Vendor: CISCO

Exam Code: 640-553

Exam Name: Implementing Cisco IOS Network Security

QUESTION 1
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

QUESTION 2
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

QUESTION 3
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

QUESTION 4
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

QUESTION 5
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

QUESTION 6
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

QUESTION 7

What is the objective of the aaa authentication login console-in local command?

A. It specifies the login authorization method list named console-in using the local RADIUS username-password database.
B. It specifies the login authorization method list named console-in using the local username-password database on the router.
C. It specifies the login authentication method list named console-in using the local user database on the router.
D. It specifies the login authentication list named console-in using the local username-password database on the router.

Answer: C

QUESTION 8

Which two ports are used with RADIUS authentication and authorization?(Choose two.)

A. TCP port 2002
B. UDP port 2000
C. UDP port 1645
D. UDP port 1812

Answer: CD

QUESTION 9
Which one of the Cisco IOS commands can be used to verify that either the Cisco IOS image, the configuration files, or both have been properly backed up and secured?

A. show flash
B. show secure bootset
C. show archive
D. show file systems

Answer: B

QUESTION 10
Which type of intrusion prevention technology will be primarily used by the Cisco IPS security appliances?

A. rule-based
B. protocol analysis-based
C. signature-based
D. profile-based

Answer: C

QUESTION 11
For the following statements, which one is perceived as a drawback of implementing Fibre Channel Authentication Protocol (FCAP)?

A. It is restricted in size to only three segments.
B. It requires the implementation of IKE.
C. It relies on an underlying Public Key Infrastructure (PKI).
D. It requires the use of netBT as the network protocol.

Answer: C

QUESTION 12
Which two actions can be configured to allow traffic to traverse an interface when zone-based security is being employed? (Choose two.)

A. Flow
B. Inspect
C. Pass
D. Allow

Answer: BC

QUESTION 13
Which statement is correct regarding the aaa configurations based on the exhibit provided?

```
R(config)# username admin privilege level 15 secret hardtOcRackPw
R(config)# aaa new-model
R(config)# aaa authentication login default tacacs+
R(config)# aaa authentication login test tacacs+ local
R(config)# line vty 0 4
R(config-line)# login authentication test
R(config-line)# line con 0
R(config-line)# end
```

A. The authentication method list used by the console port is named test.
B. The authentication method list used by the vty port is named test.
C. If the TACACS+ AAA server is not available, console access to the router can be authenticated using the local database.
D. If the TACACS+ AAA server is not available, no users will be able to establish a Telnet session with the router.

Answer: B

QUESTION 14
Which description about asymmetric encryption algorithms is correct?

A. They use different keys for decryption but the same key for encryption of data.
B. They use the same key for encryption and decryption of data.
C. They use different keys for encryption and decryption of data.
D. They use the same key for decryption but different keys for encryption of data.

Answer: C

QUESTION 15
What is the MD5 algorithm used for?

A. takes a variable-length message and produces a 168-bit message digest
B. takes a fixed-length message and produces a 128-bit message digest
C. takes a variable-length message and produces a 128-bit message digest
D. takes a message less than 2^64 bits as input and produces a 160-bit message digest

Answer: C

QUESTION 16
Which statement is true about a certificate authority (CA)?

A. A trusted third party responsible for signing the private keys of entities in a PKIbased system
B. A trusted third party responsible for signing the public keys of entities in a PKIbased system
C. An entity responsible for registering the private key encryption used in a PKI
D. An agency responsible for granting and revoking public-private key pairs

Answer: B

QUESTION 17
When configuring Cisco IOS Zone-Based Policy Firewall, what are the three actions that can be applied to a traffic class? (Choose three.)

A. Pass
B. Police
C. Inspect
D. Drop
E. Queue
F. Shape

Answer: ACD

QUESTION 18
Which option is true of intrusion prevention systems?

A. they operate in promiscuous mode
B. they operate in inline mode
C. they have no potential impact on the data segment being monitored
D. they are more vulnerable to evasion techniques than IDS

Answer: B

QUESTION 19
Which of the following is not considered a trustworthy symmetric encryption algorithm?

A. 3DES
B. IDEA
C. EDE
D. AES

Answer: C

QUESTION 20
Which statement best describes the relationships between AAA function and TACACS+, RADIUS based on the exhibit shown?

PG1	Has no option to authorize router commands
PG2	Encrypts the entire packet
PG3	Combines authentication and authorization functions
PG4	Uses TCP port 49

A. TACACS+ - PG1 and PG3
   RADIUS - PG2 and PG4
B. TACACS+ - PG2 and PG4
   RADIUS - PG1 and PG3
C. TACACS+ - PG1 and PG4
   RADIUS - PG2 and PG3
D. TACACS+ - PG2 and PG3
   RADIUS - PG1 and PG4

Answer: B