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.leads4pass.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

Information gathering is performed to:

i) Collect basic information about the target company and its network

ii) Determine the operating system used, platforms running, web server versions, etc.

iii) Find vulnerabilities and exploits

Which of the following pen testing tests yields information about a company\\'s technology infrastructure?

A. Searching for web page posting patterns

B. Analyzing the link popularity of the company\\'s website

C. Searching for trade association directories

D. Searching for a company\\'s job postings

Correct Answer: D

QUESTION 2

The framework primarily designed to fulfill a methodical and organized way of addressing five threat classes to network and that can be used to access, plan, manage, and maintain secure computers and communication networks is:

A. Nortells Unified Security Framework

B. The IBM Security Framework

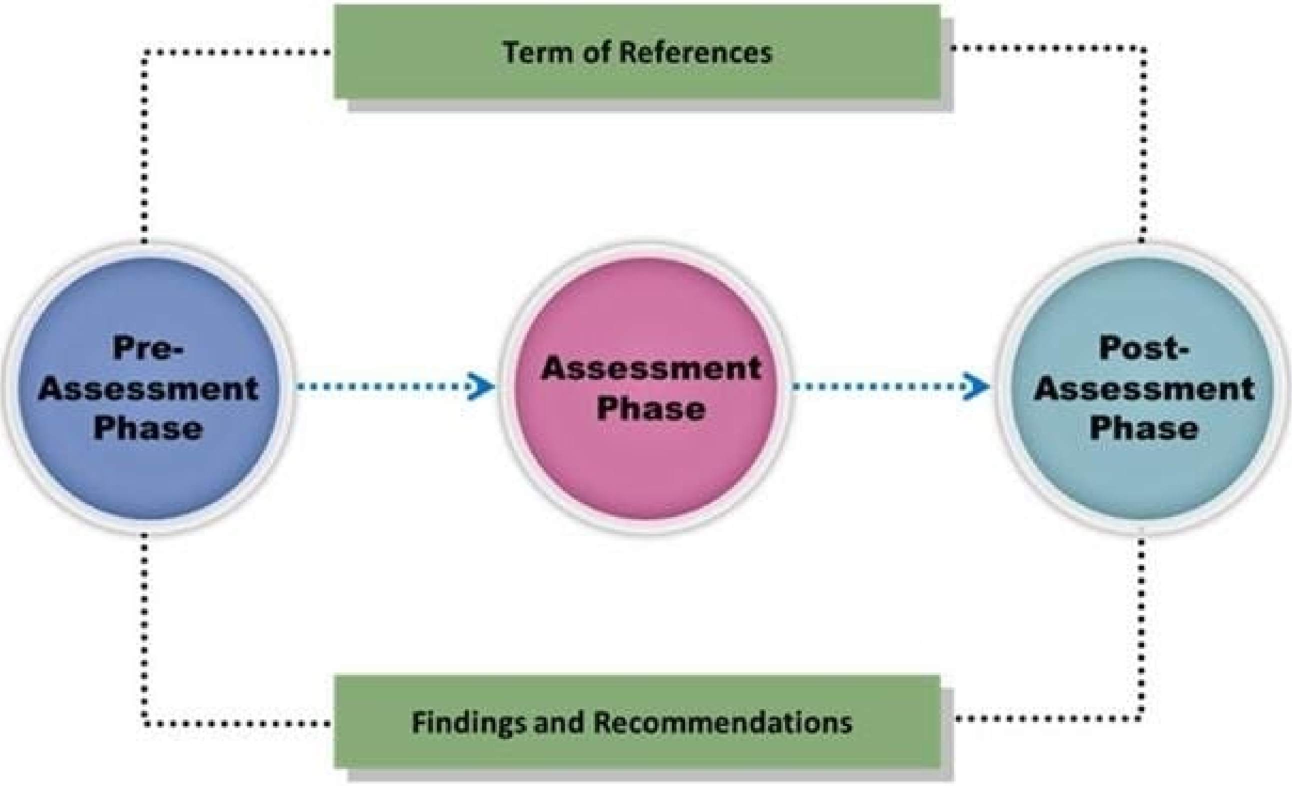
C. Bell Labs Network Security Framework

D. Microsoft Internet Security Framework

Correct Answer: C

QUESTION 3

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 4

What are placeholders (or markers) in an HTML document that the web server will dynamically replace with data just before sending the requested documents to a browser?

A. Server Side Includes

B. Sort Server Includes

C. Server Sort Includes

D. Slide Server Includes

Correct Answer: A

QUESTION 5

Which one of the following is a command line tool used for capturing data from the live network and copying those packets to a file?

A. Wireshark: Capinfos

B. Wireshark: Tcpdump

C. Wireshark: Text2pcap

D. Wireshark: Dumpcap

Correct Answer: D

QUESTION 6

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 7

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

Reference: http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

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

The first and foremost step for a penetration test is information gathering. The main objective of this test is to gather information about the target system which can be used in a malicious manner to gain access to the target systems.

Which of the following information gathering terminologies refers to gathering information through social engineering on-site visits, face-to-face interviews, and direct questionnaires?

A. Active Information Gathering

B. Pseudonymous Information Gathering

C. Anonymous Information Gathering

D. Open Source or Passive Information Gathering

Correct Answer: A

QUESTION 10

Network scanning is used to identify the available network resources. Which one of the following is also known as a half-open scan, because a full TCP connection is never completed and it is used to determine which ports are open and listening on a target device?

A. SYN Scan

B. TCP Connect Scan

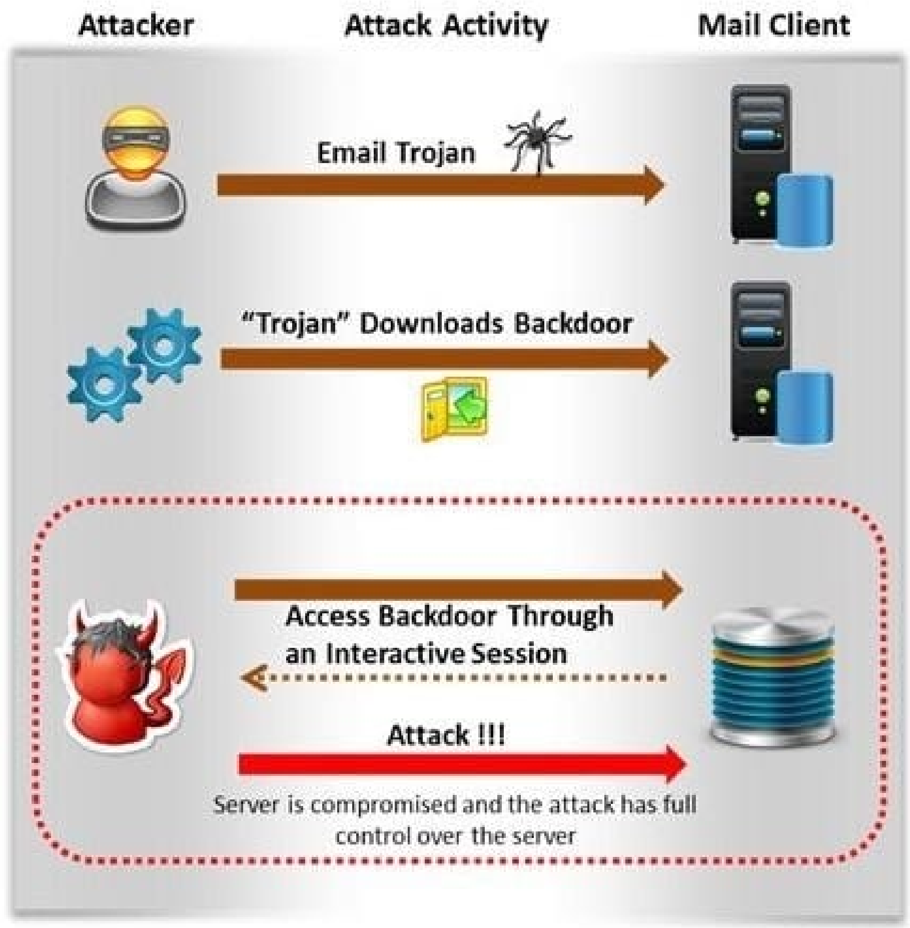
C. XMAS Scan

D. Null Scan

Correct Answer: A

QUESTION 11

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.


Attacker
Attack Activity
Mail Client
Email Trojan
"Trojan" Downloads Backdoor
Access Backdoor Through an Interactive Session
Attack !!!
Server is compromised and the attack has full control over the server

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

Correct Answer: D

QUESTION 12

To locate the firewall, SYN packet is crafted using Hping or any other packet crafter and sent to the firewall. If ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device is received, then it means which of the following type of firewall is in place?

A. Circuit level gateway

B. Stateful multilayer inspection firewall

C. Packet filter

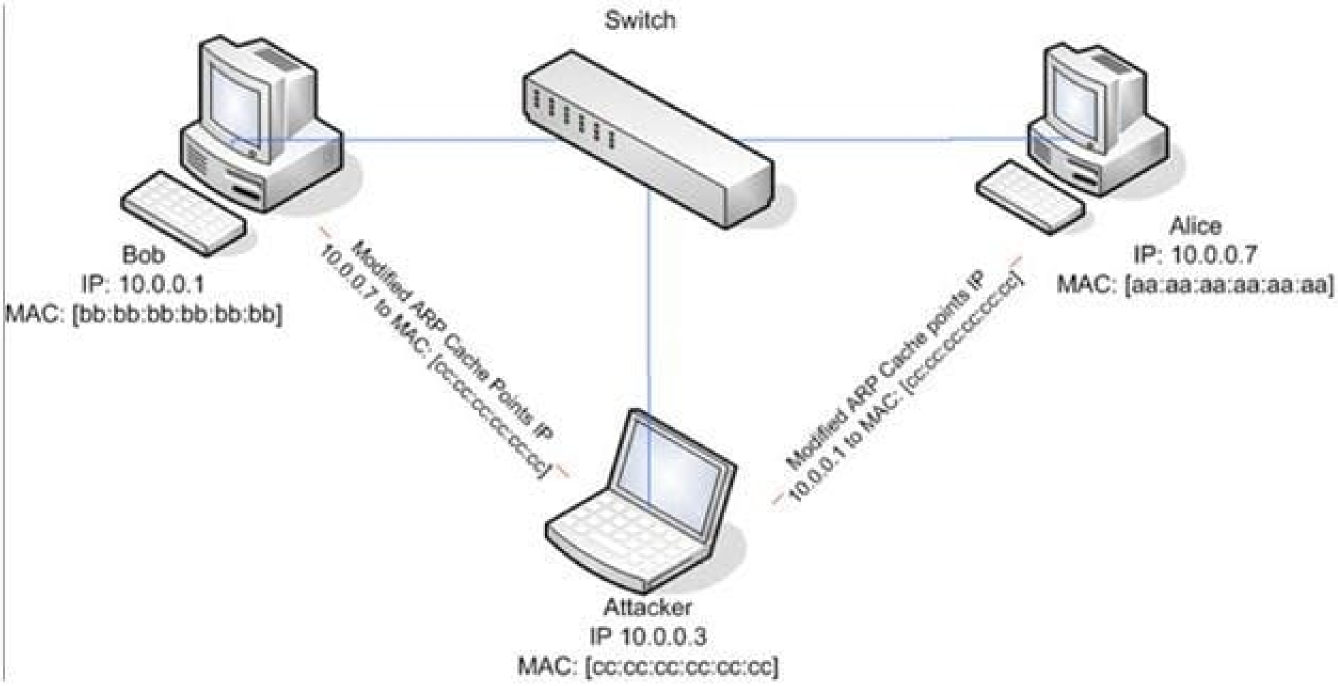
D. Application level gateway

Correct Answer: C

QUESTION 13

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker\\'s MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing attack is used as an opening for other attacks.


Switch
Bob
IP: 10.0.0.1
MAC: [bb:bb:bb:bb:bb:bb]
Alice
IP: 10.0.0.7
MAC: [aa:aa:aa:aa:aa:aa]
Modified ARP Cache Points IP 10.0.0.7 to MAC: [cc:cc:cc:cc:cc:cc]
Modified ARP Cache points IP 10.0.0.1 to MAC: [cc:cc:cc:cc:cc:cc]
Attacker
IP 10.0.0.3
MAC: [cc:cc:cc:cc:cc:cc]

What type of attack would you launch after successfully deploying ARP spoofing?

A. Parameter Filtering

B. Social Engineering

C. Input Validation

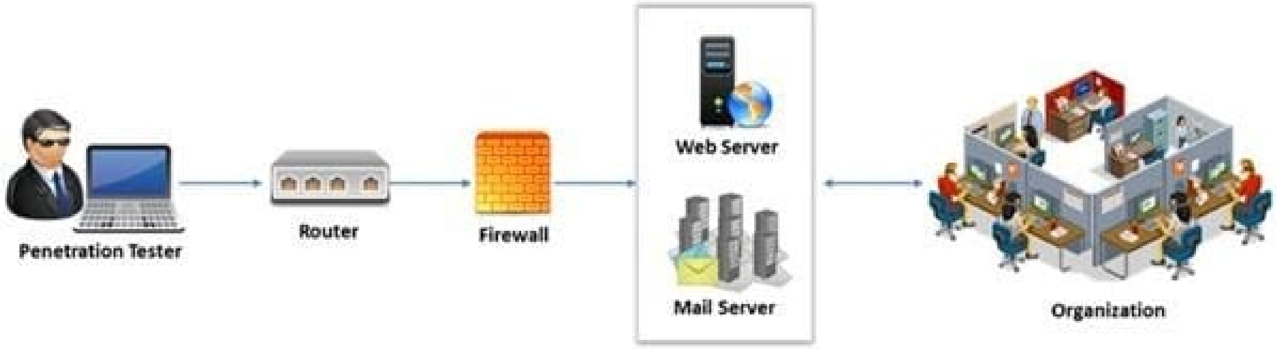
D. Session Hijacking

Correct Answer: D

Reference: http://en.wikipedia.org/wiki/ARP_spoofing

QUESTION 14

External penetration testing is a traditional approach to penetration testing and is more focused on the servers, infrastructure and the underlying software comprising the target. It involves a comprehensive analysis of publicly available information about the target, such as Web servers, Mail servers, Firewalls, and Routers.



Which of the following types of penetration testing is performed with no prior knowledge of the site?

A. Blue box testing

B. White box testing

C. Grey box testing

D. Black box testing

Correct Answer: D

Reference: http://books.google.com.pk/books?id=5m6ta2fgTswCandpg=SA5-PA4andlpg=SA5PA4anddq=penetration+testing+is+performed+with+no+prior+knowledge+of+the+siteandsourc e=blandots=8GkmyUBH2Uandsig=wdBIboWxrhk5QjlQXs3yWOcuk2Qandhl=enandsa=Xandei=SgfVI2LLc3qaOa5gIgOandved=0CCkQ6AEwAQ#v=onepageandq=penetration%20testing%20i s% 20performed%20with%20no%20prior%20knowledge%20of%20the%20siteandf=false

QUESTION 15

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

Correct Answer: D

Explanation: Refere\\' http://en.wikipedia.org/wiki/Glossary