ECSAV10Q&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:

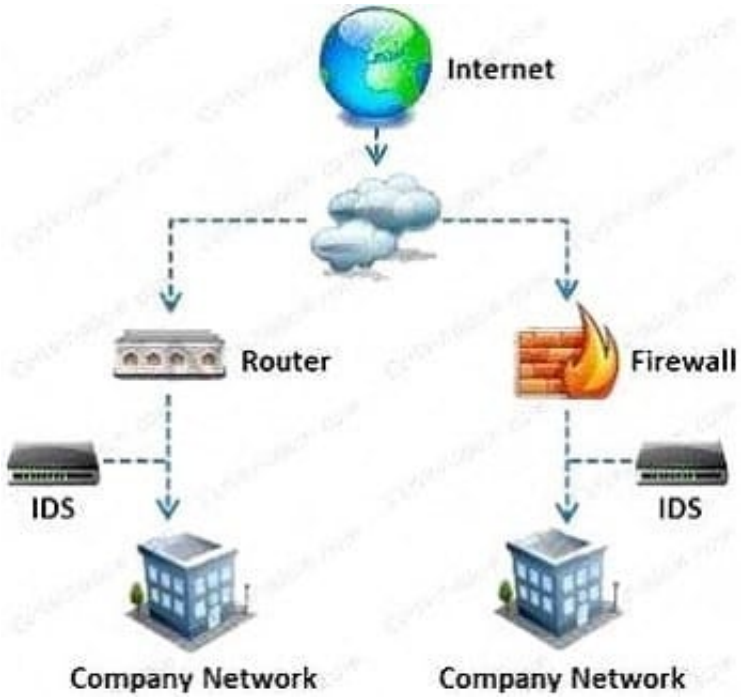
https://www.pass4itsure.com/ecsav10.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What is a difference between host-based intrusion detection systems (HIDS) and network-based intrusion detection systems (NIDS)?



A. NIDS are usually a more expensive solution to implement compared to HIDS.

B. Attempts to install Trojans or backdoors cannot be monitored by a HIDS whereas NIDS can monitor and stop such intrusion events.

C. NIDS are standalone hardware appliances that include network intrusion detection capabilities whereas HIDS consist of software agents installed on individual computers within the system.

D. HIDS requires less administration and training compared to NIDS.

Correct Answer: C

QUESTION 2

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 3

During a DHCP handshake in an IPv4 network, which of the following messages contains the actual IP addressing information for the clients to use?

A. DHCPDISCOVER

B. DHCPACK

C. REPLY

D. SOLICIT

Correct Answer: B

QUESTION 4

Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search. link:www.ghttech.net What will this search produce?

A. All sites that link to ghttech.net

B. Sites that contain the code: link:www.ghttech.net

C. All sites that ghttech.net links to

D. All search engines that link to .net domains

Correct Answer: A

QUESTION 5

Frank is performing a wireless pen testing for an organization. Using different wireless attack techniques,

he successfully cracked the WPA-PSK key. He is trying to connect to the wireless network using the WPAPSK key. However, he is unable to connect to the WLAN as the target is using MAC filtering.

What would be the easiest way for Frank to circumvent this and connect to the WLAN?

A. Attempt to crack the WEP key

B. Crack the Wi-Fi router login credentials and disable the ACL

C. Sniff traffic off the WLAN and spoof his MAC address to the one that he has captured

D. Use deauth command from aircrack-ng to deauthenticate a connected user and hijack the session

Correct Answer: C