ECSAV10Q&As

EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

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

https://www.pass4itsure.com/ecsav10.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Peter, a disgruntled ex-employee of Zapmaky Solutions Ltd., is trying to jeopardize the company\\'s website http://zapmaky.com. He conducted the port scan of the website by using the Nmap tool to extract the information about open ports and their corresponding services. While performing the scan, he recognized that some of his requests are being blocked by the firewall deployed by the IT personnel of Zapmaky and he wants to bypass the same. For evading the firewall, he wanted to employ the stealth scanning technique which is an incomplete TCP three-way handshake method that can effectively bypass the firewall rules and logging mechanisms. Which if the following Nmap commands should Peter execute to perform stealth scanning?

A. nmap -sT -v zapmaky.com

B. nmap -T4 -A -v zapmaky.com

C. nmap -sX -T4 -A -v zapmaky.com

D. nmap -sN -A zapmaky.com

Correct Answer: A

QUESTION 2

Which of the following acts is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

A. PIPEDA

B. PCI DSS

C. Human Rights Act 1998

D. Data Protection Act 1998

Correct Answer: B

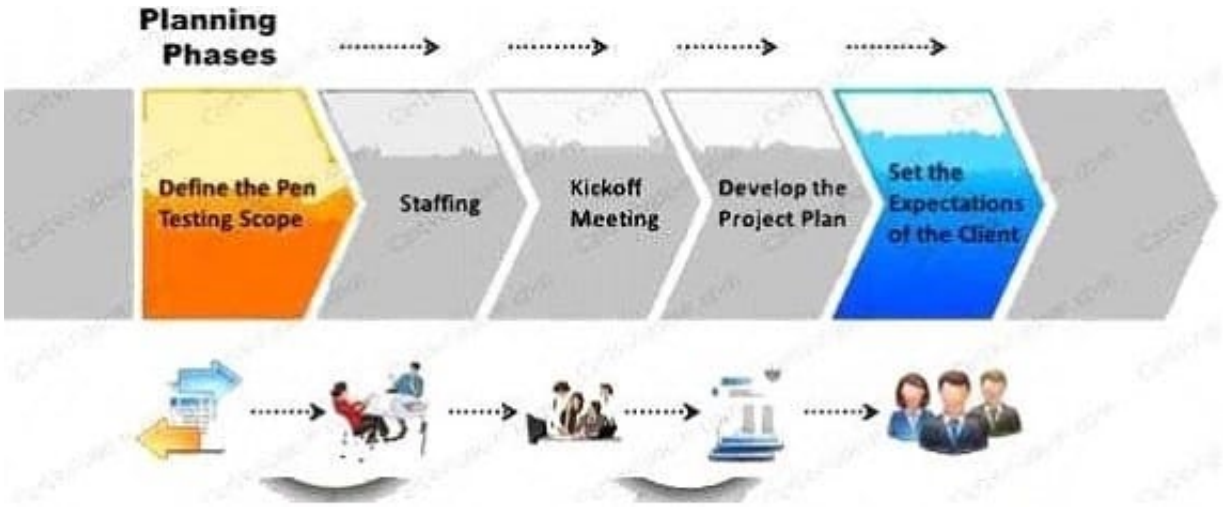
QUESTION 3

The first phase of the penetration testing plan is to develop the scope of the project in consultation with the

client. Pen testing test components depend on the client\\'s operating environment, threat perception,

security and compliance requirements, ROE, and budget.

Various components need to be considered for testing while developing the scope of the project.



Which of the following is NOT a pen testing component to be tested?

A. System Software Security

B. Intrusion Detection

C. Outside Accomplices

D. Inside Accomplices

Correct Answer: C

QUESTION 4

An attacker injects malicious query strings in user input fields to bypass web service authentication mechanisms and to access back-end databases. Which of the following attacks is this?

A. Frame Injection Attack

B. LDAP Injection Attack

C. XPath Injection Attack

D. SOAP Injection Attack

Correct Answer: D

QUESTION 5

Which of the following are the default ports used by NetBIOS service?

A. 135, 136, 139, 445

B. 134, 135, 136, 137

C. 137, 138, 139, 140

D. 133, 134, 139, 142

Correct Answer: A