ECSAV8$^{Q\&As}$

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL ECSAV8 Exam with 100% Guarantee

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

https://www.pass2lead.com/ecsav8.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which among the following information is not furnished by the Rules of Engagement (ROE) document?

A. Techniques for data collection from systems upon termination of the test

B. Techniques for data exclusion from systems upon termination of the test

C. Details on how data should be transmitted during and after the test

D. Details on how organizational data is treated throughout and after the test

Correct Answer: D

QUESTION 2

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Smurf

B. Trinoo

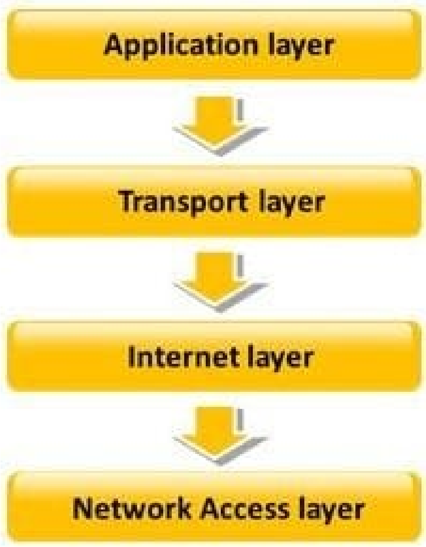
C. Fraggle

D. SYN flood

Correct Answer: A

QUESTION 3

TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network. It provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.



Which of the following TCP/IP layers selects the best path through the network for packets to travel?

A. Transport layer

B. Network Access layer

C. Internet layer

D. Application layer

Correct Answer: B

QUESTION 4

In the example of a /etc/passwd file below, what does the bold letter string indicate?

nomad:HrLNrZ3VS3TF2:501:100: Simple Nomad:/home/nomad:/bin/bash

A. Maximum number of days the password is valid

B. Group number

C. GECOS information

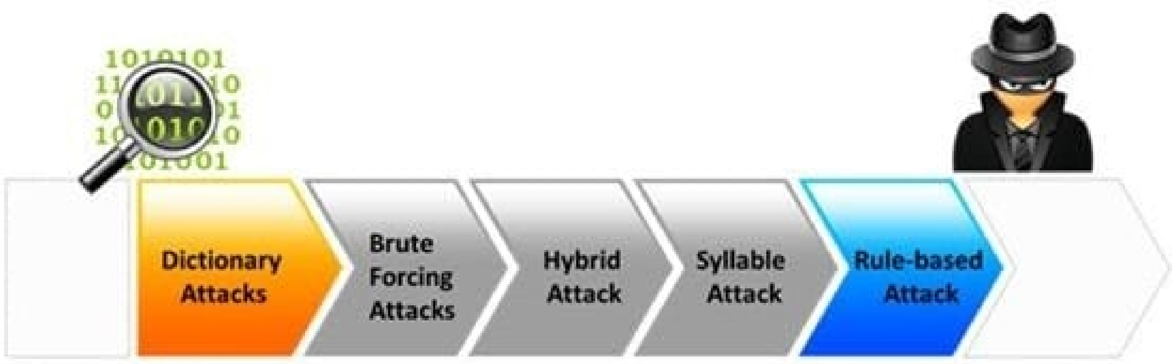
D. User number

Correct Answer: D

QUESTION 5

Passwords protect computer resources and files from unauthorized access by malicious users. Using passwords is the most capable and effective way to protect information and to increase the security level of a company.

Password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system to gain unauthorized access to a system.



Which of the following password cracking attacks tries every combination of characters until the password is broken?

A. Brute-force attack

B. Rule-based attack

C. Hybrid attack D. Dictionary attack

Correct Answer: A

Reference:

http://books.google.com.pk/books?id=m2qZNW4dcyICandpg=PA237andlpg=PA237anddq=passw ord+cracking

+attacks+tries+every+combination+of+characters+until+the+password+is+bro

kenandsource=blandots=RKEUUo6LYjandsig=MPEfFBEpoO0yvOwMxYCoPQuqM5gandhl=enandsa=

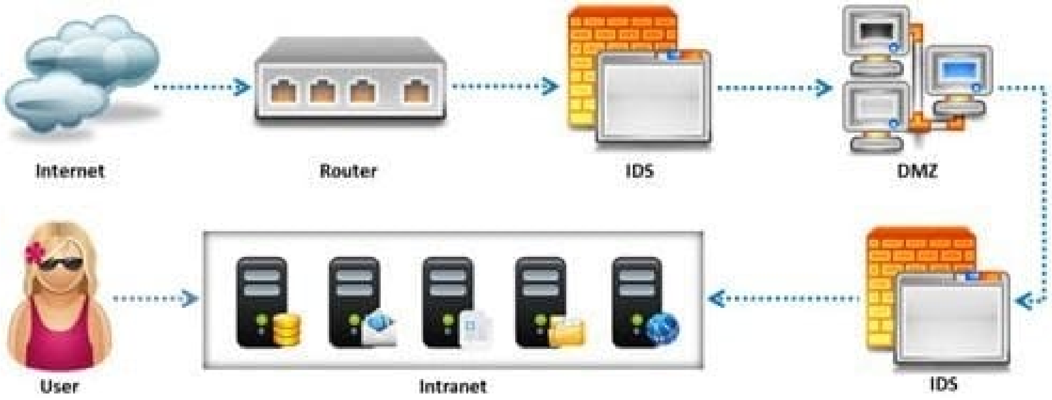
Xandei=ZdwdVJm3CoXSaPXsgPgMandved=0CCEQ6AEwAQ#v=onepageandq=password%20cr acking%

20attacks%20tries%20every%20combination%20of%20characters%20until%20th e%20password%20is%

20brokenandf=false

QUESTION 6

Due to illegal inputs, various types of TCP stacks respond in a different manner. Some IDSs do not take into account the TCP protocol\\'s urgency feature, which could allow testers to evade the IDS.



Penetration tester needs to try different combinations of TCP flags (e.g. none, SYN/FIN, SYN/RST, SYN/ FIN/ACK, SYN/RST/ACK, and All Flags) to test the IDS.

Which of the following TCP flag combinations combines the problem of initiation, midstream, and termination flags with the PSH and URG?

A. SYN/RST/ACK

B. SYN/FIN/ACK

C. SYN/FIN

D. All Flags

Correct Answer: D

Reference:

http://books.google.com.pk/books?id=tUCumJot0ocCandpg=PA63andlpg=PA63anddq=TCP+flag +combinations

+combines+the+problem+of+initiation,+midstream,+and+termination+flags+ with+the+PSH+and

+URGandsource=blandots=mIGSXBIi15andsig=WMnXlEChVSU4RhK65W_V

3tzNjnsandhl=enandsa=Xandei=H7AfVJCtLaufygO1v4DQDgandved=0CBsQ6AEwAA#v=onepageand q=TCP%

20flag%20combinations%20combines%20the%20problem%20of%20initiation%2 C%20midstream%2C%

20and%20termination%20flags%20with%20the%20PSH%20and% 20URGandf=false (see the highlighted

sentence in Table 3-1 at the end of the page)

QUESTION 7

Which of the following is developed to address security concerns on time and reduce the misuse or threat of attacks in an organization?

A. Vulnerabilities checklists

B. Configuration checklists

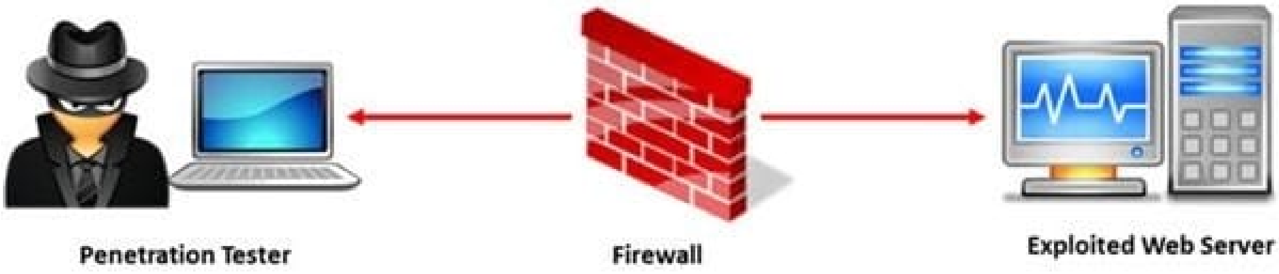
C. Action Plan

D. Testing Plan

Correct Answer: A

QUESTION 8

A penetration test will show you the vulnerabilities in the target system and the risks associated with it. An educated valuation of the risk will be performed so that the vulnerabilities can be reported as High/ Medium/Low risk issues.



What are the two types of `white-box\\' penetration testing?

A. Announced testing and blind testing

B. Blind testing and double blind testing

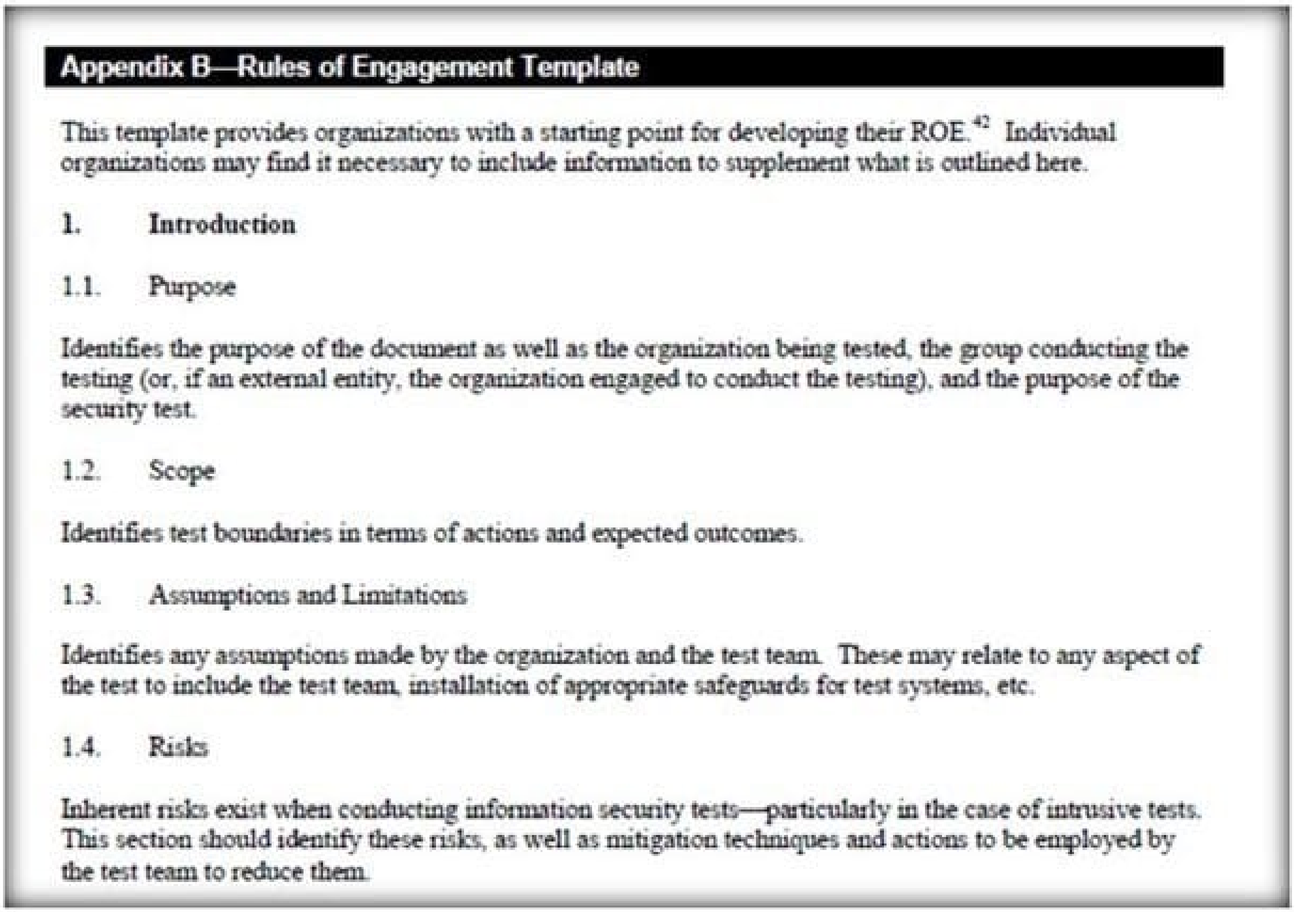
C. Blind testing and unannounced testing

D. Announced testing and unannounced testing

Correct Answer: B

QUESTION 9

Rule of Engagement (ROE) is the formal permission to conduct a pen-test. It provides top- level guidance for conducting the penetration testing. Various factors are considered while preparing the scope of ROE which clearly explain the limits associated with the security test.



Appendix B—Rules of Engagement Template

This template provides organizations with a starting point for developing their ROE.[42] Individual organizations may find it necessary to include information to supplement what is outlined here.

1. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (or, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, installation of appropriate safeguards for test systems, etc.

1.4. Risks

Inherent risks exist when conducting information security tests—particularly in the case of intrusive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

Which of the following factors is NOT considered while preparing the scope of the Rules of Engagment (ROE)?

A. A list of employees in the client organization

B. A list of acceptable testing techniques

C. Specific IP addresses/ranges to be tested

D. Points of contact for the penetration testing team

Correct Answer: A

QUESTION 10

During external penetration testing, which of the following techniques uses tools like Nmap to predict the sequence numbers generated by the targeted server and use this information to perform session hijacking techniques?

A. TCP Sequence Number Prediction

B. IPID State Number Prediction

C. TCP State Number Prediction

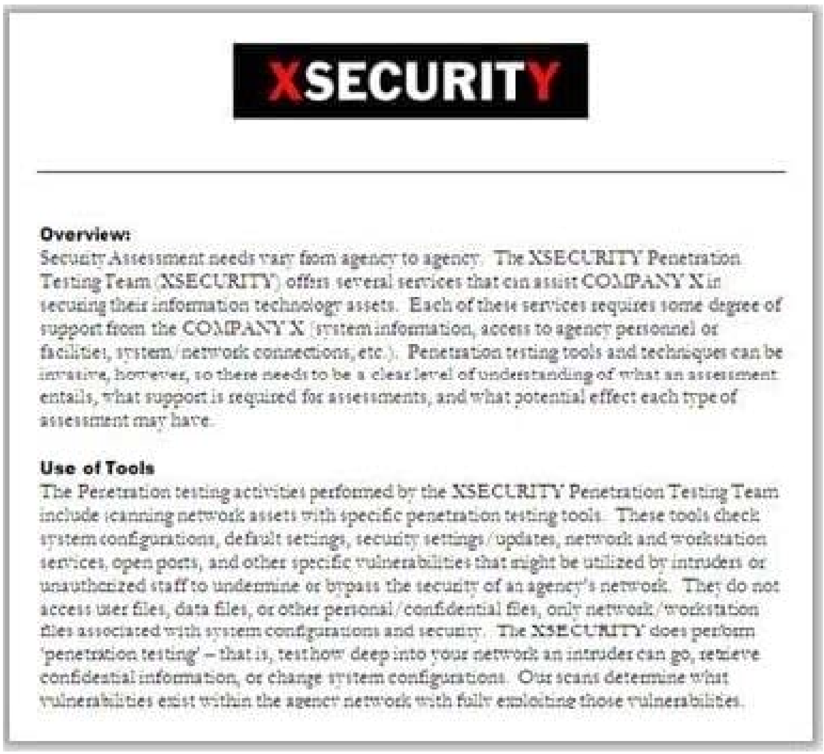
D. IPID Sequence Number Prediction

Correct Answer: A

Reference: http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration- Testing-NoRestriction (p.43)

QUESTION 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

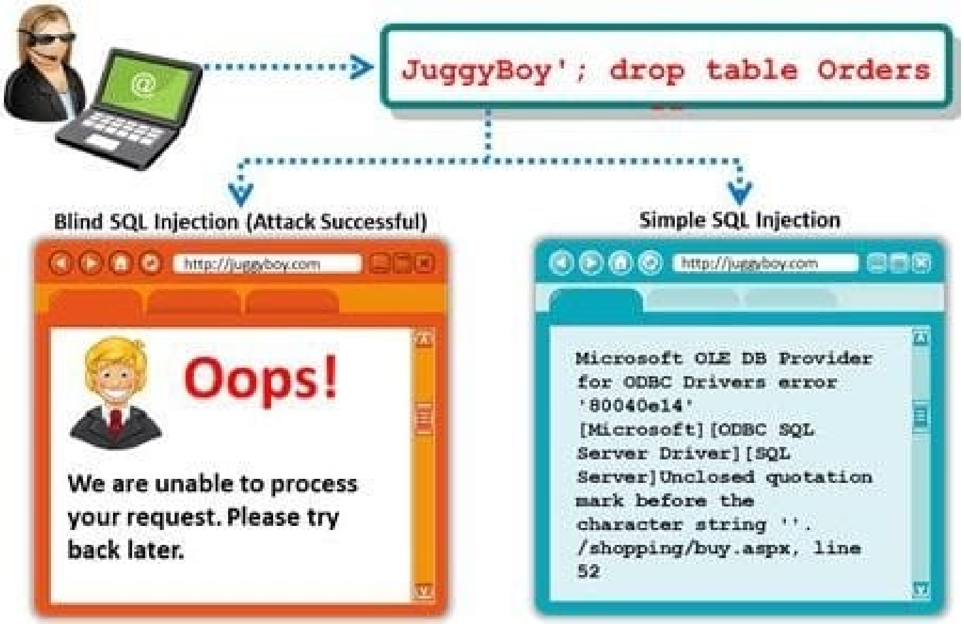
C. Rules of engagement agreement

D. Confidentiality agreement

Correct Answer: D

QUESTION 12

A Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.


JuggyBoy'; drop table Orders
Blind SQL Injection (Attack Successful)
http://juggyboy.com
Oops!
We are unable to process your request. Please try back later.
Simple SQL Injection
http://juggyboy.com
Microsoft OLE DB Provider for ODBC Drivers error '80040e14' [Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string ''. /shopping/buy.aspx, line 52

It is performed when an error message is not received from application while trying to exploit SQL vulnerabilities. The developer\\'s specific message is displayed instead of an error message. So it is quite difficult to find SQL vulnerability in such cases.

A pen tester is trying to extract the database name by using a blind SQL injection. He tests the database using the below query and finally finds the database name.

http://juggyboy.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR DELAY \\'00:00:10\\'-

http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),1,1)))=97) WAITFOR DELAY \\'00:00:10\\'-

http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),2,1)))=98) WAITFOR DELAY \\'00:00:10\\'-

http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),3,1)))=99) WAITFOR DELAY \\'00:00:10\\'-

http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY \\'00:00:10\\'-

What is the database name?

A. WXYZ

B. PQRS

C. EFGH

D. ABCD

Correct Answer: D

Reference: http://www.scribd.com/doc/184891028/CEHv8-Module-14-SQL-Injection-pdf (see module 14, page 2049 to

2051)

QUESTION 13

Which of the following attacks is an offline attack?

A. Pre-Computed Hashes

B. Hash Injection Attack

C. Password Guessing

D. Dumpster Diving

Correct Answer: A

Reference: http://nrupentheking.blogspot.com/2011/02/types-of-password-attack-2.html

QUESTION 14

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

Correct Answer: B

QUESTION 15

Identify the data security measure which defines a principle or state that ensures that an action or transaction cannot be denied.

A. Availability

B. Integrity

C. Authorization

D. Non-Repudiation

Correct Answer: D

Reference: http://en.wikipedia.org/wiki/Information_security (non-repudiation)