Eccouncil

(112-57)

Digital Forensics Essentials (DFE)

Total: **75 Questions**

Link:

MYEXAM.FR

behavior.

Key Characteristics Supporting the Choice of C. Honeypot:

Deception: Presents fake valuable resources.
Monitoring: Capable of detailed logging of attacker interactions.
Security Intelligence: Primary goal is to gather information on attack vectors and techniques.

References

1. **Honeypot Wikipedia Page** - For a comprehensive overview of Honeypots, their types, and uses: https://en.wikipedia.org/wiki/Honeypot_(computing)
2. **SANS Institute on Honeypots** - For detailed technical insights and deployment strategies: https://www.sans.org/securityawareness-training/what-is-honeypot/

Question: 4

Which of the following acts was passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

A. Information Privacy Act 2014
B. General Data Protection Regulation (GDPR)
C. Sarbanes-Oxley Act (SOX)
D. The Electronic Communications Privacy Act

Answer: C

Explanation:

Technical Justification for Correct Answer: C - Sarbanes-Oxley Act (SOX)

The correct answer is **C, Sarbanes-Oxley Act (SOX)**, for the following reasons:

Relevance to the Question's Context: The Sarbanes-Oxley Act was specifically enacted to protect investors by ensuring the transparency and reliability of corporate financial reporting, thereby safeguarding against fraudulent accounting practices.
Year of Enactment: SOX was indeed passed by the U.S. Congress in 2002, aligning perfectly with the question's timeframe.
Purpose and Scope: SOX's primary goals include enhancing corporate accountability, and providing measures to prevent and detect financial fraud, directly addressing the question's concern about protecting investors from fraudulent accounting activities.

Why Other Options are Less Suitable:

A. Information Privacy Act 2014:

Incorrect Year: Enacted in 2014, far surpassing the 2002 timeframe specified in the question.
Focus: Primarily concerned with privacy rather than financial reporting and fraud prevention.
B. General Data Protection Regulation (GDPR):

Jurisdiction: A regulation of the European Union, not a U.S. Congressional act.
Purpose: Focuses on data protection and privacy, not specifically on preventing corporate financial fraud.
D. The Electronic Communications Privacy Act:

protecting the confidentiality and integrity of the data transmitted through the tunnel, which is essential for content obfuscation.

References

1. **SSH Protocol Specification**: For detailed insights into SSH's security features, visit https://tools.ietf.org/html/rfc4253
2. **Understanding Encryption in Secure Shell**: Learn more about SSH encryption at https://www.ssh.com/ssh/encryption

Question: 7

Sandra, a hacker, targeted Johana, a software professional, to steal her banking details. She started sending frequent, random pop-up messages with malicious links to her social media page. Johana accidentally clicked on a link, causing a malicious program to get installed in her system. Subsequently, when Johana attempted to access her banking website, the URL directed her to a malicious website controlled by Sandra. Johana entered her banking credentials on the fake website, which Sandra than captured.
Identify the type of attack performed by Sandra on Johana.

A. Tailgating
B. Dumpster diving
C. Shoulder surfing
D. Pharming

Answer: D

Explanation:

Technical Justification for Correct Answer: D. Pharming

Sandra's attack on Johana is best classified as **Pharming**, making option **D** the correct answer. Here's why:

Pharming involves redirecting a user to a fake website, often by exploiting vulnerabilities in the DNS system or the victim's local environment (e.g., through malware), to capture sensitive information. In this scenario, after Johana's system was compromised with a malicious program (via a clicked link in a pop-up message), attempting to access her banking website redirected her to a malicious, fake version controlled by Sandra. This redirection, facilitated by malware on Johana's system (a form of pharming known as "DNS spoofing" at the client level), aligns perfectly with the definition of Pharming.

Why Other Options are Less Suitable:

A. Tailgating: This refers to the unauthorized access to a secure area by following an authorized person, typically in a physical context. Since the scenario is entirely digital and involves no physical access, Tailgating is not applicable.
B. Dumpster Diving: Involves physically rummaging through trash for sensitive information. This option is irrelevant as the attack was conducted digitally without any physical component.
C. Shoulder Surfing: Refers to observing a person's screen or keypad to gather information. Given the digital nature of the attack and the lack of indication that Sandra was physically present to observe Johana, Shoulder Surfing does not fit.

Detailed Breakdown of the Attack Process Supporting the Answer:

Initial Vector: Malicious links in pop-up messages (Social Engineering/Phishing attempt).

processes, allowing targeted communication.
Connection Establishment and Management: The Transport layer establishes, maintains, and terminates connections between applications running on the source and destination devices, which is crucial for sustained data exchange.

Why Other Options are Less Suitable:

B. Internet layer: While critical for routing data between networks, the Internet layer (IP layer) focuses on logical addressing and routing of packets across different networks, not on the peer-to-peer communication of specific applications or ensuring reliable data flow between them.
C. Application layer: This layer is responsible for services and interfaces for user applications (e.g., HTTP, FTP), but it does not directly manage the flow of data between devices in the way the Transport layer does. It relies on lower layers for data transfer mechanisms.
D. Network access layer: This layer (combining Data Link and Physical layers in the TCP/IP model) deals with physical network access, framing, and error detection for individual network segments. It does not handle end-to-end data flow or application-level communication across the network.

References

For detailed insights into the TCP/IP model and the role of the Transport layer, refer to RFC 2600 - Internet Protocol Encyclopedia.
Explore the protocol suite in depth at IETF (Internet Engineering Task Force) - specifically, documents related to TCP (e.g., RFC 793) and UDP (e.g., RFC 768).

Question: 11

In which of the following malware distribution techniques does the attacker use tactics such as keyword stuffing, doorway pages, page swapping, and adding unrelated keywords to improve the search-engine ranking of their malware pages?

A. Blac-khat search-engine optimization
B. Drive-by downloads
C. Social-engineered clickjacking
D. Spearphishing sites

Answer: A

Explanation:

Here is a structured technical justification for the correct answer in paragraph and bullet point formats, followed by references:

Technical Justification for Correct Answer: A. Blackhat search-engine optimization

The correct answer is A. Blackhat search-engine optimization (SEO) because this technique specifically involves manipulating search engine rankings through deceptive methods to increase the visibility of malicious content. The tactics mentioned (keyword stuffing, doorway pages, page swapping, and adding unrelated keywords) are hallmark techniques of blackhat SEO, aimed at tricking search engines into ranking the malware pages higher.

Why A is the Best Choice:

Direct Alignment: The mentioned tactics (keyword stuffing, doorway pages, page swapping, adding unrelated

Why Other Options Are Less Suitable:

A. ProcDump: Primarily used for capturing the memory contents of a running process, ProcDump is more suited for analyzing the state of applications or services rather than enumerating or managing connected storage devices. Its functionality does not align with James's task of identifying external storage devices.

C. ESEDatabaseView: Designed to view and export data from ESE (Extensible Storage Engine) databases, this tool is relevant when investigating database contents (common in email clients, Windows Search, and other applications using ESE for storage). It has no direct application in listing or managing connected external storage devices.

D. PromiscDetect: This tool is used to detect if a network interface is operating in promiscuous mode, which is relevant in network security audits to identify potential sniffing activities. While useful in a broader network forensic context, it does not serve the purpose of identifying connected external storage devices to a local machine.

References

DriveLetterView by NirSoft: https://www.nirsoft.net/utils/drive_letter_view.html
Overview of NirSoft Tools for Forensic Purposes: https://www.nirsoft.net_FORENSICSOFTWARE.htm (Note: The exact link for the overview might not be directly available as described; NirSoft's main page https://www.nirsoft.net/ is provided for accessing various tool descriptions, including their forensic applications.)

Corrected Reference for Clarity (since the second link was improperly specified)

References

DriveLetterView by NirSoft: https://www.nirsoft.net/utils/drive_letter_view.html
NirSoft Main Page (for accessing various tool descriptions): https://www.nirsoft.net/

Question: 15

Kelly, a professional hacker, used her laptop to perform illegal cyber activities for monetary gain on many victims. She securely locked her laptop using BitLocker software. Using this tool, she locked an entire volume using a secret key to deny access to the system.
Identify the anti-forensic technique used by Don in the above scenario.

A. Artifact wiping
B. Trail obfuscation
C. File carving
D. Encryption

Answer: D

Explanation:

Technical Justification for Correct Answer: D. Encryption

The correct answer is **D. Encryption**. Here's why:

Why D. Encryption is correct: In the scenario, Kelly used BitLocker software to "securely lock her laptop" and "locked an entire volume using a secret key to deny access to the system". This directly points to the use of **full-disk encryption** as the anti-forensic technique. BitLocker is a well-known full-disk encryption tool that

Question: 18

Given below is a regex signature used by security professionals for detecting an XSS attack:
/((\%3C)|<)[^\n]+((\%3E)|>)/|
Which of the following types of XSS attack does the above regex expression detect?

A. In-line comment XSS attack
B. HTML tags-based XSS attempt
C. Simple XSS attack
D. CSS attack

Answer: B

Explanation:

Technical Justification for Correct Answer: B. HTML tags-based XSS attempt

The provided regex signature /((\%3C)|<)[^\n]+((\%3E)|>)/ is designed to detect HTML tags-based XSS attempts. Here's a breakdown of why it's the most suitable choice for this type of attack and why other options are less suitable:

Why B (HTML tags-based XSS attempt) is correct:

Matching HTML Tags: The regex specifically looks for the presence of HTML tags, which are the backbone of HTML tags-based XSS attacks.

(\%3C)|< matches either the URL-encoded < (%3C) or the < character itself, indicating the start of an HTML tag.
([^\n]+) matches any character (except a newline) one or more times, capturing the content within the tags.
(\%3E)|> matches either the URL-encoded > (%3E) or the > character, marking the end of an HTML tag.
Detection Logic: By identifying strings that start with <, contain arbitrary non-newline characters, and end with >, the regex effectively detects attempts to inject HTML tags, which is a hallmark of HTML tags-based XSS attacks.

Why Other Options are Less Suitable:

A. In-line Comment XSS Attack:

Non-Matching Pattern: In-line comment XSS attacks typically involve injecting comments (<!--) followed by malicious code. The regex does not specifically target comment tags or the structure associated with in-line comment XSS.
Lack of Specificity for Comments: The broad match for any tag content ([^\n]+) doesn't uniquely identify comment-based attacks without additional context (e.g., <!--).

C. Simple XSS Attack:

Overly Broad Interpretation: "Simple XSS attack" is too vague, as XSS attacks can be simple in various forms (e.g., injecting <script>, <img>, etc.). While this regex does detect a form of simple XSS (by detecting HTML tags), the term "Simple XSS" doesn't precisely define the detected pattern's specificity for HTML tag injection.
Lacks Specific Technical Alignment: The term doesn't technically align with the regex's specific focus on detecting the presence of HTML tags, which is more precisely described by option B.

D. CSS Attack:

files present on the system at any given time.
C. $volume: This file contains metadata about the volume itself, such as the volume label, file system version, and the location of critical filesystem structures. It does not list all files on the system.
D. $quota: This file is used to store quota information for users on the filesystem, if quotas are enabled. It is unrelated to maintaining a comprehensive list of files.

Key Technical Points Supporting B. $mft:

Comprehensive Index: $mft acts as a master index.
Self-Describing Records: Each entry contains detailed file information.
Essential for File System Operation: Without $mft, the filesystem cannot accurately locate or manage its contents.

References:

Microsoft Documentation - NTFS File System (Search for "Master File Table" within the page for relevant details)
NTFS $MFT Details on Forensics Wiki (Provides in-depth insights into the $mft structure and its forensic implications)

Question: 21

Alice and John are close college friends. Alice frequently sends emails to John attaching her pies with friends. One day, Alice sent an email to John describing all the details related to the final year project without specifying the actual purpose. John missed the message as he frequently receives emails from her and did not arrive for a project seminar.
Which of the following email fields could Alice have used in the above scenario to highlight the importance of the email?

A. Bcc
B. Date
C. Subject
D. Cc

Answer: C

Explanation:

Technical Justification for Correct Answer: C. Subject

In the given scenario, Alice needed to convey the importance of an email to John, who often overlooks her messages due to their frequency. The most effective email field for highlighting the importance or drawing attention to a specific email among those received is the **Subject** line. Here's why **C. Subject** is the correct choice and why other options are less suitable:

C. Subject:

Correctness Reason: The Subject line is designed to provide a concise summary or indicator of the email's content and importance. Alice could have used keywords like "URGENT", "FINAL YEAR PROJECT DETAILS", or "PROJECT SEMINAR REMINDER" in the Subject line to immediately convey the email's significance, prompting John to open it promptly.
Effectiveness: Directly influences the recipient's decision to open an email, making it ideal for signaling importance.