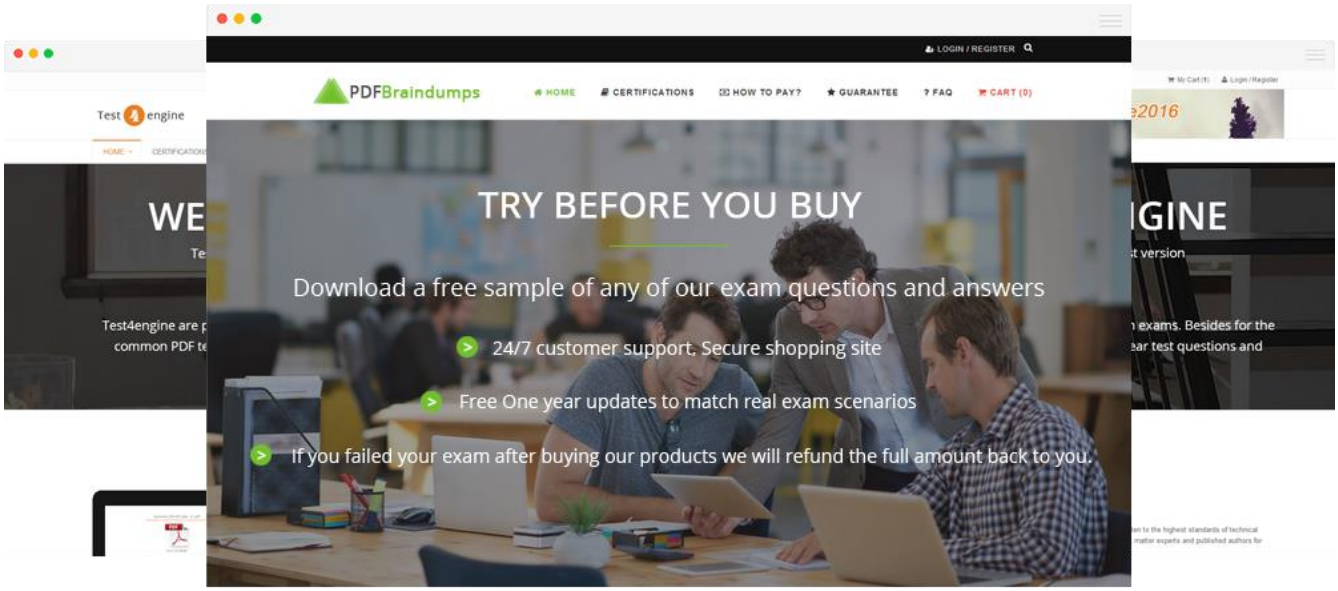
PDFBraindumps



Latest Pdf Braindumps

- LRP-614
- C-SRM-72
- BCABA
- ACMP-6.3
- JN0-740
- 1z0-100
- 250-405
- FM0-308
- DS-200
- C_SRM_72
- SDM_2002001040
- ACMP_6.3
- ST0-250
- 1z0-062
- H12-221
- A4120-784
- M2180-716

Top Certifications

- ISEB Certification
- HCNP
- OCE
- IFPUG Certifications
- NVIDIA Certifications
- dotMobi Certification
- Network+
- SCMA
- IBM Certified Integrat
- MCSD
- CCDH
- NCLP
- IBM Certified Advanc
- XMLMaster Certificat
- eserver Certified Spe
- CS5
- SAP-Certifications
- CHA
- Network Appliance N

Top Vendors

- ISEB
- Fortinet
- ASTQB
- Ericsson
- Aruba
- Liferay
- Data Center Universit
- Novell
- HRCI
- Huawei
- CIW
- RSA
- Patchlink
- MYSQL
- International Consorti
- ISM
- Acme-Packet
- CheckPoint

http://www.pdfbraindumps.com

Latest pdf braindumps provider, high pass rate

Exam : **GCED**

Title : GIAC Certified Enterprise Defender Practice Test

Vendor : GIAC

Version : DEMO

NO.1 An incident response team investigated a database breach, and determined it was likely the result of an internal user who had a default password in place. The password was changed. A week later, they discover another loss of database records. The database admin provides logs that indicate the attack came from the front-end web interface. Where did the incident response team fail?
A. They did not eradicate tools left behind by the attacker
B. They did not properly identify the source of the breach
C. They did not lock the account after changing the password
D. They did not patch the database server after the event
Answer: D

NO.2 Which of the following is an SNMPv3 security feature that was not provided by earlier versions of the protocol?
A. Authentication based on RSA key pairs
B. The ability to change default community strings
C. AES encryption for SNMP network traffic
D. The ability to send SNMP traffic over TCP ports
Answer: C

NO.3 Which Windows tool would use the following command to view a process:
process where name='suspect_malware.exe'list statistics
A. TCPView
B. Tasklist
C. WMIC
D. Netstat
Answer: C

NO.4 Before re-assigning a computer to a new employee, what data security technique does the IT department use to make sure no data is left behind by the previous user?
A. Fingerprinting
B. Digital watermarking
C. Baselining
D. Wiping
Answer: D

NO.5 What should happen before acquiring a bit-for-bit copy of suspect media during incident response?
A. Encrypt the original media to protect the data
B. Create a one-way hash of the original media
C. Decompress files on the original media
D. Decrypt the original media
Answer: B

NO.6 Why would the pass action be used in a Snort configuration file?

A. The pass action simplifies some filtering by specifying what to ignore.
B. The pass action passes the packet onto further rules for immediate analysis.
C. The pass action serves as a placeholder in the snort configuration file for future rule updates.
D. Using the pass action allows a packet to be passed to an external process.
E. The pass action increases the number of false positives, better testing the rules.
Answer: A
The pass action is defined because it is sometimes easier to specify the class of data to ignore rather than the data you want to see. This can cut down the number of false positives and help keep down the size of log data.
False positives occur because rules failed and indicated a threat that is really not one. They should be minimized whenever possible.
The pass action causes the packet to be ignored, not passed on further. It is an active command, not a placeholder.

NO.7 Which Windows CLI tool can identify the command-line options being passed to a program at startup?
A. netstat
B. attrib
C. WMIC
D. Tasklist
Answer: C

NO.8 An incident response team is handling a worm infection among their user workstations. They created an IPS signature to detect and block worm activity on the border IPS, then removed the worm's artifacts or workstations triggering the rule. Despite this action, worm activity continued for days after. Where did the incident response team fail?
A. The team did not adequately apply lessons learned from the incident
B. The custom rule did not detect all infected workstations
C. They did not receive timely notification of the security event
D. The team did not understand the worm's propagation method
Answer: B
Identifying and scoping an incident during triage is important to successfully handling a security incident.
The detection methods used by the team didn't detect all the infected workstations.