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

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

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: C

QUESTION 2

Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

A. Client-Side Test Report

B. Activity Report

C. Host Report

D. Vulnerability Report

Correct Answer: A

QUESTION 3

One needs to run "Scan Server Configuration" tool to allow a remote connection to Nessus from the remote Nessus clients. This tool allows the port and bound interface of the Nessus daemon to be configured. By default, the Nessus

daemon listens to connections on which one of the following?

A. Localhost (127.0.0.1) and port 1241

B. Localhost (127.0.0.1) and port 1240

C. Localhost (127.0.0.1) and port 1246

D. Localhost (127.0.0.0) and port 1243

Correct Answer: A

QUESTION 4

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

Correct Answer: A

QUESTION 5

Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructors, encryption used, and web page behaviors?

A. Check for Directory Consistency and Page Naming Syntax of the Web Pages

B. Examine Server Side Includes (SSI)

C. Examine Hidden Fields

D. Examine E-commerce and Payment Gateways Handled by the Web Server

Correct Answer: C

Latest ECSAV10 Dumps   ECSAV10 Practice Test   ECSAV10 Exam Questions