SY0-501$^{Q\&As}$

CompTIA Security+ Certification Exam

Pass CompTIA SY0-501 Exam with 100% Guarantee

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

https://www.passapply.com/sy0-501.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A malicious system continuously sends an extremely large number of SYN packets to a server. Which of the following BEST describes the resulting effect?

A. The server will be unable to server clients due to lack of bandwidth

B. The server\\'s firewall will be unable to effectively filter traffic due to the amount of data transmitted

C. The server will crash when trying to reassemble all the fragmented packets

D. The server will exhaust its memory maintaining half-open connections

Correct Answer: D

QUESTION 2

A security analyst captures forensic evidence from a potentially compromised system for further investigation. The evidence is documented and securely stored to FIRST:

A. maintain the chain of custody.

B. preserve the data.

C. obtain a legal hold.

D. recover data at a later time.

Correct Answer: B

QUESTION 3

Given the log output:

```
Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS:

Login Success [user: msmith] [Source: 10.0.12.45]

[localport: 23] at 00:15:23:431 CET Sun Mar 15 2015
```

Which of the following should the network administrator do to protect data security?

A. Configure port security for logons

B. Disable telnet and enable SSH

C. Configure an AAA server

D. Disable password and enable RSA authentication

Correct Answer: B

QUESTION 4

Which of the following must be intact for evidence to be admissible in court?

A. Chain of custody

B. Order of volatility

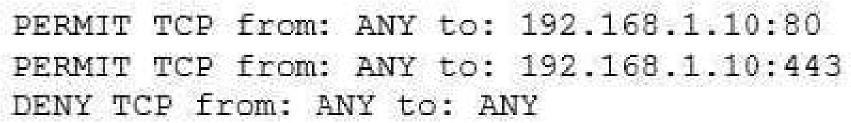
C. Legal hold

D. Preservation

Correct Answer: A

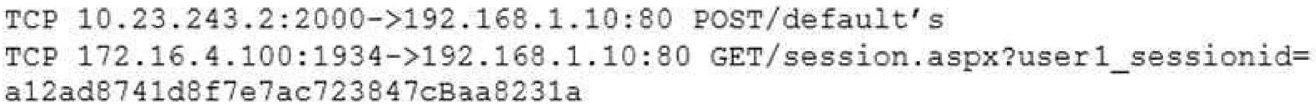
QUESTION 5

A system\\'s administrator has finished configuring firewall ACL to allow access to a new web server.



```
PERMIT TCP from: ANY to: 192.168.1.10:80
PERMIT TCP from: ANY to: 192.168.1.10:443
DENY TCP from: ANY to: ANY
```

The security administrator confirms form the following packet capture that there is network traffic from the internet to the web server:



```
TCP 10.23.243.2:2000->192.168.1.10:80 POST/default’s
TCP 172.16.4.100:1934->192.168.1.10:80 GET/session.aspx?user1_sessionid=
a12ad8741d8f7e7ac723847cBaa8231a
```

The company\\'s internal auditor issues a security finding and requests that immediate action be taken. With which of the following is the auditor MOST concerned?

A. Misconfigured firewall

B. Clear text credentials

C. Implicit deny

D. Default configuration

Correct Answer: B

[Latest SY0-501 Dumps](#) [SY0-501 Practice Test](#) [SY0-501 Exam Questions](#)