



312-50V11^{Q&As}

Certified Ethical Hacker v11 Exam

Pass EC-COUNCIL 312-50V11 Exam with 100% Guarantee

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

<https://www.geekcert.com/312-50v11.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

What two conditions must a digital signature meet?

- A. Has to be the same number of characters as a physical signature and must be unique.
- B. Has to be unforgeable, and has to be authentic.
- C. Must be unique and have special characters.
- D. Has to be legible and neat.

Correct Answer: B

QUESTION 2

Stephen, an attacker, targeted the industrial control systems of an organization. He generated a fraudulent email with a malicious attachment and sent it to employees of the target organization. An employee who manages the sales software of the operational plant opened the fraudulent email and clicked on the malicious attachment. This resulted in the malicious attachment being downloaded and malware being injected into the sales software maintained in the victim's system. Further, the malware propagated itself to other networked systems, finally damaging the industrial automation components. What is the attack technique used by Stephen to damage the industrial systems?

- A. Spear-phishing attack
- B. SMishing attack
- C. Reconnaissance attack
- D. HMI-based attack

Correct Answer: A

QUESTION 3

You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are starting an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

- A. IDS log
- B. Event logs on domain controller
- C. Internet Firewall/Proxy log.
- D. Event logs on the PC

Correct Answer: C

QUESTION 4



Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the Information, he successfully performed an attack on the target government organization without being traced. Which of the following techniques is described in the above scenario?

- A. Dark web footprinting
- B. VoIP footprinting
- C. VPN footprinting
- D. website footprinting

Correct Answer: A

VoIP (Voice over Internet Protocol) is a web convention that permits the transmission of voice brings over the web. It does as such by changing over the ordinary telephone signals into advanced signs. Virtual Private Networks(VPN) give a protected association with an associations\' organization. Along these lines, VoIP traffic can disregard a SSL-based VPN, successfully scrambling VoIP administrations. When leading surveillance, in the underlying phases of VoIP footprinting, the accompanying freely accessible data can be normal: All open ports and administrations of the gadgets associated with the VoIP organization The public VoIP worker IP address The working arrangement of the worker running VoIP The organization framework

QUESTION 5

An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections.

When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

- A. Wireshark
- B. Ettercap
- C. Aircrack-ng
- D. Tcpdump

Correct Answer: B

[312-50V11 VCE Dumps](#)

[312-50V11 Exam Questions](#)

[312-50V11 Braindumps](#)