Exam Number : SY0-301

Exam Name : Security+ Certification Exam 2011 version

Version : Demo

QUESTION NO: 1
Actively monitoring data streams in search of malicious code or behavior is an example of:
A. load balancing.
B. an Internet proxy.
C. URL filtering.
D. content inspection.

Answer: D

QUESTION NO: 2
Which of the following network devices would MOST likely be used to detect but not react to suspicious behavior on the network?
A. Firewall
B. NIDS
C. NIPS
D. HIDS

Answer: B

QUESTION NO: 3
The security administrator is getting reports from users that they are accessing certain websites and are unable to download anything off of those sites. The security administrator is also receiving several alarms from the IDS about suspicious traffic on the network. Which of the following is the MOST likely cause?
A. NIPS is blocking activities from those specific websites.
B. NIDS is blocking activities from those specific websites.
C. The firewall is blocking web activity.
D. The router is denying all traffic from those sites.

Answer: A

QUESTION NO: 4
Which of the following tools provides the ability to determine if an application is transmitting a password in clear-text?
A. Protocol analyzer
B. Port scanner
C. Vulnerability scanner
D. Honeypot

Answer: A

QUESTION NO: 5
Which of the following can a security administrator implement to help identify smurf attacks?
A. Load balancer
B. Spam filters
C. NIDS
D. Firewall

Answer: C

QUESTION NO: 6
Which of the following wireless security controls can be easily and quickly circumvented using only a network sniffer? (Select TWO).
A. MAC filtering
B. Disabled SSID broadcast
C. WPA2-Enterprise
D. EAP-TLS
E. WEP with 802.1x

Answer: A,B

QUESTION NO: 7
Which of the following functions is MOST likely performed by a web security gateway?
A. Protocol analyzer
B. Content filtering
C. Spam filtering
D. Flood guard

Answer: B

QUESTION NO: 8
Which of the following devices is often used to cache and filter content?
A. Proxies
B. Firewall
C. VPN
D. Load balancer

Answer: A

QUESTION NO: 9
In order to provide flexible working conditions, a company has decided to allow some employees remote access into corporate headquarters. Which of the

following security technologies could be used to provide remote access? (Select TWO).
A. Subnetting
B. NAT
C. Firewall
D. NAC
E. VPN

Answer: C,E

QUESTION NO: 10
Which of the following devices is used to optimize and distribute data workloads across multiple computers or networks?
A. Load balancer
B. URL filter
C. VPN concentrator
D. Protocol analyzer

Answer: A

QUESTION NO: 11
An IT administrator wants to provide 250 staff with secure remote access to the corporate network.
Which of the following BEST achieves this requirement?
A. Software based firewall
B. Mandatory Access Control (MAC)
C. VPN concentrator
D. Web security gateway

Answer: C

QUESTION NO: 12
Which of the following should be installed to prevent employees from receiving unsolicited emails?
A. Pop-up blockers
B. Virus definitions
C. Spyware definitions
D. Spam filters

Answer: D

QUESTION NO: 13
Which of the following should a security administrator implement to prevent users from disrupting network connectivity, if a user connects both ends of a

network cable to different switch ports?
A. VLAN separation
B. Access control
C. Loop protection
D. DMZ

Answer: C

QUESTION NO: 14
A user is no longer able to transfer files to the FTP server. The security administrator has verified the ports are open on the network firewall. Which of the following should the security administrator check?
A. Anti-virus software
B. ACLs
C. Anti-spam software
D. NIDS

Answer: B

QUESTION NO: 15
Which of the following BEST describes the proper method and reason to implement port security?
A. Apply a security control which ties specific ports to end-device MAC addresses and prevents additional devices from being connected to the network.
B. Apply a security control which ties specific networks to end-device IP addresses and prevents new devices from being connected to the network.
C. Apply a security control which ties specific ports to end-device MAC addresses and prevents all devices from being connected to the network.
D. Apply a security control which ties specific ports to end-device IP addresses and prevents mobile devices from being connected to the network.

Answer: A