
**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.

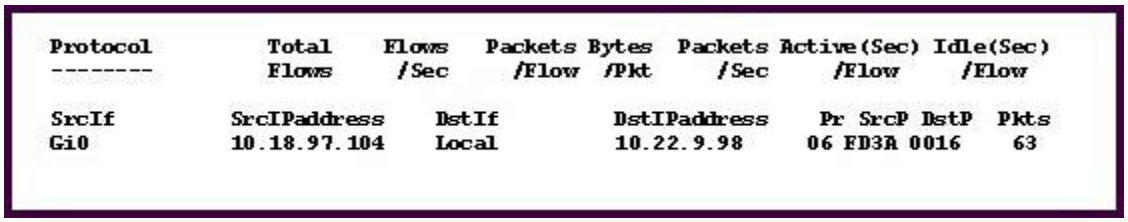
**Answer:** C

**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?



| Protocol | Total Flows | Flows /Sec | Packets /Flow | Bytes /Pkt | Packets /Sec | Active(Sec) /Flow | Idle(Sec) /Flow |
|---|---|---|---|---|---|---|---|
| --------- | | | | | | | |

| SrcIf | SrcIPaddress | DstIf | DstIPaddress | Pr | SrcP | DstP | Pkts |
|---|---|---|---|---|---|---|---|
| Gi0 | 10.18.97.104 | Local | 10.22.9.98 | 06 | FD3A | 0016 | 63 |

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

# Thank You for Trying Our Product

## Lead2pass Certification Exam Features:


★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.


★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

**10% Discount Coupon Code:** **ASTR14**