Vendor:EC-COUNCIL

Exam Code:ECSAV10

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

Version: Demo

QUESTION 1

Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels. A vulnerability assessment is used to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

Which of the following vulnerability assessment technique is used to test the web server infrastructure for any misconfiguration and outdated content?

A. Passive Assessment

B. Host-based Assessment

C. External Assessment

D. Application Assessment

Correct Answer: D

QUESTION 2

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 3

Tom is a networking manager in XYZ Inc. He and his team were assigned the task to store and update the confidential files present on a remote server using Network File System (NFS) client-server application protocol. Since the files are confidential, Tom was asked to perform this operation in a secured manner by limiting the access only to his team. As per the instructions provided to him, to use NFS securely, he employed the process of limiting the superuser access privileges only to his team by using authentication based on the team personnel identity. Identify the method employed by Tom for securing access controls in NFS?

A. Root Squashing

B. nosuid

C. noexec

D. Suid

Correct Answer: B

QUESTION 4

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida; They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company\\'s main office in Iowa; She states that she needs the receptionist\\'s network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

A. Reciprocation

B. Friendship/Liking

C. Social Validation

D. Scarcity

Correct Answer: A

QUESTION 5

Security auditors determine the use of WAPs on their networks with Nessus vulnerability scanner which identifies the commonly used WAPs. One of the plug-ins that the Nessus Vulnerability Scanner uses is ID #11026 and is named "Access Point Detection". This plug-in uses four techniques to identify the presence of a WAP. Which one of the following techniques is mostly used for uploading new firmware images while upgrading the WAP device?

A. NMAP TCP/IP fingerprinting

B. HTTP fingerprinting

C. FTP fingerprinting

D. SNMP fingerprinting

Correct Answer: C

QUESTION 6

Nancy Jones is a network admin at Society Technology Ltd. When she is trying to send data packets from

one network (Token-ring) to another network (Ethernet), she receives an error message stating:

\\'Destination unreachable\\'

What is the reason behind this?

A. Packet is lost

B. Packet fragmentation is required

C. Packet contains image data

D. Packet transmission is not done properly

Correct Answer: D

QUESTION 7

SecInfo is a leading cyber security provider who recently hired Andrew, a security analyst. He was assigned the task of identifying vulnerabilities in the NFC devices by performing an attack on them. In this process, he was present with his device in the close proximity with the NFC devices that are sharing data so that he can eavesdrop on the data and at the same time block the transmission to the receiver. He then manipulated the captured data and further relayed the data to the receiver. Identify the type of attack performed by Andrew on the target NFC devices?

A. Ticket cloning

B. MITM attack

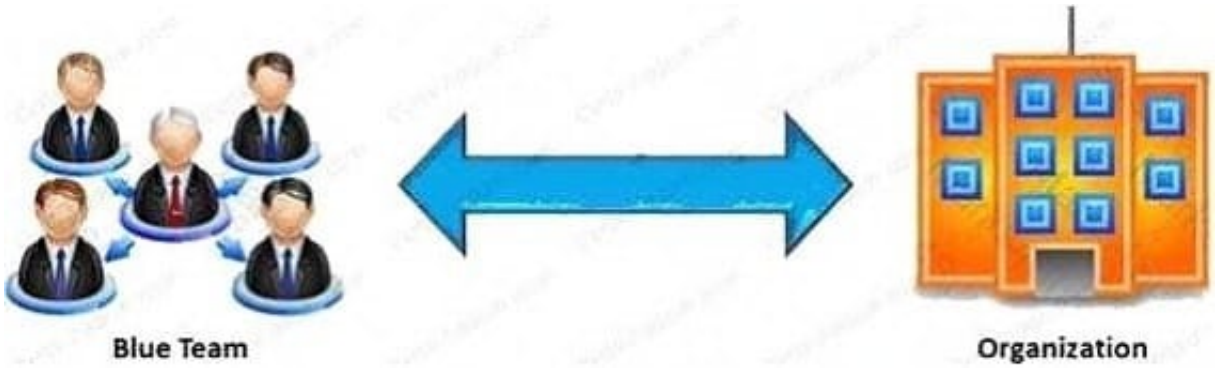
C. DoS attack

D. Virus attack

Correct Answer: B

QUESTION 8

In the context of penetration testing, what does blue teaming mean?



A. A penetration test performed with the knowledge and consent of the organization\\'s IT staff

B. It is the most expensive and most widely used

C. It may be conducted with or without warning

D. A penetration test performed without the knowledge of the organization\\'s IT staff but with permission from upper management

Correct Answer: A

QUESTION 9

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 10

Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

A. OSPF

B. BPG

C. ATM

D. UDP

Correct Answer: A

QUESTION 11

Which of the following information security acts enables to ease the transfer of financial information between institutions and banks while making the rights of the individual through security requirements more specific?

A. The Digital Millennium Copyright Act (DMCA)

B. Sarbanes Oxley Act (SOX)

C. Computer Misuse Act 1990

D. Gramm-Leach-Bliley Act (GLBA)

Correct Answer: D

QUESTION 12

You have just completed a database security audit and writing the draft pen testing report.

Which of the following will you include in the recommendation section to enhance the security of the

database server?

A. Allow direct catalog updates

B. Install SQL Server on a domain controller

C. Install a certificate to enable SSL connections

D. Grant permissions to the public database role

Correct Answer: C