212-89$^{Q\&As}$

EC-Council Certified Incident Handler

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

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

https://www.leads4pass.com/212-89.html

100% Passing Guarantee
100% Money Back Assurance

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

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 organization faced an information security incident where a disgruntled employee passed sensitive access control information to a competitor. The organization\\'s incident response manager, upon investigation, found that the incident must be handled within a few hours on the same day to maintain business continuity and market competitiveness. How would you categorize such information security incident?

A. High level incident

B. Middle level incident

C. Ultra-High level incident

D. Low level incident

Correct Answer: B

QUESTION 3

The data on the affected system must be backed up so that it can be retrieved if it is damaged during incident response. The system backup can also be used for further investigations of the incident. Identify the stage of the incident response and handling process in which complete backup of the infected system is carried out?

A. Containment

B. Eradication

C. Incident recording

D. Incident investigation

Correct Answer: A

QUESTION 4

Incidents such as DDoS that should be handled immediately may be considered as:

A. Level One incident

B. Level Two incident

C. Level Three incident

D. Level Four incident

Correct Answer: C

QUESTION 5

The main feature offered by PGP Desktop Email is:

A. Email service during incidents

B. End-to-end email communications

C. End-to-end secure email service

D. None of the above

Correct Answer: C

QUESTION 6

The service organization that provides 24x7 computer security incident response services to any user, company, government agency, or organization is known as:

A. Computer Security Incident Response Team CSIRT

B. Security Operations Center SOC

C. Digital Forensics Examiner

D. Vulnerability Assessor

Correct Answer: A

QUESTION 7

The free, open source, TCP/IP protocol analyzer, sniffer and packet capturing utility standard across many industries and educational institutions is known as:

A. Snort

B. Wireshark

C. Cain and Able

D. nmap

Correct Answer: B

QUESTION 8

________________ attach(es) to files

A. adware

B. Spyware

C. Viruses

D. Worms

Correct Answer: C

QUESTION 9

In a DDoS attack, attackers first infect multiple systems, which are then used to attack a particular target directly. Those systems are called: A. Honey Pots

B. Relays

C. Zombies

D. Handlers

Correct Answer: C

QUESTION 10

The typical correct sequence of activities used by CSIRT when handling a case is:

A. Log, inform, maintain contacts, release information, follow up and reporting

B. Log, inform, release information, maintain contacts, follow up and reporting

C. Log, maintain contacts, inform, release information, follow up and reporting

D. Log, maintain contacts, release information, inform, follow up and reporting

Correct Answer: A

QUESTION 11

Risk management consists of three processes, risk assessment, mitigation and evaluation. Risk assessment determines the extent of the potential threat and the risk associated with an IT system through its SDLC. How many primary steps does NIST\\'s risk assessment methodology involve?

A. Twelve

B. Four

C. Six

D. Nine

Correct Answer: C

QUESTION 12

Electronic evidence may reside in the following:

A. Data Files

B. Backup tapes

C. Other media sources

D. All the above

Correct Answer: D

QUESTION 13

Except for some common roles, the roles in an IRT are distinct for every organization. Which among the following is the role played by the Incident Coordinator of an IRT?

A. Links the appropriate technology to the incident to ensure that the foundation\\'s offices are returned to normal operations as quickly as possible

B. Links the groups that are affected by the incidents, such as legal, human resources, different business areas and management

C. Applies the appropriate technology and tries to eradicate and recover from the incident

D. Focuses on the incident and handles it from management and technical point of view

Correct Answer: B

QUESTION 14

Which of the following service(s) is provided by the CSIRT:

A. Vulnerability handling

B. Technology watch

C. Development of security tools

D. All the above

Correct Answer: D

QUESTION 15

Which is the incorrect statement about Anti-keyloggers scanners: A. Detect already installed Keyloggers in victim machines

B. Run in stealthy mode to record victims online activity

C. Software tools

Correct Answer: B