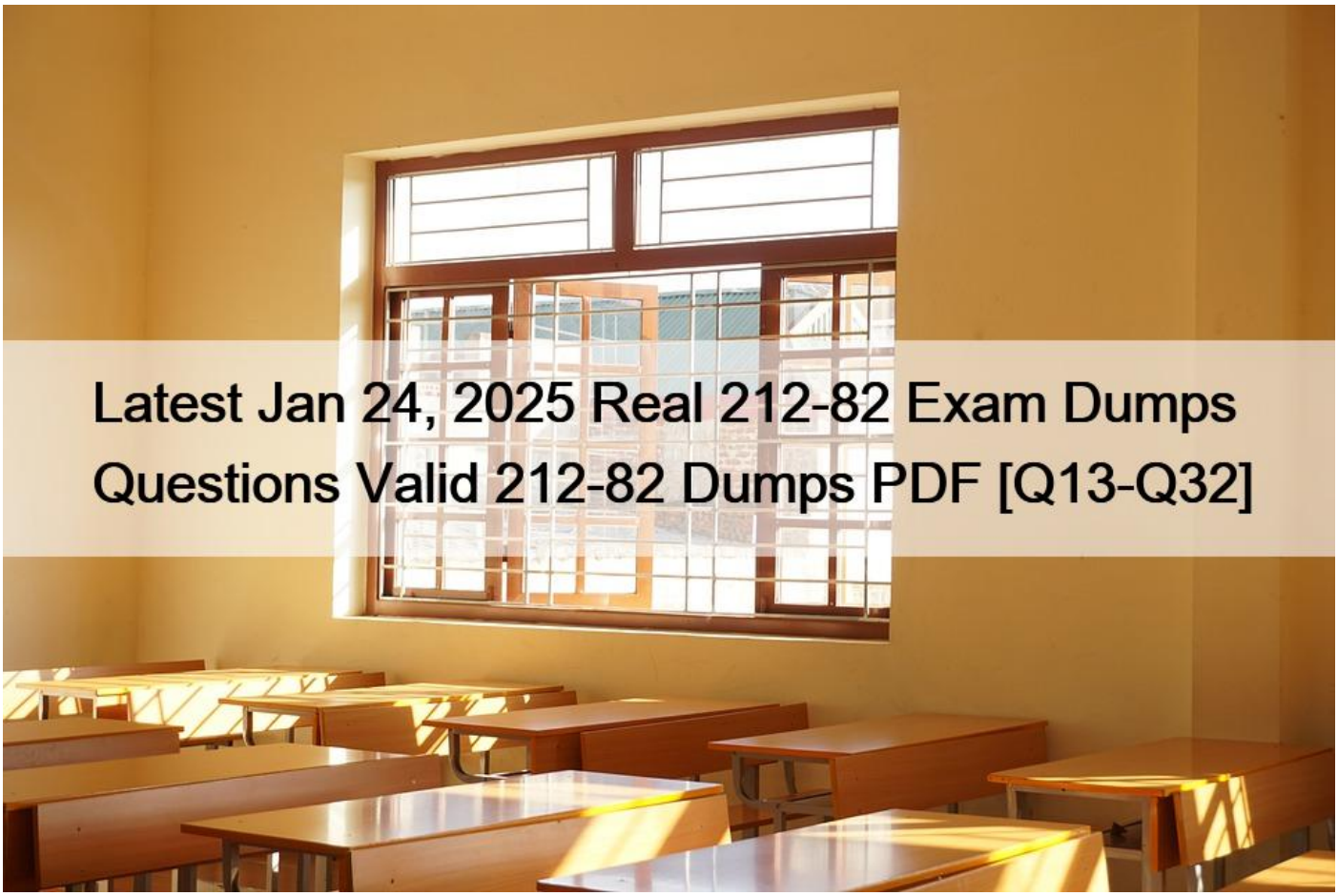
Latest Jan 24, 2025 Real 212-82 Exam Dumps Questions Valid 212-82 Dumps PDF [Q13-Q32



Latest Jan 24, 2025 Real 212-82 Exam Dumps Questions Valid 212-82 Dumps PDF
ECCouncil 212-82 Exam Dumps - PDF Questions and Testing Engine

NEW QUESTION 13

You work in a Multinational Company named Vector Inc. on Hypervisors and Virtualization Software. You are using the Operating System (OS) Virtualization and you have to handle the Security risks associated with the OS virtualization. How can you mitigate these security risks?
* All of the above
* Implement least privilege access control for users managing VMs.
* Regularly patch and update the hypervisor software for security fixes.
* Disable security features on virtual machines to improve performance.
Mitigating security risks associated with OS virtualization involves a comprehensive approach. Here’s a breakdown of the steps:

* Implement Least Privilege Access Control for Users Managing VMs:

* Limit access to only those users who need it.

* Ensure that users have only the permissions necessary to perform their tasks.

* Regularly Patch and Update the Hypervisor Software for Security Fixes:

* Keep the hypervisor and virtualization software up-to-date to protect against known vulnerabilities.

* Regular patching minimizes the risk of exploitation.

* Disable Security Features on Virtual Machines to Improve Performance:

* Note: This is actually a security risk. The correct approach is toenable and configure security featuresto protect VMs, despite the potential minor impact on performance.

Comprehensive Approach:

* A holistic security strategy includes enforcing least privilege, maintaining updated systems, and enabling security features on VMs to protect against a wide range of threats.

References:

* EC-Council Certified Ethical Hacker (CEH) materials.

* Best practices for virtualization security from NIST and other cybersecurity frameworks.

NEW QUESTION 14

Richard, a professional hacker, was hired by a marketer to gather sensitive data and information about the offline activities of users from location dat a. Richard employed a technique to determine the proximity of a user’s mobile device to an exact location using CPS features. Using this technique. Richard placed a virtual barrier positioned at a static location to interact with mobile users crossing the barrier, identify the technique employed by Richard in this scenario.

* Containerization
* Over-the-air (OTA) updates
* Full device encryption
* Ceofencing

Geofencing is a technique that uses GPS features to determine the proximity of a user’s mobile device to an exact location. Geofencing can be used to create a virtual barrier positioned at a static location to interact with mobile users crossing the barrier. Geofencing can be used for marketing, security, and tracking purposes2.

NEW QUESTION 15

The incident handling and response (IH&R) team of an organization was handling a recent cyberattack on the organization’s web server. Fernando, a member of the IH&P team, was tasked with eliminating the root cause of the incident and closing all attack vectors to prevent similar incidents in future. For this purpose. Fernando applied the latest patches to the web server and installed the latest security mechanisms on it. Identify the IH&R step performed by Fernando in this scenario.

* Notification
* Containment
* Recovery
* Eradication

Eradication is the IH&R step performed by Fernando in this scenario. Eradication is a step in IH&R that involves eliminating the root cause of the incident and closing all attack vectors to prevent similar incidents in future. Eradication can include applying patches, installing security mechanisms, removing malware, restoring backups, or reformatting systems.

NEW QUESTION 16

Henry Is a cyber security specialist hired by BlackEye – Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unkornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target system is running a Windows OS.

Identify the TTL value Henry obtained, which indicates that the target OS is Windows.
* 64
* 128
* 255
* 138

128 is the TTL value that Henry obtained, which indicates that the target OS is Windows. TTL (Time to Live) is a field in the IP (Internet Protocol) header that specifies how long a packet can remain in a network before it is discarded or dropped. TTL is usually expressed in seconds or hops (the number of routers or gateways that a packet passes through). TTL is used to prevent packets from looping endlessly in a network or consuming network resources . Different operating systems have different default TTL values for their packets. By observing the TTL value of a packet from a target system or network, one can infer the operating system of the target . Some common TTL values and their corresponding operating systems are:

* 64: Linux, Unix, Android

* 128: Windows

* 255: Cisco IOS

* 60: Mac OS

In the scenario, Henry used Nmap tool to discover the OS of the target system. Nmap (Network Mapper) is a tool that can perform various network scanning and enumerationtasks, such as port scanning, OS detection, service identification, etc . Nmap can use various techniques to detect the OS of a target system, such as TCP/IP fingerprinting, which involves analyzing various TCP/IP characteristics of packets from the target system, such as TTL value. In the scenario, Henry obtained a TTL value of 128 , which indicates that the target OS is Windows.

NEW QUESTION 17

Rhett, a security professional at an organization, was instructed to deploy an IDS solution on their corporate network to defend against evolving threats. For this purpose, Rhett selected an IDS solution that first creates models for possible intrusions and then compares these models with incoming events to make detection decisions.

Identify the detection method employed by the IDS solution in the above scenario.
* Not-use detection
* Protocol anomaly detection
* Anomaly detection
* Signature recognition

NEW QUESTION 18

A pfSense firewall has been configured to block a web application www.abchacker.com. Perform an analysis on the rules set by the admin and select the protocol which has been used to apply the rule.

Hint: Firewall login credentials are given below:

Username: admin

Password: admin@l23
* POP3
* TCP/UDP
* FTP
* ARP

TCP/UDP is the protocol that has been used to apply the rule to block the web application www.abchacker.com in the above scenario. pfSense is a firewall and router software that can be installed on a computer or a device to protect a network from variousthreats and attacks. pfSense can be configured to block or allow traffic based on various criteria, such as source, destination, port, protocol, etc. pfSense rules are applied to traffic in the order they appear in the firewall configuration . To perform an analysis on the rules set by the admin, one has to follow these steps:

* Open a web browser and type 20.20.10.26

* Press Enter key to access the pfSense web interface.

* Enter admin as username and admin@l23 as password.

* Click on Login button.

* Click on Firewall menu and select Rules option.

* Click on LAN tab and observe the rules applied to LAN interface.

The rules applied to LAN interface are:

Action	Interface	Protocol	Source	Port	Destination	Port	Description
Block	LAN	TCP/UDP	any	any	www.abchacker.com	any	Block abchacker website
Pass	LAN	any	any	any	any	any	Default allow LAN to any rule

The first rule blocks any traffic from LAN interface to www.abchacker.com website using TCP/UDP protocol.

The second rule allows any traffic from LAN interface to any destination using any protocol. Since the first rule appears before the second rule, it has higher priority and will be applied first. Therefore, TCP/UDP is the protocol that has been used to apply the rule to block the web application www.abchacker.com. POP3 (Post Office Protocol 3) is a protocol that allows downloading emails from a mail server to a client device. FTP (File Transfer Protocol) is a protocol that allows transferring files between a client and a server over a network.

ARP (Address Resolution Protocol) is a protocol that resolves IP addresses to MAC (Media Access Control) addresses on a network.

NEW QUESTION 19

Jane Is a newly appointed Chief Financial Officer at BigTech Corp. Within a week, she receives an email from a sender posing as the company’s CEO. instructing her to make an urgent wire transfer. Suspicious. Jane decides to verify the request’s authenticity. She receives another email from the same sender, now attaching a seemingly scanned Image of the CEO’s handwritten note. Simultaneously, she gets a call from an ‘IT support’ representative, instructing her to click on the attached image to download a ‘security patch’. Concerned. Jane must determine which social engineering tactics she encountered.

* Baiting via the handwritten note image and preloading through the ‘IT support’ call.
* Spear phishing through both the emails and quizzing via the ‘IT support’ call.
* Phishing through the CEO impersonation email and baiting via the ‘IT support’ call.
* Spear phishing through the CEO impersonation email and vishing via the ‘IT support’ call.

Jane encountered a combination of social engineering tactics:

* Spear Phishing:

* CEO Impersonation Email: The initial email and the follow-up with the scanned image of the CEO’s handwritten note are examples of spear phishing, where attackers target specific individuals with tailored messages to gain their trust and extract sensitive information.

* Vishing:

* ‘IT Support’ Call: The phone call from the supposed ‘IT support’ representative asking Jane to download a ‘security patch’ is a form of vishing (voice phishing). This tactic involves using phone calls to trick victims into revealing sensitive information or performing actions that compromise security.

References:

* Social Engineering Techniques: SANS Institute Reading Room

* Phishing and Vishing Explained: Norton Security

NEW QUESTION 20

In an advancedcybersecurity research lab. a team Is working on developing a new cryptographicprotocol to secure highly sensitive communication. Their goal is to create aprotocol that is resilient against quantum computing attacks, which couldpotentially break many current encryption methods. During their research, theyfocus on the use of hash functions in their protocol. The team experiments withvarious hash functions to ensure the highest level of security. Considering thethreat of quantum computing, which of the following hash functions would be themost appropriate choice fortheir protocol?

* SHA-256, due to its widespread use and proven security track record
* MD5, for its speed and efficiency in generating hash values
* HMAC. for its ability to provide data integrity and authentication
* SHA-3. as it is designed to be resistant against quantum computing attacks

In the context of developing a cryptographic protocol resilient against quantum computing attacks, SHA-3 is the most appropriate choice. Here’s why:

* Quantum Computing Threats: Quantum computers can potentially break current cryptographic methods like RSA and ECC due to

Shor’s algorithm. Traditional hash functions like SHA-256 might not offer sufficient security in a post-quantum world.

* SHA-3 Overview: SHA-3, part of the Secure Hash Algorithm family, was designed with quantum resistance in mind. It was selected through an open competition by NIST, ensuring it incorporates advanced cryptographic techniques.

* Resilience: SHA-3’s design is fundamentally different from SHA-2, providing enhanced security properties, including resistance to various attack vectors that might be feasible with quantum computing advancements.

References:

* NIST SHA-3 Standard:NIST FIPS PUB 202

* Research on quantum-resistant cryptography:IEEE Xplore

NEW QUESTION 21

Kayden successfully cracked the final round of interviews at an organization. After a few days, he received his offer letter through an official company email address. The email stated that the selected candidate should respond within a specified time. Kayden accepted the opportunity and provided an e-signature on the offer letter, then replied to the same email address. The company validated the e-signature and added his details to their database. Here, Kayden could not deny the company’s message, and the company could not deny Kayden’s signature.

Which of the following information security elements was described in the above scenario?
* Availability
* Non-repudiation
* Integrity
* Confidentiality

The correct answer is B, as it describes the information security element that was described in the above scenario. Non-repudiation is an information security element that ensures that a party cannot deny sending or receiving a message or performing an action. In the above scenario, non-repudiation was described, as Kayden could not deny company’s message, and company could not deny Kayden’s signature. Option A is incorrect, as it does not describe the information security element that was described in the above scenario. Availability is an information security element that ensures that authorized users can access and use information and resources when needed. In the above scenario, availability was not described, as there was no mention of access or use of information and resources. Option C is incorrect, as it does not describe the information security element that was described in the above scenario. Integrity is an information security element that ensures that information and resources are accurate and complete and have not been modified by unauthorized parties. In the above scenario, integrity was not described, as there was no mention of accuracy or completeness of information and resources. Option D is incorrect, as it does not describe the information security element that was described in the above scenario. Confidentiality is an information security element that ensures that information and resources are protected from unauthorized access and disclosure.In the above scenario, confidentiality was not described, as there was no mention of protection or disclosure of information and resources.

References: , Section 3.1

NEW QUESTION 22

You are the cybersecurity lead for an International financial institution. Your organization offers online banking services to millions of customers globally, and you have recently migrated your core banking system to a hybrid cloud environment to enhance scalability and cost efficiencies.

One evening, after a routine system patch, there is a surge in server-side request forgery (SSRF) alerts from your web application

firewall(WAF). Simultaneously, your intrusion detection system (IDS) flags possible attempts to interact with cloud metadata services from your application layer, which could expose sensitive cloud configuration details and API keys. This Is a clear Indication that attackers might be trying to leverage the SSRF vulnerability to breach your cloud infrastructure. Considering the critical nature of your services and the high stakes involved, how should you proceed to tackle this imminent threat while ensuring minimal disruption to your banking customers?
* Engage with a third-party cybersecurity firm specializing in cloud security to conduct an emergency audit, relying on its expertise to identify the root cause and potential breaches.
* Rollback the recent patch immediately and inform the cloud service provider about potential unauthorized access to gauge the extent of vulnerability and coordinate a joint response.
* Isolate the affected cloud servers and redirect traffic to backup servers, ensuring continuous service while initiating a deep-dive analysis of the suspicious activities using cloud-native security tools.
* Notify all banking customers about the potential security incident, urging them to change their passwords and monitor their accounts for any unauthorized activity.
In response to the SSRF alerts and potential breach attempts flagged by your IDS, the immediate priority is to contain the threat while maintaining the integrity of your services. Here’s a step-by-step approach:

* Isolation and Containment:

* Isolate Affected Servers: Disconnect the affected cloud servers from the network to prevent further unauthorized access or data exfiltration.

* Redirect Traffic: Redirect incoming traffic to backup servers that are not compromised to ensure that online banking services remain available to customers.

* Deep-Dive Analysis:

* Cloud-Native Security Tools: Utilize cloud-native security tools provided by your cloud service provider (such as AWS GuardDuty, Azure Security Center, or Google Cloud Security Command Center) to conduct a thorough investigation of the suspicious activities.

* Examine Network Logs: Analyze network logs to identify the attack vectors and understand the scope of the attack.

* Coordinate with Cloud Provider:

* Joint Response: Inform your cloud service provider about the incident to collaborate on identifying and mitigating the vulnerability. Cloud providers often have additional tools and expertise that can be leveraged during a security incident.

* Remediation:

* Patch and Harden Systems: Once the root cause is identified, apply necessary patches and harden the security posture of your cloud infrastructure to prevent similar attacks in the future.

* Communication:

* Internal Stakeholders: Keep internal stakeholders, including the executive team and legal department, informed about the incident and the steps being taken to address it.

References:

* NIST Computer Security Incident Handling Guide:NIST SP 800-61r2

* AWS Security Best Practices:AWS Documentation

NEW QUESTION 23

Kason, a forensic officer, was appointed to investigate a case where a threat actor has bullied certain children online. Before proceeding legally with the case, Kason has documented all the supporting documents, including source of the evidence and its relevance to the case, before presenting it in front of the jury.

Which of the following rules of evidence was discussed in the above scenario?
* Authentic
* Understandable
* Reliable
* Admissible

NEW QUESTION 24

Richards, a security specialist at an organization, was monitoring an IDS system. While monitoring, he suddenly received an alert of an ongoing intrusion attempt on the organization’s network. He immediately averted the malicious actions by implementing the necessary measures.

Identify the type of alert generated by the IDS system in the above scenario.
* True positive
* True negative
* False negative
* False positive

NEW QUESTION 25

Thomas, an employee of an organization, is restricted to access specific websites from his office system. He is trying to obtain admin credentials to remove the restrictions. While waiting for an opportunity, he sniffed communication between the administrator and an application server to retrieve the admin credentials. Identify the type of attack performed by Thomas in the above scenario.
* Vishing
* Eavesdropping
* Phishing
* Dumpster diving

NEW QUESTION 26

Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob’s boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?
* HIPPA/PHl
* Pll
* PCIDSS
* ISO 2002

HIPPA/PHI is the regulation that is mostly violated in the above scenario. HIPPA (Health Insurance Portability and Accountability Act) is a US federal law that sets standards for protecting the privacy and security of health information. PHI (Protected Health Information) is any information that relates to the health or health care of an individual and that can identify the individual, such as

name, address, medical records, etc.

HIPPA/PHI requires covered entities, such as health care providers, health plans, or health care clearinghouses, and their business associates, to safeguard PHI from unauthorized access, use, or disclosure .

In the scenario, the medical company experienced a major cyber security breach that exposed the personal medical records of many patients on the internet, which violates HIPPA/PHI regulations. PII (Personally Identifiable Information) is any information that can be used to identify a specific individual, such as name, address, social security number, etc. PII is not specific to health information and can be regulated by various laws, such as GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), etc.

PCI DSS (Payment Card Industry Data Security Standard)is a set of standards that applies to entities that store, process, or transmit payment card information, such as merchants, service providers, or payment processors.

PCI DSS requires them to protect cardholder data from unauthorized access, use, or disclosure. ISO 2002 (International Organization for Standardization 2002) is not a regulation, but a standard for information security management systems that provides guidelines and best practices for organizations to manage their information security risks.

NEW QUESTION 27

Dany, a member of a forensic team, was actively involved in an online crime investigation process. Dany’s main responsibilities included providing legal advice on conducting the investigation and addressing legal issues involved in the forensic investigation process. Identify the role played by Dany in the above scenario.
* Attorney
* Incident analyzer
* Expert witness
* Incident responder

Attorney is the role played by Dany in the above scenario. Attorney is a member of a forensic team who provides legal advice on conducting the investigation and addresses legal issues involved in the forensic investigation process. Attorney can help with obtaining search warrants, preserving evidence, complying with laws and regulations, and presenting cases in court3. References: Attorney Role in Forensic Investigation

NEW QUESTION 28

Perform vulnerability analysis of a web application, www.luxurytreats.com. and determine the name of the alert with WASC ID 9. (Practical Question)
* Absence of Anti-CSRF Tokens
* Application Error Disclosure
* Viewstate without MAC Signature
* X-Frame-Options Header Not Set

Performing a vulnerability analysis on a web application involves identifying specific security weaknesses. In this case, the WASC ID 9 refers to “Application Error Disclosure.”

* Vulnerability Description:

* Application Error Disclosure: This vulnerability occurs when a web application reveals too much information about internal errors, potentially aiding attackers in crafting specific attacks against the system.

* Detection and Mitigation:

* Error Handling: Ensure that error messages do not expose sensitive information and provide only necessary details to the end-user.

* Logging: Detailed error information should be logged securely for internal review without being exposed to users.

References:

* OWASP Top Ten Web Application Security Risks: OWASP

* WASC Threat Classification: WASC ID 9

NEW QUESTION 29

A software company has implemented a wireless technology to track the employees’ attendance by recording their in and out timings. Each employee in the company will have an entry card that is embedded with a tag. Whenever an employee enters the office premises, he/she is required to swipe the card at the entrance. The wireless technology uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects.

Which of the following technologies has the software company implemented in the above scenario?
* WiMAX
* RFID
* Bluetooth
* Wi-Fi
RFID (Radio Frequency Identification) is the wireless technology that the software company has implemented in the above scenario. RFID uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects1112. WiMAX (Worldwide Interoperability for Microwave Access) is a wireless technology that provides high-speed broadband access over long distances13. Bluetooth is a wireless technology that enables short-range data communication between devices, such as phones, laptops, printers, etc.14. Wi-Fi (Wireless Fidelity) is a wireless technology that allows devices to connect to a local area network or the internet using radio waves

NEW QUESTION 30

An IoT device that has been placed in a hospital for safety measures, it has sent an alert command to the server. The network traffic has been captured and stored in the Documents folder of the Attacker Machine-1. Analyze the loTdeviceTraffic.pcapng file and select the appropriate command that was sent by the IoT device over the network.
* Tempe_Low
* Low_Tempe
* Temp_High
* High_Tempe
Temp_High is the command that was sent by the IoT device over the network in the above scenario. An IoT (Internet of Things) device is a device that can connect to the internet and communicate with other devices or systems over a network. An IoT device can send or receive commands or data for various purposes, such as monitoring, controlling, or automating processes. To analyze the IoT device traffic file and determine the command that was sent by the IoT device over the network, one has to follow these steps:

Navigate to the Documents folder of Attacker-1 machine.

Double-click on loTdeviceTraffic.pcapng file to open it with Wireshark.

Click on Analyze menu and select Display Filters option.

Enter udp.port == 5000 as filter expression and click on Apply button.

Observe the packets filtered by the expression.

Click on packet number 4 and expand User Datagram Protocol section in packet details pane.

Observe the data field under User Datagram Protocol section.

The data field under User Datagram Protocol section is 54:65:6d:70:5f:48:69:67:68 , which is hexadecimal representation of Temp_High , which is the command that was sent by the IoT device over the network.

NEW QUESTION 31

Finley, a security professional at an organization, was tasked with monitoring the organizational network behavior through the SIEM dashboard. While monitoring, Finley noticed suspicious activities in the network; thus, he captured and analyzed a single network packet to determine whether the signature included malicious patterns. Identify the attack signature analysis technique employed by Finley in this scenario.

* Context-based signature analysis
* Atomic-signature-based analysis
* Composite signature-based analysis
* Content-based signature analysis

Content-based signature analysis is the attack signature analysis technique employed by Finley in this scenario. Content-based signature analysis is a technique that captures and analyzes a single network packet to determine whether the signature included malicious patterns. Content-based signature analysis can be used to detect known attacks, such as buffer overflows, SQL injections, or cross-site scripting2.

References: Content-Based Signature Analysis

NEW QUESTION 32

A disgruntled employee has set up a RAT (Remote Access Trojan) server in one of the machines in the target network to steal sensitive corporate documents. The IP address of the target machine where the RAT is installed is 20.20.10.26. Initiate a remote connection to the target machine from the “Attacker Machine-1” using the Theef client. Locate the “Sensitive Corporate Documents” folder in the target machine’s Documents directory and determine the number of files. Mint: Theef folder is located at Z:CCT-ToolsCCT Module 01 Information Security Threats and VulnerabilitiesRemote Access Trojans (RAT)Theef of the Attacker Machine1.

* 2
* 4
* 5
* 3

The number of files in the “Sensitive Corporate Documents” folder is 4. This can be verified by initiating a remote connection to the target machine from the “Attacker Machine-1” using Theef client. Theef is a Remote Access Trojan (RAT) that allows an attacker to remotely control a victim’s machine and perform various malicious activities. To connect to the target machine using Theef client, one can follow these steps:

Launch Theef client from Z:CCT-ToolsCCT Module 01 Information Security Threats and VulnerabilitiesRemote Access Trojans (RAT)Theef on the “Attacker Machine-1”.

Enter the IP address of the target machine (20.20.10.26) and click on Connect.

Wait for a few seconds until a connection is established and a message box appears saying “Connection Successful”.

Click on OK to close the message box and access the remote desktop of the target machine.

Navigate to the Documents directory and locate the “Sensitive Corporate Documents” folder.

Open the folder and count the number of files in it. The screenshot below shows an example of performing these steps: Reference: [Theef Client Tutorial], [Screenshot of Theef client showing remote desktop and folder]

Reliable Cyber Technician (CCT) 212-82 Dumps PDF Jan 24, 2025 Recently Updated Questions:
https://www.testkingfree.com/ECCouncil/212-82-practice-exam-dumps.html]