



Free Questions for ECSAv10 by [braindumpscollection](#)

Shared by [Foley](#) on [29-01-2024](#)

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

Question Type: MultipleChoice

Which of the following scan option is able to identify the SSL services?

Options:

A- --sS

B- --sV

C- --sU

D- --sT

Answer:

B

Question 2

Question Type: MultipleChoice

An automated electronic mail message from a mail system which indicates that the user does not exist on that server is called as?

Options:

- A- SMTP Queue Bouncing
- B- SMTP Message Bouncing
- C- SMTP Server Bouncing
- D- SMTP Mail Bouncing

Answer:

D

Question 3

Question Type: MultipleChoice

What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

Options:

- A- Service account passwords in plain text
- B- Cached password hashes for the past 20 users
- C- IAS account names and passwords
- D- Local store PKI Kerberos certificates

Answer:

A

Question 4

Question Type: MultipleChoice

John, the penetration testing manager in a pen testing firm, needs to prepare a pen testing pricing report for a client. Which of the following factors does he need to consider while preparing the pen testing pricing report?



Options:

- A-** Number of employees in the client organization
- B-** Complete structure of the organization
- C-** Number of client computers to be tested and resources required to perform a pen test
- D-** Number of servers available in the client organization

Answer:

C

Question 5

Question Type: MultipleChoice

After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the Restrict Anonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server.

Using User info tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

Options:

- A- Restrict Anonymous must be set to '2' for complete security
- B- Restrict Anonymous must be set to '3' for complete security
- C- There is no way to always prevent an anonymous null session from establishing
- D- Restrict Anonymous must be set to '10' for complete security

Answer:

A

Question 6

Question Type: MultipleChoice

Which of the following is the objective of Gramm-Leach-Bliley Act?

Options:

- A- To ease the transfer of financial information between institutions and banks
- B- To protect the confidentiality, integrity, and availability of data
- C- To set a new or enhanced standards for all U.S. public company boards, management and public accounting firms
- D- To certify the accuracy of the reported financial statement

Answer:

A

Question 7

Question Type: MultipleChoice

A Demilitarized Zone (DMZ) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. Usage of a protocol within a DMZ environment is highly variable based on the specific needs of an organization.

Privilege escalation, system is compromised when the code runs under root credentials, and DoS attacks are the basic weakness of which one of the following Protocol?

Options:

- A- Lightweight Directory Access Protocol (LDAP)
- B- Simple Network Management Protocol (SNMP)
- C- Telnet
- D- Secure Shell (SSH)

Answer:

D

Question 8

Question Type: MultipleChoice

Why is a legal agreement important to have before launching a penetration test?

Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be Tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: _____ (Business Owner)

_____ (Data Custodian)

_____ (CIO)

_____ (CISO)

Testing Complete: _____ Date: _____

Review/Closeout Discussion Completed (Date): _____

Options:

- A- Guarantees your consultant fees
- B- Allows you to perform a penetration test without the knowledge and consent of the organization's upper management
- C- It establishes the legality of the penetration test by documenting the scope of the project and the consent of the company.
- D- It is important to ensure that the target organization has implemented mandatory security policies

Answer:

C

Question 9

Question Type: MultipleChoice

What is the following command trying to accomplish?

```
C:\> nmap -sU -p445 192.168.0.0/24
```

Options:

- A- Verify that NETBIOS is running for the 192.168.0.0 network
- B- Verify that TCP port 445 is open for the 192.168.0.0 network
- C- Verify that UDP port 445 is open for the 192.168.0.0 network
- D- Verify that UDP port 445 is closed for the 192.168.0.0 networks

Answer:

C

Question 10

Question Type: MultipleChoice

Which of the following equipment could a pen tester use to perform shoulder surfing?

Options:

- A- Binoculars
- B- Painted ultraviolet material
- C- Microphone

D- All the above

Answer:

A

Question 11

Question Type: MultipleChoice

As a security analyst you setup a false survey website that will require users to create a username and a strongpassword. You send the link to all the employees of the company. What information will you be able to gather?

Options:

- A-** The employees network usernames and passwords
- B-** The MAC address of the employees' computers
- C-** The IP address of the employees computers
- D-** Bank account numbers and the corresponding routing numbers

Answer:

C

To Get Premium Files for ECSAv10 Visit

<https://www.p2pexams.com/products/ecsav10>

For More Free Questions Visit

<https://www.p2pexams.com/eccouncil/pdf/ecsav10>

