ECSAV10Q&As

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

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

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

https://www.passapply.com/ecsav10.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A team of cyber criminals in Germany has sent malware-based emails to workers of a fast-food center which is having multiple outlets spread geographically. When any of the employees click on the malicious email, it will give backdoor access to the point of sale (POS) systems located at various outlets. After gaining access to the POS systems, the criminals will be able to obtain credit card details of the fast-food center\\'s customers. In the above scenario, identify the type of attack being performed on the fast-food center?

A. Phishing

B. Vishing

C. Tailgating

D. Dumpster diving

Correct Answer: A

QUESTION 2

Transmission Control Protocol (TCP) is a connection-oriented four layer protocol. It is responsible for breaking messages into segments, re-assembling them at the destination station, and re-sending. Which one of the following protocols does not use the TCP?

A. Reverse Address Resolution Protocol (RARP)

B. HTTP (Hypertext Transfer Protocol)

C. SMTP (Simple Mail Transfer Protocol)

D. Telnet

Correct Answer: A

QUESTION 3

Which of the following acts is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

A. PIPEDA

B. PCI DSS

C. Human Rights Act 1998

D. Data Protection Act 1998

Correct Answer: B

QUESTION 4

Which of the following scan option is able to identify the SSL services?

A. -sS

B. -sV

C. -sU

D. -sT

Correct Answer: B

QUESTION 5

You are assisting a Department of Defense contract company to become compliant with the stringent

security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections

that were first initiated by internal computers.

What type of firewall must you implement to abide by this policy?

A. Circuit-level proxy firewall

B. Packet filtering firewall

C. Application-level proxy firewall

D. Statefull firewall

Correct Answer: D

QUESTION 6

Which one of the following Snort logger mode commands is associated to run a binary log file through Snort in sniffer mode to dump the packets to the screen?

A. ./snort -dvr packet.log icmp

B. ./snort -dev -l ./log

C. ./snort -dv -r packet.log

D. ./snort -l ./log -b

Correct Answer: C

QUESTION 7

Which of the following acts provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information?

A. PCI-DSS

B. SOX

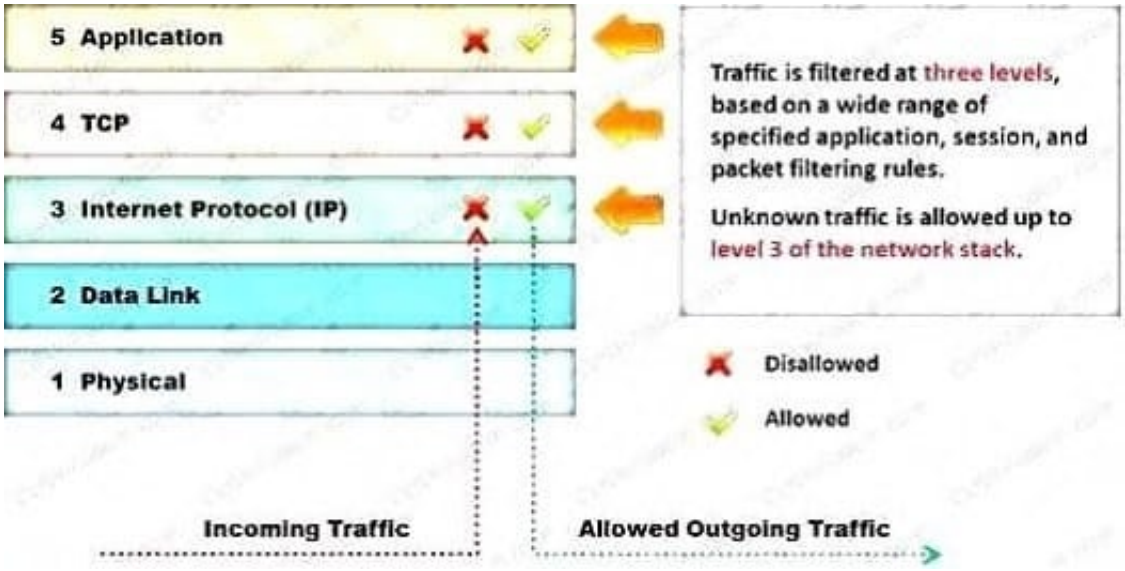
C. HIPAA

D. GLBA

Correct Answer: C

QUESTION 8

Identify the type of firewall represented in the diagram below:



A. Stateful multilayer inspection firewall

B. Application level gateway

C. Packet filter

D. Circuit level gateway

Correct Answer: A

QUESTION 9

Which of the following is not the SQL injection attack character?

A. $

B. PRINT

C. #

D. @@variable

Correct Answer: A

QUESTION 10

Identify the policy that defines the standards for the organizational network connectivity and security standards for computers that are connected in the organizational network.

A. Information-Protection Policy

B. Special-Access Policy

C. Remote-Access Policy

D. Acceptable-Use Policy

Correct Answer: C

QUESTION 11

Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

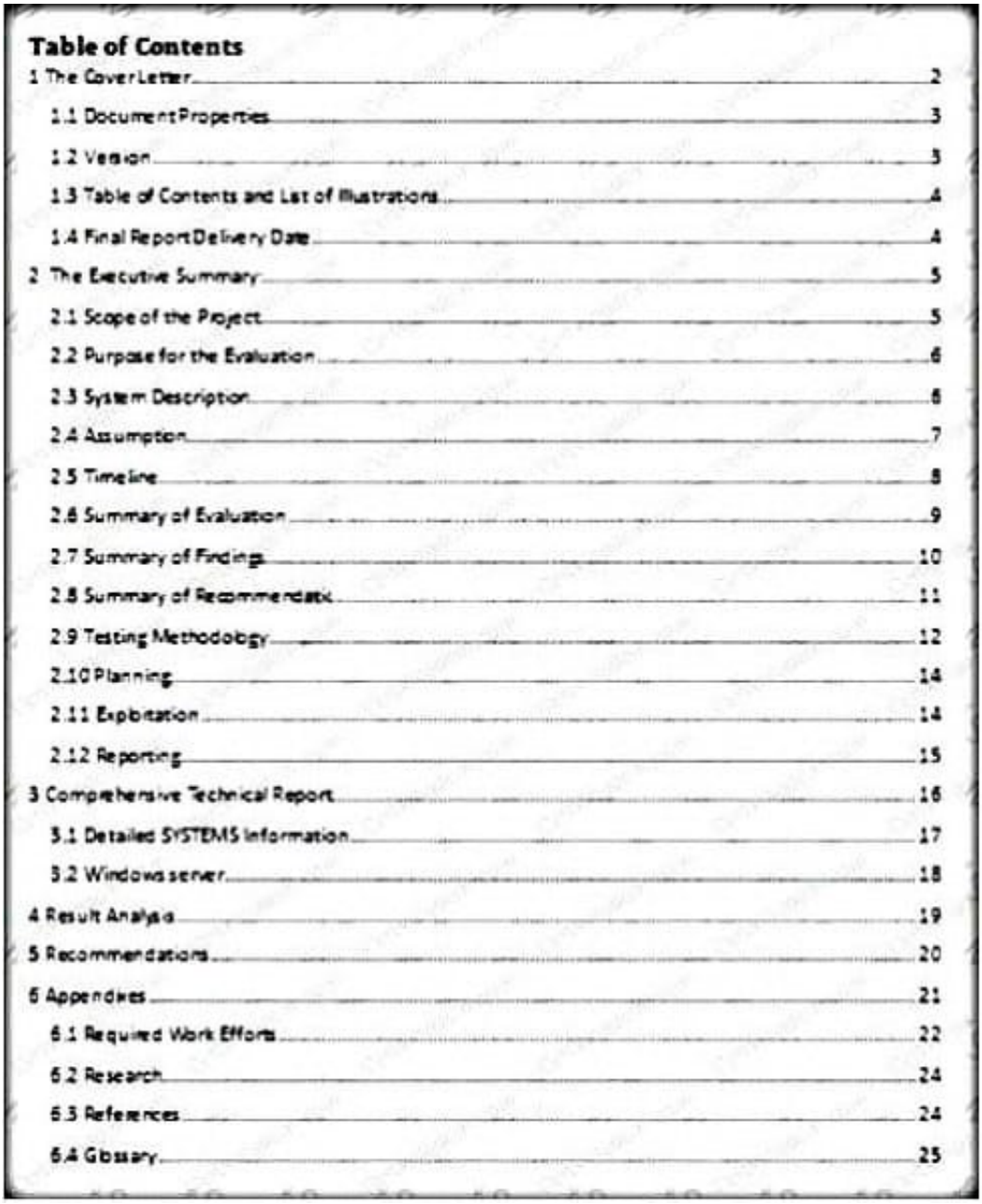


Table of Contents

A. Client-Side Test Report

B. Activity Report

C. Host Report

D. Vulnerability Report

Correct Answer: A

QUESTION 12

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.

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: D

QUESTION 13

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 14

After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts responds to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A. A switched network will not respond to packets sent to the broadcast address

B. Only IBM AS/400 will reply to this scan

C. Only Unix and Unix-like systems will reply to this scan

D. Only Windows systems will reply to this scan

Correct Answer: C

QUESTION 15

A framework is a fundamental structure used to support and resolve complex issues. The framework that delivers an efficient set of technologies in order to develop applications which are more secure in using Internet and Intranet is:

A. Microsoft Internet Security Framework

B. Information System Security Assessment Framework (ISSAF)

C. Bell Labs Network Security Framework

D. The IBM Security Framework

Correct Answer: A