Vendor: Cisco

Exam Code: 600-199

Exam Name: Securing Cisco Networks with Threat Detection and Analysis (SCYBER)

Version: Demo

QUESTION 1
Which network management protocol relies on multiple connections between a managed device and the management station where such connections can be independently initiated by either side?

A. SSH
B. SNMP
C. Telnet
D. NetFlow

Correct Answer: B

QUESTION 2
When an IDS generates an alert for a correctly detected network attack, what is this event called?

A. false positive
B. true negative
C. true positive
D. false negative

Correct Answer: C

QUESTION 3
When is it recommended to establish a traffic profile baseline for your network?

A. outside of normal production hours
B. during a DDoS attack
C. during normal production hours
D. during monthly file server backup

Correct Answer: C

QUESTION 4
Which two activities would you typically be expected to perform as a Network Security Analyst? (Choose two.)

A. Verify user login credentials.
B. Troubleshoot firewall performance.
C. Monitor database applications.
D. Create security policies on routers.

Correct Answer: BD

QUESTION 5
Which protocol is typically considered critical for LAN operation?

A. BGP
B. ARP
C. SMTP
D. GRE

Correct Answer: B

QUESTION 6
Which two measures would you recommend to reduce the likelihood of a successfully executed network attack from the Internet? (Choose two.)

A. Completely disconnect the network from the Internet.
B. Deploy a stateful edge firewall.
C. Buy an insurance policy against attack-related business losses.
D. Implement a password management policy for remote users.

Correct Answer: BD

QUESTION 7
Which attack exploits incorrect boundary checking in network software?

A. Slowloris
B. buffer overflow
C. man-in-the-middle
D. Smurf

Correct Answer: B

QUESTION 8
Where should you report suspected security vulnerability in Cisco router software?

A. Cisco TAC
B. Cisco IOS Engineering
C. Cisco PSIRT
D. Cisco SIO

Correct Answer: C

QUESTION 9
When investigating potential network security issues, which two pieces of useful information would be found in a syslog message? (Choose two.)

A. product serial number
B. MAC address
C. IP address
D. product model number
E. broadcast address

Correct Answer: BC

QUESTION 10
Which command would provide you with interface status information on a Cisco IOS router?

A. show status interface
B. show running-config
C. show ip interface brief
D. show interface snmp

Correct Answer: C

QUESTION 11
Refer to the exhibit.

Query Type	count	%
A?	9	23.7
NS?	1	2.6
SOA?	1	2.6
PTR?	15	39.5
MX?	10	26.3
TXT?	2	5.3

Which DNS Query Types pertains to email?

A. A?
B. NS?
C. SOA?
D. PTR?
E. MX?
F. TXT?

Correct Answer: E

QUESTION 12
A server administrator tells you that the server network is potentially under attack. Which piece of information is critical to begin your network investigation?

A. cabinet location of the servers
B. administrator password for the servers
C. OS that is used on the servers
D. IP addresses/subnets used for the servers

Correct Answer: D

QUESTION 13
Which describes the best method for preserving the chain of evidence?

A. Shut down the machine that is infected, remove the hard drive, and contact the local authorities.
B. Back up the hard drive, use antivirus software to clean the infected machine, and contact the local authorities.
C. Identify the infected machine, disconnect from the network, and contact the local authorities.
D. Allow user(s) to perform any business-critical tasks while waiting for local authorities.

Correct Answer: C

QUESTION 14
Which will be provided as output when issuing the show processes cpu command on a Cisco IOS router?

A. router configuration
B. CPU utilization of device
C. memory used by device processes
D. interface processing statistics

Correct Answer: B

QUESTION 15
Refer to the exhibit.

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

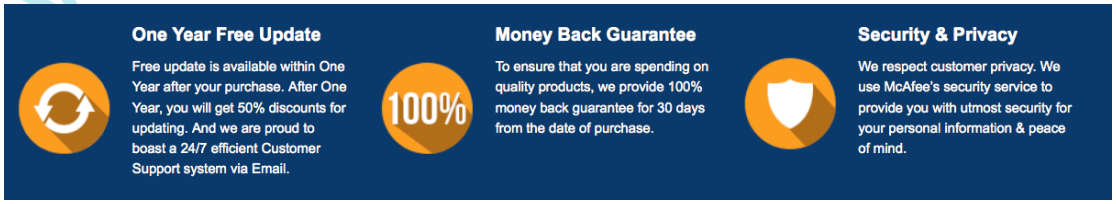
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.