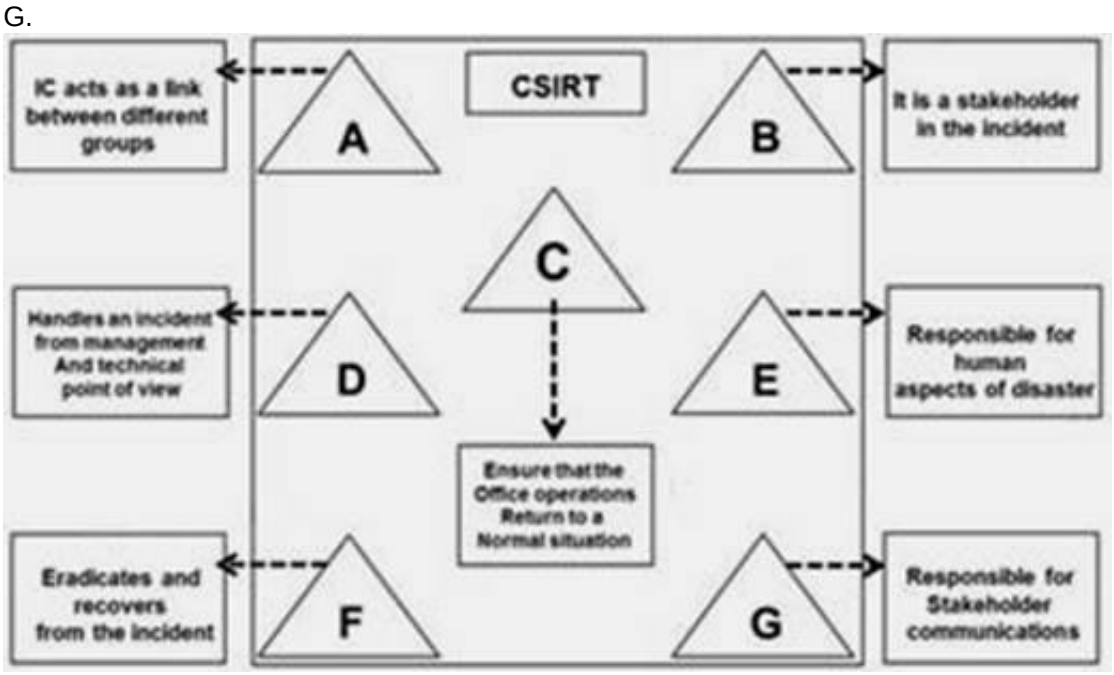
EC-Council

Exam Questions 212-89

EC Council Certified Incident Handler (ECIH v2)

NEW QUESTION 1
The flow chart gives a view of different roles played by the different personnel of CSIRT. Identify the incident response personnel denoted by A, B, C, D, E, F and G.



A. A-Incident Analyst, B- Incident Coordinator, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Manager
B. A- Incident Coordinator, B-Incident Analyst, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Manager
C. A- Incident Coordinator, B- Constituency, C-Administrator, D-Incident Manager, E- Human Resource, FIncident Analyst, G-Public relations
D. A- Incident Manager, B-Incident Analyst, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Coordinator

Answer: C

NEW QUESTION 2
A computer Risk Policy is a set of ideas to be implemented to overcome the risk associated with computer security incidents. Identify the procedure that is NOT part of the computer risk policy?

A. Procedure to identify security funds to hedge risk
B. Procedure to monitor the efficiency of security controls
C. Procedure for the ongoing training of employees authorized to access the system
D. Provisions for continuing support if there is an interruption in the system or if the system crashes

Answer: C

NEW QUESTION 3
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 4
Computer forensics is methodical series of techniques and procedures for gathering evidence from computing equipment, various storage devices and or digital media that can be presented in a course of law in a coherent and meaningful format. Which one of the following is an appropriate flow of steps in the computer forensics process:

A. Examination> Analysis > Preparation > Collection > Reporting
B. Preparation > Analysis > Collection > Examination > Reporting
C. Analysis > Preparation > Collection > Reporting > Examination
D. Preparation > Collection > Examination > Analysis > Reporting

Answer: D

NEW QUESTION 5
The network perimeter should be configured in such a way that it denies all incoming and outgoing traffic/ services that are not required. Which service listed below, if blocked, can help in preventing Denial of Service attack?

A. SAM service
B. POP3 service
C. SMTP service
D. Echo service

Answer: D

NEW QUESTION 6
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 7
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 8
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

Answer: D

NEW QUESTION 9
Which policy recommends controls for securing and tracking organizational resources:

A. Access control policy
B. Administrative security policy
C. Acceptable use policy
D. Asset control policy

Answer: D

NEW QUESTION 10
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 10
In which of the steps of NIST's risk assessment methodology are the boundary of the IT system, along with the resources and the information that constitute the system identified?

A. Likelihood Determination
B. Control recommendation
C. System characterization
D. Control analysis

Answer: C

NEW QUESTION 14
ADAM, an employee from a multinational company, uses his company's accounts to send e-mails to a third party with their spoofed mail address. How can you categorize this type of account?

A. Inappropriate usage incident
B. Unauthorized access incident
C. Network intrusion incident
D. Denial of Service incident

Answer: A

NEW QUESTION 16
An estimation of the expected losses after an incident helps organization in prioritizing and formulating their incident response. The cost of an incident can be categorized as a tangible and intangible cost. Identify the tangible cost associated with virus outbreak?

A. Loss of goodwill
B. Damage to corporate reputation
C. Psychological damage
D. Lost productivity damage

Answer: D

NEW QUESTION 18
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 23
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 26
If the loss anticipated is greater than the agreed upon threshold; the organization will:

A. Accept the risk
B. Mitigate the risk
C. Accept the risk but after management approval
D. Do nothing

Answer: B

NEW QUESTION 28
Overall Likelihood rating of a Threat to Exploit a Vulnerability is driven by :

A. Threat-source motivation and capability
B. Nature of the vulnerability
C. Existence and effectiveness of the current controls
D. All the above

Answer: D

NEW QUESTION 29
The left over risk after implementing a control is called:

A. Residual risk
B. Unaccepted risk
C. Low risk
D. Critical risk

Answer: A

NEW QUESTION 32
Which of the following is a risk assessment tool:

A. Nessus
B. Wireshark
C. CRAMM
D. Nmap

Answer: C

NEW QUESTION 36
In NIST risk assessment/ methodology; the process of identifying the boundaries of an IT system along with the resources and information that constitute the system is known as:

A. Asset Identification
B. System characterization
C. Asset valuation
D. System classification

Answer: B

NEW QUESTION 41
The correct sequence of Incident Response and Handling is:

A. Incident Identification, recording, initial response, communication and containment
B. Incident Identification, initial response, communication, recording and containment
C. Incident Identification, communication, recording, initial response and containment
D. Incident Identification, recording, initial response, containment and communication

Answer: A

NEW QUESTION 46
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 51
Incident Response Plan requires

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

Answer: D

NEW QUESTION 54
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

Answer: C

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 63
Changing the web server contents, Accessing the workstation using a false ID and Copying sensitive data without authorization are examples of:

A. DDoS attacks

B. Unauthorized access attacks
C. Malware attacks
D. Social Engineering attacks

Answer: B

NEW QUESTION 68
The very well-known free open source port, OS and service scanner and network discovery utility is called:

A. Wireshark
B. Nmap (Network Mapper)
C. Snort
D. SAINT

Answer: B

NEW QUESTION 69
_____ record(s) user's typing.

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

Answer: A

NEW QUESTION 70
Which of the following is a characteristic of adware?

A. Gathering information
B. Displaying popups
C. Intimidating users
D. Replicating

Answer: B

NEW QUESTION 71
A malicious security-breaking code that is disguised as any useful program that installs an executable programs when a file is opened and allows others to control the victim's system is called:

A. Trojan
B. Worm
C. Virus
D. RootKit

Answer: A

NEW QUESTION 75
A software application in which advertising banners are displayed while the program is running that delivers ads to display pop-up windows or bars that appears on a computer screen or browser is called:

A. adware (spelled all lower case)
B. Trojan
C. RootKit
D. Virus
E. Worm

Answer: A

NEW QUESTION 76
Which of the following is NOT one of the common techniques used to detect Insider threats:

A. Spotting an increase in their performance
B. Observing employee tardiness and unexplained absenteeism
C. Observing employee sick leaves
D. Spotting conflicts with supervisors and coworkers

Answer: A

NEW QUESTION 79
Keyloggers do NOT:

A. Run in the background
B. Alter system files
C. Secretly records URLs visited in browser, keystrokes, chat conversations, ...etc

D. Send log file to attacker's email or upload it to an ftp server

Answer: B

NEW QUESTION 80
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 85
What command does a Digital Forensic Examiner use to display the list of all open ports and the associated IP addresses on a victim computer to identify the established connections on it:

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

Answer: B

NEW QUESTION 88
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 89
A methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format is called:

A. Forensic Analysis
B. Computer Forensics
C. Forensic Readiness
D. Steganalysis

Answer: B

NEW QUESTION 90
The product of intellect that has commercial value and includes copyrights and trademarks is called:

A. Intellectual property
B. Trade secrets
C. Logos
D. Patents

Answer: A

NEW QUESTION 92
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 97
Bit stream image copy of the digital evidence must be performed in order to:

A. Prevent alteration to the original disk
B. Copy the FAT table
C. Copy all disk sectors including slack space
D. All the above

Answer: C

NEW QUESTION 98

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

212-89 Practice Exam Features:

* 212-89 Questions and Answers Updated Frequently

* 212-89 Practice Questions Verified by Expert Senior Certified Staff

* 212-89 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 212-89 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year