DUMPSARENA

EC Council Certified Incident Handler (ECIH v3)

ECCouncil 212-89

Version Demo

Total Demo Questions: 10

Total Premium Questions: 163

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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

ANSWER: A

QUESTION NO: 2

Ensuring the integrity, confidentiality and availability of electronic protected health information of a patient is known as:

A. Gramm-Leach-Bliley Act

B. Health Insurance Portability and Privacy Act

C. Social Security Act

D. Sarbanes-Oxley Act

ANSWER: B

QUESTION NO: 3

Which of the following can be considered synonymous:

A. Hazard and Threat

B. Threat and Threat Agent

C. Precaution and countermeasure

D. Vulnerability and Danger

ANSWER: A

QUESTION NO: 4

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

ANSWER: A

QUESTION NO: 5

Identify the network security incident where intended authorized users are prevented from using system, network, or applications by flooding the network with high volume of traffic that consumes all existing network resources.

A. URL Manipulation

B. XSS Attack

C. SQL Injection

D. Denial of Service Attack

ANSWER: D

QUESTION NO: 6

Identify a standard national process which establishes a set of activities, general tasks and a management structure to certify and accredit systems that will maintain the information assurance (IA) and security posture of a system or site.

A. NIASAP

B. NIAAAP

C. NIPACP

D. NIACAP

ANSWER: D

QUESTION NO: 7

Based on the some statistics; what is the typical number one top incident?

A. Phishing

B. Policy violation

C. Un-authorized access

D. Malware

ANSWER: A

QUESTION NO: 8

In a qualitative risk analysis, risk is calculated in terms of:

A. (Attack Success + Criticality) –(Countermeasures)

B. Asset criticality assessment – (Risks and Associated Risk Levels)

C. Probability of Loss X Loss

D. (Countermeasures + Magnitude of Impact) – (Reports from prior risk assessments)

ANSWER: C

QUESTION NO: 9

The correct sequence of incident management process is:

A. Prepare, protect, triage, detect and respond

B. Prepare, protect, detect, triage and respond

C. Prepare, detect, protect, triage and respond

D. Prepare, protect, detect, respond and triage

ANSWER: B

QUESTION NO: 10

One of the main objectives of incident management is to prevent incidents and attacks by tightening the physical security of the system or infrastructure. According to CERT's incident management process, which stage focuses on implementing infrastructure improvements resulting from postmortem reviews or other process improvement mechanisms?

A. Protection

B. Preparation

C. Detection

D. Triage

ANSWER: A