EC-Council Certified Security Analyst (ECSA) v9

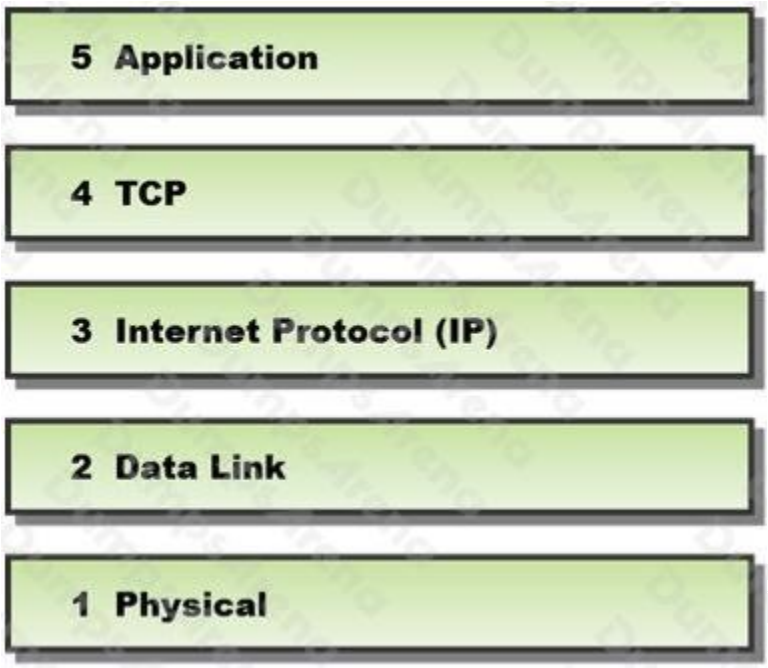
ECCouncil 412-79v9

Total Questions: 10
Version Demo

https://dumpsarena.com
sales@dumpsarena.com

QUESTION NO: 1

In a TCP packet filtering firewall, traffic is filtered based on specified session rules, such as when a session is initiated by a recognized computer.



Identify the level up to which the unknown traffic is allowed into the network stack.

A. Level 5 – Application
B. Level 2 – Data Link
C. Level 4 – TCP
D. Level 3 – Internet Protocol (IP)

Answer: D
Reference:
http://books.google.com.pk/books?id=KPjLAyA7HgoC&pg=PA208&lpg=PA208&dq=TCP+packet+filtering+firewall+level+up+to+which+the+unknown+traffic+is+allowed+into+the+network+stack&source=bl&ots=zRrbchVYng&sig=q5G3T8lggTfAMNRkL7Kp0SRslHU&hl=en&sa=X&ei=5PUeVLSbC8TmaMzrgZgC&ved=0CBsQ6AEwAA#v=onepage&q=TCP%20packet%20filtering%20firewall%20level%20up%20to%20which%20the%20unknown%20traffic%20is%20allowed%20into%20the%20network%20stack&f=false

QUESTION NO: 2

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

Answer: D

QUESTION NO: 3

Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?

A. Testing to provide a more complete view of site security
B. Testing focused on the servers, infrastructure, and the underlying software, including the target
C. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections
D. Testing performed from a number of network access points representing each logical and physical segment

Answer: B

QUESTION NO: 4

The first phase of the penetration testing plan is to develop the scope of the project in consultation with the client. Pen testing test components depend on the client's operating environment, threat perception, security and compliance requirements, ROE, and budget. Various components need to be considered for testing while developing the scope of the project.

Which of the following is NOT a pen testing component to be tested?

A. System Software Security
B. Intrusion Detection
C. Outside Accomplices
D. Inside Accomplices

Answer: C

QUESTION NO: 5

Which one of the following tools of trade is an automated, comprehensive penetration testing product for assessing the specific information security threats to an organization?

A. Sunbelt Network Security Inspector (SNSI)
B. CORE Impact
C. Canvas
D. Microsoft Baseline Security Analyzer (MBSA)

Answer: C

QUESTION NO: 6

Which of the following appendices gives detailed lists of all the technical terms used in the report?

A. Required Work Efforts
B. References
C. Research
D. Glossary

Answer: D
Refere' http://en.wikipedia.org/wiki/Glossary

QUESTION NO: 7

Which of the following methods is used to perform server discovery?

A. Banner Grabbing
B. Whois Lookup
C. SQL Injection
D. Session Hijacking

Answer: B
Reference: http://luizfirmino.blogspot.com/2011/09/server-discovery.html

QUESTION NO: 8

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

Answer: D

QUESTION NO: 9

Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.

Which of the following techniques do attackers use to create backdoors to covertly gather critical information about a target machine?

A. Internal network mapping to map the internal network of the target machine
B. Port scanning to determine what ports are open or in use on the target machine
C. Sniffing to monitor all the incoming and outgoing network traffic
D. Social engineering and spear phishing attacks to install malicious programs on the target machine

Answer: D

QUESTION NO: 10

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

Answer: B
Reference: http://luizfirmino.blogspot.com/2011_09_01_archive.html (see authorization attack)