

Eccouncil

212-89 Exam

EC Council Certified Incident Handler v3



Thank you for Downloading 212-89 exam PDF Demo

You can also try our 212-89 Full Version Download

<https://www.certkillers.net/Exam/212-89>

<https://www.certkillers.net>

Version: 9.0

Question: 1

ZYX company experienced a DoS/DDoS attack on their network. Upon investigating the incident, they concluded that the attack is an application-layer attack. Which of the following attacks did the attacker use?

- A. Slowloris attack
- B. UDP flood attack
- C. SYN flood attack
- D. Ping of ceath

Answer: A

Question: 2

Ross is an incident manager (IM) at an organization, and his team provides support to all users in the organization who are affected by threats or attacks. David, who is the organization's internal auditor, is also part of Ross's incident response team. Which of the following is David's responsibility?

- A. Configure information security controls.
- B. Identify and report security loopholes to the management for necessary action.
- C. Coordinate incicent containment activities with the information security officer (ISO).
- D. Perform the- necessary action to block the network traffic from the suspectoc intruder.

Answer: B

Question: 3

Dash wants to perform a DoS attack over 256 target URLs simultaneously.

Which of the following tools can Dash employ to achieve his objective?

- A. HOIC
- B. IDAPro
- C. Ollydbg
- D. OpenVAS

Answer: A

Question: 4

Which of the following information security personnel handles incidents from management and technical point of view?

- A. Network administrators
- B. Incident manager (IM)
- C. Threat researchers
- D. Forensic investigators

Answer: B

Question: 5

Francis received a spoof email asking for his bank information. He decided to use a tool to analyze the email headers. Which of the following should he use?

- A. EventLog Analyzer
- B. MxToolbox
- C. Email Checker
- D. PoliteMail

Answer: B

Thank You for trying 212-89 PDF Demo

To try our 212-89 Full Version Download visit link below

<https://www.certkillers.net/Exam/212-89>

Start Your 212-89 Preparation

Use Coupon “**CKNET**” for Further discount on the purchase of Full Version Download. Test your 212-89 preparation with actual exam questions.

<https://www.certkillers.net>