**Vendor:**Pegasystems

**Exam Code:**312-39

**Exam Name:**Certified SOC Analyst (CSA)

**Version:**Demo

**QUESTION 1**

Which of the following fields in Windows logs defines the type of event occurred, such as Correlation Hint, Response Time, SQM, WDI Context, and so on?

A. Keywords

B. Task Category

C. Level

D. Source

Correct Answer: A

---

**QUESTION 2**

Which of the following Windows features is used to enable Security Auditing in Windows?

A. Bitlocker

B. Windows Firewall

C. Local Group Policy Editor

D. Windows Defender

Correct Answer: C

Reference: https://resources.infosecinstitute.com/topic/how-to-audit-windows-10-application-logs/

---

**QUESTION 3**

Identify the attack, where an attacker tries to discover all the possible information about a target network before launching a further attack.

A. DoS Attack

B. Man-In-Middle Attack

C. Ransomware Attack

D. Reconnaissance Attack

Correct Answer: D

Reference: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101july2017.pdf

---

**QUESTION 4**

Identify the attack in which the attacker exploits a target system through publicly known but still unpatched vulnerabilities.

A. Slow DoS Attack

B. DHCP Starvation

C. Zero-Day Attack

D. DNS Poisoning Attack

Correct Answer: C

Reference: https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/what-arezero-day-attacks.aspx

---

**QUESTION 5**

Banter is a threat analyst in Christine Group of Industries. As a part of the job, he is currently formatting and structuring the raw data.

He is at which stage of the threat intelligence life cycle?

A. Dissemination and Integration

B. Processing and Exploitation

C. Collection

D. Analysis and Production

Correct Answer: B

Reference: https://socradar.io/5-stages-of-the-threat-intelligence-lifecycle/

---

**QUESTION 6**

What is the process of monitoring and capturing all data packets passing through a given network using different tools?

A. Network Scanning

B. DNS Footprinting

C. Network Sniffing

D. Port Scanning

Correct Answer: C

Reference: https://www.greycampus.com/opencampus/ethical-hacking/sniffing-and-its-types

---

**QUESTION 7**

Which of the following is a Threat Intelligence Platform?

A. SolarWinds MS

B. TC Complete

C. Keepnote

D. Apility.io

Correct Answer: A

Reference: https://www.esecurityplanet.com/products/threat-intelligence-platforms/

**QUESTION 8**

Mike is an incident handler for PNP Infosystems Inc. One day, there was a ticket raised regarding a critical incident and Mike was assigned to handle the incident. During the process of incident handling, at one

stage, he has performed incident analysis and validation to check whether the incident is a true incident or a false positive.

Identify the stage in which he is currently in.

A. Post-Incident Activities

B. Incident Recording and Assignment

C. Incident Triage

D. Incident Disclosure

Correct Answer: B

**QUESTION 9**

John, a SOC analyst, while monitoring and analyzing Apache web server logs, identified an event log matching Regex /(\.|(%|%25)2E)(\.|(%|%25)2E)(\/|(%|%25)2F|\\|(%|%25)5C)/i.

What does this event log indicate?

A. XSS Attack

B. SQL injection Attack

C. Directory Traversal Attack

D. Parameter Tampering Attack

Correct Answer: A

---

**QUESTION 10**

Which of the following data source will a SOC Analyst use to monitor connections to the insecure ports?

A. Netstat Data

B. DNS Data

C. IIS Data

D. DHCP Data

Correct Answer: A

---

**QUESTION 11**

Charline is working as an L2 SOC Analyst. One day, an L1 SOC Analyst escalated an incident to her for further investigation and confirmation. Charline, after a thorough investigation, confirmed the incident and assigned it with an initial priority.

What would be her next action according to the SOC workflow?

A. She should immediately escalate this issue to the management

B. She should immediately contact the network administrator to solve the problem

C. She should communicate this incident to the media immediately

D. She should formally raise a ticket and forward it to the IRT

Correct Answer: B

---

**QUESTION 12**

An attacker, in an attempt to exploit the vulnerability in the dynamically generated welcome page, inserted

code at the end of the company\\'s URL as follows:

http://technosoft.com.com/alert("WARNING: The application has encountered an error");.

Identify the attack demonstrated in the above scenario.

A. Cross-site Scripting Attack

B. SQL Injection Attack

C. Denial-of-Service Attack

D. Session Attack

Correct Answer: D