DUMPSQUEEN

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

ECCouncil ECSAv10

Version Demo

Total Demo Questions: 10

Total Premium Questions: 150

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

An attacker targeted to attack network switches of an organization to steal confidential information such as network subscriber information, passwords, etc. He started transmitting data through one switch to another by creating and sending two 802.1Q tags, one for the attacking switch and the other for victim switch. By sending these frames. The attacker is fooling the victim switch into thinking that the frame is intended for it. The target switch then forwards the frame to the victim port.

Identify the type of attack being performed by the attacker?

A. SNMP brute forcing

B. MAC flooding

C. IP spoofing

D. VLAN hopping

ANSWER: D

QUESTION NO: 2

Jack, a network engineer, is working on an IPv6 implementation for one of his clients. He deployed IPv6 on IPv4 networks using a mechanism where a node can choose from IPv6 or IPv4 based on the DNS value. This makes the network resources work simpler. What kind of technique did Jack use?

A. Dual stacks

B. Filtering

C. Translation

D. Tunneling

ANSWER: A

QUESTION NO: 3

Allen and Greg, after investing in their startup company called Zamtac Ltd., developed a new web application for their company. Before hosting the application, they want to test the robustness and immunity of the developed web application against attacks like buffer overflow, DOS, XSS, and SQL injection.

What is the type of the web application security test Allen and Greg should perform?

A. Web fuzzing

B. Web crawling

C. Web spidering

D. Web mirroring

ANSWER: A

QUESTION NO: 4

Peter works as a lead penetration tester in a security service firm named Xsecurity. Recently, Peter was assigned a white-box pen test assignment testing the security of an IDS system deployed by a client. During the preliminary information gathering, Peter discovered the TTL to reach the IDS system from his end is 30. Peter created a Trojan and fragmented it in to 1-character packets using the Colasoft packet builder tool. He then used a packet flooding utility to bombard the IDS with these fragmented packets with the destination address of a target host behind the IDS whose TTL is 35. What is Peter trying to achieve?

A. Peter is trying to bypass the IDS system using a Trojan

B. Peter is trying to bypass the IDS system using the broadcast address

C. Peter is trying to bypass the IDS system using the insertion attack

D. Peter is trying to bypass the IDS system using inconsistent packets

ANSWER: D

QUESTION NO: 5

AB Cloud services provide virtual platform services for the users in addition to storage. The company offers users with APIs, core connectivity and delivery, abstraction and hardware as part of the service. What is the name of the service AB Cloud services offer?

A. Web Application Services

B. Platform as a service (PaaS)

C. Infrastructure as a service (IaaS)

D. Software as a service (SaaS)

ANSWER: C

QUESTION NO: 6

Adam is an IT administrator for Syncan Ltd. He is designated to perform various IT tasks like setting up new user accounts, managing backup/restores, security authentications and passwords, etc. Whilst performing his tasks, he was asked to employ the latest and most secure authentication protocol to encrypt the passwords of users that are stored in the Microsoft Windows OS-based systems.

Which of the following authentication protocols should Adam employ in order to achieve the objective?

A. LANMAN

B. Kerberos

C. NTLM

D. NTLMv2

ANSWER: C

QUESTION NO: 7

Sandra, a wireless network auditor, discovered her client is using WEP. To prove the point that the WEP encryption is very weak, she wants to decrypt some WEP packets. She successfully captured the WEP data packets, but could not reach the content as the data is encrypted. Which of the following will help Sandra decrypt the data packets without knowing the key?

A. Fragmentation Attack

B. Chopchop Attack

C. ARP Poisoning Attack

D. Packet injection Attack

ANSWER: B

QUESTION NO: 8

Charles, a network penetration tester, is part of a team assessing the security of perimeter devices of an organization. He is using the following Nmap command to bypass the firewall:

nmap -D 10.10.8.5, 192.168.168.9, 10.10.10.12 What Charles is trying to do?

A. Packet Fragmentation

B. Cloaking a scan with decoys

C. Spoofing source address

D. Spoofing source port number

ANSWER: C

QUESTION NO: 9

Which of the following pre-engagement documents identifies the systems to be tested, types of tests, and the depth of the testing?

A. Draft Report

B. Letter of Intent

C. Rule of Engagement

D. Authorization Letter

ANSWER: C

QUESTION NO: 10

Fred, who owns a company called Skyfeit Ltd., wants to test the enterprise network for presence of any vulnerabilities and loopholes. He employed a third-party penetration testing team and asked them to perform the penetration testing over his organizational infrastructure. Fred briefed the team about his network infrastructure and provided them with a set of IP addresses on which they can perform tests. He gave them strict instruction not to perform DDoS attacks or access the domain servers in the company. He also instructed them that they can carry out the penetration tests even when the regular employees are on duty since they lack the clue about the happenings. However, he asked the team to take care that no interruption in business continuity should be caused. He also informed the penetration testing team that they get only 1 month to carry out the test and submit the report.

What kind of penetration test did Fred ask the third-party penetration testing team to perform?

A. Announced testing

B. Blind testing

C. Grey-Box testing

D. Unannounced testing

ANSWER: D