ECSAV8 Q&As

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL ECSAV8 Exam with 100% Guarantee

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

https://www.pass4itsure.com/ecsav8.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

John, the penetration testing manager in a pen testing firm, needs to prepare a pen testing pricing report

for a client.

Which of the following factors does he need to consider while preparing the pen testing pricing report?

A. Number of employees in the client organization

B. Complete structure of the organization

C. Number of client computers to be tested and resources required to perform a pen test

D. Number of servers available in the client organization

Correct Answer: B

QUESTION 2

Which of the following statements is true about the LM hash?

A. Disabled in Windows Vista and 7 OSs

B. Separated into two 8-character strings

C. Letters are converted to the lowercase

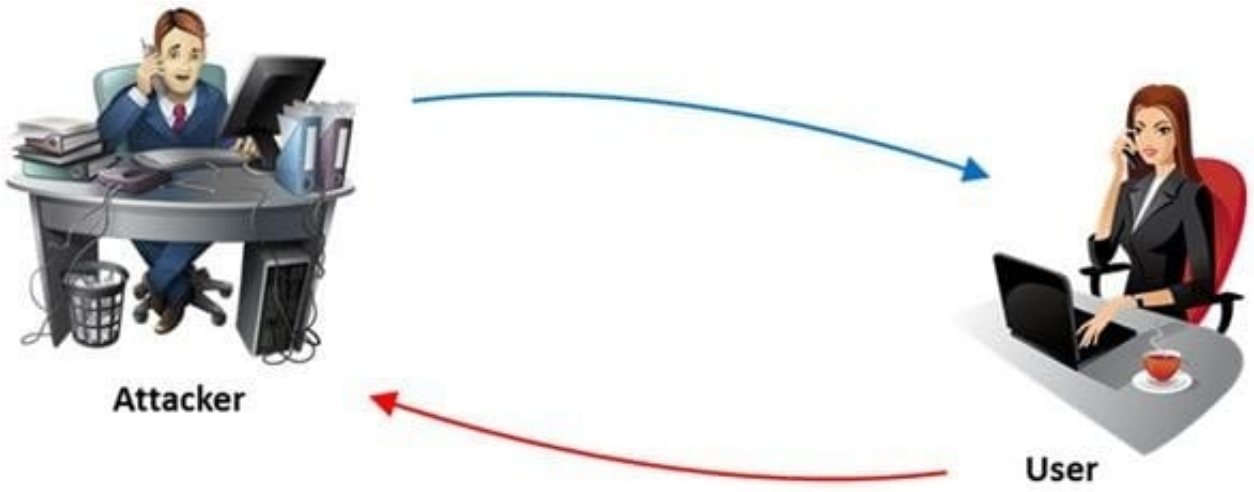
D. Padded with NULL to 16 characters

Correct Answer: A

Reference: http://www.onlinehashcrack.com/how_to_crack_windows_passwords.php (first paragraph of the page)

QUESTION 3

The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?

A. Phishing

B. Spoofing

C. Tapping

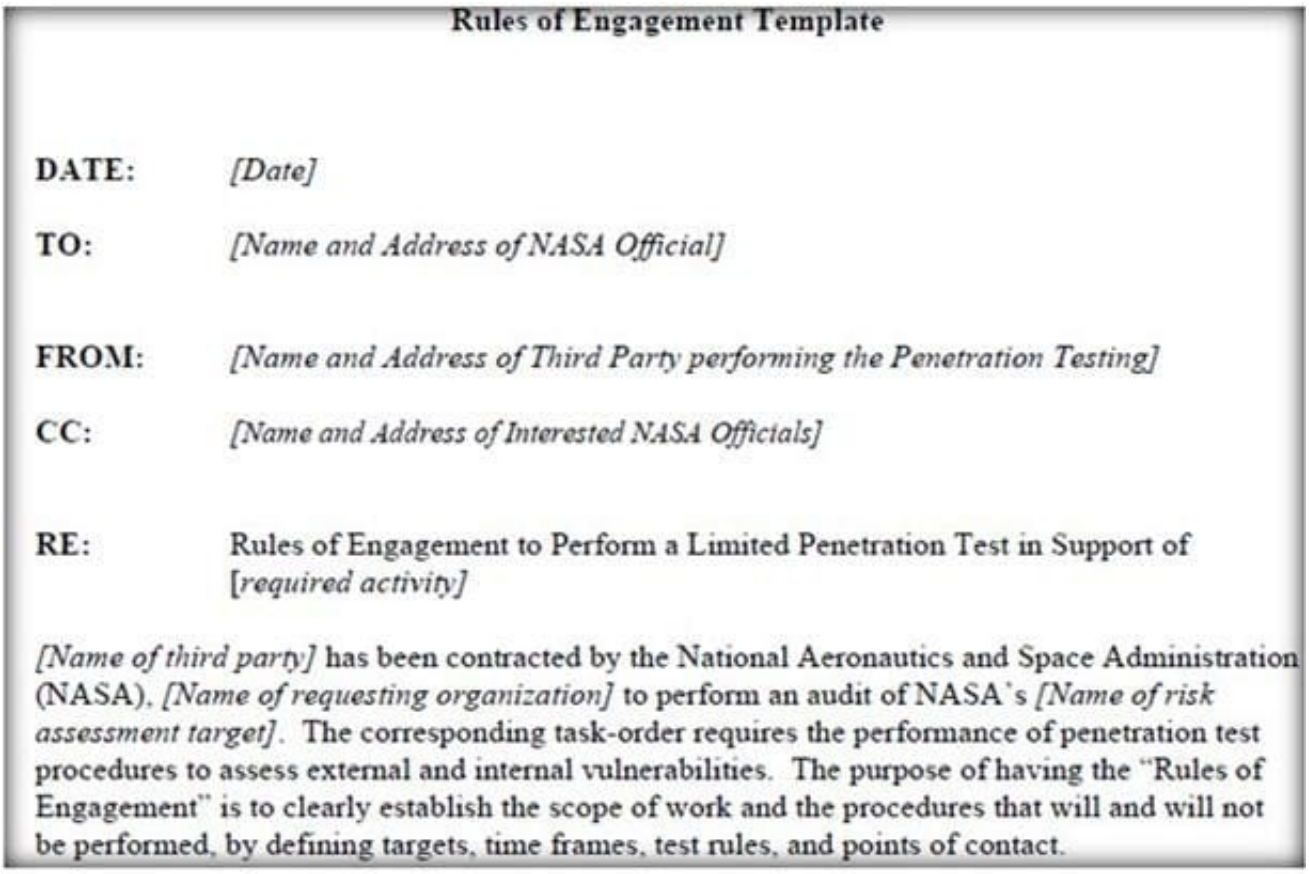
D. Vishing

Correct Answer: A

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

QUESTION 4

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 5

Which among the following information is not furnished by the Rules of Engagement (ROE) document?

A. Techniques for data collection from systems upon termination of the test

B. Techniques for data exclusion from systems upon termination of the test

C. Details on how data should be transmitted during and after the test

D. Details on how organizational data is treated throughout and after the test

Correct Answer: D

QUESTION 6

Which of the following policy forbids everything with strict restrictions on all usage of the company systems and network?

A. Information-Protection Policy

B. Paranoid Policy

C. Promiscuous Policy

D. Prudent Policy

Correct Answer: B

QUESTION 7

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 8

Due to illegal inputs, various types of TCP stacks respond in a different manner. Some IDSs do not take into account the TCP protocol\\'s urgency feature, which could allow testers to evade the IDS.

Penetration tester needs to try different combinations of TCP flags (e.g. none, SYN/FIN, SYN/RST, SYN/ FIN/ACK, SYN/RST/ACK, and All Flags) to test the IDS.

Which of the following TCP flag combinations combines the problem of initiation, midstream, and termination flags with the PSH and URG?

A. SYN/RST/ACK

B. SYN/FIN/ACK

C. SYN/FIN

D. All Flags

Correct Answer: D

Reference:

http://books.google.com.pk/books?id=tUCumJot0ocCandpg=PA63andlpg=PA63anddq=TCP+flag +combinations

+combines+the+problem+of+initiation,+midstream,+and+termination+flags+ with+the+PSH+and

+URGandsource=blandots=mIGSXBIi15andsig=WMnXlEChVSU4RhK65W_V

3tzNjnsandhl=enandsa=Xandei=H7AfVJCtLaufygO1v4DQDgandved=0CBsQ6AEwAA#v=onepageand q=TCP%

20flag%20combinations%20combines%20the%20problem%20of%20initiation%2 C%20midstream%2C%

20and%20termination%20flags%20with%20the%20PSH%20and% 20URGandf=false (see the highlighted

sentence in Table 3-1 at the end of the page)

QUESTION 9

HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using %xx notation, where \\'xx\\' is the

A. ASCII value of the character

B. Binary value of the character

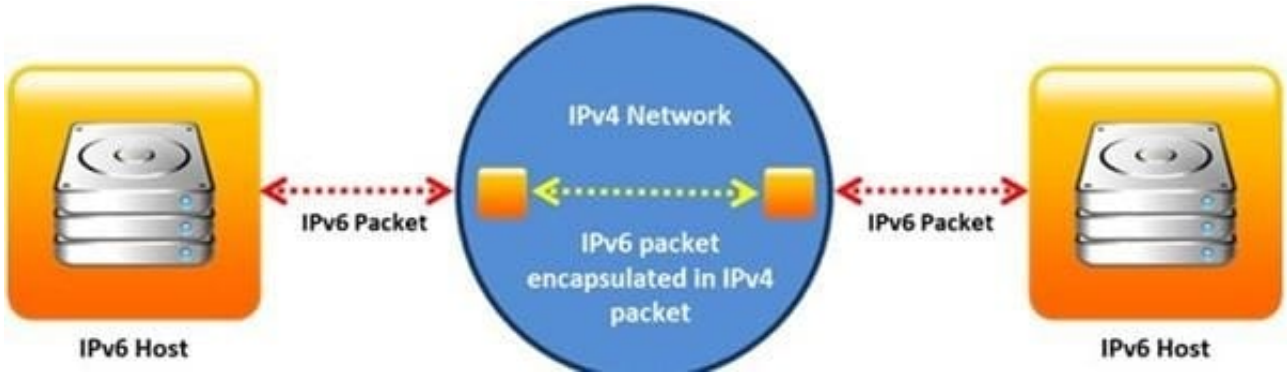
C. Decimal value of the character

D. Hex value of the character

Correct Answer: C

QUESTION 10

Identify the transition mechanism to deploy IPv6 on the IPv4 network from the following diagram.



A. Translation

B. Tunneling

C. Dual Stacks

D. Encapsulation

Correct Answer: D

QUESTION 11

Before performing the penetration testing, there will be a pre-contract discussion with different pen-testers (the team of penetration testers) to gather a quotation to perform pen testing.

Which of the following factors is NOT considered while preparing a price quote to perform pen testing?

A. Total number of employees in the client organization

B. Type of testers involved

C. The budget required

D. Expected time required to finish the project

Correct Answer: A

QUESTION 12

A man enters a PIN number at an ATM machine, being unaware that the person next to him was watching. Which of the following social engineering techniques refers to this type of information theft?

A. Shoulder surfing

B. Phishing

C. Insider Accomplice

D. Vishing

Correct Answer: A

QUESTION 13

Which of the following policies helps secure data and protects the privacy of organizational information?

A. Special-Access Policy

B. Document retention Policy

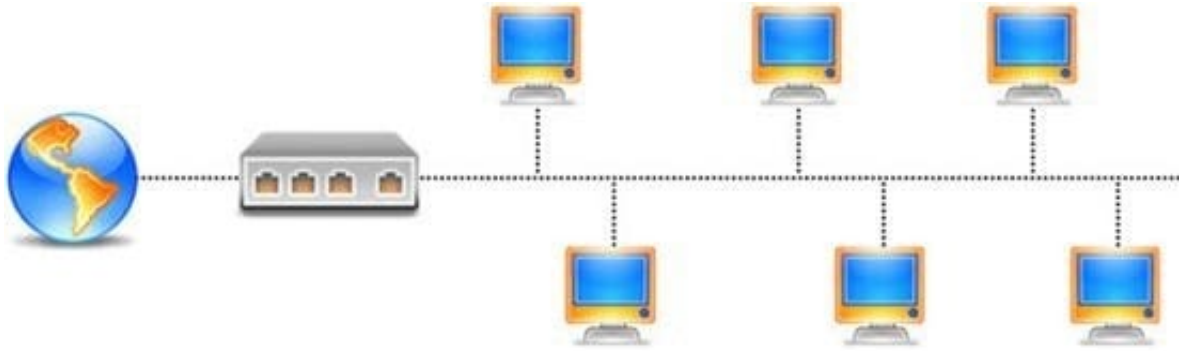
C. Cryptography Policy

D. Personal Security Policy

Correct Answer: C

QUESTION 14

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: C

Reference: http://stackoverflow.com/questions/136709/what-port-number-should-i-use- when-testingconnections-in-my-local-intranet-in (see post 4)

QUESTION 15

Which of the following policies states that the relevant application owner must authorize requests for additional access to specific business applications in writing to the IT Department/resource?

A. Special-Access Policy

B. User Identification and Password Policy

C. Personal Computer Acceptable Use Policy

D. User-Account Policy

Correct Answer: B