212-89 Dumps

EC Council Certified Incident Handler (ECIH v2)

https://www.certleader.com/212-89-dumps.html

NEW QUESTION 1
Which of the following terms may be defined as "a measure of possible inability to achieve a goal, objective, or target within a defined security, cost plan and technical limitations that adversely affects the organization's operation and revenues?

A. Risk
B. Vulnerability
C. Threat
D. Incident Response

Answer: A

NEW QUESTION 2
A distributed Denial of Service (DDoS) attack is a more common type of DoS Attack, where a single system is targeted by a large number of infected machines over the Internet. In a DDoS attack, attackers first infect multiple systems which are known as:

A. Trojans
B. Zombies
C. Spyware
D. Worms

Answer: B

NEW QUESTION 3
The goal of incident response is to handle the incident in a way that minimizes damage and reduces recovery time and cost. Which of the following does NOT constitute a goal of incident response?

A. Dealing with human resources department and various employee conflict behaviors.
B. Using information gathered during incident handling to prepare for handling future incidents in a better way and to provide stronger protection for systems and data.
C. Helping personal to recover quickly and efficiently from security incidents, minimizing loss or theft and disruption of services.
D. Dealing properly with legal issues that may arise during incidents.

Answer: A

NEW QUESTION 4
Which of the following is an appropriate flow of the incident recovery steps?

A. System Operation-System Restoration-System Validation-System Monitoring
B. System Validation-System Operation-System Restoration-System Monitoring
C. System Restoration-System Monitoring-System Validation-System Operations
D. System Restoration-System Validation-System Operations-System Monitoring

Answer: D

NEW QUESTION 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

NEW QUESTION 6
Incident handling and response steps help you to detect, identify, respond and manage an incident. Which of the following steps focus on limiting the scope and extent of an incident?

A. Eradication
B. Containment
C. Identification
D. Data collection

Answer: B

NEW QUESTION 7
Identify the malicious program that is masked as a genuine harmless program and gives the attacker unrestricted access to the user's information and system. These programs may unleash dangerous programs that may erase the unsuspecting user's disk and send the victim's credit card numbers and passwords to a stranger.

A. Cookie tracker
B. Worm
C. Trojan

D. Virus

Answer: C

NEW QUESTION 8
A US Federal agency network was the target of a DoS attack that prevented and impaired the normal authorized functionality of the networks. According to agency's reporting timeframe guidelines, this incident
should be reported within two (2) HOURS of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate the activity. Which incident category of the US Federal Agency does this incident belong to?

A. CAT 5
B. CAT 1
C. CAT 2
D. CAT 6

Answer: C

NEW QUESTION 9
Policies are designed to protect the organizational resources on the network by establishing the set rules and procedures. Which of the following policies authorizes a group of users to perform a set of actions on a set of resources?

A. Access control policy
B. Audit trail policy
C. Logging policy
D. Documentation policy

Answer: A

NEW QUESTION 10
When an employee is terminated from his or her job, what should be the next immediate step taken by an organization?

A. All access rights of the employee to physical locations, networks, systems, applications and data should be disabled
B. The organization should enforce separation of duties
C. The access requests granted to an employee should be documented and vetted by the supervisor
D. The organization should monitor the activities of the system administrators and privileged users who have permissions to access the sensitive information

Answer: A

NEW QUESTION 10
An incident is analyzed for its nature, intensity and its effects on the network and systems. Which stage of the incident response and handling process involves auditing the system and network log files?

A. Incident recording
B. Reporting
C. Containment
D. Identification

Answer: D

NEW QUESTION 14
Which among the following CERTs is an Internet provider to higher education institutions and various other research institutions in the Netherlands and deals with all cases related to computer security incidents in which a customer is involved either as a victim or as a suspect?

A. NET-CERT
B. DFN-CERT
C. Funet CERT
D. SURFnet-CERT

Answer: D

NEW QUESTION 15
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

NEW QUESTION 17
Organizations or incident response teams need to protect the evidence for any future legal actions that may be taken against perpetrators that intentionally attacked the computer system. EVIDENCE PROTECTION is also required to meet legal compliance issues. Which of the following documents helps in protecting

evidence from physical or logical damage:

A. Network and host log records
B. Chain-of-Custody
C. Forensic analysis report
D. Chain-of-Precedence

Answer: B

NEW QUESTION 20
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

NEW QUESTION 22
The type of relationship between CSIRT and its constituency have an impact on the services provided by the CSIRT. Identify the level of the authority that enables members of CSIRT to undertake any necessary actions on behalf of their constituency?

A. Full-level authority
B. Mid-level authority
C. Half-level authority
D. Shared-level authority

Answer: A

NEW QUESTION 23
Which of the following incidents are reported under CAT -5 federal agency category?

A. Exercise/ Network Defense Testing
B. Malicious code
C. Scans/ probes/ Attempted Access
D. Denial of Service DoS

Answer: C

NEW QUESTION 25
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

Answer: B

NEW QUESTION 30
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

Answer: B

NEW QUESTION 35
An assault on system security that is derived from an intelligent threat is called:

A. Threat Agent
B. Vulnerability
C. Attack
D. Risk

Answer: C

NEW QUESTION 37
The IDS and IPS system logs indicating an unusual deviation from typical network traffic flows; this is called:

A. A Precursor

B. An Indication
C. A Proactive
D. A Reactive

Answer: B

NEW QUESTION 41
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

Answer: C

NEW QUESTION 45
What is the best staffing model for an incident response team if current employees' expertise is very low?

A. Fully outsourced
B. Partially outsourced
C. Fully insourced
D. All the above

Answer: A

NEW QUESTION 47
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

NEW QUESTION 52
Incident response team must adhere to the following:

A. Stay calm and document everything
B. Assess the situation
C. Notify appropriate personnel
D. All the above

Answer: D

NEW QUESTION 55
Incident Response Plan requires

A. Financial and Management support
B. Expert team composition
C. Resources
D. All the above

Answer: D

NEW QUESTION 58
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

Answer: D

NEW QUESTION 60
The program that helps to train people to be better prepared to respond to emergency situations in their communities is known as:

A. Community Emergency Response Team (CERT)
B. Incident Response Team (IRT)
C. Security Incident Response Team (SIRT)
D. All the above

Answer: A

NEW QUESTION 61
To respond to DDoS attacks; one of the following strategies can be used:

A. Using additional capacity to absorb attack
B. Identifying none critical services and stopping them
C. Shut down some services until the attack has subsided
D. All the above

Answer: D

NEW QUESTION 66
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

Answer: C

NEW QUESTION 67
_____ record(s) user's typing.

A. Spyware
B. adware
C. Virus
D. Malware

Answer: A

NEW QUESTION 72
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

Answer: C

NEW QUESTION 73
The main difference between viruses and worms is:

A. Worms require a host file to propagate while viruses don't
B. Viruses require a host file to propagate while Worms don't
C. Viruses don't require user interaction; they are self-replicating malware
D. Viruses and worms are common names for the same malware

Answer: B

NEW QUESTION 74
Spyware tool used to record malicious user's computer activities and keyboard stokes is called:

A. adware
B. Keylogger
C. Rootkit
D. Firewall

Answer: B

NEW QUESTION 78
Insiders may be:

A. Ignorant employees
B. Carless administrators
C. Disgruntled staff members
D. All the above

Answer: D

NEW QUESTION 81
Which of the following may be considered as insider threat(s):

A. An employee having no clashes with supervisors and coworkers

B. Disgruntled system administrators
C. An employee who gets an annual 7% salary raise
D. An employee with an insignificant technical literacy and business process knowledge

Answer: B

NEW QUESTION 85
The Linux command used to make binary copies of computer media and as a disk imaging tool if given a raw disk device as its input is:

A. "dd" command
B. "netstat" command
C. "nslookup" command
D. "find" command

Answer: A

NEW QUESTION 86
What command does a Digital Forensic Examiner use to display the list of all IP addresses and their associated MAC addresses on a victim computer to identify the machines that were communicating with it:

A. "arp" command
B. "netstat –an" command
C. "dd" command
D. "ifconfig" command

Answer: A

NEW QUESTION 91
The individual who recovers, analyzes, and preserves computer and related materials to be presented as evidence in a court of law and identifies the evidence, estimates the potential impact of the malicious activity on the victim, and assesses the intent and identity of the perpetrator is called:

A. Digital Forensic Examiner
B. Computer Forensic Investigator
C. Computer Hacking Forensic Investigator
D. All the above

Answer: D

NEW QUESTION 92
Electronic evidence may reside in the following:

A. Data Files
B. Backup tapes
C. Other media sources
D. All the above

Answer: D

NEW QUESTION 95
Incidents are reported in order to:

A. Provide stronger protection for systems and data
B. Deal properly with legal issues
C. Be prepared for handling future incidents
D. All the above

Answer: D

NEW QUESTION 99
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

NEW QUESTION 104
According to the Fourth Amendment of USA PATRIOT Act of 2001; if a search does NOT violate a person's "reasonable" or "legitimate" expectation of privacy then it is considered:

A. Constitutional/ Legitimate
B. Illegal/ illegitimate
C. Unethical

D. None of the above

Answer: A

NEW QUESTION 106
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your 212-89 Exam with Our Prep Materials Via below:

https://www.certleader.com/212-89-dumps.html