



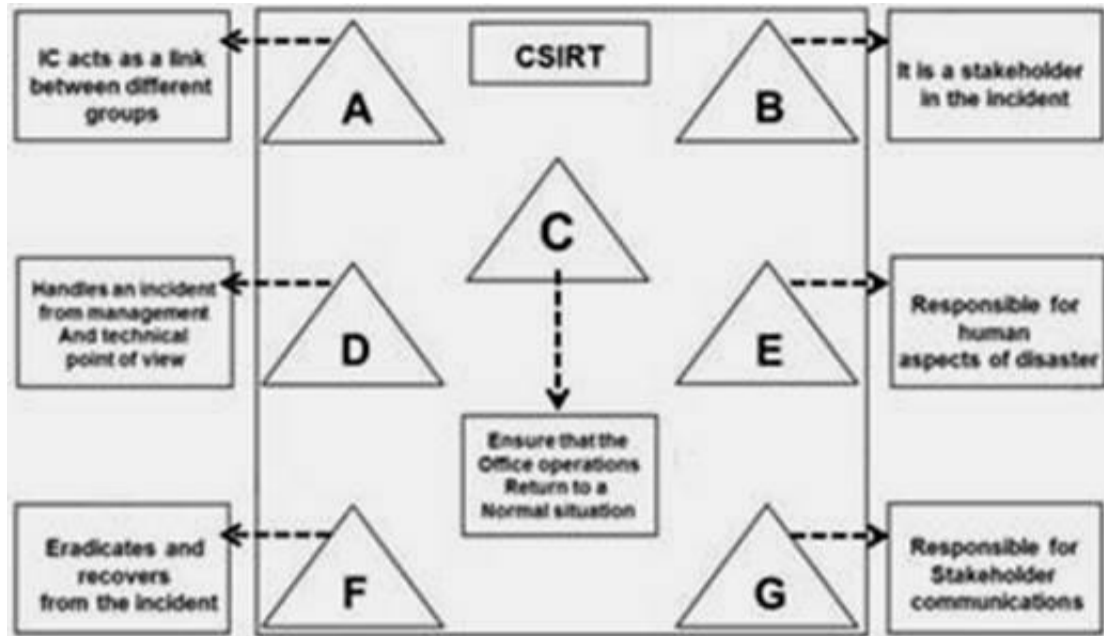
EC-Council

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

An incident recovery plan is a statement of actions that should be taken before, during or after an incident. Identify which of the following is NOT an objective of the incident recovery plan?

- A. Creating new business processes to maintain profitability after incident
 B. Providing a standard for testing the recovery plan
 C. Avoiding the legal liabilities arising due to incident
 D. Providing assurance that systems are reliable

Answer: A

NEW QUESTION 4

Risk is defined as the probability of the occurrence of an incident. Risk formulation generally begins with the likeliness of an event's occurrence, the harm it may cause and is usually denoted as Risk = ?(events)X (Probability of occurrence)X?

- A. Magnitude
 B. Probability
 C. Consequences
 D. Significance

Answer: A

NEW QUESTION 5

An audit trail policy collects all audit trails such as series of records of computer events, about an operating system, application or user activities. Which of the following statements is NOT true for an audit trail policy:

- A. It helps calculating intangible losses to the organization due to incident
 B. It helps tracking individual actions and allows users to be personally accountable for their actions
 C. It helps in compliance to various regulatory laws, rules,and guidelines
 D. It helps in reconstructing the events after a problem has occurred

Answer: A

NEW QUESTION 6

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 7

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

NEW QUESTION 8

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 9

US-CERT and Federal civilian agencies use the reporting timeframe criteria in the federal agency reporting categorization. What is the timeframe required to report an incident under the CAT 4 Federal Agency category?

- A. Weekly
- B. Within four (4) hours of discovery/detection if the successful attack is still ongoing and agency is unable to successfully mitigate activity
- C. Within two (2) hours of discovery/detection
- D. Monthly

Answer: A

NEW QUESTION 10

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

A threat source does not present a risk if NO vulnerability that can be exercised for a particular threat source. Identify the step in which different threat sources are defined:



- A. Identification Vulnerabilities
- B. Control analysis
- C. Threat identification
- D. System characterization

Answer: C

NEW QUESTION 13

In the Control Analysis stage of the NIST's risk assessment methodology, technical and none technical control methods are classified into two categories. What are these two control categories?

- A. Preventive and Detective controls

- B. Detective and Disguised controls
- C. Predictive and Detective controls
- D. Preventive and predictive controls

Answer: A

NEW QUESTION 15

Which of the following incident recovery testing methods works by creating a mock disaster, like fire to identify the reaction of the procedures that are implemented to handle such situations?

- A. Scenario testing
- B. Facility testing
- C. Live walk-through testing
- D. Procedure testing

Answer: D

NEW QUESTION 19

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 22

Insider threats can be detected by observing concerning behaviors exhibited by insiders, such as conflicts with supervisors and coworkers, decline in performance, tardiness or unexplained absenteeism. Select the technique that helps in detecting insider threats:

- A. Correlating known patterns of suspicious and malicious behavior
- B. Protecting computer systems by implementing proper controls
- C. Making is compulsory for employees to sign a none disclosure agreement
- D. Categorizing information according to its sensitivity and access rights

Answer: A

NEW QUESTION 26

Contingency planning enables organizations to develop and maintain effective methods to handle emergencies. Every organization will have its own specific requirements that the planning should address. There are five major components of the IT contingency plan, namely supporting information, notification activation, recovery and reconstitution and plan appendices. What is the main purpose of the reconstitution plan?

- A. To restore the original site, tests systems to prevent the incident and terminates operations
- B. To define the notification procedures, damage assessments and offers the plan activation
- C. To provide the introduction and detailed concept of the contingency plan
- D. To provide a sequence of recovery activities with the help of recovery procedures

Answer: A

NEW QUESTION 31

The insider risk matrix consists of technical literacy and business process knowledge vectors. Considering the matrix, one can conclude that:

- A. If the insider's technical literacy is low and process knowledge is high, the risk posed by the threat will be insignificant.
- B. If the insider's technical literacy and process knowledge are high, the risk posed by the threat will be insignificant.
- C. If the insider's technical literacy is high and process knowledge is low, the risk posed by the threat will be high.
- D. If the insider's technical literacy and process knowledge are high, the risk posed by the threat will be high.

Answer: D

NEW QUESTION 35

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 39

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 40

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

Answer: A

NEW QUESTION 43

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 47

Incident handling and response steps help you to detect, identify, respond and manage an incident. Which of the following helps in recognizing and separating the infected hosts from the information system?

- A. Configuring firewall to default settings
- B. Inspecting the process running on the system
- C. Browsing particular government websites
- D. Sending mails to only group of friends

Answer: B

NEW QUESTION 49

Computer viruses are malicious software programs that infect computers and corrupt or delete the data on them. Identify the virus type that specifically infects Microsoft Word files?

- A. Micro Virus
- B. File Infector
- C. Macro Virus
- D. Boot Sector virus

Answer: C

NEW QUESTION 53

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 58

Digital evidence plays a major role in prosecuting cyber criminals. John is a cyber-crime investigator, is asked to investigate a child pornography case. The personal computer of the criminal in question was confiscated by the county police. Which of the following evidence will lead John in his investigation?

- A. SAM file
- B. Web serve log
- C. Routing table list
- D. Web browser history

Answer: D

NEW QUESTION 60

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 61

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 63

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 67

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

NEW QUESTION 70

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 72

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 77

The largest number of cyber-attacks are conducted by:

- A. Insiders
- B. Outsiders
- C. Business partners
- D. Suppliers

Answer: B

NEW QUESTION 80

The sign of incident that may happen in the future is called:

- A. A Precursor

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

Answer: A

NEW QUESTION 84

Total cost of disruption of an incident is the sum of

- A. Tangible and Intangible costs
- B. Tangible cost only
- C. Intangible cost only
- D. Level Two and Level Three incidents cost

Answer: A

NEW QUESTION 89

An information security incident is

- A. Any real or suspected adverse event in relation to the security of computer systems or networks
- B. Any event that disrupts normal today's business functions
- C. Any event that breaches the availability of information assets
- D. All of the above

Answer: D

NEW QUESTION 94

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

NEW QUESTION 97

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 101

Absorbing minor risks while preparing to respond to major ones is called:

- A. Risk Mitigation
- B. Risk Transfer
- C. Risk Assumption
- D. Risk Avoidance

Answer: C

NEW QUESTION 103

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 104

Performing Vulnerability Assessment is an example of a:

- A. Incident Response
- B. Incident Handling
- C. Pre-Incident Preparation
- D. Post Incident Management

Answer: C

NEW QUESTION 105

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 106

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 111

Removing or eliminating the root cause of the incident is called:

- A. Incident Eradication
- B. Incident Protection
- C. Incident Containment
- D. Incident Classification

Answer: A

NEW QUESTION 113

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 114

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 115

The role that applies appropriate technology and tries to eradicate and recover from the incident is known as:

- A. Incident Manager
- B. Incident Analyst
- C. Incident Handler
- D. Incident coordinator

Answer: B

NEW QUESTION 117

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 119

CSIRT can be implemented at:

- A. Internal enterprise level
- B. National, government and military level
- C. Vendor level
- D. All the above

Answer: D

NEW QUESTION 120

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

Answer: A

NEW QUESTION 122

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 123

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 124

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 126

A Malicious code attack using emails is considered as:

- A. Malware based attack
- B. Email attack
- C. Inappropriate usage incident
- D. Multiple component attack

Answer: D

NEW QUESTION 128

_____ attach(es) to files

- A. adware
- B. Spyware
- C. Viruses
- D. Worms

Answer: C

NEW QUESTION 132

The message that is received and requires an urgent action and it prompts the recipient to delete certain files or forward it to others is called:

- A. An Adware
- B. Mail bomb
- C. A Virus Hoax
- D. Spear Phishing

Answer: C

NEW QUESTION 135

The sign(s) of the presence of malicious code on a host infected by a virus which is delivered via e-mail could be:

- A. Antivirus software detects the infected files
- B. Increase in the number of e-mails sent and received
- C. System files become inaccessible
- D. All the above

Answer: D

NEW QUESTION 137

Which of the following is NOT one of the techniques used to respond to insider threats:

- A. Placing malicious users in quarantine network, so that attack cannot be spread
- B. Preventing malicious users from accessing unclassified information
- C. Disabling the computer systems from network connection
- D. Blocking malicious user accounts

Answer: B

NEW QUESTION 142

Authorized users with privileged access who misuse the corporate informational assets and directly affects the confidentiality, integrity, and availability of the assets are known as:

- A. Outsider threats
- B. Social Engineers
- C. Insider threats
- D. Zombies

Answer: C

NEW QUESTION 145

Spyware tool used to record malicious user's computer activities and keyboard strokes is called:

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

Answer: B

NEW QUESTION 148

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 152

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 154

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 158

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 159

Any information of probative value that is either stored or transmitted in a digital form during a computer crime is called:

- A. Digital evidence
- B. Computer Emails
- C. Digital investigation
- D. Digital Forensic Examiner

Answer: A

NEW QUESTION 162

Digital evidence must:

- A. Be Authentic, complete and reliable
- B. Not prove the attackers actions
- C. Be Volatile
- D. Cast doubt on the authenticity and veracity of the evidence

Answer: A

NEW QUESTION 163

Which of the following is NOT one of the Computer Forensic types:

- A. USB Forensics
- B. Email Forensics
- C. Forensic Archaeology
- D. Image Forensics

Answer: C

NEW QUESTION 167

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 172

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 173

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 175

Agencies do NOT report an information security incident is because of:

- A. Afraid of negative publicity
- B. Have full knowledge about how to handle the attack internally
- C. Do not want to pay the additional cost of reporting an incident
- D. All the above

Answer: A

NEW QUESTION 177

Incident may be reported using/ by:

- A. Phone call
- B. Facsimile (Fax)
- C. Email or on-line Web form
- D. All the above

Answer: D

NEW QUESTION 180

To whom should an information security incident be reported?

- A. It should not be reported at all and it is better to resolve it internally
- B. Human resources and Legal Department
- C. It should be reported according to the incident reporting & handling policy
- D. Chief Information Security Officer

Answer: C

NEW QUESTION 183

Business Continuity planning includes other plans such as:

- A. Incident/disaster recovery plan
- B. Business recovery and resumption plans
- C. Contingency plan
- D. All the above

Answer: D

NEW QUESTION 185

Which test is conducted to determine the incident recovery procedures effectiveness?

- A. Live walk-throughs of procedures
- B. Scenario testing
- C. Department-level test
- D. Facility-level test

Answer: A

NEW QUESTION 188

Business Continuity provides a planning methodology that allows continuity in business operations:

- A. Before and after a disaster
- B. Before a disaster
- C. Before, during and after a disaster
- D. During and after a disaster

Answer: C

NEW QUESTION 190

The policy that defines which set of events needs to be logged in order to capture and review the important data in a timely manner is known as:

- A. Audit trail policy
- B. Logging policy
- C. Documentation policy
- D. Evidence Collection policy
- E. Distributed and communicated
- F. Enforceable and Regularly updated
- G. Written in simple language
- H. All the above

Answer: D

NEW QUESTION 193

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 196

The most common type(s) of intellectual property is(are):

- A. Copyrights and Trademarks
- B. Patents
- C. Industrial design rights & Trade secrets
- D. All the above

Answer: D

NEW QUESTION 201

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 203

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * 212-89 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 212-89 Practice Test Here](#)