
C. Performing end-user training on the use of antispyware software
D. Performing virus scans
Answer: ABD

11.Which is the main difference between host-based and network-based intrusion prevention?
A. Network-based IPS is better suited for inspection of SSL and TLS encrypted data flows.
B. Host-based IPS can work in promiscuous mode or inline mode.
C. Network-based IPS can provide protection to desktops and servers without the need of installing specialized software on the end hosts and servers.
D. Host-based IPS deployment requires less planning than network-based IPS.
Answer: C

12.Which one is the most important based on the following common elements of a network design?
A. Business needs
B. Best practices
C. Risk analysis
D. Security policy
Answer: A

13.Given the exhibit below. You are a network manager of your company. You are reading your Syslog server reports. On the basis of the Syslog message shown, which two descriptions are correct? (Choose two.)

```
Feb 1 10:12:08 PST: %SYS-5-CONFIG_1: Configured from console by vty0 (10.2.2.6)
```

A. This message is a level 5 notification message.
B. This message is unimportant and can be ignored.
C. This is a normal system-generated information message and does not require further investigation.
D. Service timestamps have been globally enabled
Answer: AD

14.Examine the following items, which one offers a variety of security solutions, including firewall, IPS, VPN, antispyware, antivirus, and antiphishing features?
A. Cisco 4200 series IPS appliance
B. Cisco ASA 5500 series security appliance
C. Cisco IOS router
D. Cisco PIX 500 series security appliance
Answer: B

15.The enable secret password appears as an MD5 hash in a router's configuration file, whereas the enable password is not hashed (or encrypted, if the password-encryption
service is not enabled). What is the reason that Cisco still support the use of both enable secret and enable passwords in a router's configuration?
A. The enable password is used for IKE Phase I, whereas the enable secret password is used for IKE Phase II.
B. The enable password is considered to be a router's public key, whereas the enable secret password is considered to be a router's private key.
C. Because the enable secret password is a hash, it cannot be decrypted. Therefore, the enable password is used to match the password that
was entered, and the enable secret is used to verify that the enable password has not been modified since the hash was generated.
D. The enable password is present for backward compatibility.
Answer: D

16.How does CLI view differ from a privilege level?
A. A CLI view supports only commands configured for that specific view, whereas a privilege level

supports commands available to that level and all the lower levels.
B. A CLI view supports only monitoring commands, whereas a privilege level allows a user to make changes to an IOS configuration.
C. A CLI view and a privilege level perform the same function. However, a CLI view is used on a Catalyst switch, whereas a privilege level is used on an IOS router.
D. A CLI view can function without a AAA configuration, whereas a privilege level requires AAA to be configured.
Answer: A

17.When configuring Cisco IOS login enhancements for virtual connections, what is the "quiet period"?
A. A period of time when no one is attempting to log in
B. The period of time in which virtual logins are blocked as security services fully initialize
C. The period of time in which virtual login attempts are blocked, following repeated failed login attempts
D. The period of time between successive login attempts
Answer: C

18.Which result is of securing the Cisco IOS image by use of the Cisco IOS image resilience feature?
A. When the router boots up, the Cisco IOS image will be loaded from a secured FTP location.
B. The Cisco IOS image file will not be visible in the output from the show flash command.
C. The show version command will not show the Cisco IOS image file location.
D. The running Cisco IOS image will be encrypted and then automatically backed up to a TFTP server.
Answer: B

19.Which three statements are valid SDM configuration wizards? (Choose three.)
A. Security Audit
B. VPN
C. STP
D. NAT
Answer: ABD

20.How do you define the authentication method that will be used with AAA?
A. With a method list
B. With the method command
C. With the method aaa command
D. With a method statement
Answer: A