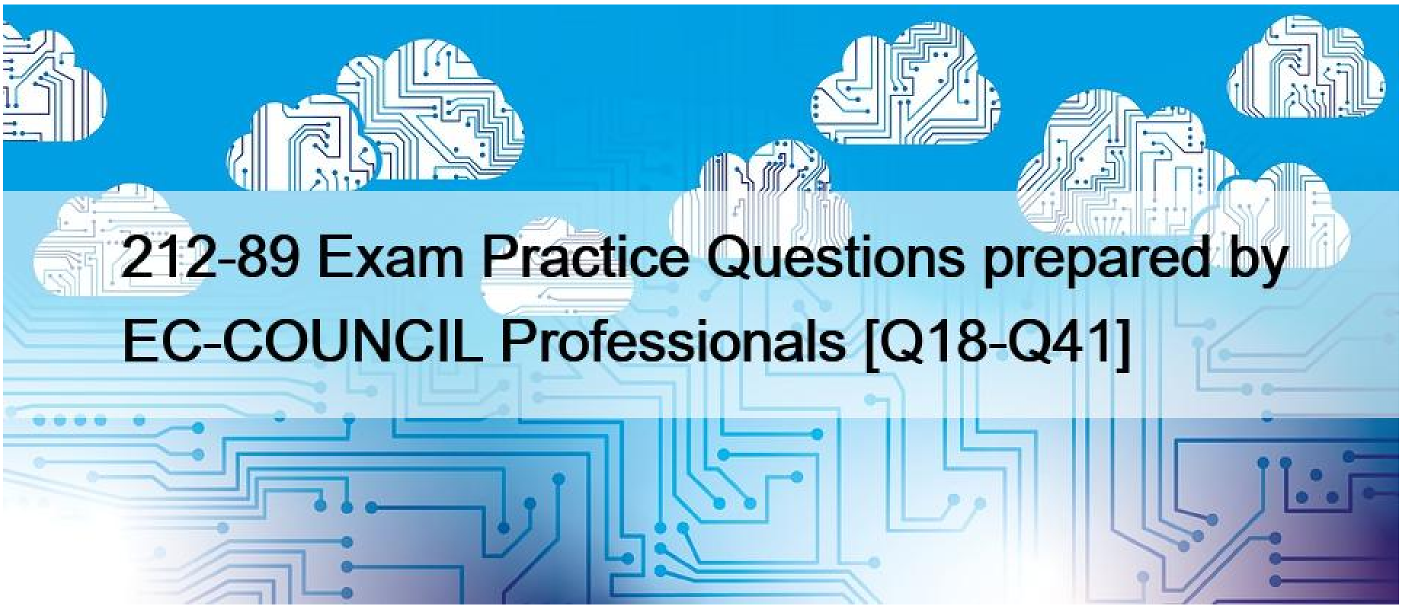
212-89 Exam Practice Questions prepared by EC-COUNCIL Professionals [Q18-Q41



212-89 Exam Practice Questions prepared by EC-COUNCIL Professionals
Use Valid New 212-89 Questions - Top choice Help You Gain Success

NEW QUESTION 18

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:
* Trojans
* Zombies
* Spyware
* Worms

NEW QUESTION 19

Common name(s) for CSIRT is(are)
* Incident Handling Team (IHT)
* Incident Response Team (IRT)
* Security Incident Response Team (SIRT)
* All the above

NEW QUESTION 20

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:
* &#8220;arp&#8221; command

* &#8220;netstat -an&#8221; command
* &#8220;dd&#8221; command
* &#8220;ifconfig&#8221; command

NEW QUESTION 21

Keyloggers do NOT:
* Run in the background
* Alter system files
* Secretly records URLs visited in browser, keystrokes, chat conversations, &#8230;etc
* Send log file to attacker&#8217;s email or upload it to an ftp server

NEW QUESTION 22

To whom should an information security incident be reported?
* It should not be reported at all and it is better to resolve it internally
* Human resources and Legal Department
* It should be reported according to the incident reporting & handling policy
* Chief Information Security Officer

NEW QUESTION 23

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?
* Eradication
* Containment
* Identification
* Data collection

NEW QUESTION 24

Business continuity is defined as the ability of an organization to continue to function even after a disastrous event, accomplished through the deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup and recovery strategy. Identify the plan which is mandatory part of a business continuity plan?
* Forensics Procedure Plan
* Business Recovery Plan
* Sales and Marketing plan
* New business strategy plan

NEW QUESTION 25

Based on the some statistics; what is the typical number one top incident?
* Phishing
* Policy violation
* Un-authorized access
* Malware

NEW QUESTION 26

A computer forensic investigator must perform a proper investigation to protect digital evidence. During the investigation, an investigator needs to process large amounts of data using a combination of automated and manual methods. Identify the computer forensic process involved:

* Analysis
* Preparation
* Examination
* Collection

NEW QUESTION 27

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:

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

NEW QUESTION 28

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

* Copyrights and Trademarks
* Patents
* Industrial design rights & Trade secrets
* All the above

NEW QUESTION 29

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:

* Asset Identification
* System characterization
* Asset valuation
* System classification

NEW QUESTION 30

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

* Vulnerability handling
* Technology watch
* Development of security tools
* All the above

NEW QUESTION 31

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

* Copyrights and Trademarks
* Patents
* Industrial design rights & Trade secrets
* All the above

Explanation/Reference:

NEW QUESTION 32

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:
* Asset Identification
* System characterization
* Asset valuation
* System classification

NEW QUESTION 33

In which of the steps of NIST&#8217;s risk assessment methodology are the boundary of the IT system, along with the resources and the information that constitute the system identified?
* Likelihood Determination
* Control recommendation
* System characterization
* Control analysis

NEW QUESTION 34

An information security incident is
* Any real or suspected adverse event in relation to the security of computer systems or networks
* Any event that disrupts normal today&#8217;s business functions
* Any event that breaches the availability of information assets
* All of the above

NEW QUESTION 35

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&#8217;s system is called:
* Trojan
* Worm
* Virus
* RootKit

NEW QUESTION 36

Business continuity is defined as the ability of an organization to continue to function even after a disastrous

event, accomplished through the deployment of redundant hardware and software, the use of fault tolerant

systems, as well as a solid backup and recovery strategy. Identify the plan which is mandatory part of a

business continuity plan?
* Forensics Procedure Plan
* Business Recovery Plan
* Sales and Marketing plan
* New business strategy plan

NEW QUESTION 37

The role that applies appropriate technology and tries to eradicate and recover from the incident is known as:
* Incident Manager
* Incident Analyst
* Incident Handler
* Incident coordinator

NEW QUESTION 38

A Host is infected by worms that propagates through a vulnerable service; the sign(s) of the presence of the worm include:
* Decrease in network usage
* Established connection attempts targeted at the vulnerable services
* System becomes instable or crashes
* All the above

NEW QUESTION 39

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

NEW QUESTION 40

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&#8217;s system is called:
* Trojan
* Worm
* Virus
* RootKit
Explanation

NEW QUESTION 41

Risk is defined as the probability of the occurrence of an incident. Risk formulation generally begins with the likeliness of an event&#8217;s occurrence, the harm it may cause and is usually denoted as Risk = ?(events)X(Probability of occurrence)X?
* Magnitude
* Probability
* Consequences
* Significance

212-89 Exam Practice Materials Collection: https://www.dumpsmaterials.com/212-89-real-torrent.html]