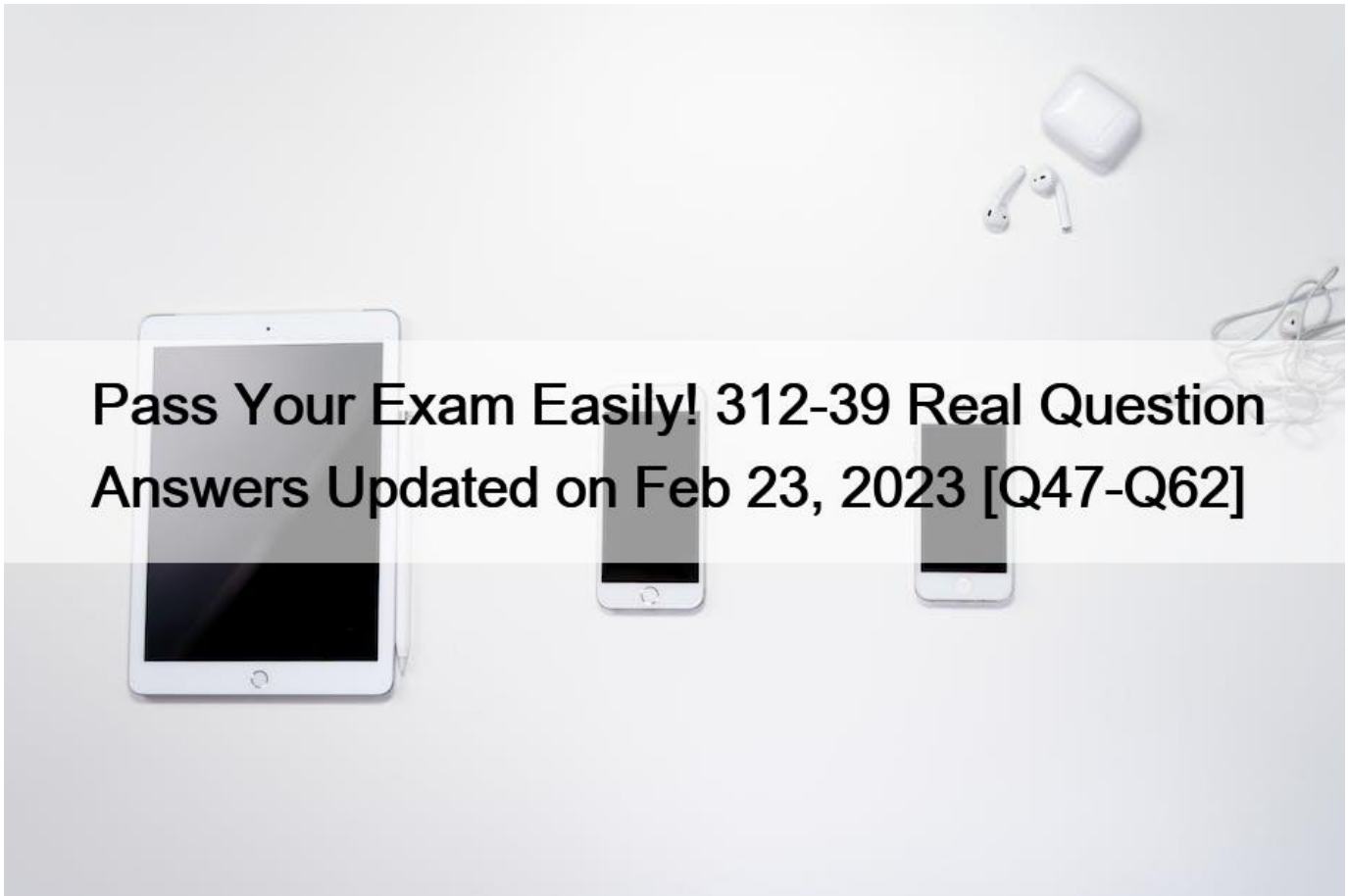


## Pass Your Exam Easily! 312-39 Real Question Answers Updated on Feb 23, 2023 [Q47-Q62]



**Pass Your Exam Easily! 312-39 Real Question Answers Updated on Feb 23, 2023 Actual Questions Answers Pass With Real 312-39 Exam Dumps NO.47** If the SIEM generates the following four alerts at the same time:

I.Firewall blocking traffic from getting into the network alerts

II.SQL injection attempt alerts

III.Data deletion attempt alerts

IV.Brute-force attempt alerts

Which alert should be given least priority as per effective alert triaging?

- \* III
- \* IV
- \* II
- \* I

**NO.48** 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?

- \* Incident Response Intelligence
- \* Incident Response Mission
- \* Incident Response Vision
- \* Incident Response Resources

#### Define IR Vision and Mission

CISA  
Certified Incident Response Analyst



**NO.49** Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?

- \* Windows Event Log
- \* Web Server Logs
- \* Router Logs
- \* Switch Logs

**NO.50** Which of the following is a Threat Intelligence Platform?

- \* SolarWinds MS
- \* TC Complete
- \* Keepnote
- \* Apility.io

**NO.51** An organization wants to implement a SIEM deployment architecture. However, they have the capability to do only log collection and the rest of the SIEM functions must be managed by an MSSP.

Which SIEM deployment architecture will the organization adopt?

- \* Cloud, MSSP Managed
- \* Self-hosted, Jointly Managed
- \* Self-hosted, MSSP Managed
- \* Self-hosted, Self-Managed

**NO.52** Which of the following process refers to the discarding of the packets at the routing level without informing the source that the data did not reach its intended recipient?

- \* Load Balancing
- \* Rate Limiting
- \* Black Hole Filtering

\* Drop Requests

**NO.53** Which of the following directory will contain logs related to printer access?

- \* /var/log/cups/Printer\_log file
- \* /var/log/cups/access\_log file
- \* /var/log/cups/accesslog file
- \* /var/log/cups/Printeraccess\_log file

Explanation

Graphical user interface Description automatically generated with low confidence

Mac Log Files



Log file	Location	Description
crashreporter.log	/var/log/crashreporter.log	Application usage history and application crash information written to this file
access_log	/var/log/cups/access_log	Printer access log information
error_log	/var/log/cups/error_log	Printer connection information and its error logs found here
daily.out	/var/log/daily.out	Network Interface History
log.nmbd	/var/log/samba/log.nmbd	Samba (Windows-based machine) connection information
Logs	~/Library/Logs	Home directory users and application-specific logs can found here
DiscRecording.log	~/Library/Logs/DiscRecording.log	Home users' CD & DVD media burning logs written to this file
DiskUtility.log	~/Library/Logs/DiskUtility.log	This file contains hard disk partitioning logs, CD/DVD burned media logs, ISO/DMG images files mount, unmount history, and file permission repair history
iChatConnectionErrors	/Library/Logs/iChatConnectionErrors	Log history of iChat connection attempts. Data such as username, IP address, and Date & Time of the attempt
Sync	/Library/Logs/Sync	This log file gives information on synchronized Mac systems and mobile devices such as cell phones and iPods, and their activities with date and time

**NO.54** Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.

- \* Dictionary Attack
- \* Rainbow Table Attack
- \* Bruteforce Attack
- \* Syllable Attack

**NO.55** Which of the following formula represents the risk levels?

- \* Level of risk = Consequence \* Severity
- \* Level of risk = Consequence \* Impact
- \* Level of risk = Consequence \* Likelihood
- \* Level of risk = Consequence \* Asset Value

**NO.56** Which of the following attack can be eradicated by converting all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums?

- \* Broken Access Control Attacks
- \* Web Services Attacks
- \* XSS Attacks
- \* Session Management Attacks

**NO.57** Which of the log storage method arranges event logs in the form of a circular buffer?

- \* FIFO
- \* LIFO
- \* non-wrapping
- \* wrapping

There are two ways of arranging the event records:

- **Nonwrapping method:** In this method, the oldest record is inserted just after the event log header and new records are inserted just before the ELF\_EOF\_RECORD. In the below example, event records are organized as per the nonwrapping method:

```
HEADER      (ELF_LOGFILE_HEADER)
EVENT RECORD 1 (EVENT_RECORD)
EVENT RECORD 2 (EVENTLOGRECORD)
EVENT RECORD 3 (ELF_EOF_RECORD)
```

Nonwrapping can perform every time when the event log is generated or deleted. The event log records continue to organize as per nonwrapping until the event log size reaches its maximum limit. The event log size is depending either upon the MaxSize configuration value or the number of system resources. When the event log size reaches to its last limit, then it will start using wrapping.

- **Wrapping method:** In this method, event logs are arranged in the form of a circular buffer. It replaces the oldest event logs by the new event logs. Consider the below example to understand wrapping method:

```
HEADER      (ELF_LOGFILE_HEADER)
```

**NO.58** Which of the following can help you eliminate the burden of investigating false positives?

- \* Keeping default rules
- \* Not trusting the security devices
- \* Treating every alert as high level
- \* Ingesting the context data

#### Eliminating False Positives (Cont'd)



6 Choose SIEM that should ingest context data. Ingesting context data can help reduce/reasonable false positives

7 Trust security devices in place. The alerts are raised as firewall blocks certain traffic from getting into the network. For this type of alert, you don't need to investigate

8 Define low level alerts for your environment and ignore them

9 Tune your rules on periodic basis

**NO.59** Robin, a SOC engineer in a multinational company, is planning to implement a SIEM. He realized that his organization is capable of performing only Correlation, Analytics, Reporting, Retention, Alerting, and Visualization required for the SIEM implementation and has to take collection and aggregation services from a Managed Security Services Provider (MSSP).

What kind of SIEM is Robin planning to implement?

- \* Self-hosted, Self-Managed
- \* Self-hosted, MSSP Managed
- \* Hybrid Model, Jointly Managed

\* Cloud, Self-Managed

**NO.60** Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.

i	Time	Event
>	2/7/19 5:47:29.000 PM	2019-02-07 12:17:29 10.10.10.12 GET /OrderDetail.aspx?id=ORD-001117 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 191 cs_uri_query = id-ORD-001117   host = WinServer2012   source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log   sourcetype = iis
>	2/7/19 5:47:25.000 PM	2019-02-07 12:17:25 10.10.10.12 GET /OrderDetail.aspx?id=ORD-001116 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 133 cs_uri_query = id-ORD-001116   host = WinServer2012   source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log   sourcetype = iis
>	2/7/19 5:47:21.000 PM	2019-02-07 12:17:21 10.10.10.12 GET /OrderDetail.aspx?id=ORD-001115 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 207 cs_uri_query = id-ORD-001115   host = WinServer2012   source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log   sourcetype = iis
>	2/7/19 5:47:16.000 PM	2019-02-07 12:17:16 10.10.10.12 GET /OrderDetail.aspx?id=ORD-001114 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 173 cs_uri_query = id-ORD-001114   host = WinServer2012   source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log

What does this event log indicate?

- \* Directory Traversal Attack
- \* XSS Attack
- \* SQL Injection Attack
- \* Parameter Tampering Attack

**NO.61** What does [-n] in the following checkpoint firewall log syntax represents?

fw log [-f [-t]] [-n] [-l] [-o] [-c action] [-h host] [-s starttime] [-e endtime] [-b starttime endtime] [-u unification\_scheme\_file] [-m unification\_mode(initial|semi|raw)] [-a] [-k (alert name|all)] [-g] [logfile]

- \* Display both the date and the time for each log record
- \* Speed up the process by not performing IP addresses DNS resolution in the Log files
- \* Display account log records only
- \* Display detailed log chains (all the log segments a log record consists of)

**NO.62** Which of the following is a correct flow of the stages in an incident handling and response (IH&R) process?

- \* Containment -> Incident Recording -> Incident Triage -> Preparation -> Recovery -> Eradication -> Post-Incident Activities
- \* Preparation -> Incident Recording -> Incident Triage -> Containment -> Eradication -> Recovery -> Post-Incident Activities
- \* Incident Triage -> Eradication -> Containment -> Incident Recording -> Preparation -> Recovery -> Post-Incident Activities
- \* Incident Recording -> Preparation -> Containment -> Incident Triage -> Recovery -> Eradication -> Post-Incident Activities

## Career Prospects

Those candidates who achieve the passing score in the certification exam are entitled to earn the CSA certification as well as membership privileges. The certified individuals are in high demand with numerous job openings that they can explore. Without a doubt, this EC-Council certificate is a highly rewarding option that allows the professionals to take up different job roles. Some career paths that they can explore include a Security & Network Administrator, a Network Defense Analyst, a Security & Network Engineer, a Network Security Specialist, a Network Defense Technician, a Network Security Operator, and a Cybersecurity Analyst, among others.

### **New 312-39 Dumps - Real EC-COUNCIL Exam Questions:**

<https://www.examcollectionpass.com/EC-COUNCIL/312-39-practice-exam-dumps.html>