Vendor: Cisco

Exam Code: 600-199

Exam Name: Securing Cisco Networks with Threat Detection and Analysis

Version: DEMO

QUESTION 1
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.

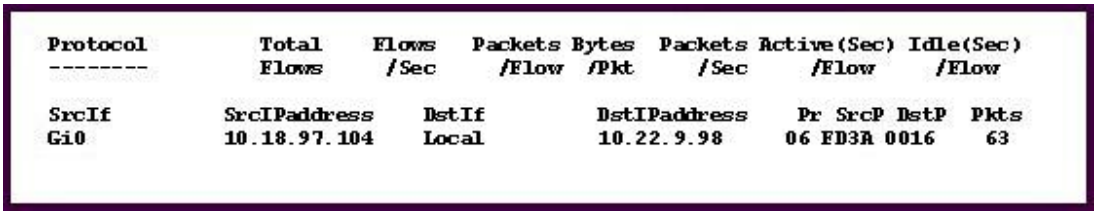
Answer: C

QUESTION 2
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

Answer: B

QUESTION 3
Refer to the exhibit. Which protocol is used in this network traffic flow?



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

Answer: B

QUESTION 4
Which two types of data are relevant to investigating network security issues? (Choose two.)

A. NetFlow
B. device model numbers
C. syslog
D. routing tables
E. private IP addresses

Answer: AC

QUESTION 5
In the context of a network security device like an IPS, which event would qualify as having the highest severity?

A. remote code execution attempt
B. brute force login attempt
C. denial of service attack
D. instant messenger activity

Answer: A

QUESTION 6
Which event is likely to be a false positive?

A. Internet Relay Chat signature with an alert context buffer containing #IPS_ROCS Yay
B. a signature addressing an ActiveX vulnerability alert on a Microsoft developer network documentation page
C. an alert for a long HTTP request with an alert context buffer containing a large HTTP GET request
D. BitTorrent activity detected on ephemeral ports

Answer: B

QUESTION 7
Given a Linux machine running only an SSH server, which chain of alarms would be most concerning?

A. brute force login attempt from outside of the network, followed by an internal network scan
B. root login attempt followed by brute force login attempt
C. Microsoft RPC attack against the server
D. multiple rapid login attempts

Answer: A

QUESTION 8
If a company has a strict policy to limit potential confidential information leakage, which three alerts would be of concern? (Choose three.)

A. P2P activity detected
B. Skype activity detected
C. YouTube viewing activity detected
D. Pastebin activity detected
E. Hulu activity detected

Answer: ABD

Ensurepass.com Members Features:

1. Verified Answers researched by industry experts.
2. Q&As are downloadable in PDF and VCE format.
3. 98% success Guarantee and **Money Back** Guarantee.
4. Free updates for **180** Days.

View list of All Exam provided:
http://www.ensurepass.com/certfications?index=A

To purchase Lifetime Full Access Membership click here:
http://www.ensurepass.com/user/register

Valid Discount Code for 2014: SFOH-FZA0-7Q2S

To purchase the HOT Exams:

Cisco		CompTIA		Oracle	VMWare	IBM
100-101	640-554	220-801	LX0-101	1Z0-051	VCAD510	C2170-011
200-120	640-802	220-802	N10-005	1Z0-052	VCP510	C2180-319
300-206	640-816	BR0-002	SG0-001	1Z0-053	VCP550	C4030-670
300-207	640-822	CAS-001	SG1-001	1Z0-060	VCAC510	C4040-221
300-208	640-864	CLO-001	SK0-002	1Z0-474	VCP5-DCV	RedHat
350-018	642-467	ISS-001	SK0-003	1Z0-482	VCP510PSE	EX200
352-001	642-813	JK0-010	SY0-101	1Z0-485		EX300
400-101	642-902	JK0-801	SY0-301	1Z0-580		
640-461	700-302			1Z0-820