Vendor:EC-COUNCIL

Exam Code:ECSAV8

Exam Name:EC-Council Certified Security Analyst (ECSA)

Version: Demo

QUESTION 1

Which of the following is not a condition specified by Hamel and Prahalad (1990)?

A. Core competency should be aimed at protecting company interests

B. Core competency is hard for competitors to imitate

C. Core competency provides customer benefits

D. Core competency can be leveraged widely to many products and markets

Correct Answer: A

Reference: http://www.studymode.com/essays/Hamel-Prahalad-Core-Competency- 1228370.html

---

QUESTION 2

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

Correct Answer: C

QUESTION 3

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:

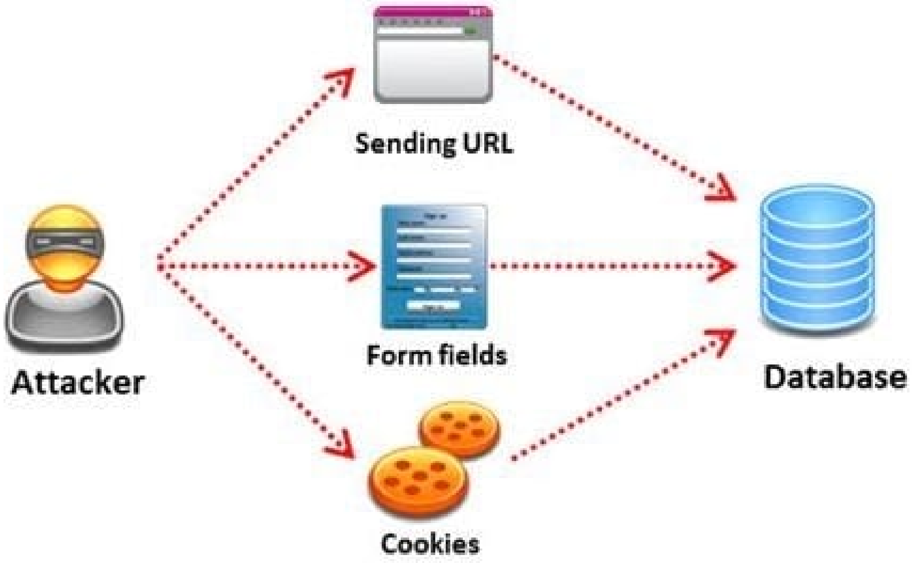
i)Read sensitive data from the database

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: A

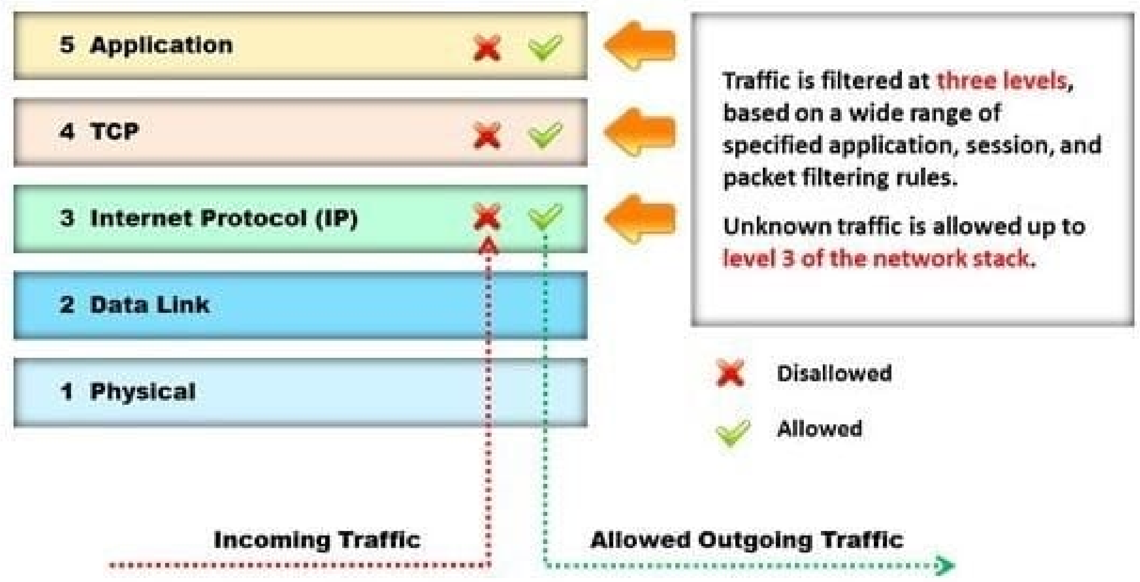
Reference:

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

20SQL.pdf

QUESTION 4

Identify the type of firewall represented in the diagram below:


5 Application
4 TCP
3 Internet Protocol (IP)
2 Data Link
1 Physical
Traffic is filtered at three levels, based on a wide range of specified application, session, and packet filtering rules.
Unknown traffic is allowed up to level 3 of the network stack.
Disallowed
Allowed
Incoming Traffic
Allowed Outgoing Traffic

A. Stateful multilayer inspection firewall

B. Application level gateway

C. Packet filter

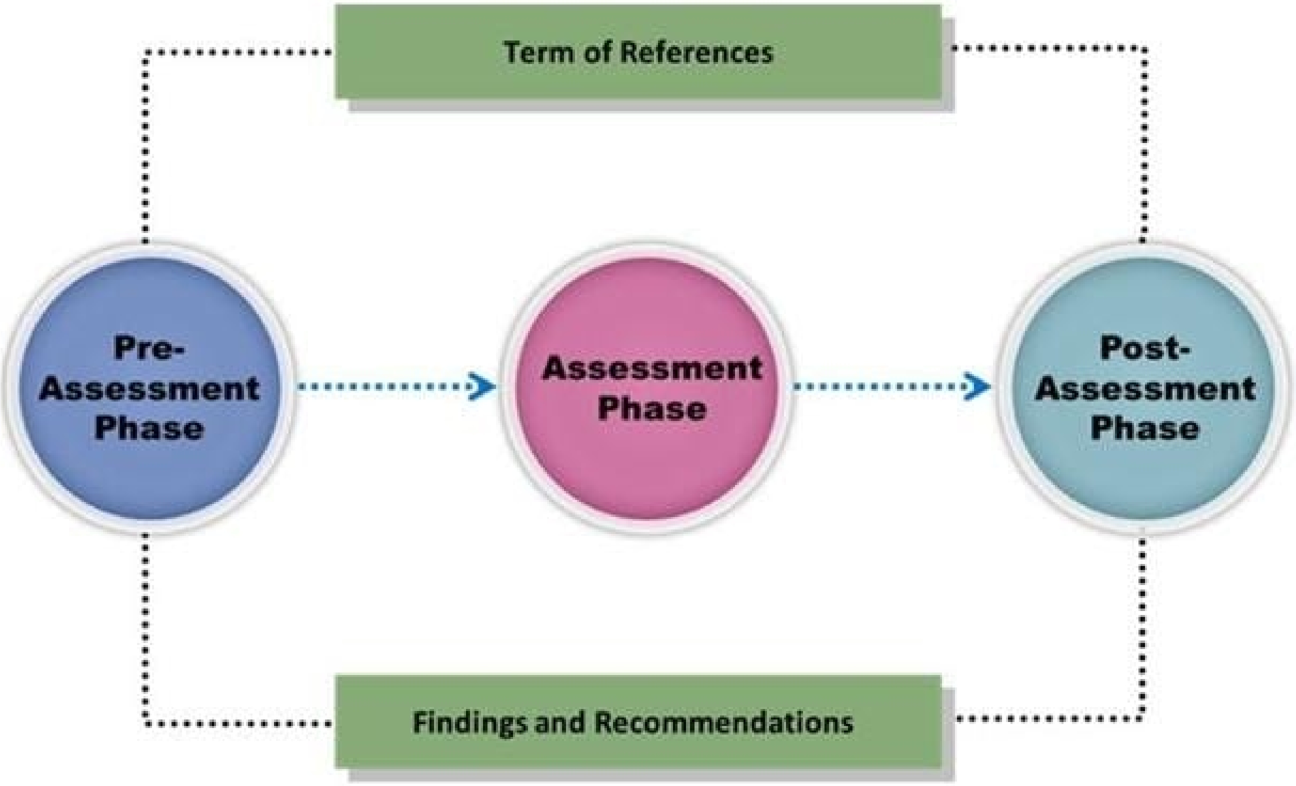
D. Circuit level gateway

Correct Answer: B

Reference: http://www.technicolorbroadbandpartner.com/getfile.php?id=4159 (page 13)

QUESTION 5

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

Correct Answer: B

QUESTION 6

Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

A. Decreases consumed employee time and increases system uptime

B. Increases detection and reaction time

C. Increases response time

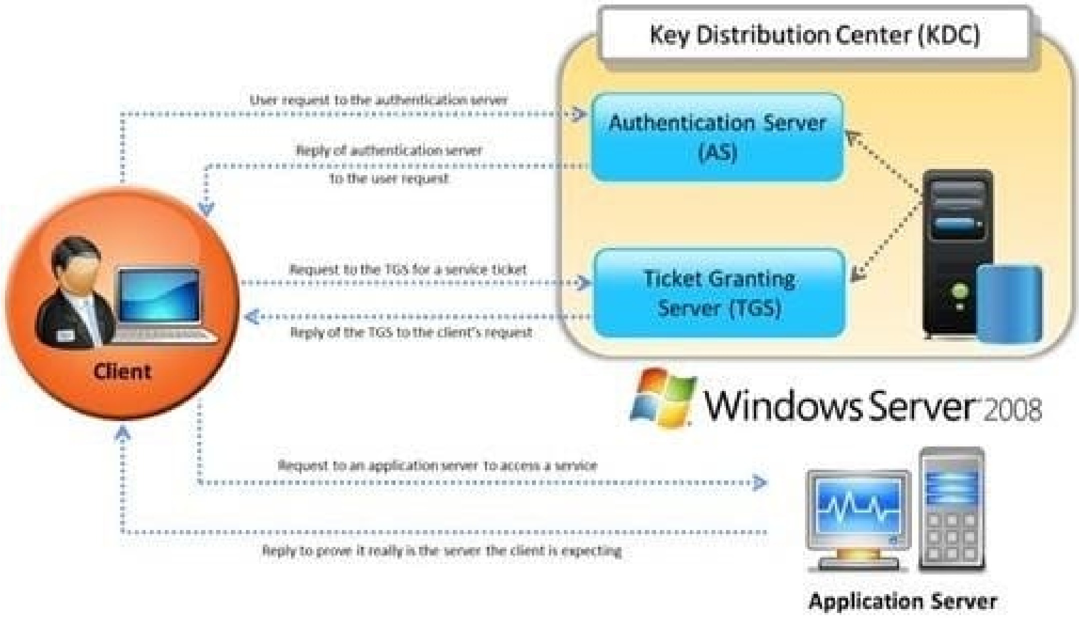
D. Both a and c

Correct Answer: A

Reference: http://www.symantec.com/connect/articles/multi-layer-intrusion-detection- systems (economic advantages, first para)

QUESTION 7

Identify the type of authentication mechanism represented below: A. NTLMv1


Key Distribution Center (KDC)
User request to the authentication server
Authentication Server (AS)
Reply of authentication server to the user request
Request to the TGS for a service ticket
Ticket Granting Server (TGS)
Reply of the TGS to the client's request
Client
Windows Server 2008
Request to an application server to access a service
Reply to prove it really is the server the client is expecting
Application Server

B. NTLMv2

C. LAN Manager Hash

D. Kerberos

Correct Answer: D

The client authenticates itself to the Authentication Server (AS) which forwards the username to a key distribution center (KDC). The KDC issues a ticket granting ticket (TGT), which is time stamped, encrypts it using the user\\'s password and returns the encrypted result to the user\\'s workstation. This is done infrequently, typically at user logon; the TGT expires at some point, though may be transparently renewed by the user\\'s session manager while they are logged in.

When the client needs to communicate with another node ("principal" in Kerberos parlance) the client sends the TGT to the ticket granting service (TGS), which usually shares the same host as the KDC. After verifying the TGT is valid and the user is permitted to access the requested service, the TGS issues a ticket and session keys, which are returned to the client. The client then sends the ticket to the service server (SS) along with its service request.

Reference: http://en.wikipedia.org/wiki/Kerberos_(protocol)

QUESTION 8

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 9

Which of the following password hashing algorithms is used in the NTLMv2 authentication mechanism?

A. AES

B. DES (ECB mode)

C. MD5

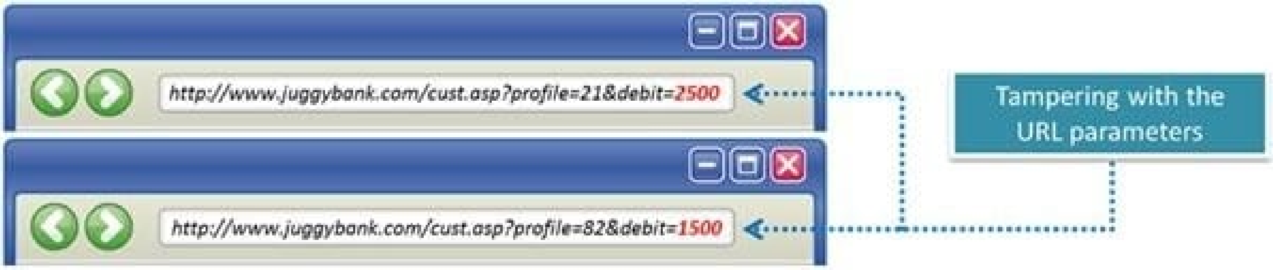
D. RC5

Correct Answer: C

QUESTION 10

The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations. Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.



http://www.juggybank.com/cust.asp?profile=21&debit=2500

http://www.juggybank.com/cust.asp?profile=82&debit=1500

What is the best way to protect web applications from parameter tampering attacks?

A. Validating some parameters of the web application

B. Minimizing the allowable length of parameters

C. Using an easily guessable hashing algorithm

D. Applying effective input field filtering parameters

Correct Answer: B

QUESTION 11

A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the database using the below query and finds the table:

http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype=\\'U\\')=3) WAITFOR DELAY \\'00:00:10\\'-

http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY \\'00:00:10\\'-

http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY \\'00:00:10\\'-

http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY \\'00:00:10\\'-

What is the table name?

A. CTS

B. QRT

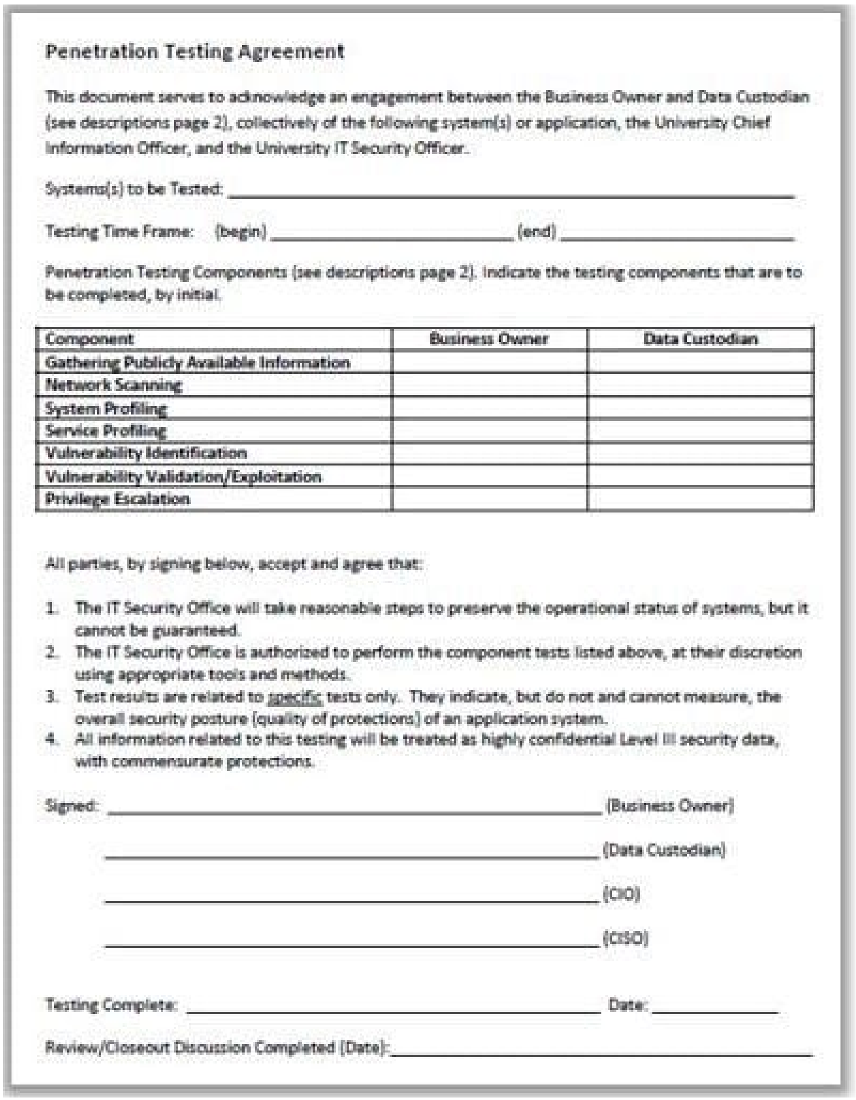
C. EMP

D. ABC

Correct Answer: C

QUESTION 12

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): ______________________________

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

Correct Answer: C