# Free Questions for 312-39 by actualtestdumps

## Shared by Vazquez on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

**Question Type:** **MultipleChoice**

The threat intelligence, which will help you, understand adversary intent and make informed decision to ensure appropriate security in alignment with risk.

What kind of threat intelligence described above?

## Options:

**A-** Tactical Threat Intelligence

**B-** Strategic Threat Intelligence

**C-** Functional Threat Intelligence

**D-** Operational Threat Intelligence

## Answer:

B

# Question 2

**Question Type:** MultipleChoice

Which of the following Windows Event Id will help you monitors file sharing across the network?

## Options:

**A-** 7045

**B-** 4625

**C-** 5140

**D-** 4624

## Answer:

C

# Question 3

**Question Type:** MultipleChoice

Jane, a security analyst, while analyzing IDS logs, detected an event matching Regex /((\%3C)|)/|.

What does this event log indicate?

## Options:

**A-** Directory Traversal Attack

**B-** Parameter Tampering Attack

**C-** XSS Attack

**D-** SQL Injection Attack

## Answer:

C

## Explanation:

%253C)%7C<)((%5C%2569)%7Ci%7C(%5C%2549))((%5C%256D)%7Cm%7C(%5C%254D))((%5C%2567)%7Cg%7C(%5C%2547))%5B%5E%5Cn%5D%2B((%5C%253E)%7C>)/%

7C&source=bl&ots=kOBHNfJmtq&sig=ACfU3U2CG_hELc1HMb1chdc9OS4ooXPlMg&hl=en&sa=X&ved=2ahUKEwjYwJmlt_buAhUFShUIHTBNAs8Q6AEwBXoECAUQAw#v=onepage&q&f=false

## Question 4

**Question Type:** **MultipleChoice**

In which of the following incident handling and response stages, the root cause of the incident must be found from the forensic results?

### Options:

**A-** Evidence Gathering

**B-** Evidence Handling

**C-** Eradication

**D-** Systems Recovery

### Answer:

A

## Question 5

**Question Type:** **MultipleChoice**

Which of the following formula represents the risk levels?

## Options:

**A-** Level of risk = Consequence Severity

**B-** Level of risk = Consequence Impact

**C-** Level of risk = Consequence Likelihood

**D-** Level of risk = Consequence Asset Value

## Answer:

C

# Question 6

**Question Type: MultipleChoice**

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/. Identify the attack demonstrated in the above scenario.

## Options:

**A-** Cross-site Scripting Attack

**B-** SQL Injection Attack

**C-** Denial-of-Service Attack

**D-** Session Attack

## Answer:

A

# Question 7

**Question Type: MultipleChoice**

Wesley is an incident handler in a company named Maddison Tech. One day, he was learning techniques for eradicating the insecure deserialization attacks.

What among the following should Wesley avoid from considering?

### Options:

**A-** Deserialization of trusted data must cross a trust boundary

**B-** Understand the security permissions given to serialization and deserialization

**C-** Allow serialization for security-sensitive classes

**D-** Validate untrusted input, which is to be serialized to ensure that serialized data contain only trusted classes

### Answer:

C

## Question 8

**Question Type: MultipleChoice**

What is the correct sequence of SOC Workflow?

### Options:

**A-** Collect, Ingest, Validate, Document, Report, Respond

**B-** Collect, Ingest, Document, Validate, Report, Respond

**C-** Collect, Respond, Validate, Ingest, Report, Document

**D-** Collect, Ingest, Validate, Report, Respond, Document

### Answer:

D

## Question 9

**Question Type:** **MultipleChoice**

Jason, a SOC Analyst with Maximus Tech, was investigating Cisco ASA Firewall logs and came across the following log entry:

May 06 2018 21:27:27 asa 1: %ASA -5 -- 11008: User 'enable_15' executed the 'configure term' command What does the security level in the above log indicates?

### Options:

**A-** Warning condition message

**B-** Critical condition message

**C-** Normal but significant message

**D-** Informational message

### Answer:

C

## Question 10

**Question Type:** **MultipleChoice**

According to the Risk Matrix table, what will be the risk level when the probability of an attack is very high, and the impact of that attack is major?

NOTE: It is mandatory to answer the question before proceeding to the next one.

### Options:

**A-** High

**B-** Extreme

**C-** Low

**D-** Medium

### Answer:

A

### Explanation:

special_issue

simple_characterisations_and_communication_of_risks.htm

## Question 11

**Question Type:** **MultipleChoice**

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?

### Options:

**A-** XSS Attack

**B-** SQL injection Attack

**C-** Directory Traversal Attack

**D-** Parameter Tampering Attack

### Answer:

C

## Question 12

**Question Type:** **MultipleChoice**

Daniel is a member of an IRT, which was started recently in a company named Mesh Tech. He wanted to find the purpose and scope of the planned incident response capabilities.

What is he looking for?

### Options:

**A-** Incident Response Intelligence

**B-** Incident Response Mission

**C-** Incident Response Vision

**D-** Incident Response Resources

## Answer:

B