

100% Pass Ensure 600-199 Dumps with Free VCE and PDF (Question 26 - Question 30)

New 600-199 exam questions from PassLeader 600-199 dumps! Welcome to download the newest PassLeader 600-199 VCE and PDF dumps: <http://www.passleader.com/600-199.html> (60 Q&As)

P.S. Free 600-199 dumps are available on Google Drive shared by PassLeader:

https://drive.google.com/open?id=0B-ob6L_QjGLpR0ozaTdjbGpid28

QUESTION 26

In a network security policy, which procedure should be documented ahead of time to speed the communication of a network attack?

- A. restoration plans for compromised systems
- B. credentials for packet capture devices
- C. Internet service provider contact information
- D. risk analysis tool credentials
- E. a method of communication and who to contact

Answer: E

QUESTION 27

Which data is the most useful to determine if a network attack was occurring from inbound Internet traffic?

- A. syslogs from all core switches
- B. NetFlow data from border firewall(s)
- C. VPN connection logs
- D. DNS request logs
- E. Apache server logs

Answer: B

QUESTION 28

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.

Answer: A

QUESTION 29

After an attack has occurred, which two options should be collected to help remediate the problem? (Choose two.)

- A. packet captures
- B. NAT translation table
- C. syslogs from affected devices
- D. connection table information
- E. NetFlow data

Answer: CE

QUESTION 30

Which source should be used to recommend preventative measures against security vulnerabilities regardless of operating system or platform?

- A. Microsoft security bulletins
- B. Cisco PSIRT notices
- C. Common Vulnerabilities and Exposure website
- D. Mozilla Foundation security advisories
- E. zero-day attack wiki

Answer: C

New 600-199 exam questions from PassLeader 600-199 dumps! Welcome to download the newest PassLeader 600-199 VCE and PDF dumps: <http://www.passleader.com/600-199.html> (60 Q&As)

P.S. Free 600-199 dumps are available on Google Drive shared by PassLeader:

https://drive.google.com/open?id=0B-ob6L_QjGLpR0ozaTdjbGpid28