Vendor: EC-Council

Exam Code: 312-50v10

Exam Name: Certified Ethical Hacker v10

Version: DEMO

QUESTION 1
Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Suppose a malicious user Rob tries to get access to the account of a benign user Ned. Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

A. "GET/restricted/goldtransfer?to=Rob&from=1 or 1=1' HTTP/1.1Host: westbank.com"
B. "GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com"
C. "GET/restricted/bank.getaccount(`Ned') HTTP/1.1 Host: westbank.com"
D. "GET/restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com"

Answer: B

QUESTION 2
Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

A. Metasploit
B. Cain & Abel
C. Maltego
D. Wireshark

Answer: C

QUESTION 3
Which of these is capable of searching for and locating rogue access points?

A. HIDS
B. NIDS
C. WISS
D. WIPS

Answer: D

QUESTION 4
A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes.
Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

A. White Hat
B. Suicide Hacker
C. Gray Hat
D. Black Hat

Answer: C

QUESTION 5

Websites and web portals that provide web services commonly use the Simple Object Access Protocol (SOAP). Which of the following is an incorrect definition or characteristics of the protocol?

A. Based on XML
B. Only compatible with the application protocol HTTP
C. Exchanges data between web services
D. Provides a structured model for messaging

Answer: B

QUESTION 6
You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?

A. John the Ripper
B. SET
C. CHNTPW
D. Cain & Abel

Answer: C

QUESTION 7
What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

A. Cross-site request forgery
B. Cross-site scripting
C. Session hijacking
D. Server side request forgery

Answer: A

QUESTION 8
When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

A. At least twice a year or after any significant upgrade or modification
B. At least once a year and after any significant upgrade or modification
C. At least once every two years and after any significant upgrade or modification
D. At least once every three years or after any significant upgrade or modification

Answer: B

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: BDNT2014