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.leads4pass.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

Which type of penetration testing will require you to send the Internal Control Questionnaires (ICQ) to the client?

A. White-box testing

B. Black-box testing

C. Blind testing

D. Unannounced testing

Correct Answer: A

QUESTION 2

Identify the framework that comprises of five levels to guide agency assessment of their security programs and assist in prioritizing efforts for improvement:

A. Information System Security Assessment Framework (ISSAF)

B. Microsoft Internet Security Framework

C. Nortells Unified Security Framework

D. Federal Information Technology Security Assessment Framework

Correct Answer: D

QUESTION 3

Watson works as a Penetrating test engineer at Neo security services. The company found its wireless network operating in an unusual manner, with signs that a possible cyber attack might have happened. Watson was asked to resolve this problem. Watson starts a wireless penetrating test, with the first step of

discovering wireless networks by war-driving. After several thorough checks, he identifies that there is

some problem with rogue access points and resolves it. Identifying rogue access points involves a series

of steps.

Which of the following arguments is NOT valid when identifying the rogue access points?

A. If a radio media type used by any discovered AP is not present in the authorized list of media types, it is considered as a rogue AP

B. If any new AP which is not present in the authorized list of APs is detected, it would be considered as a rogue AP

C. If the radio channel used by any discovered AP is not present in the authorized list of channels, it is considered as a rogue AP

D. If the MAC of any discovered AP is present in the authorized list of MAC addresses, it would be considered as a rogue AP

Correct Answer: D

QUESTION 4

Which one of the following architectures has the drawback of internally considering the hosted services individually?

A. Weak Screened Subnet Architecture

B. "Inside Versus Outside" Architecture

C. "Three-Homed Firewall" DMZ Architecture

D. Strong Screened-Subnet Architecture

Correct Answer: C

QUESTION 5

DMZ is a network designed to give the public access to the specific internal resources and you might want to do the same thing for guests visiting organizations without compromising the integrity of the internal resources. In general, attacks on the wireless networks fall into four basic categories. Identify the attacks that fall under Passive attacks category.

A. Wardriving

B. Spoofing

C. Sniffing

D. Network Hijacking

Correct Answer: A