600-199 Q&As

Securing Cisco Networks with Threat Detection and Analysis

Pass Cisco 600-199 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.lead4pass.com/600-199.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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 2

Which three tools should be used for incident response? (Choose three.)

A. screwdriver

B. sniffer

C. antivirus/anti-malware software

D. video player

E. CPU

F. RAM

Correct Answer: ABC

QUESTION 3

Refer to the exhibit.

Which protocol is used in this network traffic flow?

A. SNMP

B. SSH

C. DNS

D. Telnet

Correct Answer: B

QUESTION 4

Which step should be taken first when a server on a network is compromised?

A. Refer to the company security policy.

B. Email all server administrators.

C. Determine which server has been compromised.

D. Find the serial number of the server.

Correct Answer: A

QUESTION 5

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 6

As a part of incident response, which action should be performed?

A. watch to see if the incident reoccurs

B. custody of information

C. maintain data security and custody for future forensics use

D. classify the problem

Correct Answer: C

QUESTION 7

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

Correct Answer: AC

QUESTION 8

What is the most important reason for documenting an incident?

A. It could be used as evidence for a criminal case.

B. It could be used to identify the person responsible for allowing it into the network.

C. To train others on what they should not do.

D. To use it for future incident response handling.

Correct Answer: A

QUESTION 9

Which three post-mortem steps are critical to help prevent a network attack from reoccurring? (Choose three.)

A. Document the incident in a report.

B. Collect "show" outputs after the attack.

C. Involve law enforcement officials.

D. Create a "lessons learned" collection.

E. Update the security rules for edge devices.

F. Revise the network security policy.

Correct Answer: ADF

QUESTION 10

Which two tools are used to help with traffic identification? (Choose two.)

A. network sniffer

B. ping

C. traceroute

D. route table

E. NetFlow

F. DHCP

Correct Answer: AE

QUESTION 11

What does the acronym "CSIRT" stand for?

A. Computer Security Identification Response Team

B. Cisco Security Incident Response Team

C. Cisco Security Identification Response Team

D. Computer Security Incident Response Team

Correct Answer: D

QUESTION 12

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

Correct Answer: A

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.

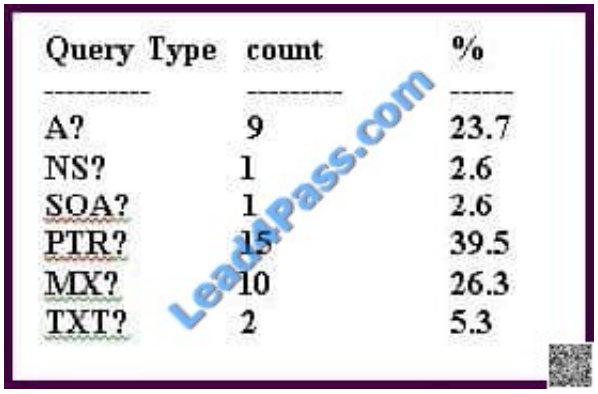
C. Identify the infected machine, disconnect from the network, and contact the local authorities.

D. Allow user(s) to perform any business-critical tasks while waiting for local authorities.

Correct Answer: C

QUESTION 14

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 15

What is the maximum size of an IP datagram?

A. There is no maximum size.

B. It is limited only by the memory on the host computers at either end of the connection and the intermediate routers.

C. 1024 bytes

D. 65535 bytes

E. 32768 bytes

Correct Answer: D

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try 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 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.lead4pass.com/allproducts

Need Help

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