ECSAV10$^{Q\&As}$

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

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

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

https://www.geekcert.com/ecsav10.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

While auditing a web application for vulnerabilities, Donald uses Burp proxy and modifies the get requests

as below:

http://www.example.com/GET/process.php./../../../../../../../../etc/password

What is Donald trying to achieve?

A. Donald is modifying process.php file to extract /etc/password file

B. Donald is trying directory traversal to extract /etc/password file

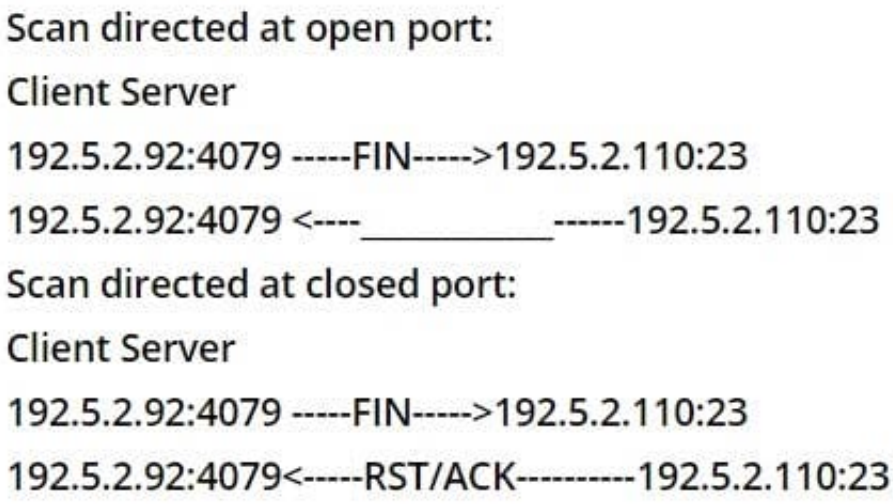
C. Donald is trying SQL injection to extract the contents of /etc/password file

D. Donald is trying to upload /etc/password file to the web server root folder

Correct Answer: B

QUESTION 2

As a part of the pen testing process, James performs a FIN scan as given below:



What will be the response if the port is open?

A. No response

B. FIN/RST

C. FIN/ACK

D. RST

Correct Answer: A

QUESTION 3

Which of the following is not the SQL injection attack character?

A. $

B. PRINT

C. #

D. @@variable

Correct Answer: A

QUESTION 4

You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Metamorphic

B. Oligomorhic

C. Polymorphic

D. Transmorphic

Correct Answer: A

QUESTION 5

You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. intitle:"exchange server"

B. outlook:"search"

C. locate:"logon page"

D. allinurl:"exchange/logon.asp"

Correct Answer: D