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.pass4itsure.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 user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site. Upon Investigation, a security analyst identifies the following:

*

The legitimate website\\'s IP address is 10.1.1.20 and eRecruit.local resolves to this IP.

*

The forged website\\'s IP address appears to be 10.2.12.99. based on NetFlow records.

*

All three of the organization\\'s DNS servers show the website correctly resolves to the legitimate IP.

*

DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise. Which of the following MOST likely occurred?

A.

A reverse proxy was used to redirect network traffic.

B.

An SSL strip MITM attack was performed.

C.

An attacker temporarily poisoned a name server.

D.

An ARP poisoning attack was successfully executed.

Correct Answer: B

QUESTION 2

A company notices that at 10 a.m. every Thursday, three users\\' computers become inoperable. The security analyst team discovers a file called where.pdf.exe that runs on system startup. The contents of where.pdf.exe are shown below:

@echo off if [c:\file.txt] deltree C:\

Based on the above information, which of the following types of malware was discovered?

A. Rootkit

B. Backdoor

C. Logic bomb

D. RAT

Correct Answer: C

QUESTION 3

Which of the following is a benefit of credentialed vulnerability scans?

A. Credentials provide access to scan documents to identify possible data theft.

B. The vulnerability scanner is able to inventory software on the target.

C. A scan will reveal data loss in real time.

D. Black-box testing can be performed.

Correct Answer: B

QUESTION 4

A workstation puts out a network request to locate another system. Joe, a hacker on the network, responds before the real system does, and he tricks the workstation into communicating with him. Which of the following BEST describes what occurred?

A. The hacker used a race condition.

B. The hacker used a pass-the-hash attack.

C. The hacker-exploited improper key management.

D. The hacker exploited weak switch configuration.

Correct Answer: D

QUESTION 5

A systems engineer is configuring a wireless network. The network must not require installation of third-party software. Mutual authentication of the client and the server must be used. The company has an internal PKI. Which of the following configurations should the engineer choose?

A. EAP-TLS

B. EAP-TTLS

C. EAP-FAST

D. EAP-MD5

E. PEAP

Correct Answer: A

EAP-TLS uses the TLS public key certificate authentication mechanism within EAP to provide mutual authentication of client to server and server to client. With EAP-TLS, both the client and the server must be assigned a digital certificate signed by a Certificate Authority (CA) that they both trust.