412-79V10 Q&As

EC-Council Certified Security Analyst (ECSA) V10

Pass EC-COUNCIL 412-79V10 Exam with 100% Guarantee

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

https://www.pass2lead.com/412-79v10.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Identify the person who will lead the penetration-testing project and be the client point of contact.

A. Database Penetration Tester

B. Policy Penetration Tester

C. Chief Penetration Tester

D. Application Penetration Tester

Correct Answer: C

Reference: http://www.scribd.com/doc/133635286/LPTv4-Module-15-Pre-Penetration- Testing-Checklist-NoRestriction (page 15)

QUESTION 2

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

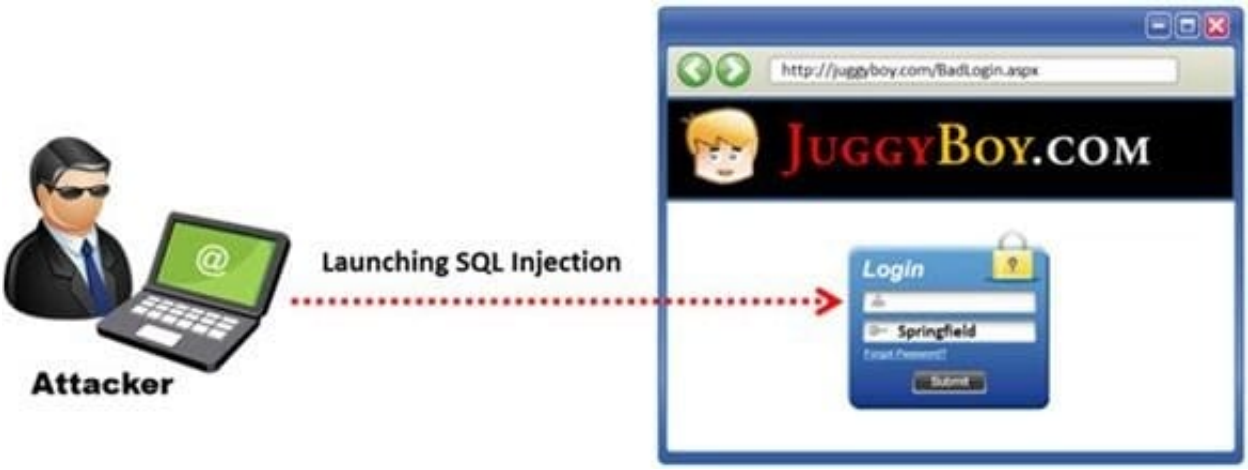
Correct Answer: D

QUESTION 3

SQL injection attacks are becoming significantly more popular amongst hackers and there has been an estimated 69 percent increase of this attack type.

This exploit is used to great effect by the hacking community since it is the primary way to steal sensitive data from web applications. It takes advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a back- end database.

The below diagram shows how attackers launched SQL injection attacks on web applications.



Which of the following can the attacker use to launch an SQL injection attack?

A. Blah\\' "2=2 ?

B. Blah\\' and 2=2 -

C. Blah\\' and 1=1 -

D. Blah\\' or 1=1 -

Correct Answer: D

QUESTION 4

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 5

Which one of the following scans starts, but does not complete the TCP handshake sequence for each port selected, and it works well for direct scanning and often works well through firewalls?

A. SYN Scan

B. Connect() scan

C. XMAS Scan

D. Null Scan

Correct Answer: A

QUESTION 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

Correct Answer: B

QUESTION 7

SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the

data input or transmitted from the client (browser) to the web application.

A successful SQL injection attack can:

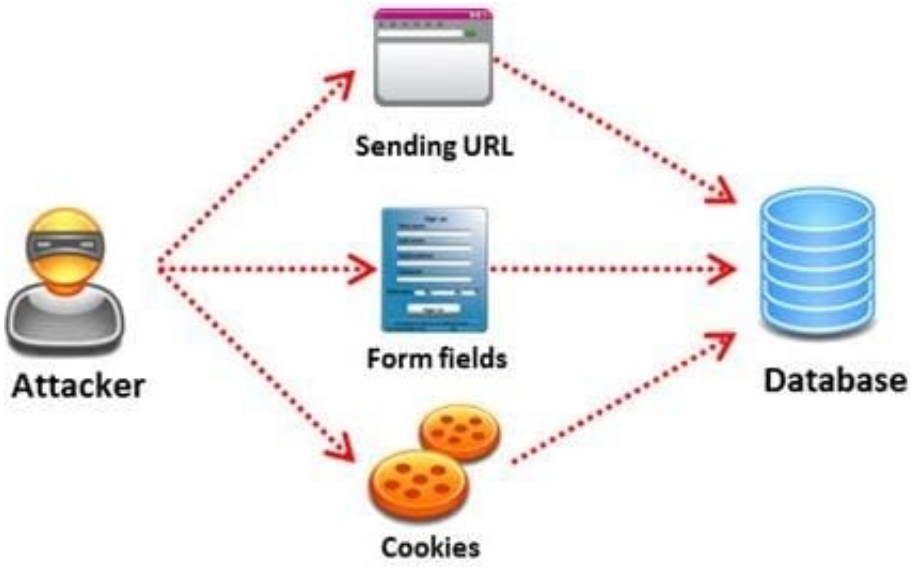
i)Read sensitive data from the database

iii)Modify database data (insert/update/delete)

iii)Execute administration operations on the database (such as shutdown the DBMS)

iV)Recover the content of a given file existing on the DBMS file system or write files into the file system

v)Issue commands to the operating system



Pen tester needs to perform various tests to detect SQL injection vulnerability. He has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate an error.

In which of the following tests is the source code of the application tested in a non-runtime environment to detect the SQL injection vulnerabilities?

A. Automated Testing

B. Function Testing

C. Dynamic Testing

D. Static Testing

Correct Answer: D

Reference:

http://ijritcc.org/IJRITCC%20Vol_2%20Issue_5/Removal%20of%20Data%20Vulnerabilities %20Using%

20SQL.pdf

QUESTION 8

Which one of the following is a supporting tool for 802.11 (wireless) packet injections, it spoofs 802.11 packets to verify whether the access point is valid or not?

A. Airsnort

B. Aircrack

C. Airpwn

D. WEPCrack

Correct Answer: C

QUESTION 9

Which of the following attributes has a LM and NTLMv1 value as 64bit + 64bit + 64bit and NTLMv2 value as 128 bits?

A. Hash Key Length

B. C/R Value Length

C. C/R Key Length

D. Hash Value Length

Correct Answer: B

Reference: http://books.google.com.pk/books?id=QWQRSTnkFsQCandpg=SA4-PA5andlpg=SA4PA5anddq=attributes+has+a+LM+and+NTLMv1+value+as+64bit+%2B+64bit+%2B+64bit+and+NTLMv2 +value+as+128+bitsandsource=blandots=wJPR32BaF6andsig=YEt9LNfQAbm2Mc6obVggKCkQ2sandhl=enandsa=Xandei=scMfVMfdC8u7ygP4xYGQDgandved=0CCkQ6AEwAg#v=onepageandq=attributes%20has%20a%20LM%20and%20NTLMv1%20value%20as%2064 bit%20%2B%2064bit%20%2B%2064bit%20and%20NTLMv2%20value%20as%20128%20 bitsandf=false (see Table 4-1)

QUESTION 10

In which of the following IDS evasion techniques does IDS reject the packets that an end system accepts?

A. IPS evasion technique

B. IDS evasion technique

C. UDP evasion technique

D. TTL evasion technique

Correct Answer: D

Reference: http://is.muni.cz/th/172999/fi_m/MT_Bukac.pdf (page 24)

QUESTION 11

Traffic on which port is unusual for both the TCP and UDP ports?

A. Port 81

B. Port 443

C. Port 0

D. Port21

Correct Answer: C

QUESTION 12

Logs are the record of the system and network activities. Syslog protocol is used for delivering log information across an IP network. Syslog messages can be sent via which one of the following?

A. UDP and TCP

B. TCP and SMTP

C. SMTP

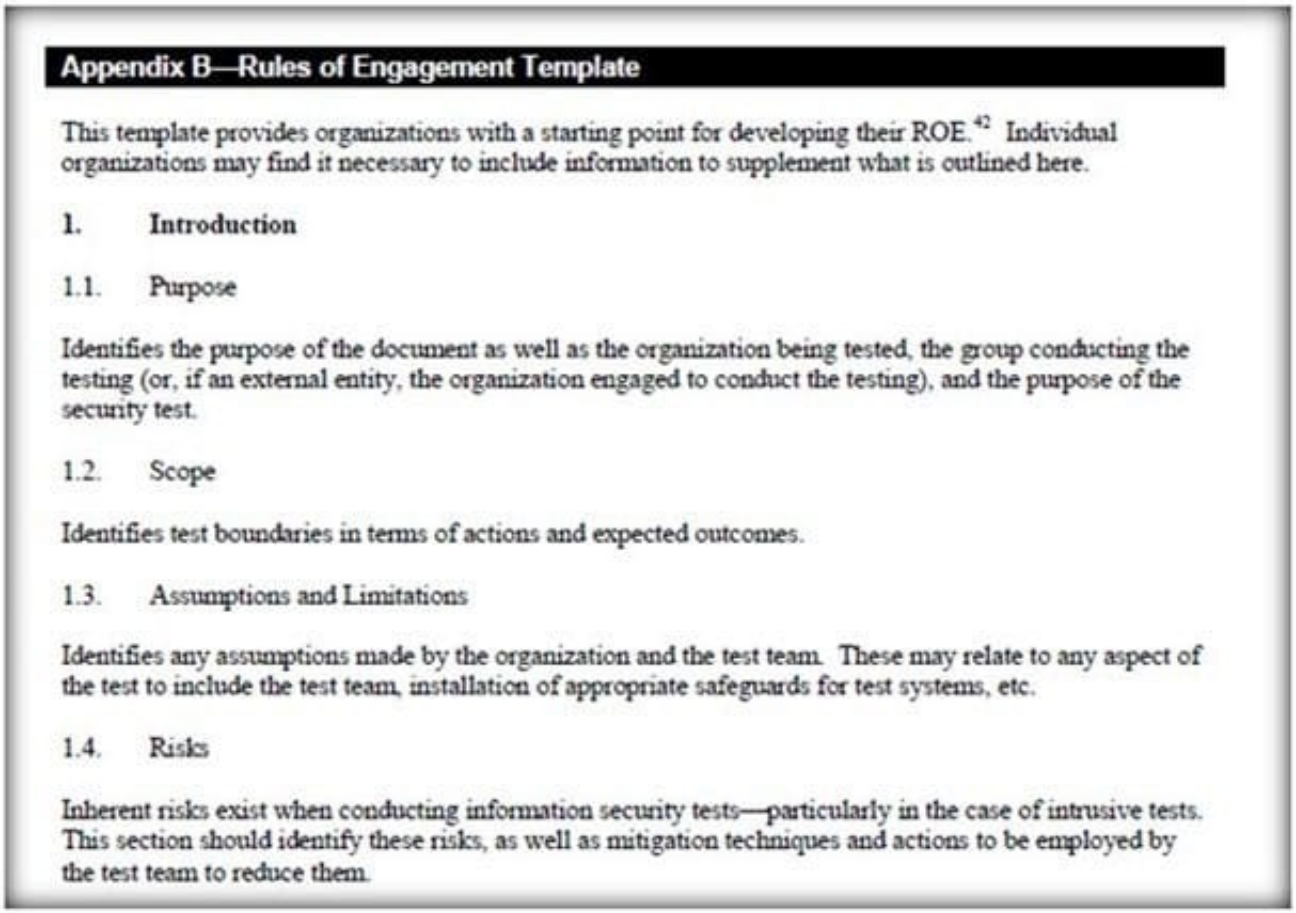
D. UDP and SMTP

Correct Answer: A

QUESTION 13

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 14

Which of the following shields Internet users from artificial DNS data, such as a deceptive or mischievous address instead of the genuine address that was requested?

A. DNSSEC

B. Firewall

C. Packet filtering

D. IPSec

Correct Answer: A

Reference: http://tools.ietf.org/html/draft-osterweil-dane-ipsec-01 (abstract, first para)

QUESTION 15

Which of the following contents of a pen testing project plan addresses the strengths, weaknesses, opportunities, and threats involved in the project?

A. Project Goal

B. Success Factors

C. Objectives

D. Assumptions

Correct Answer: D