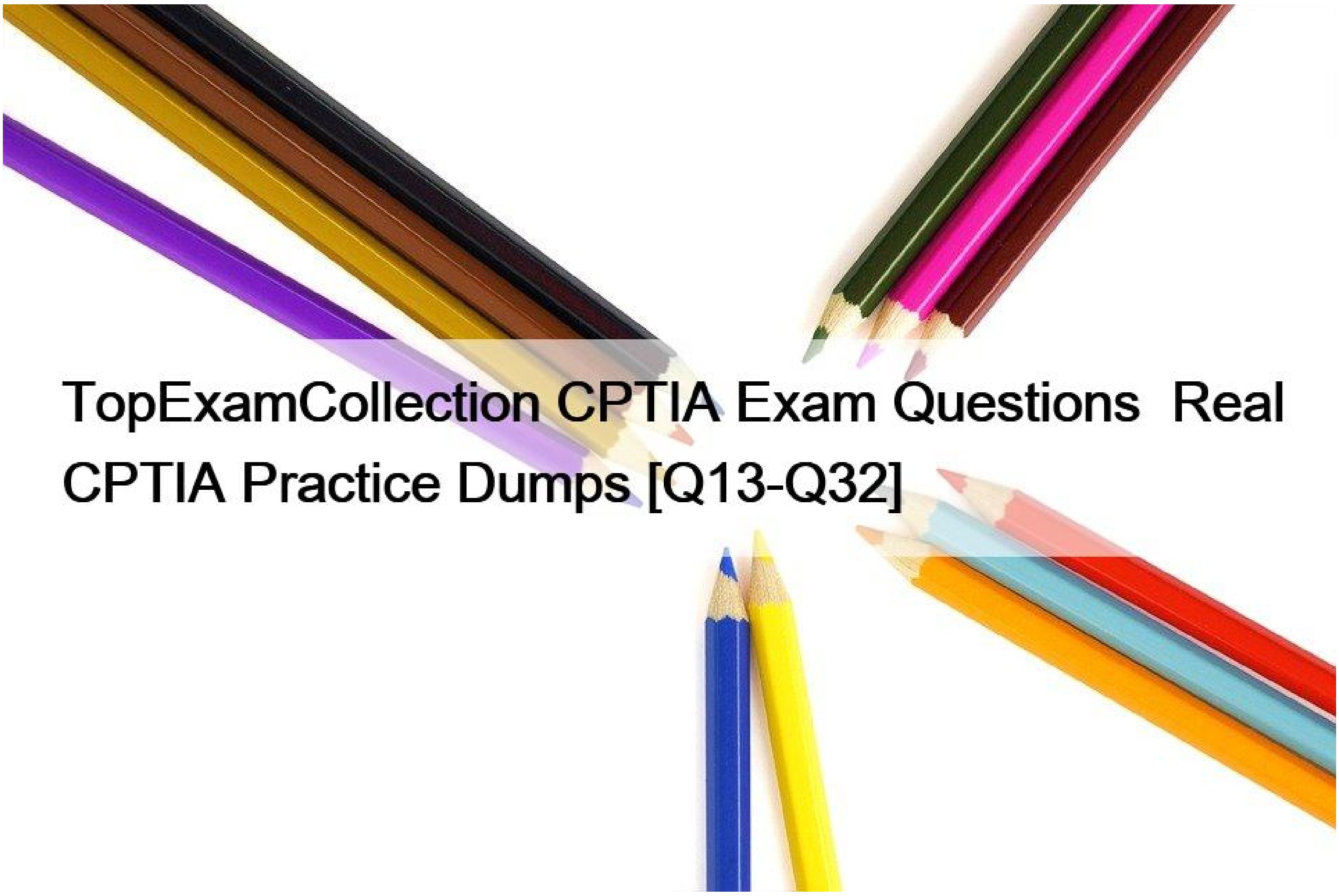
TopExamCollection CPTIA Exam Questions Real CPTIA Practice Dumps [Q13-Q32



TopExamCollection CPTIA Exam Questions | Real CPTIA Practice Dumps
Verified CPTIA Exam Dumps Q&As - Provide CPTIA with Correct Answers

NO.13 Which of the following is an attack that attempts to prevent the use of systems, networks, or applications by the intended users?
* Denial of service (DoS) attack
* Fraud and theft
* Unauthorized access
* Malicious code or insider threat attack
A Denial of Service (DoS) attack aims to make a computer resource, network, or application unavailable to its intended users, thereby preventing legitimate users from using the service. This is achieved by overwhelming the target with a flood of internet traffic or sending information that triggers a crash. In contrast, fraud and theft involve the unauthorized acquisition of data or assets, unauthorized access refers to gaining entry into systems without permission, and malicious code or insider threat attacks relate to software designed to cause harm or unauthorized actions by trusted users within the organization. The specific intent of a DoS attack is to disrupt service, making it a distinct category focused on denial of availability.References:The Incident Handler (CREST CPTIA) certification materials discuss various types of cybersecurity threats, including DoS attacks, outlining their methods, objectives, and impacts on targeted systems or networks.

NO.14 Steve works as an analyst in a UK-based firm. He was asked to perform network monitoring to find any evidence of compromise. During the network monitoring, he came to know that there are multiple logins from different locations in a short time span. Moreover, he also observed certain irregular log in patterns from locations where the organization does not have business relations. This resembles that somebody is trying to steal confidential information.

Which of the following key indicators of compromise does this scenario present?
* Unusual outbound network traffic
* Unexpected patching of systems
* Unusual activity through privileged user account
* Geographical anomalies
The scenario described by Steve&#8217;s observations, where multiple logins are occurring from different locations in a short time span, especially from locations where the organization has no business relations, points to

&#8216;Geographical anomalies&#8217; as a key indicator of compromise (IoC). Geographical anomalies in logins suggest unauthorized access attempts potentially made by attackers using compromised credentials. This is particularly suspicious when the locations of these logins do not align with the normal geographical footprint of the organization&#8217;s operations or employee locations. Monitoring for such anomalies can help in the early detection of unauthorized access and potential data breaches.References:

* SANS Institute Reading Room, &#8220;Indicators of Compromise: Reality&#8217;s Version of the Minority Report&#8221;

* &#8220;Identifying Indicators of Compromise&#8221; by CERT-UK

NO.15 Mr. Bob, a threat analyst, is performing analysis of competing hypotheses (ACH). He has reached to a stage where he is required to apply his analysis skills effectively to reject as many hypotheses and select the best hypotheses from the identified bunch of hypotheses, and this is done with the help of listed evidence. Then, he prepares a matrix where all the screened hypotheses are placed on the top, and the listed evidence for the hypotheses are placed at the bottom.

What stage of ACH is Bob currently in?
* Diagnostics
* Evidence
* Inconsistency
* Refinement
In the Analysis of Competing Hypotheses (ACH) process, the stage where Mr. Bob is applying analysis to reject hypotheses and select the most likely one based on listed evidence, followed by preparing a matrix with screened hypotheses and evidence, is known as the &#8216;Refinement&#8217; stage. This stage involves refining the list of hypotheses by systematically evaluating the evidence against each hypothesis, leading to the rejection of inconsistent hypotheses and the strengthening of the most plausible ones. The preparation of a matrix helps visualize the relationship between each hypothesis and the available evidence, facilitating a more objective and structured analysis.References:

* &#8220;Psychology of Intelligence Analysis&#8221; by Richards J. Heuer, Jr., for the CIA&#8217;s Center for the Study of Intelligence

* &#8220;A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis&#8221; by the CIA

NO.16 Tim is working as an analyst in an ABC organization. His organization had been facing many challenges in converting the raw threat intelligence data into meaningful contextual information. After inspection, he found that it was due to noise obtained from misrepresentation of data from huge data collections. Hence, it is important to clean the data before performing data analysis using techniques such as data reduction. He needs to choose an appropriate threat intelligence framework that automatically performs data collection, filtering, and analysis for his organization.

Which of the following threat intelligence frameworks should he choose to perform such task?
* HighCharts
* SIGVERIF
* Threat grid
* TC complete
Threat Grid is a threat intelligence and analysis platform that offers advanced capabilities for automatic data collection, filtering, and analysis. It is designed to help organizations convert raw threat data into meaningful, actionable intelligence. By employing advanced analytics and machine learning, Threat Grid can reduce noise from large data sets, helping to eliminate misrepresentations and enhance the quality of the threat intelligence.

This makes it an ideal choice for Tim, who is looking to address the challenges of converting raw data into contextual information and managing the noise from massive data collections.References:

* &#8220;Cisco Threat Grid: Unify Your Threat Defense,&#8221; Cisco

* &#8220;Integrating and Automating Threat Intelligence,&#8221; by Threat Grid

NO.17 John is a professional hacker who is performing an attack on the target organization where he tries to redirect the connection between the IP address and its target server such that when the users type in the Internet address, it redirects them to a rogue website that resembles the original website. He tries this attack using cache poisoning technique. Identify the type of attack John is performing on the target organization.
* War driving
* Pharming
* Skimming
* Pretexting
Pharming is a cyber attack intended to redirect a website&#8217;s traffic to another, bogus website. By poisoning a DNS server&#8217;s cache, attackers can redirect users from the site they intended to visit to one that is malicious, without the user&#8217;s knowledge or any action on their part, such as clicking a deceptive link. This technique is particularly insidious because it can affect well-intentioned users who type the correct URL into their browsers but are still redirected. War driving involves searching for wireless networks from a moving vehicle, skimming refers to stealing credit card information using a device placed on ATMs or point-of-sale terminals, and pretexting is a form of social engineering where the attacker lies to obtain privileged data.References:The Incident Handler (CREST CPTIA) certification program covers a variety of cyber attacks and techniques, including DNS poisoning and pharming, explaining how attackers exploit vulnerabilities to redirect users to fraudulent sites.

NO.18 Sam. an employee of a multinational company, sends emails to third-party organizations with a spoofed email address of his organization. How can you categorize this type of incident?
* Network intrusion incident
* Inappropriate usage incident
* Unauthorized access incident.
* Denial-of-service incicent
An inappropriate usage incident involves misuse of the organization&#8217;s resources or violations of its acceptable use policies. Sam&#8217;s actions, where he sends emails to third-party organizations with a spoofed email address of his employer, constitute misuse of the organization&#8217;s email system and misrepresentation of the organization. This behavior can harm the organization&#8217;s reputation, violate policy, and potentially lead to legal consequences. Inappropriate usage incidents can range from unauthorized use of systems for personal gain to the dissemination of unapproved content.

References:The Incident Handler (CREST CPTIA) by EC-Council includes discussions on various types of security incidents, emphasizing the importance of addressing and mitigating not just external threats but also internal misuse and policy violations.

NO.19 Sam works as an analyst in an organization named InfoTech Security. He was asked to collect information from various threat intelligence sources. In meeting the deadline, he forgot to verify the threat intelligence sources and used data from an open-source data provider, who offered it at a very low cost. Through it was beneficial at the initial stage but relying on such data providers can produce unreliable data and noise putting the organization network into risk.

What mistake Sam did that led to this situation?

* Sam used unreliable intelligence sources.
* Sam used data without context.
* Sam did not use the proper standardization formats for representing threat data.
* Sam did not use the proper technology to use or consume the information.

Sam&#8217;s mistake was using threat intelligence from sources that he did not verify for reliability. Relying on intelligence from unverified or unreliable sources can lead to the incorporation of inaccurate, outdated, or irrelevant information into the organization&#8217;s threat intelligence program. This can result in &#8220;noise,&#8221; which refers to irrelevant or false information that can distract from real threats, and potentially put the organization&#8217;s network at risk. Verifying the credibility and reliability of intelligence sources is crucial to ensure that the data used for making security decisions is accurate and actionable.References:

* &#8220;Best Practices for Threat Intelligence Sharing,&#8221; by FIRST (Forum of Incident Response and Security Teams)

* &#8220;Evaluating Cyber Threat Intelligence Sources,&#8221; by Jon DiMaggio, SANS Institute InfoSec Reading Room

NO.20 Enrage Tech Company hired Enrique, a security analyst, for performing threat intelligence analysis. While performing data collection process, he used a counterintelligence mechanism where a recursive DNS server is employed to perform interserver DNS communication and when a request is generated from any name server to the recursive DNS server, the recursive DNS servers log the responses that are received. Then it replicates the logged data and stores the data in the central database. Using these logs, he analyzed the malicious attempts that took place over DNS infrastructure.

Which of the following cyber counterintelligence (CCI) gathering technique has Enrique used for data collection?

* Data collection through passive DNS monitoring
* Data collection through DNS interrogation
* Data collection through DNS zone transfer
* Data collection through dynamic DNS (DDNS)

Passive DNS monitoring involves collecting data about DNS queries and responses without actively querying DNS servers, thereby not altering or interfering with DNS traffic. This technique allows analysts to track changes in DNS records and observe patterns that may indicate malicious activity. In the scenario described, Enrique is employing passive DNS monitoring by using a recursive DNS server to log the responses received from name servers, storing these logs in a central database for analysis. This approach is effective for identifying malicious domains, mapping malware campaigns, and understanding threat actors&#8217; infrastructure without alerting them to the fact that they are being monitored. This method is distinct from active techniques such as DNS interrogation or zone transfers, which involve sending queries to DNS servers, and dynamic DNS, which refers to the automatic updating of DNS records.References:

* SANS Institute InfoSec Reading Room, &#8220;Using Passive DNS to Enhance Cyber Threat Intelligence&#8221;

* &#8220;Passive DNS Replication,&#8221; by Florian Weimer, FIRST Conference Presentation

NO.21 Alison, an analyst in an XYZ organization, wants to retrieve information about a company&#8217;s website from the time of its inception as well as the removed information from the target website.

What should Alison do to get the information he needs.

- Alison should use SmartWhois to extract the required website information.
- Alison should use https://archive.org to extract the required website information.
- Alison should run the Web Data Extractor tool to extract the required website information.
- Alison should recover cached pages of the website from the Google search engine cache to extract the required website information.

To retrieve historical information about a company&#8217;s website, including content that may have been removed or altered, Alison should use the Internet Archive&#8217;s Wayback Machine, accessible athttps://archive.org. The Wayback Machine is a digital archive of the World Wide Web and other information on the Internet, providing free access to snapshots of websites at various points in time. This tool is invaluable for researchers and analysts looking to understand the evolution of a website or recover lost information.References:

* &#8220;Using the Wayback Machine for Cybersecurity Research,&#8221; Internet Archive Blogs

* &#8220;Digital Forensics with the Archive&#8217;s Wayback Machine,&#8221; by Jeff Kaplan, Internet Archive

NO.22 Which of the following is a standard framework that provides recommendations for implementing information security controls for organizations that initiate, implement, or maintain information security management systems (ISMSs)?

- ISO/IEC 27002
- ISO/IEC 27035
- PCI DSS
- RFC 219G

ISO/IEC 27002 is a standard that provides best practice recommendations on information security controls for use by those responsible for initiating, implementing, or maintaining information security management systems (ISMSs). It covers areas such as risk assessment, human resource security, operational security, and communications security, among others, providing a framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS. ISO/IEC 27035 pertains to information security incident management, PCI DSS (Payment Card Industry Data Security Standard) deals with the security of cardholder data, and RFC 2196 is a guide for computer security incident response teams (CSIRTs), not a standard for implementing ISMSs.References:The CREST CPTIA curriculum includes the study of various standards and frameworks that support information security management and governance, including ISO/IEC

27002, highlighting its role in guiding organizations in implementing effective security controls.

NO.23 Robert is an incident handler working for Xsecurity Inc. One day, his organization faced a massive cyberattack and all the websites related to the organization went offline. Robert was on duty during the incident and he was responsible to handle the incident and maintain business continuity. He immediately restored the web application service with the help of the existing backups.

According to the scenario, which of the following stages of incident handling and response (IH&R) process does Robert performed?

- Evidence gathering and forensics analysis
- Eradication
- Notification
- Recovery

Restoring web application services with the help of existing backups, as performed by Robert, falls under the Recovery stage of the Incident Handling and Response (IH&R) process. The Recovery stage involves actions taken to return the organization to normal operations after an incident, which includes restoring systems to their operational state using backups, patching vulnerabilities, and ensuring that all systems are clean and secure before being brought back online. This step is crucial for resuming business operations and mitigating the impact of the incident.

NO.24 Eric works as a system administrator in ABC organization. He granted privileged users with unlimited permissions to access the systems. These privileged users can misuse their rights unintentionally or maliciously or attackers can trick them to perform malicious activities.

Which of the following guidelines helps incident handlers to eradicate insider attacks by privileged users?
* Do not use encryption methods to prevent administrators and privileged users from accessing backup tapes and sensitive information
* Do not control the access to administrators and privileged users
* Do not enable the default administrative accounts to ensure accountability
* Do not allow administrators to use unique accounts during the installation process

The guideline that helps incident handlers to eradicate insider attacks by privileged users is to ensure accountability by not enabling default administrative accounts. Instead, organizations should require administrators and privileged users to use individual accounts that can be audited and traced back to specific actions and users. This practice enhances security by ensuring that all actions taken on the system can be attributed to individual users, reducing the risk of misuse of privileges and making it easier to identify the source of malicious activities or policy violations. The other options listed either present insecure practices or misunderstandings of security protocols that would not help in eradicating insider attacks.References:The CREST materials discuss strategies for managing and mitigating the risks associated with privileged users, including the importance of accountability and the controlled use of administrative privileges to prevent insider threats.

NO.25 Eric is an incident responder and is working on developing incident-handling plans and procedures. As part of this process, he is performing an analysis on the organizational network to generate a report and develop policies based on the acquired results. Which of the following tools will help him in analyzing his network and the related traffic?
* Whois
* Burp Suite
* FaceNiff
* Wireshark

Wireshark is a widely used network protocol analyzer that helps in capturing and interactively browsing the traffic on a network. It is an essential tool for incident responders like Eric who are developing incident- handling plans and procedures. By analyzing network traffic, Wireshark allows users to see what is happening on their network at a microscopic level, making it invaluable for troubleshooting network problems, analyzing security incidents, and understanding network behavior. Whois is used for querying databases that store registered users or assignees of an Internet resource. Burp Suite is a tool for testing web application security, and FaceNiff is used for session hijacking within a WiFi network, which makes Wireshark the best choice for analyzing network traffic.References:CREST materials often reference Wireshark as a fundamental tool for network analysis, crucial for incident handlers in the analysis phase of incident response.

NO.26 Oscar receives an email from an unknown source containing his domain name oscar.com. Upon checking the link, he found that it contains a malicious URL that redirects to the website evilsite.org. What type of vulnerability is this?
* Malware
* Bolen
* Unvalidated redirects and forwards
* SQL injection

The scenario described, where Oscar receives an email with a link that contains a malicious URL redirecting to evilsite.org, exemplifies a vulnerability related to unvalidated redirects and forwards. This type of vulnerability occurs when a web application accepts untrusted input thatcould cause the web application to redirect the request to a URL contained within untrusted input. Attackers can exploit this vulnerability by crafting a malicious URL that leads unsuspecting users to phishing sites or other malicious websites, under the guise of a legitimate domain. This is distinct from malware, which refers to malicious software; SQL injection, which involves inserting malicious SQL queries through input fields to manipulate or exploit databases; and is not a term related to cybersecurity vulnerabilities.References:The Incident Handler (CREST CPTIA) certification materials often cover web application vulnerabilities, including unvalidated redirects and forwards, emphasizing the need for proper validation and sanitization of user input to prevent such exploits.

NO.27 Johnson an incident handler is working on a recent web application attack faced by the organization. As part of this process, he performed data preprocessing in order to analyzing and detecting the watering hole attack. He preprocessed the outbound network traffic data collected from firewalls and proxy servers and started analyzing the user activities within a certain time period to create time-ordered domain sequences to perform further analysis on sequential patterns.

Identify the data-preprocessing step performed by Johnson.
* Filtering invalid host names
* Identifying unpopular domains
* Host name normalization
* User-specific sessionization
The data preprocessing step performed by Johnson, where he analyzes user activities within a certain time period to create time-ordered domain sequences for further analysis on sequential patterns, is known as user- specific sessionization. This process involves aggregating all user activities and requests into discrete sessions based on the individual user, allowing for a coherent analysis of user behavior over time. This is critical for identifying patterns that may indicate a watering hole attack, where attackers compromise a site frequently visited by the target group to distribute malware. User-specific sessionization helps in isolating and examining sequences of actions taken by users, making it easier to detect anomalies or patterns indicative of such an attack.References:The CREST materials discuss various data preprocessing techniques used in the analysis of cyber attacks, including the concept of sessionization to better understand user behavior and detect threats.

NO.28 Sam received an alert through an email monitoring tool indicating that their company was targeted by a phishing attack. After analyzing the incident, Sam identified that most of the targets of the attack are high- profile executives of the company. What type of phishing attack is this?
* Pharming
* Whaling
* Puddle phishing
* Spear phishing
Whaling is a specific type of phishing attack that targets high-profile executives or individuals within an organization, often with the intent to steal sensitive information or gain access to their accounts for financial fraud. The term &#8220;whaling&#8221; is used because it targets the &#8220;big fish&#8221; of an organization. Given that Sam identified the targets of the attack as high-profile executives, the described scenario is indicative of a whaling attack.

References:The CREST CPTIA curriculum includes a section on different types of phishing attacks, including whaling, emphasizing the strategies attackers use to target individuals based on their roles within an organization.

NO.29 A team of threat intelligence analysts is performing threat analysis on malware, and each of them has come up with their own theory and evidence to support their theory on a given malware.

Now, to identify the most consistent theory out of all the theories, which of the following analytic processes must threat intelligence manager use?
* Threat modelling
* Application decomposition and analysis (ADA)
* Analysis of competing hypotheses (ACH)
* Automated technical analysis
Analysis of Competing Hypotheses (ACH) is an analytic process designed to help an analyst or a team of analysts evaluate multiple competing hypotheses on an issue fairly and objectively. ACH assists in identifying and analyzing the evidence for and against each hypothesis, ultimately aiding in determining the most likely explanation. In the scenario where a team of threat intelligence analysts has various theories on a particular malware, ACH would be the most appropriate method to assess these competing theories systematically. ACH involves listing all possible hypotheses, collecting data and evidence, and assessing the evidence&#8217;s consistency with each hypothesis. This process helps in minimizing cognitive biases and making a more informed decision on the most consistent theory.References:

* Richards J. Heuer Jr., &#8220;Psychology of Intelligence Analysis,&#8221; Central Intelligence Agency

* &#8220;A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis,&#8221; Central Intelligence Agency

NO.30 An analyst is conducting threat intelligence analysis in a client organization, and during the information gathering process, he gathered information from the publicly available sources and analyzed to obtain a rich useful form of intelligence. The information source that he used is primarily used for national security, law enforcement, and for collecting intelligence required for business or strategic decision making.

Which of the following sources of intelligence did the analyst use to collect information?
* OPSEC
* ISAC
* OSINT
* SIGINT
The analyst used Open Source Intelligence (OSINT) to gather information from publicly available sources.

OSINT involves collecting and analyzing information from publicly accessible sources to produce actionable intelligence. This can include media reports, public government data, professional and academic publications, and information available on the internet. OSINT is widely used for national security, law enforcement, and business intelligence purposes, providing a rich source of information for making informed decisions and understanding the threat landscape.References:

* &#8220;Open Source Intelligence (OSINT) Tools and Techniques,&#8221; by SANS Institute

* &#8220;The Role of OSINT in Cybersecurity and Threat Intelligence,&#8221; by Recorded Future

NO.31 Tracy works as a CISO in a large multinational company. She consumes threat intelligence to understand the changing trends of cyber security. She requires intelligence to understand the current business trends and make appropriate decisions regarding new technologies, security budget, improvement of processes, and staff.

The intelligence helps her in minimizing business risks and protecting the new technology and business initiatives.

Identify the type of threat intelligence consumer is Tracy.
* Tactical users
* Strategic users
* Operational users
* Technical users
Tracy, as a Chief Information Security Officer (CISO), requires intelligence that aids in understanding broader business and cybersecurity trends, making informed decisions regarding new technologies, security budgets, process improvements, and staffing. This need aligns with the role of a strategic user of threat intelligence. Strategic users leverage intelligence to guide long-term planning and decision-making, focusing on minimizing business risks and safeguarding against emerging threats to new technology and business initiatives. This type of intelligence is less about the technical specifics of individual threats and more about understanding the overall threat landscape, regulatory environment, and industry trends to inform high-level strategy and policy.References:

* &#8220;The Role of Strategic Intelligence in Cybersecurity,&#8221; Journal of Cybersecurity Education, Research and Practice

* &#8220;Cyber Threat Intelligence and the Lessons from Law Enforcement,&#8221; by Robert M. Lee and David Bianco, SANS Institute Reading Room

NO.32 Which of the following is an attack that occurs when a malicious program causes a user&#8217;s browser to perform an unwanted action on a trusted site for which the user is currently authenticated?
* Cross-site scripting
* Insecure direct object references
* Cross-site request forgery
* SQL injection
Cross-site request forgery (CSRF or XSRF) is an attack that tricks the victim&#8217;s browser into executing unauthorized actions on a website where they are currently authenticated. In this scenario, the attacker exploits the trust that a site has in the user&#8217;s browser, effectively forcing the browser to perform actions without the user&#8217;s knowledge or consent. For example, if the user is logged into their bank&#8217;s website, an attacker could craft a malicious request to transfer funds without the user&#8217;s direct interaction. CSRF attacks rely on authenticated sessions and typically target state-changing requests to compromise user or application data.

References:The Certified Incident Handler (CREST CPTIA) curriculum by EC-Council discusses various web-based attacks, including CSRF, detailing their mechanisms, implications, and preventive measures to safeguard against such threats.

Get Top-Rated CREST CPTIA Exam Dumps Now: https://www.topexamcollection.com/CPTIA-vce-collection.html]