DUMPSARENA

EC-Council Certified Security Analyst (ECSA)

ECCouncil 412-79

Version Demo

Total Demo Questions: 15

Total Premium Questions: 203

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following will not handle routing protocols properly?

A. “Internet-router-firewall-net architecture”

B. “Internet-firewall-router-net architecture”

C. “Internet-firewall -net architecture”

D. “Internet-firewall/router(edge device)-net architecture”

ANSWER: B

QUESTION NO: 2

How many bits is Source Port Number in TCP Header packet?

A. 48

B. 32

C. 64

D. 16

ANSWER: D

QUESTION NO: 3

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

A. SMTP Queue Bouncing

B. SMTP Message Bouncing

C. SMTP Server Bouncing

D. SMTP Mail Bouncing

ANSWER: D

Explanation:

Reference: http://en.wikipedia.org/wiki/Bounce_message

QUESTION NO: 4

Which of the following statements is true about the LM hash?

A. Disabled in Windows Vista and 7 OSs

B. Separated into two 8-character strings

C. Letters are converted to the lowercase

D. Padded with NULL to 16 characters

ANSWER: A

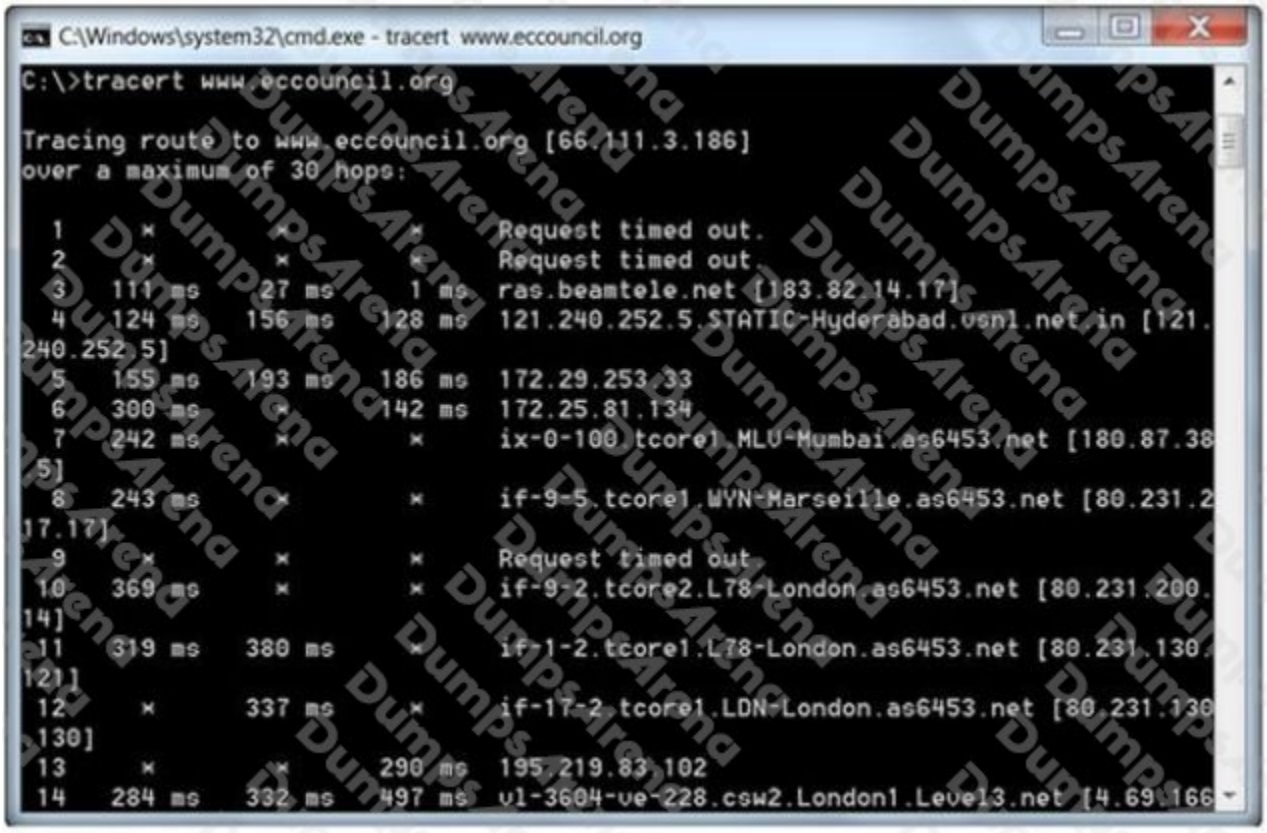
Explanation:

Reference: http://www.onlinehashcrack.com/how_to_crack_windows_passwords.php (first paragraph of the page)

QUESTION NO: 5

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of three Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host.

The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.



During routing, each router reduces packets' TTL value by

A. 3

B. 1

C. 4

D. 2

ANSWER: B

Explanation:

Reference: http://www.packetu.com/2009/10/09/traceroute-through-the-asa/

QUESTION NO: 6

DNS information records provide important data about:

A. Phone and Fax Numbers

B. Location and Type of Servers

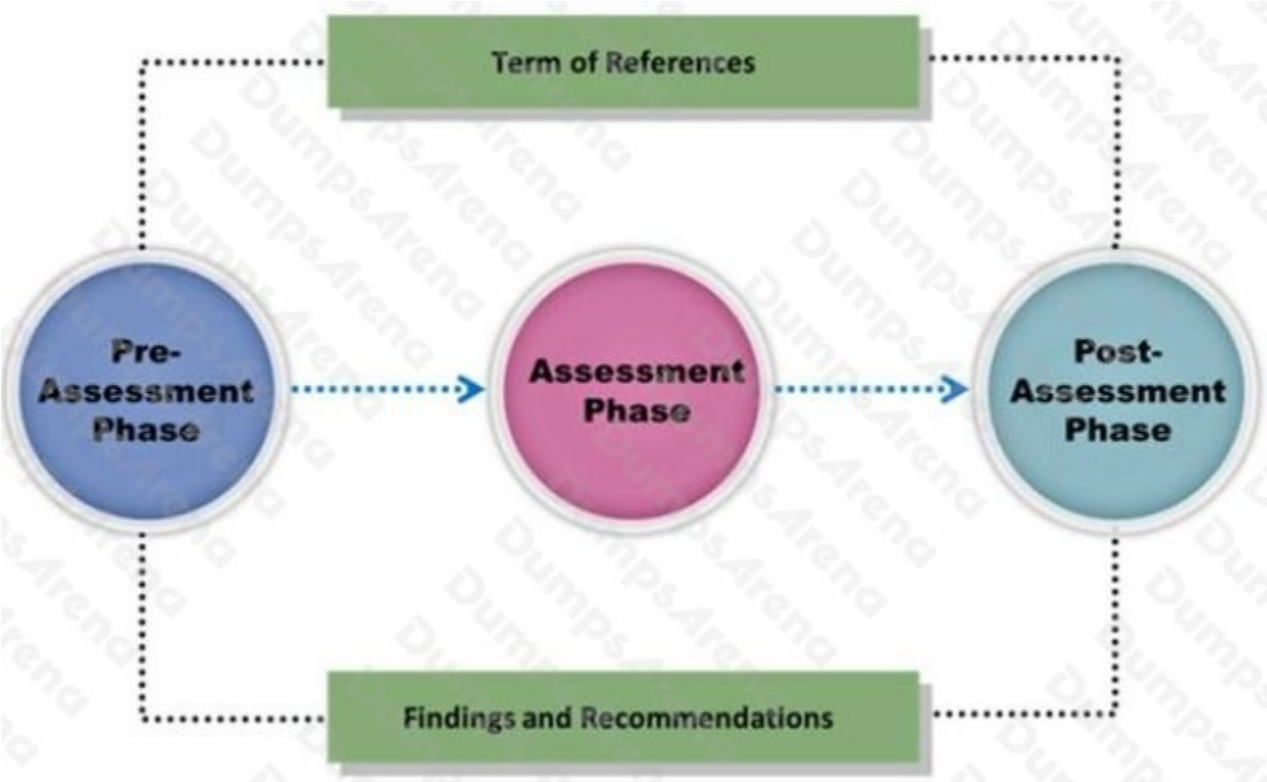
C. Agents Providing Service to Company Staff

D. New Customer

ANSWER: B

QUESTION NO: 7

Vulnerability assessment is an examination of the ability of a system or application, including the current security procedures and controls, to withstand assault.



What does a vulnerability assessment identify?

A. Disgruntled employees

B. Weaknesses that could be exploited

C. Physical security breaches

D. Organizational structure

ANSWER: B

QUESTION NO: 8

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

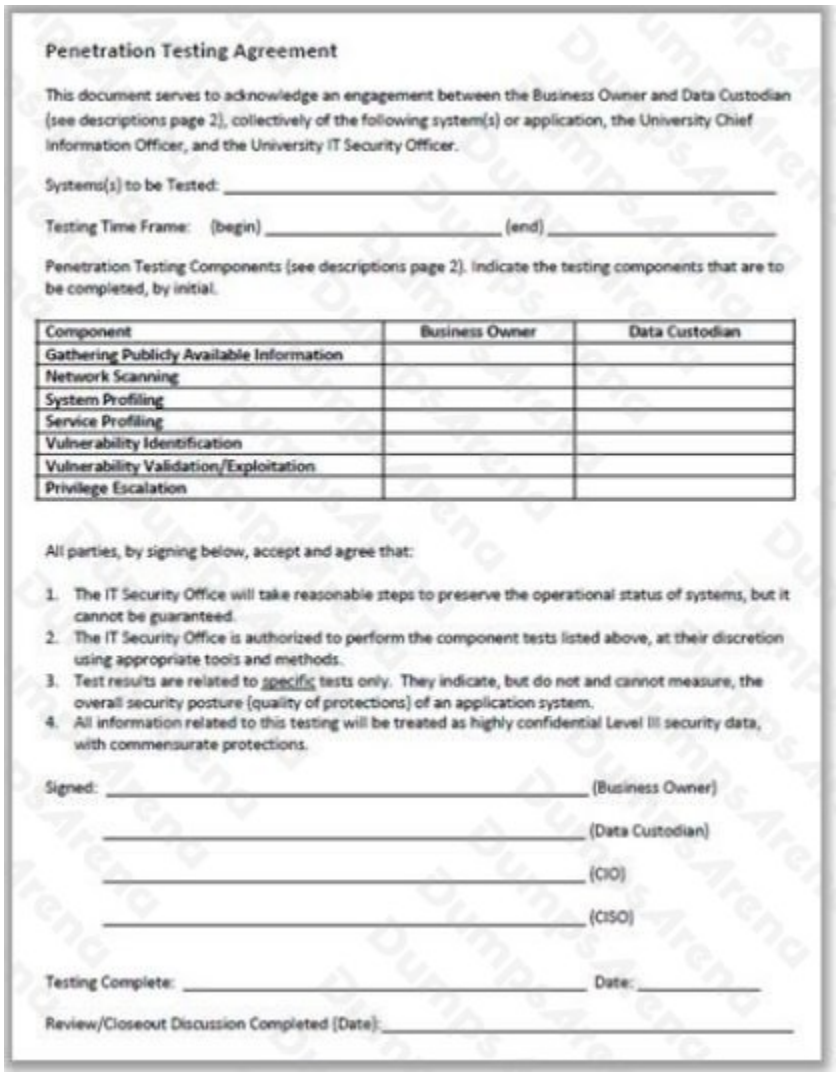
D. 133, 134, 139, 142

ANSWER: A

Explanation:

QUESTION NO: 9

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.

System(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): _____

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 NO: 10

How many possible sequence number combinations are there in TCP/IP protocol?

A. 320 billion

B. 32 million

C. 4 billion

D. 1 billion

ANSWER: C

QUESTION NO: 11

Amazon Consulting Corporation provides penetration testing and managed security services to companies. Legality and regulatory compliance is one of the important components in conducting a successful security audit.

Before starting a test, one of the agreements both the parties need to sign relates to limitations, constraints, liabilities, code of conduct, and indemnification considerations between the parties.

XSECURITY

Overview

Security Assessment needs vary from agency to agency. The XSECURITY Penetration Testing Team (XSECURITY) offers several services that can assist COMPANY X in securing their information technology assets. Each of these services requires some degree of support from the COMPANY X (system information, access to agency personnel or facilities, system/network connections, etc.). Penetration testing tools and techniques can be invasive, however, so there needs to be a clear level of understanding of what an assessment entails, what support is required for assessments, and what potential effect each type of assessment may have.

Use of Tools

The Penetration testing activities performed by the XSECURITY Penetration Testing Team include scanning network assets with specific penetration testing tools. These tools check system configurations, default settings, security settings/updates, network and workstation services, open ports, and other specific vulnerabilities that might be utilized by intruders or unauthorized staff to undermine or bypass the security of an agency's network. They do not access user files, data files, or other personal/confidential files, only network/workstation files associated with system configurations and security. The XSECURITY does perform 'penetration testing' – that is, test how deep into your network an intruder can go, retrieve confidential information, or change system configurations. Our scans determine what vulnerabilities exist within the agency network with fully exploiting those vulnerabilities.

Which agreement requires a signature from both the parties (the penetration tester and the company)?

A. Non-disclosure agreement

B. Client fees agreement

C. Rules of engagement agreement

D. Confidentiality agreement

ANSWER: C

QUESTION NO: 12

The objective of social engineering pen testing is to test the strength of human factors in a security chain within the organization. It is often used to raise the level of security awareness among employees.

The tester should demonstrate extreme care and professionalism during a social engineering pen test as it might involve legal issues such as violation of privacy and may result in an embarrassing situation for the organization.

Which of the following methods of attempting social engineering is associated with bribing, handing out gifts, and becoming involved in a personal relationship to befriend someone inside the company?

A. Accomplice social engineering technique

B. Identity theft

C. Dumpster diving

D. Phishing social engineering technique

ANSWER: A

QUESTION NO: 13

To locate the firewall, SYN packet is crafted using Hping or any other packet crafter and sent to the firewall. If ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device is received, then it means which of the following type of firewall is in place?

A. Circuit level gateway

B. Stateful multilayer inspection firewall

C. Packet filter

D. Application level gateway

ANSWER: C

QUESTION NO: 14

During the process of fingerprinting a web application environment, what do you need to do in order to analyze HTTP and HTTPS request headers and the HTML source code?

A. Examine Source of the Available Pages

B. Perform Web Spidering

C. Perform Banner Grabbing

D. Check the HTTP and HTML Processing by the Browser

ANSWER: D

Explanation:

QUESTION NO: 15

This is a group of people hired to give details of the vulnerabilities present in the system found after a penetration test. They are elite and extremely competent penetration testers and intrusion analysts. This team prepares a report on the vulnerabilities in the system, attack methods, and how to defend against them.

What is this team called?

A. Blue team

B. Tiger team

C. Gorilla team

D. Lion team

ANSWER: B