212-89 Q&As

EC-Council Certified Incident Handler

Pass EC-COUNCIL 212-89 Exam with 100% Guarantee

QUESTION 1

A Host is infected by worms that propagates through a vulnerable service; the sign(s) of the presence of the worm include:

A. Decrease in network usage

B. Established connection attempts targeted at the vulnerable services

C. System becomes instable or crashes

D. All the above

Correct Answer: C

QUESTION 2

An adversary attacks the information resources to gain undue advantage is called:

A. Defensive Information Warfare

B. Offensive Information Warfare

C. Electronic Warfare

D. Conventional Warfare

Correct Answer: B

QUESTION 3

A risk mitigation strategy determines the circumstances under which an action has to be taken to minimize and overcome risks. Identify the risk mitigation strategy that focuses on minimizing the probability of risk and losses by searching for vulnerabilities in the system and appropriate controls:

A. Risk Assumption

B. Research and acknowledgment

C. Risk limitation

D. Risk absorption

Correct Answer: B

QUESTION 4

Insiders understand corporate business functions. What is the correct sequence of activities performed by Insiders to damage company assets:

A. Gain privileged access, install malware then activate

B. Install malware, gain privileged access, then activate

C. Gain privileged access, activate and install malware

D. Activate malware, gain privileged access then install malware

Correct Answer: A

QUESTION 5

Multiple component incidents consist of a combination of two or more attacks in a system. Which of the following is not a multiple component incident?

A. An insider intentionally deleting files from a workstation

B. An attacker redirecting user to a malicious website and infects his system with Trojan

C. An attacker infecting a machine to launch a DDoS attack

D. An attacker using email with malicious code to infect internal workstation

Correct Answer: A