412-79V8 Q&As

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL 412-79V8 Exam with 100% Guarantee

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

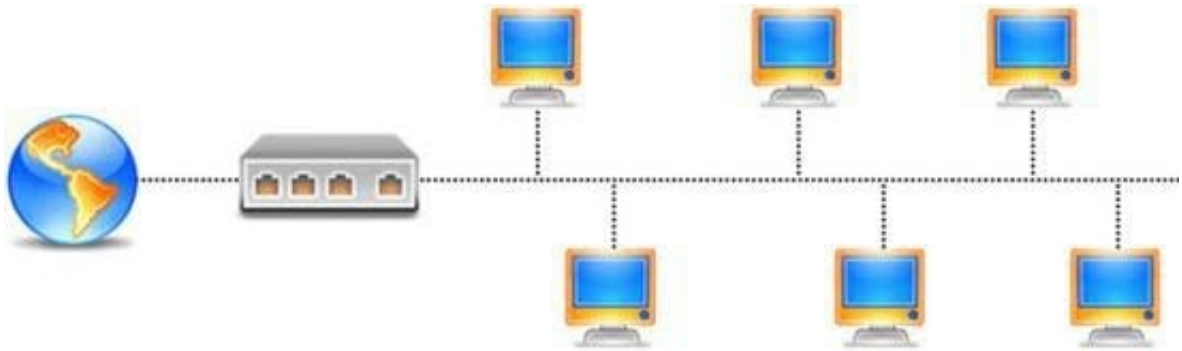
https://www.pass4itsure.com/412-79v8.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Port numbers are used to keep track of different conversations crossing the network at the same time. Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers have the assigned ranges.



Port numbers above 1024 are considered which one of the following?

A. Dynamically assigned port numbers

B. Statically assigned port numbers

C. Well-known port numbers

D. Unregistered port numbers

Correct Answer: A

QUESTION 2

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

QUESTION 3

John, a penetration tester, was asked for a document that defines the project, specifies goals, objectives, deadlines, the resources required, and the approach of the project. Which of the following includes all of these requirements?

A. Penetration testing project plan

B. Penetration testing software project management plan

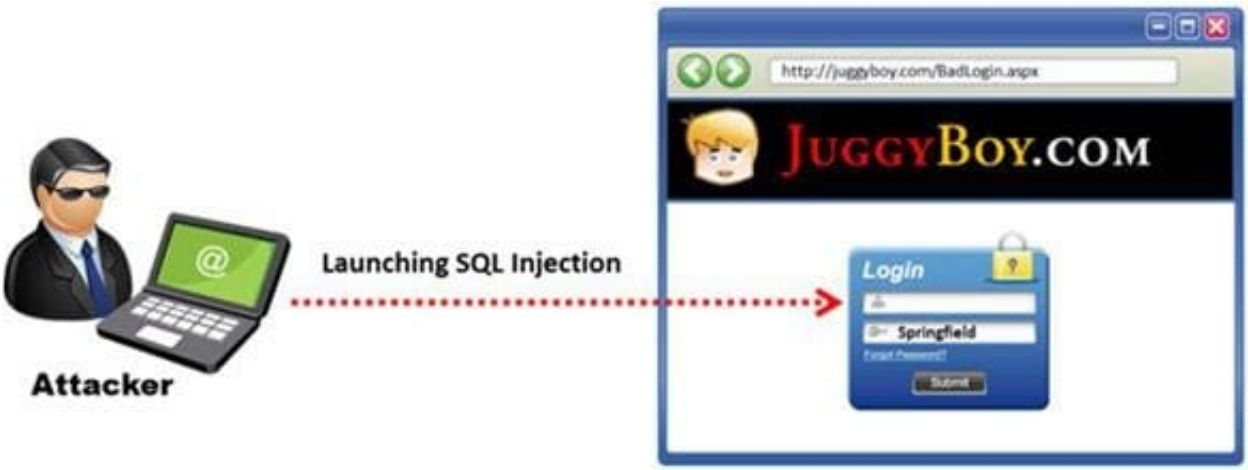
C. Penetration testing project scope report

D. Penetration testing schedule plan

Correct Answer: A

QUESTION 4

SQL injection attacks are becoming significantly more popular amongst hackers and there has been an estimated 69 percent increase of this attack type. This exploit is used to great effect by the hacking community since it is the primary way to steal sensitive data from web applications. It takes advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a back-end database. The below diagram shows how attackers launched SQL injection attacks on web applications.



Which of the following can the attacker use to launch an SQL injection attack?

A. Blah\\' "2=2 "

B. Blah\\' and 2=2 -

C. Blah\\' and 1=1 -

D. Blah\\' or 1=1 -

Correct Answer: D

QUESTION 5

A Demilitarized Zone (DMZ) is a computer host or small network inserted as a "neutral zone" between a company\\'s private network and the outside public network. Usage of a protocol within a DMZ environment is highly variable based on the specific needs of an organization. Privilege escalation, system is compromised when the code runs under root credentials, and DoS attacks are the basic weakness of which one of the following Protocol?

A. Lightweight Directory Access Protocol (LDAP)

B. Simple Network Management Protocol (SNMP)

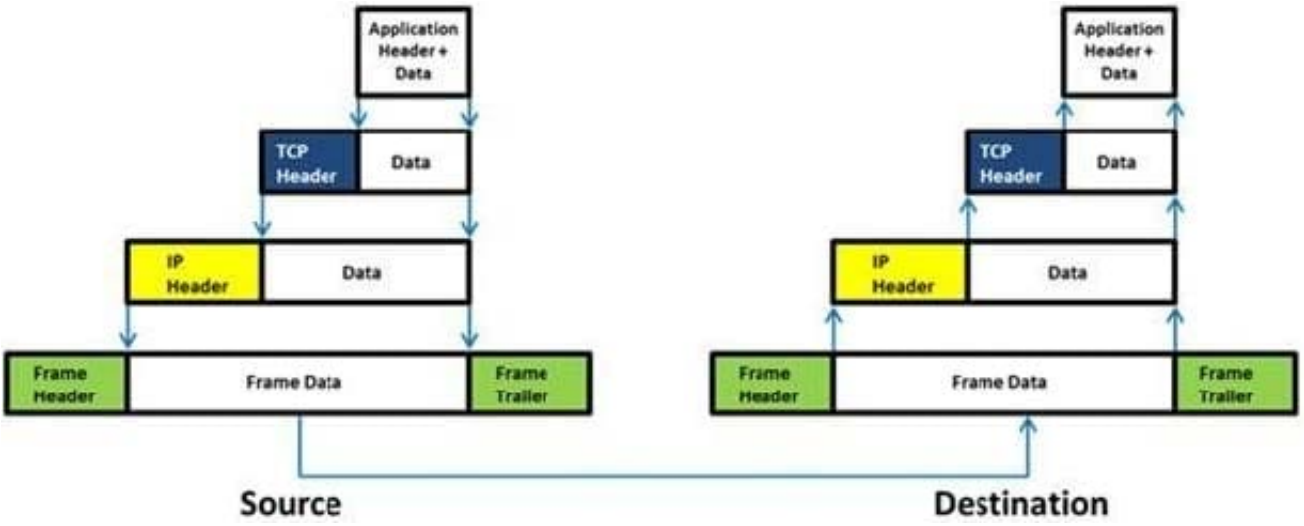
C. Telnet

D. Secure Shell (SSH)

Correct Answer: D

QUESTION 6

Which of the following statement holds true for TCP Operation?



A. Port numbers are used to know which application the receiving host should pass the data to

B. Sequence numbers are used to track the number of packets lost in transmission

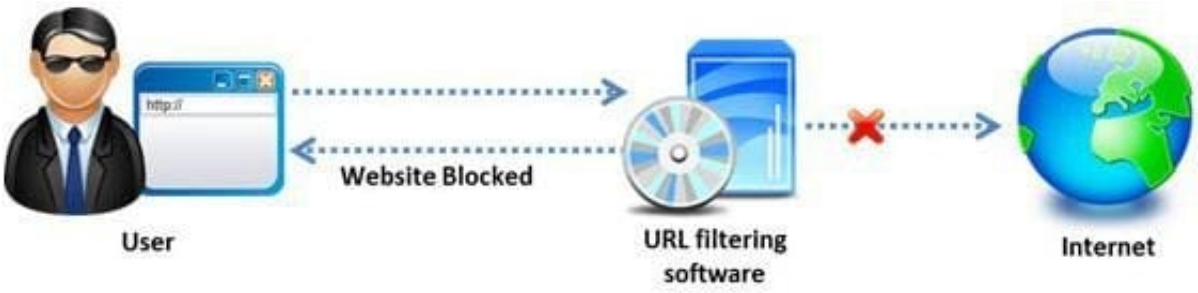
C. Flow control shows the trend of a transmitting host overflowing the buffers in the receiving host

D. Data transfer begins even before the connection is established

Correct Answer: C

QUESTION 7

Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing. Management decide to block all such web sites using URL filtering software.



How can employees continue to see the blocked websites?

A. Using session hijacking

B. Using proxy servers

C. Using authentication

D. Using encryption

Correct Answer: B

QUESTION 8

What information can be collected by dumpster diving?

A. Sensitive documents

B. Email messages

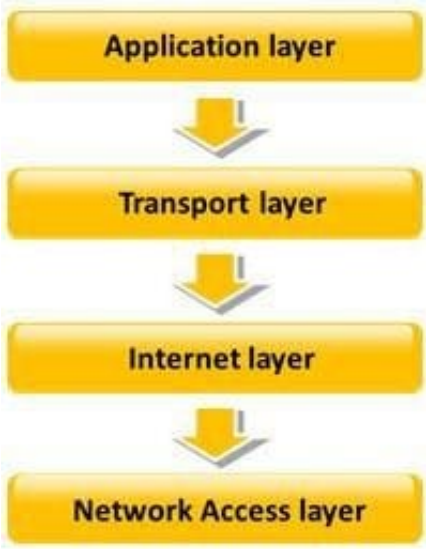
C. Customer contact information

D. All the above

Correct Answer: A

QUESTION 9

TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network. It provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.



Which of the following TCP/IP layers selects the best path through the network for packets to travel?

A. Transport layer

B. Network Access layer

C. Internet layer

D. Application layer

Correct Answer: B

QUESTION 10

Which of the following is the objective of Gramm-Leach-Bliley Act?

A. To ease the transfer of financial information between institutions and banks

B. To protect the confidentiality, integrity, and availability of data

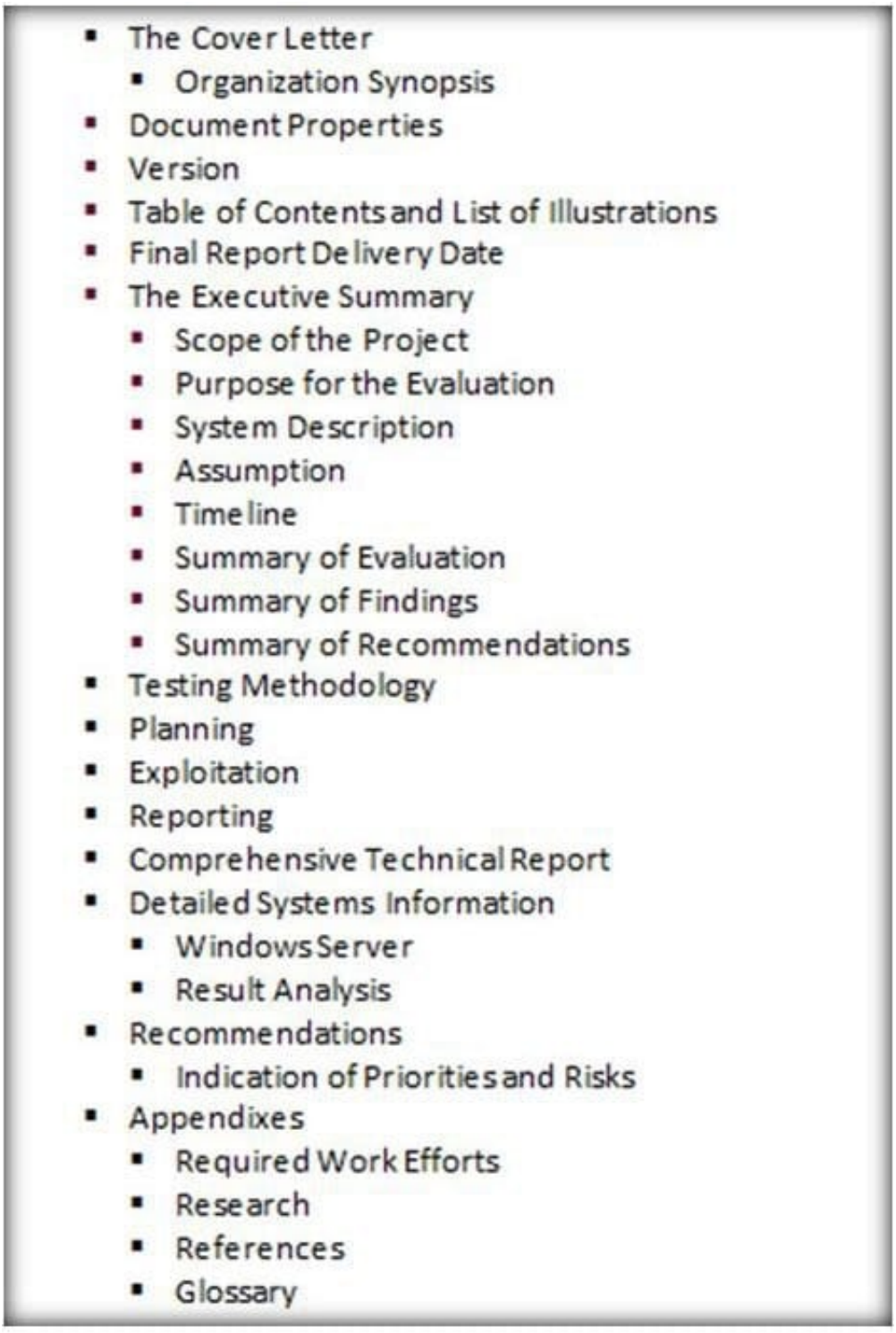
C. To set a new or enhanced standards for all U.S. public company boards, management and public accounting firms

D. To certify the accuracy of the reported financial statement

Correct Answer: B

QUESTION 11

What is a goal of the penetration testing report?



A. The penetration testing report helps you comply with local laws and regulations related to environmental conditions in the organization.

B. The penetration testing report allows you to sleep better at night thinking your organization is protected

C. The pen testing report helps executive management to make decisions on implementing security controls in the organization and helps the security team implement security controls and patch any flaws discovered during testing.

D. The penetration testing report allows you to increase sales performance by effectively communicating with the

internal security team.

Correct Answer: C

QUESTION 12

Which type of vulnerability assessment tool provides security to the IT system by testing for vulnerabilities in the applications and operation system?

A. Active/Passive Tools

B. Application-layer Vulnerability Assessment Tools

C. Location/Data Examined Tools

D. Scope Assessment Tools

Correct Answer: D

QUESTION 13

During external penetration testing, which of the following techniques uses tools like Nmap to predict the sequence numbers generated by the targeted server and use this information to perform session hijacking techniques?

A. TCP Sequence Number Prediction

B. IPID State Number Prediction

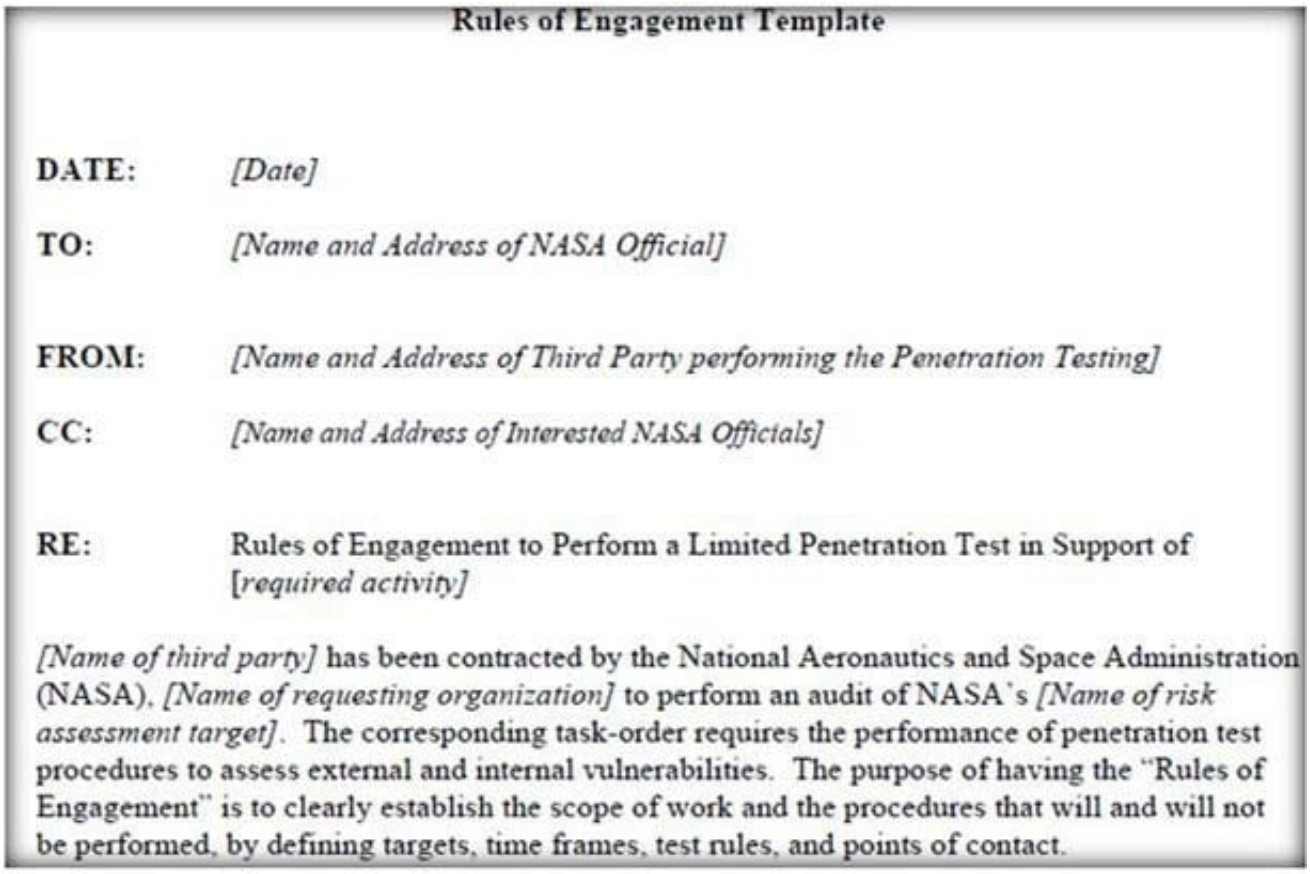
C. TCP State Number Prediction

D. IPID Sequence Number Prediction

Correct Answer: A

QUESTION 14

Rules of Engagement (ROE) document provides certain rights and restriction to the test team for performing the test and helps testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.



Rules of Engagement Template

DATE: *[Date]*

TO: *[Name and Address of NASA Official]*

FROM: *[Name and Address of Third Party performing the Penetration Testing]*

CC: *[Name and Address of Interested NASA Officials]*

RE: Rules of Engagement to Perform a Limited Penetration Test in Support of *[required activity]*

[Name of third party] has been contracted by the National Aeronautics and Space Administration (NASA), *[Name of requesting organization]* to perform an audit of NASA's *[Name of risk assessment target]*. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

What is the last step in preparing a Rules of Engagement (ROE) document?

A. Conduct a brainstorming session with top management and technical teams

B. Decide the desired depth for penetration testing

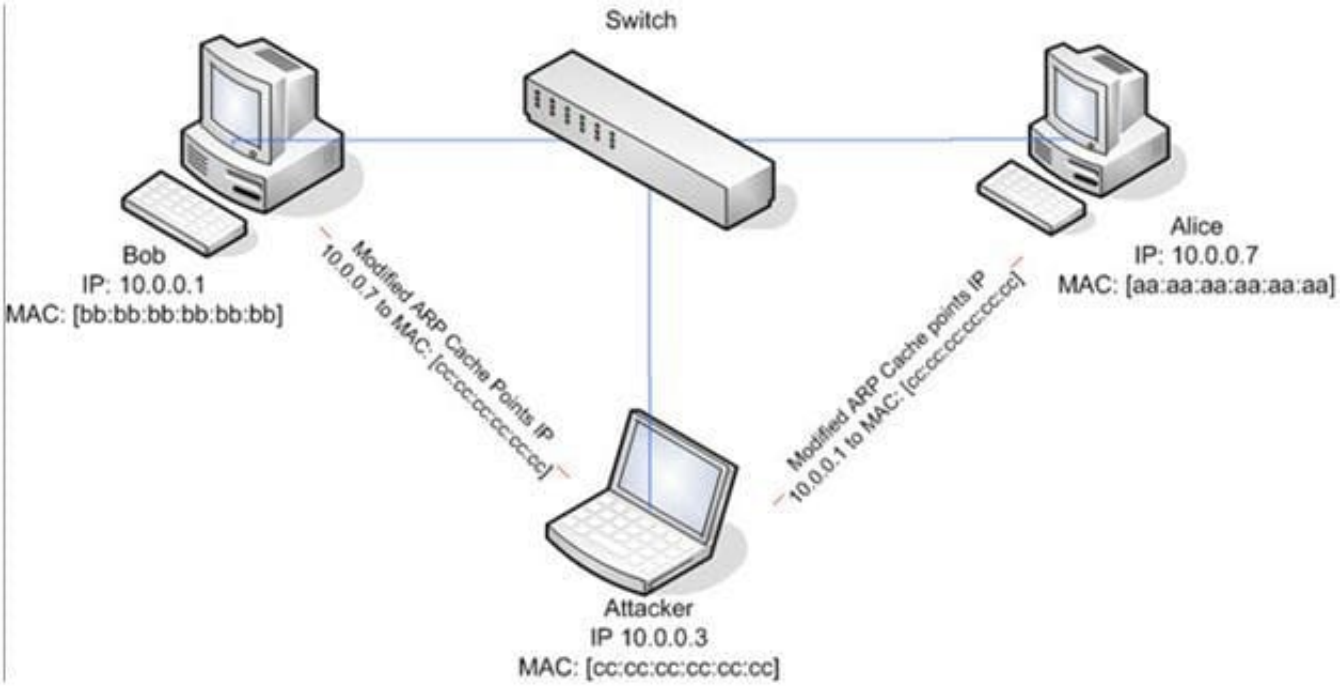
C. Conduct a brainstorming session with top management and technical teams

D. Have pre-contract discussions with different pen-testers

Correct Answer: B

QUESTION 15

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.



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