ECSAV10$^{Q\&As}$

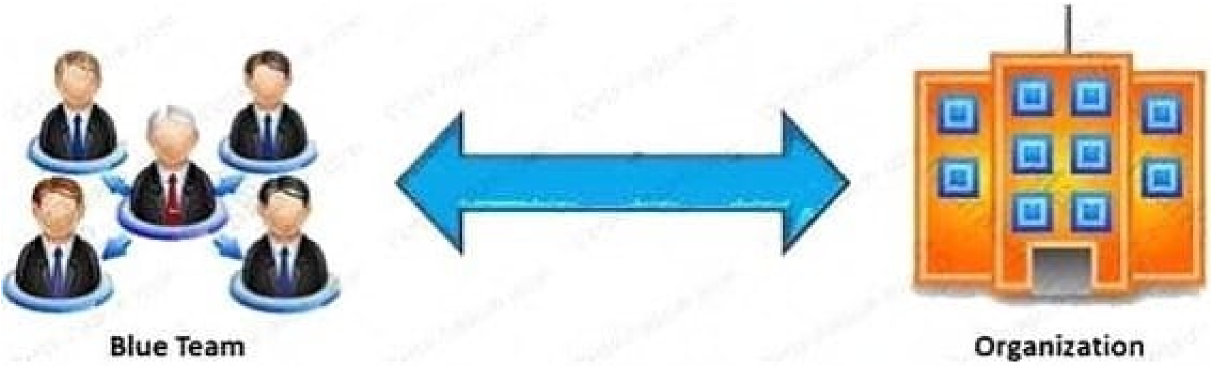
EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

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

QUESTION 1

In the context of penetration testing, what does blue teaming mean?



A. A penetration test performed with the knowledge and consent of the organization\\'s IT staff

B. It is the most expensive and most widely used

C. It may be conducted with or without warning

D. A penetration test performed without the knowledge of the organization\\'s IT staff but with permission from upper management

Correct Answer: A

QUESTION 2

George, a freelance Security Auditor and Penetration Tester, was working on a pen testing assignment for Xsecurity. George is an ESCA certified professional and was following the LPT methodology in performing a comprehensive security assessment of the company. After the initial reconnaissance, scanning and enumeration phases, he successfully recovered a user password and was able to log on to a Linux machine located on the network. He was also able to access the / etc/passwd file; however, the passwords were stored as a single "x" character.

What will George do to recover the actual encrypted passwords?

A. George will perform sniffing to capture the actual passwords

B. George will perform replay attack to collect the actual passwords

C. George will escalate his privilege to root level and look for /etc/shadow file

D. George will perform a password attack using the pre-computed hashes also known as a rainbow attack

Correct Answer: C

QUESTION 3

Rock is a disgruntled employee of XYZ Inc. He wanted to take revenge. For that purpose, he created a malicious software that automatically visits every page on the company\\'s website, checks pages for important links to other content recursively, and indexes them in a logical flow. By using this malicious software, he gathered a lot of crucial information that is required to exploit the organization. What is the type of software that Rock developed?

A. Web spider

B. Web fuzzer

C. Web scanner

D. Web proxy

Correct Answer: A

QUESTION 4

An organization has deployed a web application that uses encoding technique before transmitting the data over the Internet. This encoding technique helps the organization to hide the confidential data such as user credentials, email attachments, etc. when in transit. This encoding technique takes 3 bytes of binary data and divides it into four chunks of 6 bits. Each chunk is further encoded into respective printable character. Identify the encoding technique employed by the organization?

A. Unicode encoding

B. Base64 encoding

C. URL encoding

D. HTMS encoding

Correct Answer: B

QUESTION 5

An "idle" system is also referred to as what?

A. Zombie

B. PC not being used

C. Bot

D. PC not connected to the Internet

Correct Answer: A

QUESTION 6

In the process of hacking a web application, attackers manipulate the HTTP requests to subvert the application authorization schemes by modifying input fields that relate to the user ID, username, access group, cost, file names, file identifiers, etc. They first access the web application using a low privileged account and then escalate privileges to access protected resources. What attack has been carried out?

A. XPath Injection Attack

B. Authorization Attack

C. Authentication Attack

D. Frame Injection Attack

Correct Answer: B

QUESTION 7

Henderson has completed the pen testing tasks. He is now compiling the final report for the client. Henderson needs to include the result of scanning that revealed a SQL injection vulnerability and different SQL queries that he used to bypass web application authentication.

In which section of the pen testing report, should Henderson include this information?

A. General opinion section

B. Methodology section

C. Comprehensive technical report section

D. Executive summary section

Correct Answer: C

QUESTION 8

What is the purpose of the Traceroute command?

A. For extracting information about the network topology, trusted routers, and firewall locations

B. For extracting information about closed ports

C. For extracting information about the server functioning

D. For extracting information about opened ports

Correct Answer: A

QUESTION 9

Dale is a penetration tester and security expert. He works at Sam Morrison Inc. based in Detroit. He was assigned to do an external penetration testing on one of its clients. Before digging into the work, he wanted to start with reconnaissance and grab some details about the organization. He used tools like Netcraft and SHODAN and grabbed the internal URLs of his client. What information do the internal URLs provide?

A. Internal URLs provide an insight into various departments and business units in an organization

B. Internal URLs provide database related information

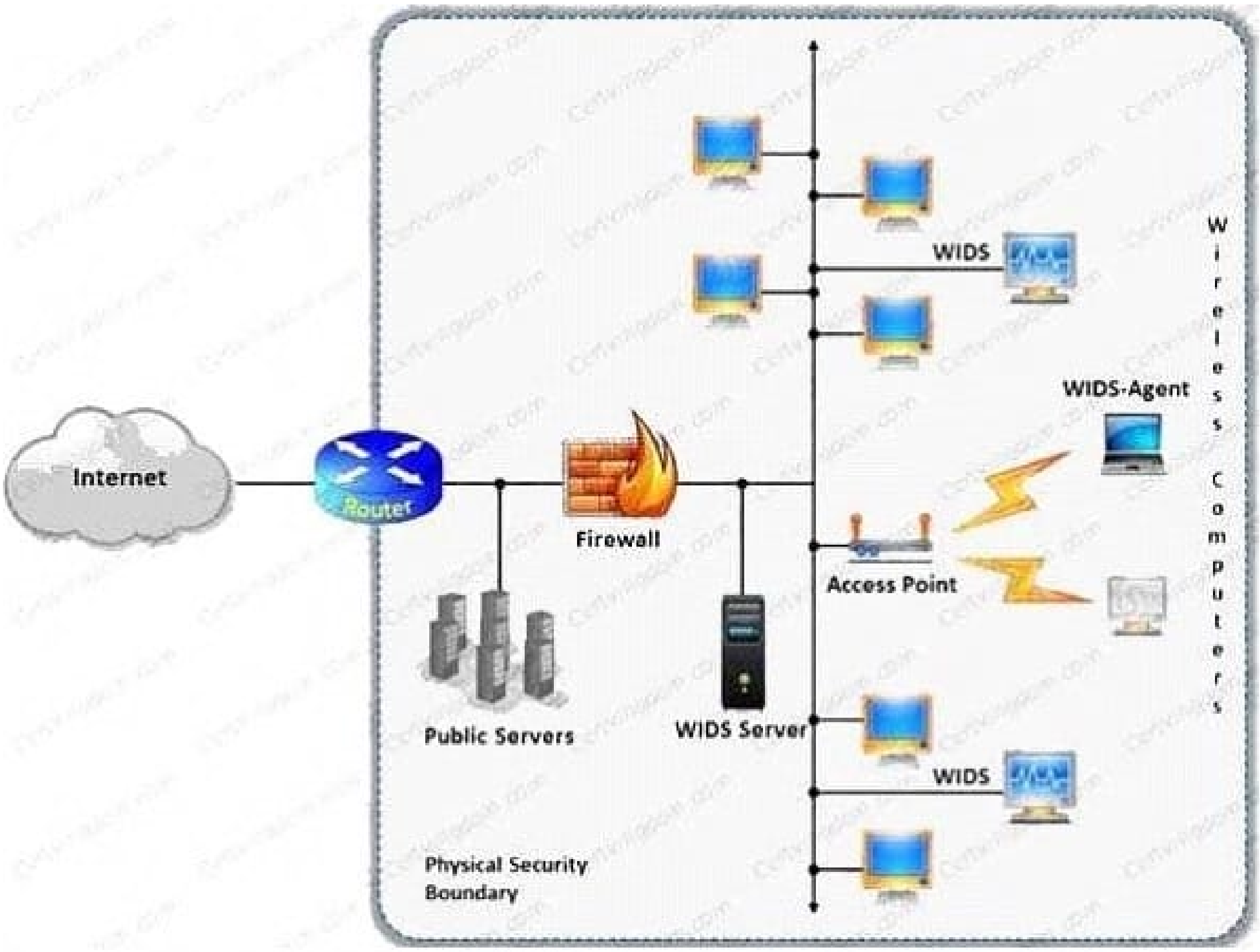
C. Internal URLs provide server related information

D. Internal URLs provide vulnerabilities of the organization

Correct Answer: A

QUESTION 10

A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices. Which of the following attacks can be detected with the help of wireless intrusion detection system (WIDS)?



A. Social engineering

B. SQL injection

C. Parameter tampering

D. Man-in-the-middle attack

Correct Answer: D

QUESTION 11

The framework primarily designed to fulfill a methodical and organized way of addressing five threat classes to network and that can be used to access, plan, manage, and maintain secure computers and communication networks is:

A. Nortells Unified Security Framework

B. The IBM Security Framework

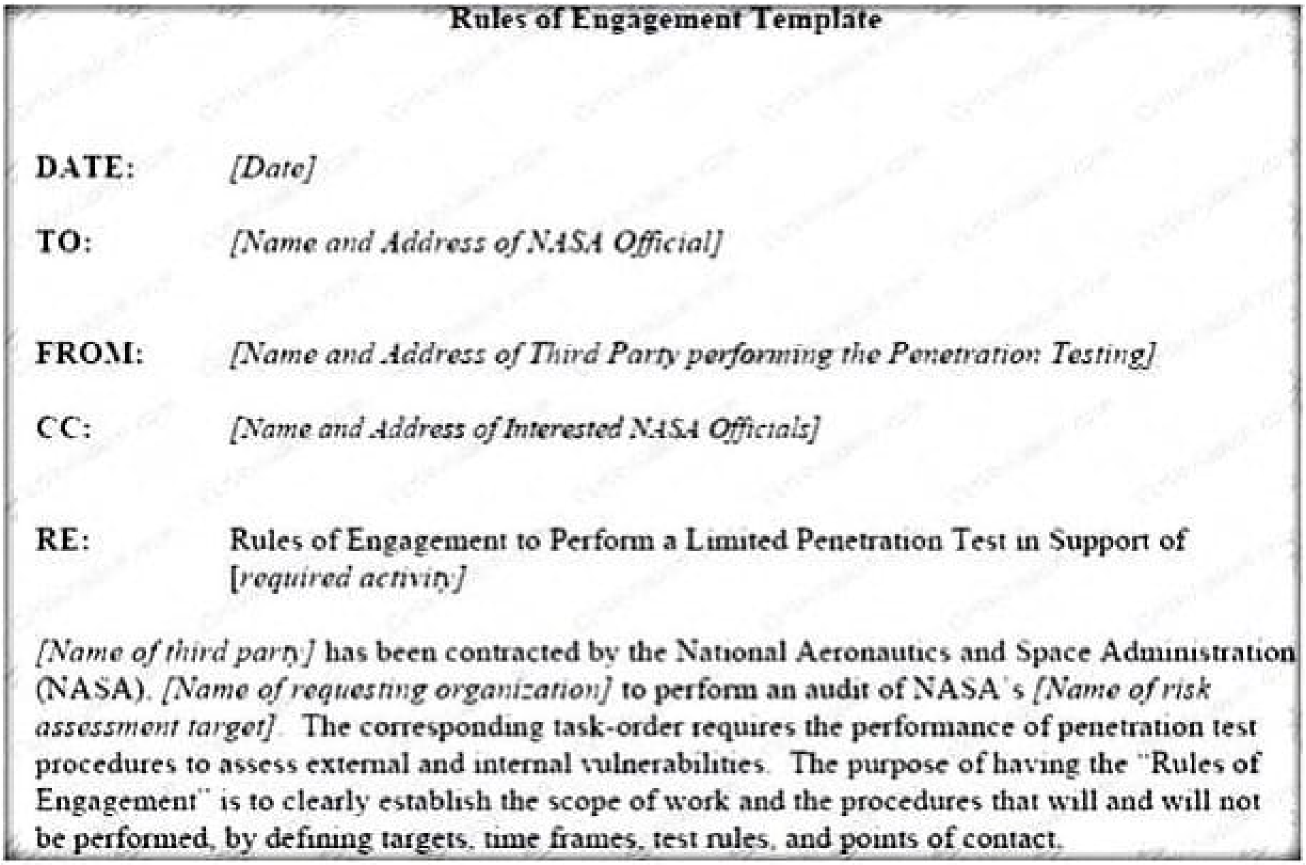
C. Bell Labs Network Security Framework

D. Microsoft Internet Security Framework

Correct Answer: C

QUESTION 12

Rules of Engagement (ROE) document provides certain rights and restriction to the test team for performing the test and helps testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.



Rules of Engagement Template

DATE: *[Date]*

TO: *[Name and Address of NASA Official]*

FROM: *[Name and Address of Third Party performing the Penetration Testing]*

CC: *[Name and Address of Interested NASA Officials]*

RE: Rules of Engagement to Perform a Limited Penetration Test in Support of *[required activity]*

[Name of third party] has been contracted by the National Aeronautics and Space Administration (NASA). *[Name of requesting organization]* to perform an audit of NASA's *[Name of risk assessment target]*. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

What is the last step in preparing a Rules of Engagement (ROE) document?

A. Conduct a brainstorming session with top management and technical teams

B. Decide the desired depth for penetration testing

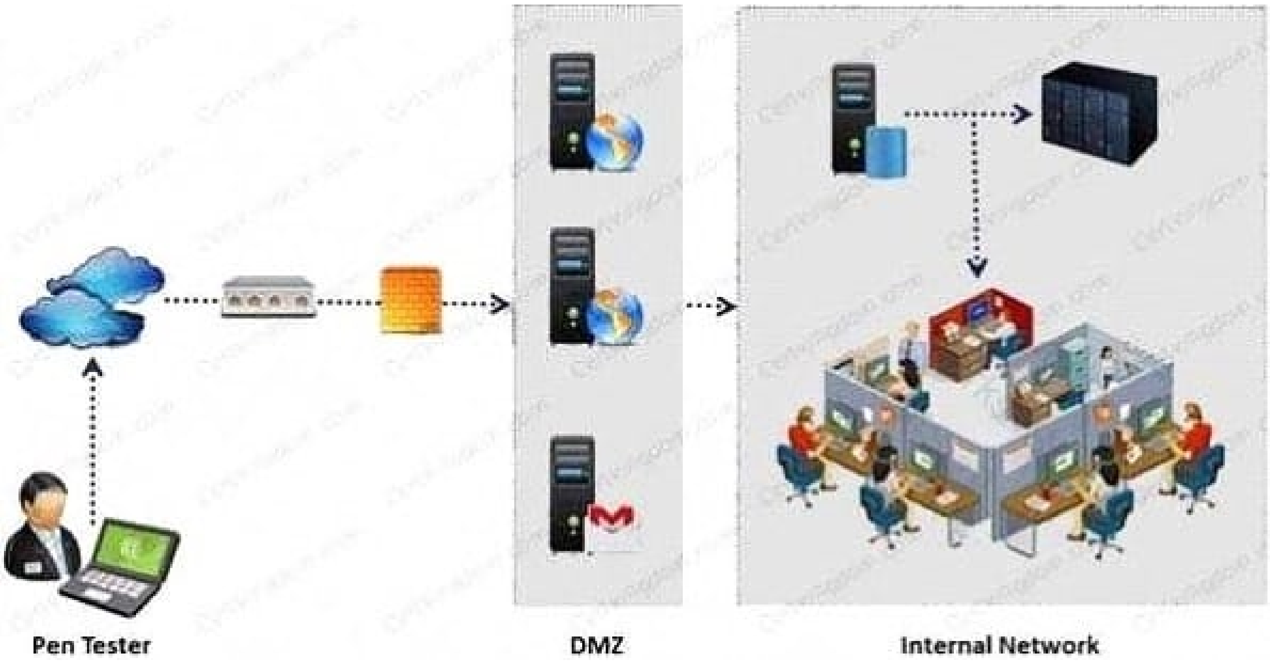
C. Conduct a brainstorming session with top management and technical teams

D. Have pre-contract discussions with different pen-testers

Correct Answer: C

QUESTION 13

An external intrusion test and analysis identify security weaknesses and strengths of the client\\'s systems and networks as they appear from outside the client\\'s security perimeter, usually from the Internet. The goal of an external intrusion test and analysis is to demonstrate the existence of known vulnerabilities that could be exploited by an external attacker.



During external penetration testing, which of the following scanning techniques allow you to determine a port\\'s state without making a full connection to the host?

A. XMAS Scan

B. SYN scan

C. FIN Scan

D. NULL Scan

Correct Answer: B

QUESTION 14

Rebecca, a security analyst, was auditing the network in her organization. During the scan, she found a service running on a remote host, which helped her to enumerate information related to user accounts, network interfaces, network routing and TCP connections.

Which among the following services allowed Rebecca to enumerate the information?

A. NTP

B. SNMP

C. SMPT

D. SMB

Correct Answer: B

QUESTION 15

A firewall\\'s decision to forward or reject traffic in network filtering is dependent upon which of the following?

A. Destination address

B. Port numbers

C. Source address

D. Protocol used

Correct Answer: D

Latest ECSAV10 Dumps ECSAV10 VCE Dumps ECSAV10 Exam Questions