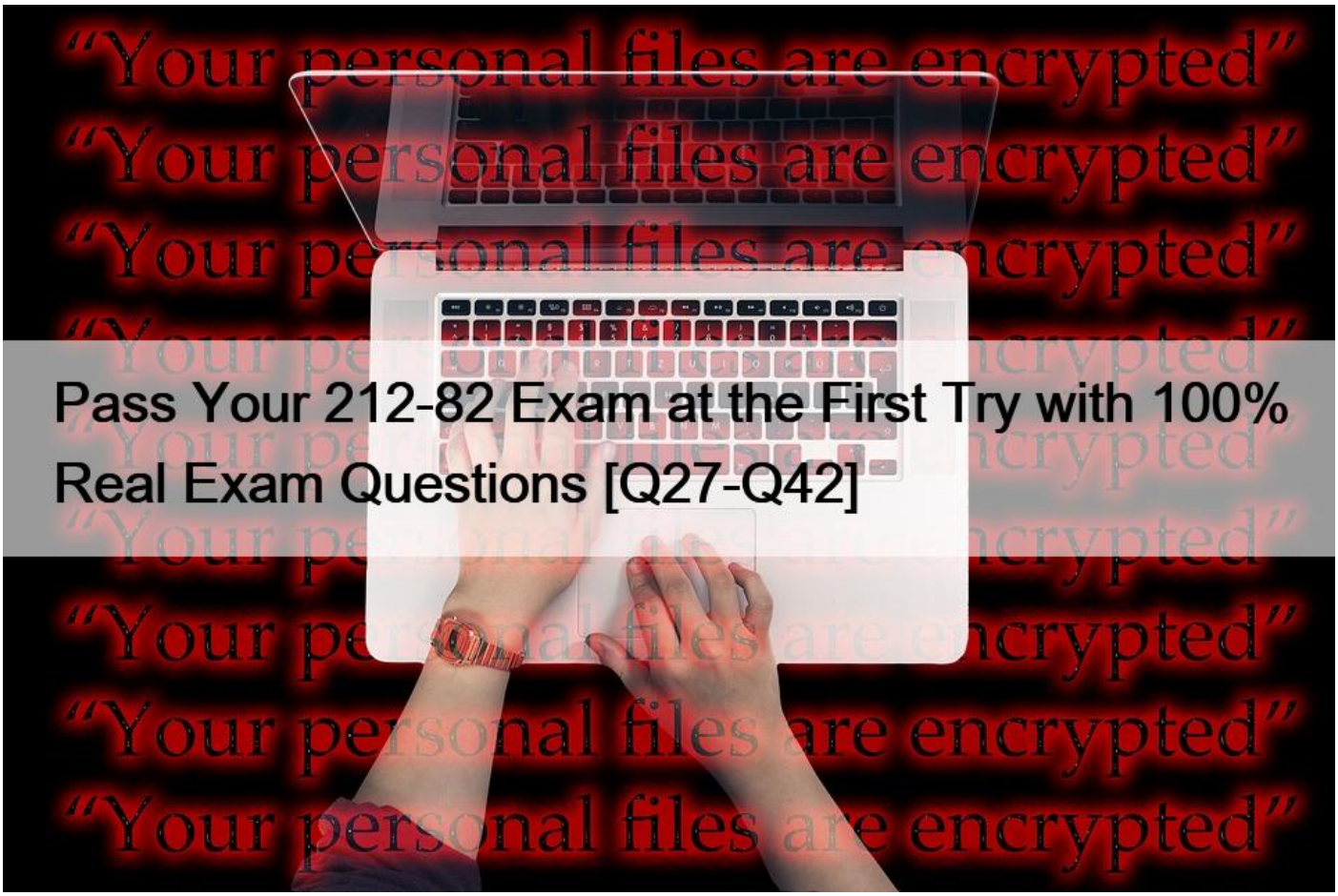
Pass Your 212-82 Exam at the First Try with 100% Real Exam Questions [Q27-Q42



Pass Your 212-82 Exam at the First Try with 100% Real Exam Questions
New ECCouncil 212-82 Dumps & Questions Updated on 2023

NO.27 Warren, a member of IH&R team at an organization, was tasked with handling a malware attack launched on one of servers connected to the organization’s network. He immediately implemented appropriate measures to stop the infection from spreading to other organizational assets and to prevent further damage to the organization.

Identify the IH&R step performed by Warren in the above scenario.
* Containment
* Recovery
* Eradication
* Incident triage

NO.28 Shawn, a forensic officer, was appointed to investigate a crime scene that had occurred at a coffee shop. As a part of investigation, Shawn collected the mobile device from the victim, which may contain potential evidence to identify the culprits.

Which of the following points must Shawn follow while preserving the digital evidence? (Choose three.)

* Never record the screen display of the device
* Turn the device ON if it is OFF
* Do not leave the device as it is if it is ON
* Make sure that the device is charged

NO.29 Kevin, a professional hacker, wants to penetrate CyberTech Inc.’s network. He employed a technique, using which he encoded packets with Unicode characters. The company’s IDS cannot recognize the packet, but the target web server can decode them.

What is the technique used by Kevin to evade the IDS system?
* Desynchronization
* Obfuscating
* Session splicing
* Urgency flag

NO.30 Sam, a software engineer, visited an organization to give a demonstration on a software tool that helps in business development. The administrator at the organization created a least privileged account on a system and allocated that system to Sam for the demonstration. Using this account, Sam can only access the files that are required for the demonstration and cannot open any other file in the system.

Which of the following type of accounts the organization has given to Sam in the above scenario?
* Service account
* Guest account
* User account
* Administrator account

NO.31 Nicolas, a computer science student, decided to create a guest OS on his laptop for different lab operations. He adopted a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment. The virtual machine manager (VMM) will directly interact with the computer hardware, translate commands to binary instructions, and forward them to the host OS.

Which of the following virtualization approaches has Nicolas adopted in the above scenario?
* Hardware-assisted virtualization
* Full virtualization
* Hybrid virtualization
* OS-assisted virtualization

NO.32 Zion belongs to a category of employees who are responsible for implementing and managing the physical security equipment installed around the facility. He was instructed by the management to check the functionality of equipment related to physical security. Identify the designation of Zion.
* Supervisor
* Chief information security officer
* Guard
* Safety officer

NO.33 Malachi, a security professional, implemented a firewall in his organization to trace incoming and outgoing traffic. He deployed a firewall that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate.

Identify the firewall technology implemented by Malachi in the above scenario.

* Next generation firewall (NGFW)
* Circuit-level gateways
* Network address translation (NAT)
* Packet filtering

NO.34 Leilani, a network specialist at an organization, employed Wireshark for observing network traffic. Leilani navigated to the Wireshark menu icon that contains items to manipulate, display and apply filters, enable, or disable the dissection of protocols, and configure user-specified decodes.

Identify the Wireshark menu Leilani has navigated in the above scenario.
* Statistics
* Capture
* Main toolbar
* Analyze

NO.35 Cassius, a security professional, works for the risk management team in an organization. The team is responsible for performing various activities involved in the risk management process. In this process, Cassius was instructed to select and implement appropriate controls on the identified risks in order to address the risks based on their severity level.

Which of the following risk management phases was Cassius instructed to perform in the above scenario?
* Risk analysis
* Risk treatment
* Risk prioritization
* Risk identification

NO.36 Walker, a security team member at an organization, was instructed to check if a deployed cloud service is working as expected. He performed an independent examination of cloud service controls to verify adherence to standards through a review of objective evidence. Further, Walker evaluated the services provided by the CSP regarding security controls, privacy impact, and performance.

Identify the role played by Walker in the above scenario.
* Cloud auditor
* Cloud provider
* Cloud carrier
* Cloud consumer

NO.37 A threat intelligence feed data file has been acquired and stored in the Documents folder of Attacker Machine-1 (File Name: Threatfeed.txt). You are a cybersecurity technician working for an ABC organization. Your organization has assigned you a task to analyze the data and submit a report on the threat landscape. Select the IP address linked with http://securityabc.s21sec.com.
* 5.9.200.200
* 5.9.200.150
* 5.9.110.120
* 5.9.188.148

NO.38 Riley sent a secret message to Louis. Before sending the message, Riley digitally signed the message using his private key. Louis received the message, verified the digital signature using the corresponding key to ensure that the message was not tampered during transit.

Which of the following keys did Louis use to verify the digital signature in the above scenario?
* Riley’s public key

* Louis’s public key
* Riley’s private key
* Louis’s private key

NO.39 Arabella, a forensic officer, documented all the evidence related to the case in a standard forensic investigation report template. She filled different sections of the report covering all the details of the crime along with the daily progress of the investigation process.

In which of the following sections of the forensic investigation report did Arabella record the “nature of the claim and information provided to the officers”?
* Investigation process
* Investigation objectives
* Evidence information
* Evaluation and analysis process

NO.40 Mark, a security analyst, was tasked with performing threat hunting to detect imminent threats in an organization’s network. He generated a hypothesis based on the observations in the initial step and started the threat hunting process using existing data collected from DNS and proxy logs.

Identify the type of threat hunting method employed by Mark in the above scenario.
* Entity-driven hunting
* TTP-driven hunting
* Data-driven hunting
* Hybrid hunting

NO.41 An organization hired a network operations center (NOC) team to protect its IT infrastructure from external attacks. The organization utilized a type of threat intelligence to protect its resources from evolving threats. The threat intelligence helped the NOC team understand how attackers are expected to perform an attack on the organization, identify the information leakage, and determine the attack goals as well as attack vectors.

Identify the type of threat intelligence consumed by the organization in the above scenario.
* Operational threat intelligence
* Strategic threat intelligence
* Technical threat intelligence
* Tactical threat intelligence

NO.42 Matias, a network security administrator at an organization, was tasked with the implementation of secure wireless network encryption for their network. For this purpose, Matias employed a security solution that uses 256-bit Galois/Counter Mode Protocol (GCMP-256) to maintain the authenticity and confidentiality of dat a.

Identify the type of wireless encryption used by the security solution employed by Matias in the above scenario.
* WPA2 encryption
* WPA3 encryption
* WEP encryption
* WPA encryption

ECCouncil 212-82 Exam Syllabus Topics:

TopicDetailsTopic 1- Business Continuity and Disaster Recovery- Network Security FundamentalsTopic 2- Network Security Controls ? Physical Controls- Wireless Network SecurityTopic 3- Network Logs Monitoring and Analysis- Information Security AttacksTopic 4- Information Security Threats and Vulnerabilities- Network Traffic MonitoringTopic 5- Network Security Controls ? Technical Controls- IoT and OT Security

Updated Exam 212-82 Dumps with New Questions: https://www.validbraindumps.com/212-82-exam-prep.html]