[Q56-Q74 Updated Aug-2024 Exam Engine or PDF for the EC-COUNCIL 312-39 test to help you quickly prepare for the EC-COUNCIL exam!

Updated Aug-2024 Test Engine or PDF for the EC-COUNCIL 312-39 test to help you quickly prepare for the EC-COUNCIL exam! Full 312-39 Practice Test and 102 unique questions with explanations waiting just for you, get it now! QUESTION 56

Which of the following Windows features is used to enable Security Auditing in Windows?
* Bitlocker
* Windows Firewall
* Local Group Policy Editor
* Windows Defender

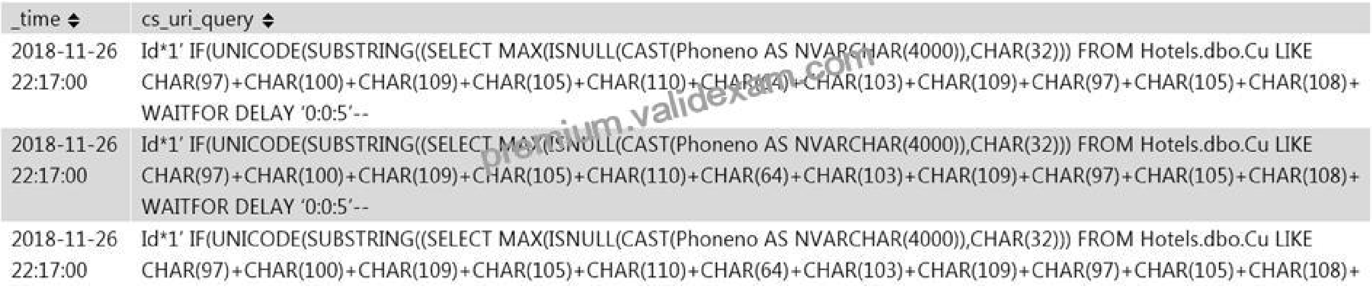
QUESTION 57

What does the HTTP status codes 1XX represents?
* Informational message
* Client error
* Success
* Redirection
The HTTP status codes that fall within the range of 1XX represent informational messages. These are provisional responses that indicate the initial part of a request has been received and has not yet been rejected by the server. The server is informing the client that it has received the header of the request and the client should continue to send the request body if it has not already done so. These status codes are used to provide an interim response to the client while the server processes the full request.

References: The EC-Council&#8217;s Certified SOC Analyst (C|SA) program includes the study of HTTP status codes as part of understanding web server logs and troubleshooting web server issues. The informational responses (1XX status codes) are covered in the curriculum and can be found in the official EC-Council SOC Analyst study guides and courses. The information is also consistent with the standard definitions provided by the Internet Engineering Task Force (IETF) in RFC 9110, as well as other reputable sources such as MDN Web Docs1 and Wikipedia2.

QUESTION 58

Jony, a security analyst, while monitoring IIS logs, identified events shown in the figure below.



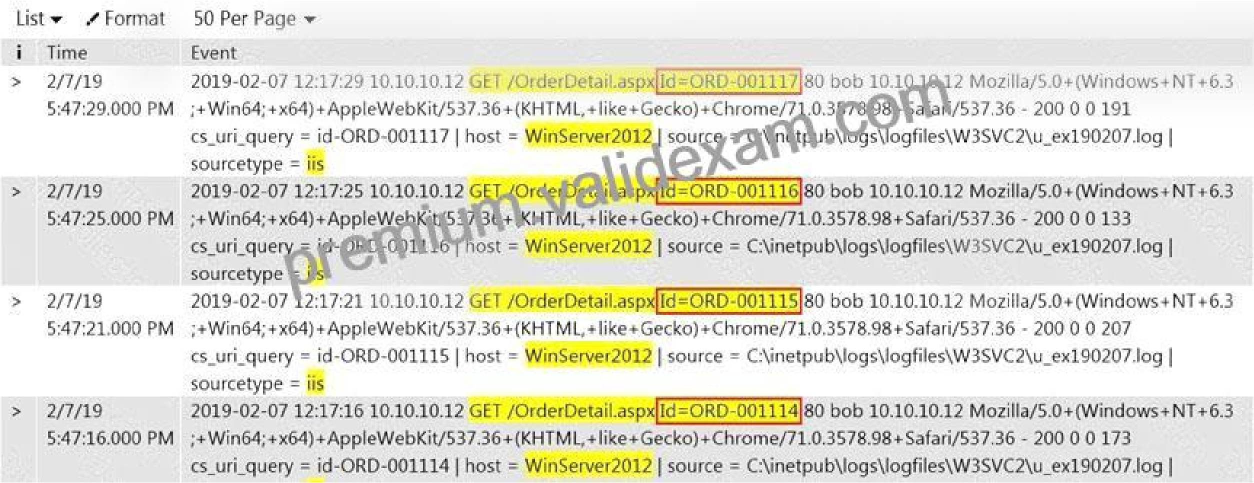
_time ⬍	cs_uri_query ⬍
2018-11-26 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+ WAITFOR DELAY '0:0:5'--
2018-11-26 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+ WAITFOR DELAY '0:0:5'--
2018-11-26 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+

What does this event log indicate?

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

QUESTION 59

Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.



```
i  Time              Event
>  2/7/19            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
   5:47:29.000 PM    ;+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            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
   5:47:25.000 PM    ;+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            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
   5:47:21.000 PM    ;+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            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
   5:47:16.000 PM    ;+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

QUESTION 60

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

QUESTION 61

What type of event is recorded when an application driver loads successfully in Windows?
* Error
* Success Audit
* Warning
* Information

QUESTION 62

Which encoding replaces unusual ASCII characters with &#8220;%&#8221; followed by the character&#8217;s two-digit ASCII

code expressed in hexadecimal?
* Unicode Encoding
* UTF Encoding
* Base64 Encoding
* URL Encoding

QUESTION 63

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

QUESTION 64

Which attack works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?
* Hybrid Attack
* Bruteforce Attack
* Rainbow Table Attack
* Birthday Attack

QUESTION 65

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.
* Post-Incident Activities
* Incident Recording and Assignment
* Incident Triage
* Incident Disclosure

QUESTION 66

Which of the following threat intelligence helps cyber security professionals such as security operations managers, network operations center and incident responders to understand how the adversaries are expected to perform the attack on the organization, and the technical capabilities and goals of the attackers along with the attack vectors?
* Analytical Threat Intelligence
* Operational Threat Intelligence
* Strategic Threat Intelligence
* Tactical Threat Intelligence

QUESTION 67

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
In the context of alert triaging within a Security Operations Center (SOC), the priority of alerts is typically determined based on the potential impact and urgency of the threat they represent.

* Firewall blocking traffic alerts indicate that the firewall is effectively doing its job by blocking unwanted traffic. While it&#8217;s important to review these alerts to ensure legitimate traffic isn&#8217;t being blocked, they generally represent a lower priority because the immediate threat has been mitigated by the firewall.

* SQL injection attempt alerts are of high priority because they indicate an active attempt to exploit a security vulnerability in order to manipulate or steal data.

* Data deletion attempt alerts also carry high priority as they could signify an attempt to remove or corrupt critical data, which could have significant impact on the availability and integrity of data.

* Brute-force attempt alerts are important as they may indicate an ongoing attempt to gain unauthorized access to systems. However, if the attempts are being blocked, these alerts may be of a slightly lower priority compared to an active exploit attempt like SQL injection.

Given these considerations, the alert for the firewall blocking traffic would generally be given the least priority, as it indicates a threat that has already been contained.

References: The EC-Council&#8217;s Certified SOC Analyst (CSA) program covers the fundamentals of SOC operations, including the management of alerts and the triaging process. The program emphasizes the importance of prioritizing alerts based on the severity and potential impact of the threat12. For more detailed information, the EC-Council&#8217;s official CSA study guides and courses should be consulted. These resources provide in-depth knowledge on how to effectively manage and prioritize alerts in a SOC environment.

QUESTION 68

Jane, a security analyst, while analyzing IDS logs, detected an event matching Regex /((%3C)|<)((%69)|i|(%

49))((%6D)|m|(%4D))((%67)|g|(%47))[n]+((%3E)|>)/|.

What does this event log indicate?
* Directory Traversal Attack
* Parameter Tampering Attack

* XSS Attack
* SQL Injection Attack

QUESTION 69

Bonney&#8217;s system has been compromised by a gruesome malware.

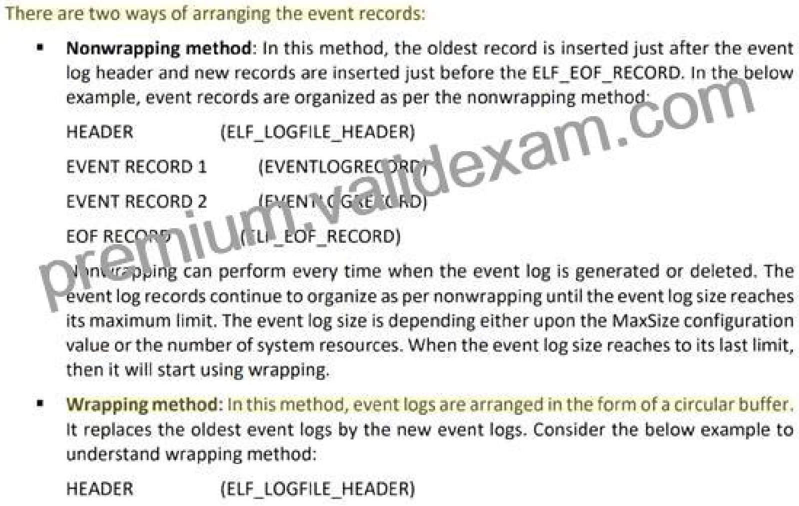
What is the primary step that is advisable to Bonney in order to contain the malware incident from spreading?
* Complaint to police in a formal way regarding the incident
* Turn off the infected machine
* Leave it to the network administrators to handle
* Call the legal department in the organization and inform about the incident
The primary step in containing a malware incident is to isolate the infected machine to prevent the malware from spreading to other systems. This can be done by disconnecting it from the network and turning it off.

This action helps to contain the incident and allows for a proper investigation without the risk of further infection or data loss.

References: The EC-Council&#8217;s Certified SOC Analyst (CSA) program emphasizes the importance of quick response to security incidents, including malware infections. The training includes understanding security threats, attacks, vulnerabilities, and the appropriate responses to such incidents. The CSA program also covers the procedures for incident response, which includes the containment strategies for incidents like malware outbreaks123.

QUESTION 70

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 (EVENTLOGRECORD)

  EVENT RECORD 2 (EVENTLOGRECORD)

  EOF RECORD (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:

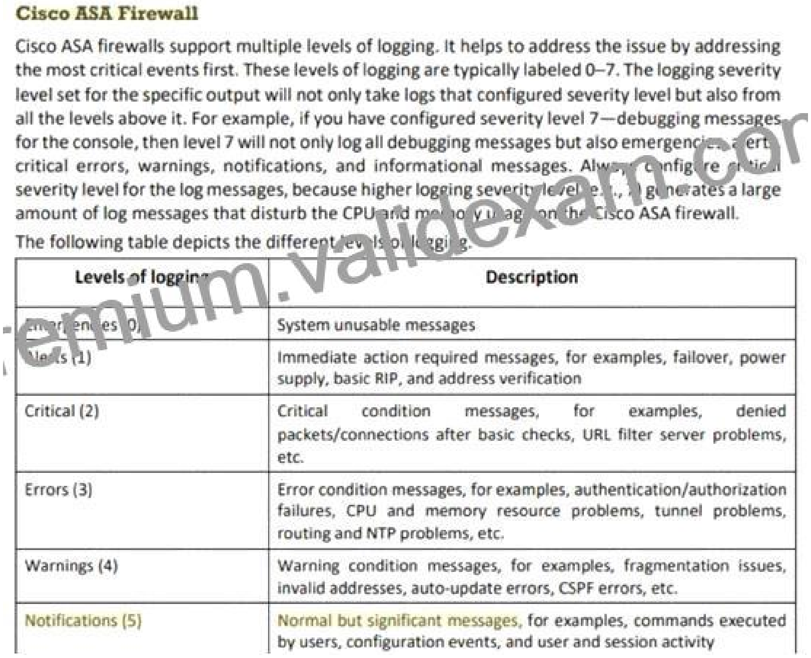
  HEADER (ELF_LOGFILE_HEADER)

QUESTION 71

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 &#8211; 11008: User &#8216;enable_15&#8217; executed the &#8216;configure term&#8217; command What does the security level in the above log indicates?

* Warning condition message
* Critical condition message
* Normal but significant message
* Informational message



Cisco ASA Firewall

Cisco ASA firewalls support multiple levels of logging. It helps to address the issue by addressing the most critical events first. These levels of logging are typically labeled 0–7. The logging severity level set for the specific output will not only take logs that configured severity level but also from all the levels above it. For example, if you have configured severity level 7—debugging messages for the console, then level 7 will not only log all debugging messages but also emergencies, alerts, critical errors, warnings, notifications, and informational messages. Always configure critical severity level for the log messages, because higher logging severity level (e.g., 7) generates a large amount of log messages that disturb the CPU and memory usage on the Cisco ASA firewall.

The following table depicts the different levels of logging.

Levels of logging	Description
Emergencies (0)	System unusable messages
Alerts (1)	Immediate action required messages, for examples, failover, power supply, basic RIP, and address verification
Critical (2)	Critical condition messages, for examples, denied packets/connections after basic checks, URL filter server problems, etc.
Errors (3)	Error condition messages, for examples, authentication/authorization failures, CPU and memory resource problems, tunnel problems, routing and NTP problems, etc.
Warnings (4)	Warning condition messages, for examples, fragmentation issues, invalid addresses, auto-update errors, CSPF errors, etc.
Notifications (5)	Normal but significant messages, for examples, commands executed by users, configuration events, and user and session activity

QUESTION 72

Which of the following technique involves scanning the headers of IP packets leaving a network to make sure that the unauthorized or malicious traffic never leaves the internal network?

* Egress Filtering
* Throttling
* Rate Limiting
* Ingress Filtering

QUESTION 73

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

* High
* Extreme
* Low
* Medium

QUESTION 74

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

* Netstat Data
* DNS Data

* IIS Data
* DHCP Data
A SOC Analyst would use Netstat Data to monitor connections to insecure ports. Netstat, which stands for network statistics, is a command-line tool that displays incoming and outgoing network connections (both TCP and UDP), routing tables, and a number of network interface and network protocol statistics. It is available on various operating systems, including Windows, Linux, and Unix, and is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement.

References: The use of Netstat for monitoring network connections is a common practice and is covered in EC-Council&#8217;s SOC Analyst curriculum, which provides foundational knowledge for security operations center (SOC) team members on various tools and techniques for monitoring and analyzing network traffic12. Additionally, Netstat&#8217;s capabilities are well-documented in various technical resources that detail its usage for security analysis purposes34.