312-39.VCEplus.premium.exam.100q

Number: 312-39
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

312-39

Certified SOC Analyst

Version 1.0

Exam A

QUESTION 1
Bonney'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?

A. Complaint to police in a formal way regarding the incident
B. Turn off the infected machine
C. Leave it to the network administrators to handle
D. Call the legal department in the organization and inform about the incident

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
According to the forensics investigation process, what is the next step carried out right after collecting the evidence?

A. Create a Chain of Custody Document
B. Send it to the nearby police station
C. Set a Forensic lab
D. Call Organizational Disciplinary Team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3 Which one of the following is the correct flow for Setting Up a Computer Forensics Lab?

A. Planning and budgeting –> Physical location and structural design considerations –> Work area considerations –> Human resource considerations –> Physical security recommendations –> Forensics lab licensing B. Planning and budgeting –> Physical location and structural design considerations–> Forensics lab licensing –> Human resource considerations –> Work area considerations –> Physical security recommendations
C. Planning and budgeting –> Forensics lab licensing –> Physical location and structural design considerations –> Work area considerations –> Physical security recommendations –> Human resource considerations
D. Planning and budgeting –> Physical location and structural design considerations –> Forensics lab licensing –>Work area considerations –> Human resource considerations –> Physical security recommendations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://info-savvy.com/setting-up-a-computer-forensics-lab/

QUESTION 4 Which of the following directory will contain logs related to printer access?

A. /var/log/cups/Printer_log file
B. /var/log/cups/access_log file
C. /var/log/cups/accesslog file
D. /var/log/cups/Printeraccess_log file

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 5 Which of the following command is used to enable logging in iptables?

A. $ iptables -B INPUT -j LOG
B. $ iptables -A OUTPUT -j LOG
C. $ iptables -A INPUT -j LOG
D. $ iptables -B OUTPUT -j LOG

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://tecadmin.net/enable-logging-in-iptables-on-linux/

QUESTION 6
Ray is a SOC analyst in a company named Queens Tech. One Day, Queens Tech is affected by a DoS/DDoS attack. For the containment of this incident, Ray and his team are trying to provide additional bandwidth to the network devices and increasing the capacity of the servers.

What is Ray and his team doing?

A. Blocking the Attacks
B. Diverting the Traffic
C. Degrading the services
D. Absorbing the Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Identify the attack when an attacker by several trial and error can read the contents of a password file present in the restricted etc folder just by manipulating the URL in the browser as shown:

http://www.terabytes.com/process.php./../../../../etc/passwd

A. Directory Traversal Attack
B. SQL Injection Attack
C. Denial-of-Service Attack
D. Form Tampering Attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://doc.lagout.org/security/SQL%20Injection%20Attacks%20and%20Defense.pdf

QUESTION 8
Which encoding replaces unusual ASCII characters with "%" followed by the character’s two-digit ASCII code expressed in hexadecimal?

A. Unicode Encoding
B. UTF Encoding
C. Base64 Encoding
D. URL Encoding

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://ktflash.gitbooks.io/ceh_v9/content/125_countermeasures.html

QUESTION 9 Which of the following formula represents the risk?

A. Risk = Likelihood × Severity × Asset Value
B. Risk = Likelihood × Consequence × Severity
C. Risk = Likelihood × Impact × Severity
D. Risk = Likelihood × Impact × Asset Value

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10 The Syslog message severity levels are labelled from level 0 to level 7.

What does level 0 indicate?

A. Alert
B. Notification
C. Emergency
D. Debugging

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11 Where will you find the reputation IP database, if you want to monitor traffic from known bad IP reputation using OSSIM SIEM?

A. /etc/ossim/reputation
B. /etc/ossim/siem/server/reputation/data
C. /etc/siem/ossim/server/reputation.data
D. /etc/ossim/server/reputation.data

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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?

A. High
B. Extreme
C. Low
D. Medium

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.moheri.gov.om/userupload/Policy/IT%20Risk%20Management%20Framework.pdf (17)

QUESTION 13 Which of the following command is used to view iptables logs on Ubuntu and Debian distributions?

A. $ tailf /var/log/sys/kern.log
B. $ tailf /var/log/kern.log
C. # tailf /var/log/messages
D. # tailf /var/log/sys/messages

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://tecadmin.net/enable-logging-in-iptables-on-linux/

QUESTION 14
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?

A. Egress Filtering
B. Throttling
C. Rate Limiting
D. Ingress Filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://grokdesigns.com/wp-content/uploads/2018/04/CEH-v9-Notes.pdf (99)

QUESTION 15 Which of the following formula is used to calculate the EPS of the organization?

A. EPS = average number of correlated events / time in seconds
B. EPS = number of normalized events / time in seconds
C. EPS = number of security events / time in seconds
D. EPS = number of correlated events / time in seconds

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16 Juliea a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads.

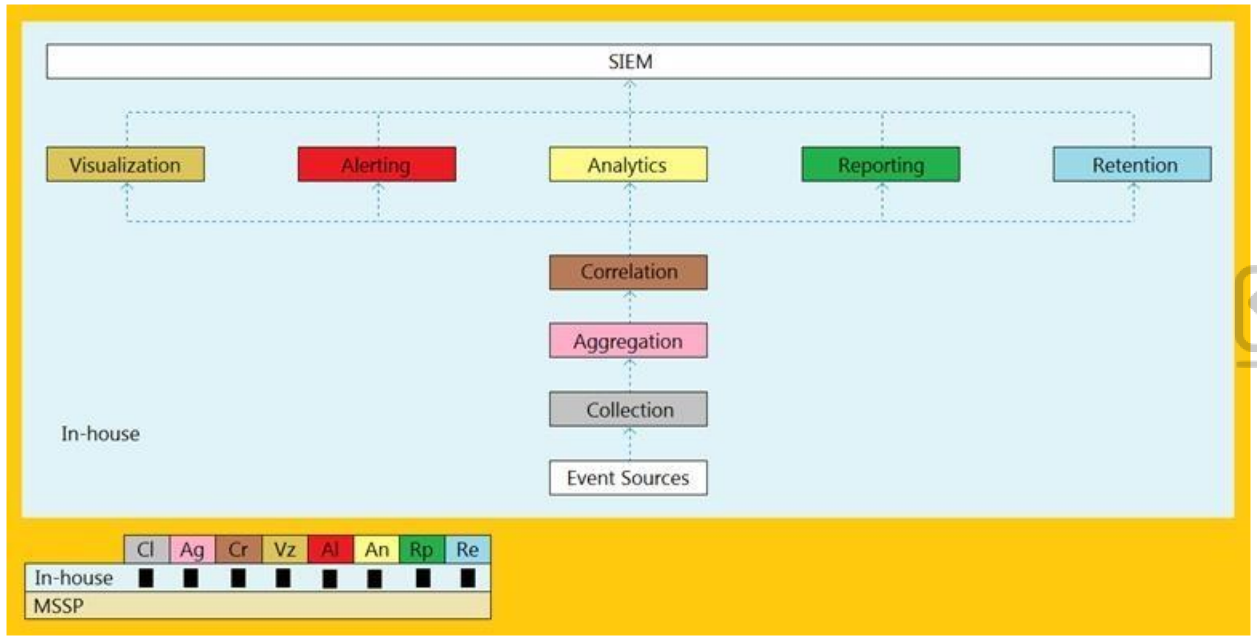
What does this indicate?

A. Concurrent VPN Connections Attempt
B. DNS Exfiltration Attempt
C. Covering Tracks Attempt
D. DHCP Starvation Attempt

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj8gZaKq_PuAhWGi1wKHfQTC0oQFjAAegQIARAD&url=https%3A%2F%2Fconf.splunk.com%2Fsession%2F2014%2Fconf2014_FredWilmotSanfordOwings_Splunk_Security.pdf&usg=AOvVaw3ZLfzGqM-VUG7xKtze67ac

QUESTION 17
An organization is implementing and deploying the SIEM with following capabilities.



What kind of SIEM deployment architecture the organization is planning to implement?

A. Cloud, MSSP Managed
B. Self-hosted, Jointly ManagedC. Self-hosted, Self-Managed
D. Self-hosted, MSSP Managed

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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
Section: (none)
Explanation

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

QUESTION 19
Which of the following is a report writing tool that will help incident handlers to generate efficient reports on detected incidents during incident response process?

A. threat_note
B. MagicTree
C. IntelMQ
D. Malstrom

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20 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
Section: (none)
Explanation

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

QUESTION 21 Which of the following attack can be eradicated by filtering improper XML syntax?

A. CAPTCHA Attacks
B. SQL Injection Attacks
C. Insufficient Logging and Monitoring Attacks
D. Web Services Attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following attack can be eradicated by using a safe API to avoid the use of the interpreter entirely?
A. Command Injection Attacks

B. SQL Injection Attacks
C. File Injection Attacks
D. LDAP Injection Attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.kiuwan.com/owasp-top-10-a1-injection/

QUESTION 23
Shawn is a security manager working at Lee Inc Solution. His organization wants to develop threat intelligent strategy plan. As a part of threat intelligent strategy plan, he suggested various components, such as threat intelligence requirement analysis, intelligence and collection planning, asset identification, threat reports, and intelligence buy-in.

Which one of the following components he should include in the above threat intelligent strategy plan to make it effective?

A. Threat pivoting
B. Threat trending
C. Threat buy-in
D. Threat boosting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24 Which of the following can help you eliminate the burden of investigating false positives?

A. Keeping default rules
B. Not trusting the security devices
C. Treating every alert as high level
D. Ingesting the context data

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://stratozen.com/9-ways-eliminate-siem-false-positives/

QUESTION 25 Which of the following event detection techniques uses User and Entity Behavior Analytics (UEBA)?

A. Rule-based detection
B. Heuristic-based detection
C. Anomaly-based detection
D. Signature-based detection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 26

Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.

A. Dictionary Attack
B. Rainbow Table Attack
C. Bruteforce Attack
D. Syllable Attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic7-final/report.pdf

QUESTION 27 Which of the log storage method arranges event logs in the form of a circular buffer?

A. FIFO
B. LIFO
C. non-wrapping
D. wrapping

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Circular_buffer

QUESTION 28
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?

A. Cloud, MSSP Managed
B. Self-hosted, Jointly Managed
C. Self-hosted, MSSP Managed
D. Self-hosted, Self-Managed

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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

Section: (none)
Explanation

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

QUESTION 30 Which of the following attacks causes sudden changes in file extensions or increase in file renames at rapid speed?

A. Ransomware Attack
B. DoS Attack
C. DHCP starvation Attack
D. File Injection Attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.netfort.com/category/ransomware-detection/

QUESTION 31 Which of the following security technology is used to attract and trap people who attempt unauthorized or illicit utilization of the host system?

A. De-Militarized Zone (DMZ)
B. Firewall
C. Honeypot
D. Intrusion Detection System

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

QUESTION 32 Identify the event severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future problem.

A. Failure Audit
B. Warning
C. Error
D. Information

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/windows/win32/eventlog/event-types

QUESTION 33 Which of the following factors determine the choice of SIEM architecture?

A. SMTP Configuration
B. DHCP Configuration
C. DNS Configuration
D. Network Topology

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
What does HTTPS Status code 403 represents?

A. Unauthorized Error
B. Not Found Error
C. Internal Server Error
D. Forbidden Error

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/HTTP_403

QUESTION 35 Which of the following Windows event is logged every time when a user tries to access the "Registry" key?

A. 4656
B. 4663
C. 4660
D. 4657

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4657

QUESTION 36 Which of the following are the responsibilities of SIEM Agents?

1. Collecting data received from various devices sending data to SIEM before forwarding it to the central engine.
2. Normalizing data received from various devices sending data to SIEM before forwarding it to the central engine.
3. Co-relating data received from various devices sending data to SIEM before forwarding it to the central engine.
4. Visualizing data received from various devices sending data to SIEM before forwarding it to the central engine.

A. 1 and 2
B. 2 and 3
C. 1 and 4
D. 3 and 1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Sam, a security analyst with INFOSOL INC., while monitoring and analyzing IIS logs, detected an event matching regex /\\w*((\%27)|(\’))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix.

What does this event log indicate?

A. SQL Injection Attack
B. Parameter Tampering Attack
C. XSS Attack
D. Directory Traversal Attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=001f5e09-88b4-4a9a-b310-4c20578eecf9&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

QUESTION 38 Which of the following framework describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering?

A. COBIT
B. ITIL
C. SSE-CMM
D. SOC-CMM

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.iso.org/standard/44716.html

QUESTION 39 What does Windows event ID 4740 indicate?

A. A user account was locked out.
B. A user account was disabled.
C. A user account was enabled.
D. A user account was created.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4740#:~:text=For%204740(S)%3A%20A,Security%20ID”%20is%20not%20SYSTEM.

QUESTION 40 Which of the following is a Threat Intelligence Platform?

A. SolarWinds MS
B. TC Complete
C. Keepnote
D. Apility.io

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 41
A type of threat intelligent that find out the information about the attacker by misleading them is known as __________.

A. Threat trending Intelligence
B. Detection Threat Intelligence
C. Operational Intelligence
D. Counter Intelligence

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.recordedfuture.com/threat-intelligence/

QUESTION 42
Chloe, a SOC analyst with Jake Tech, is checking Linux systems logs. She is investigating files at /var/log/wtmp.

What Chloe is looking at?

A. Error log
B. System boot log
C. General message and system-related stuff
D. Login records

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://stackify.com/linux-logs/

QUESTION 43 Which of the following threat intelligence is used by a SIEM for supplying the analysts with context and "situational awareness" by using threat actor TTPs, malware campaigns, tools used by threat actors.

1. Strategic threat intelligence
2. Tactical threat intelligence
3. Operational threat intelligence
4. Technical threat intelligence

A. 2 and 3
B. 1 and 3
C. 3 and 4
D. 1 and 2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf (38)

QUESTION 44 Properly applied cyber threat intelligence to the SOC team help them in discovering TTPs.

What does these TTPs refer to?

A. Tactics, Techniques, and Procedures
B. Tactics, Threats, and Procedures
C. Targets, Threats, and Process
D. Tactics, Targets, and Process

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf

QUESTION 45 Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?

A. Windows Event Log
B. Web Server Logs
C. Router Logs
D. Switch Logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
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?

A. Incident Response Intelligence
B. Incident Response Mission
C. Incident Response Vision
D. Incident Response Resources

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://blog.eccouncil.org/phases-of-an-incident-response-plan/

QUESTION 47
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
Section: (none)
Explanation

Explanation/Reference:
QUESTION 48
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.

A. High
B. Extreme
C. Low
D. Medium

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://onlinelibrary.wiley.com/page/journal/15396924/homepage/special_issue__simple_characterisations_and_communication_of_risks.htm

QUESTION 49 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?

A. Warning condition message
B. Critical condition message
C. Normal but significant message
D. Informational message

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50 What is the correct sequence of SOC Workflow?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
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?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
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/<script>alert("WARNING:

The application has encountered an error");</script>.

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53 Which of the following formula represents the risk levels?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54 In which of the following incident handling and response stages, the root cause of the incident must be found from the forensic results?

A. Evidence Gathering
B. Evidence HandlingC. Eradication
D. Systems Recovery

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.eccouncil.org/wp-content/uploads/2019/02/ECIH-V2-Brochure.pdf

QUESTION 55

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?

A. Directory Traversal Attack
B. Parameter Tampering Attack
C. XSS Attack
D. SQL Injection Attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://books.google.com.pk/books?id=PDR4nOAP8qUC&pg=PA87&lpg=PA87&dq=regex+/((%5C%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 56 Which of the following Windows Event Id will help you monitors file sharing across the network?

A. 7045
B. 4625
C. 5140
D. 4624

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=5140

QUESTION 57
The threat intelligence, which will help you, understand adversary intent and make informed decision to ensure appropriate security in alignment with risk.

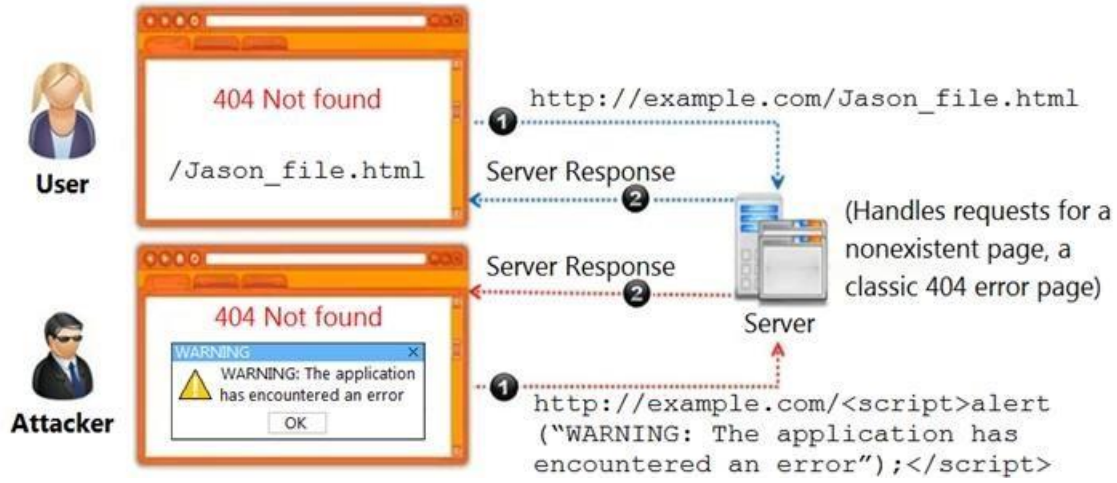
What kind of threat intelligence described above?

A. Tactical Threat Intelligence
B. Strategic Threat Intelligence
C. Functional Threat Intelligence
D. Operational Threat Intelligence

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/threat-intelligence/what-is-threat-intelligence/

QUESTION 58
Identify the type of attack, an attacker is attempting on www.example.com website.


User
404 Not found
/Jason_file.html
http://example.com/Jason_file.html
1
Server Response
2
(Handles requests for a nonexistent page, a classic 404 error page)
Server
Server Response
2
Attacker
404 Not found
WARNING
WARNING: The application has encountered an error
OK
1
http://example.com/<script>alert ("WARNING: The application has encountered an error");</script>

A. Cross-site Scripting Attack
B. Session Attack
C. Denial-of-Service Attack
D. SQL Injection Attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60 Which of the following tool is used to recover from web application incident?

A. CrowdStrike Falcon^{TM} Orchestrator
B. Symantec Secure Web Gateway
C. Smoothwall SWGD. Proxy Workbench

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61

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?

A. Self-hosted, Self-Managed
B. Self-hosted, MSSP Managed
C. Hybrid Model, Jointly Managed
D. Cloud, Self-Managed

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62 What type of event is recorded when an application driver loads successfully in Windows?

A. Error
B. Success Audit
C. Warning
D. Information

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.manageengine.com/network-monitoring/Eventlog_Tutorial_Part_I.html

QUESTION 63
An attacker exploits the logic validation mechanisms of an e-commerce website. He successfully purchases a product worth $100 for $10 by modifying the URL exchanged between the client and the server.

Original URL: http://www.buyonline.com/product.aspx?profile=12&debit=100 Modified
URL: http://www.buyonline.com/product.aspx?profile=12&debit=10

Identify the attack depicted in the above scenario.

A. Denial-of-Service Attack
B. SQL Injection Attack
C. Parameter Tampering Attack
D. Session Fixation Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
John, a threat analyst at GreenTech Solutions, wants to gather information about specific threats against the organization. He started collecting information from various sources, such as humans, social media, chat room, and so on, and created a report that contains malicious activity.

Which of the following types of threat intelligence did he use?

A. Strategic Threat Intelligence

B. Technical Threat Intelligence
C. Tactical Threat Intelligence
D. Operational Threat Intelligence

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65 Which of the following is a default directory in a Mac OS X that stores security-related logs?

A. /private/var/log
B. /Library/Logs/Sync
C. /var/log/cups/access_log
D. ~/Library/Logs

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66 John, SOC analyst wants to monitor the attempt of process creation activities from any of their Windows endpoints.

Which of following Splunk query will help him to fetch related logs associated with process creation?

A. index=windows LogName=Security EventCode=4678 NOT (Account_Name=*$) .. ..
B. index=windows LogName=Security EventCode=4688 NOT (Account_Name=*$) .. .. ..
C. index=windows LogName=Security EventCode=3688 NOT (Account_Name=*$) .. .. ..
D. index=windows LogName=Security EventCode=5688 NOT (Account_Name=*$) ... ...

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/5a3187b4419202f0fb8b2dd1/1513195444728/Windows+Splunk+Logging+Cheat+Sheet+v2.2.pdf

QUESTION 67
Harley is working as a SOC analyst with Powell Tech. Powell Inc. is using Internet Information Service (IIS) version 7.0 to host their website.

Where will Harley find the web server logs, if he wants to investigate them for any anomalies?

A. SystemDrive%\inetpub\logs\LogFiles\W3SVCN
B. SystemDrive%\LogFiles\inetpub\logs\W3SVCN
C. %SystemDrive%\LogFiles\logs\W3SVCN
D. SystemDrive%\ inetpub\LogFiles\logs\W3SVCN

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/sitedefaults/logfile/

QUESTION 68 What does the Security Log Event ID 4624 of
Windows 10 indicate?

A. Service added to the endpoint
B. A share was assessed
C. An account was successfully logged on
D. New process executed

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

QUESTION 69 Which of the following is a set of standard guidelines for ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection?

A. FISMA
B. HIPAA
C. PCI-DSS
D. DARPA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://library.educause.edu/topics/policy-and-law/pci-dss

QUESTION 70 What does the HTTP status codes
1XX represents?

A. Informational message
B. Client error
C. Success
D. Redirection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/List_of_HTTP_status_codes#:~:text=1xx%20informational%20response%20–%20the%20request,syntax%20or%20cannot%20be%20fulfilled

QUESTION 71
In which phase of Lockheed Martin's – Cyber Kill Chain Methodology, adversary creates a deliverable malicious payload using an exploit and a backdoor?

A. Reconnaissance
B. Delivery
C. Weaponization
D. Exploitation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Reference: https://securityboulevard.com/2018/08/the-cyber-kill-chain-what-you-need-to-know/

QUESTION 72
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
Section: (none)
Explanation

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

QUESTION 73 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]

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk25532

QUESTION 74
Which of the following attack inundates DHCP servers with fake DHCP requests to exhaust all available IP addresses?

A. DHCP Starvation Attacks
B. DHCP Spoofing Attack
C. DHCP Port Stealing
D. DHCP Cache Poisoning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cbtnuggets.com/blog/technology/networking/what-is-a-dhcp-starvation-attack

QUESTION 75
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
Section: (none)
Explanation

Explanation/Reference:

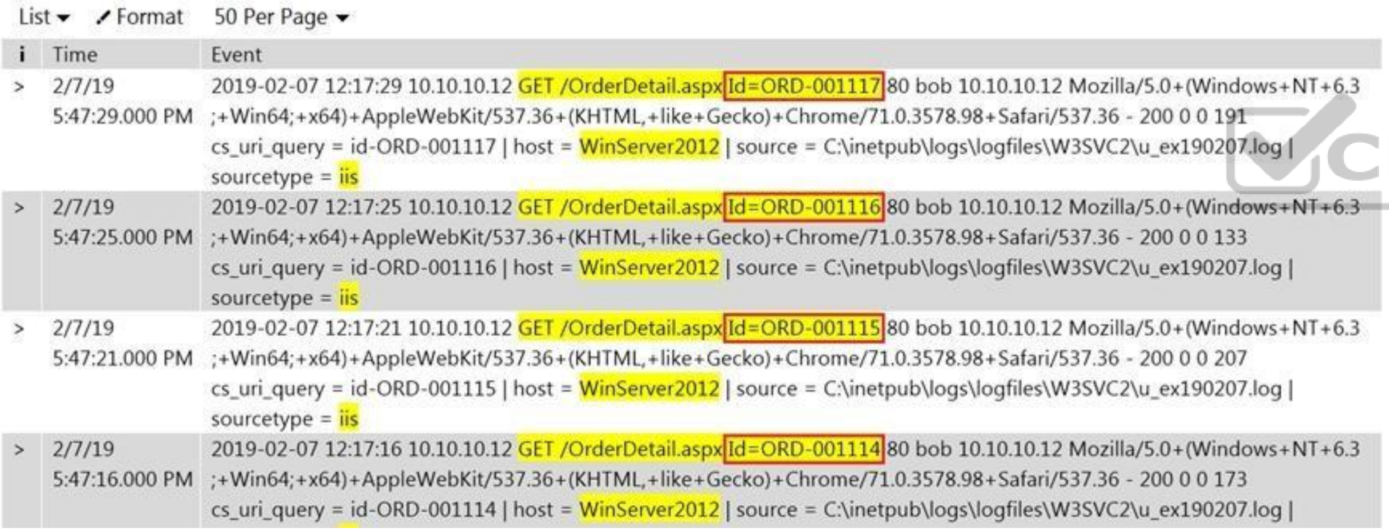
QUESTION 76 Which of the following is a correct flow of the stages in an incident handling and response (IH&R) process?

A. Containment –> Incident Recording –> Incident Triage –> Preparation –> Recovery –> Eradication –> Post-Incident Activities B. Preparation –> Incident Recording –> Incident Triage –> Containment –> Eradication –> Recovery –> Post-Incident Activities C. Incident Triage –> Eradication –> Containment –> Incident Recording –> Preparation –> Recovery –> Post-Incident Activities D. Incident Recording –> Preparation –> Containment –> Incident Triage –> Recovery –> Eradication –> Post-Incident Activities

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://blog.elearnsecurity.com/the-4-steps-of-incident-handling-response.html

QUESTION 77
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?

A. Directory Traversal Attack
B. XSS Attack
C. SQL Injection Attack
D. Parameter Tampering Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://infosecwriteups.com/what-is-parameter-tampering-5b1beb12c5ba

QUESTION 78
Peter, a SOC analyst with Spade Systems, is monitoring and analyzing the router logs of the company and wanted to check the logs that are generated by access control list numbered 210.

What filter should Peter add to the 'show logging' command to get the required output?

A. show logging | access 210
B. show logging | forward 210
C. show logging | include 210
D. show logging | route 210

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79 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
Section: (none)
Explanation

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

QUESTION 80 In which log collection mechanism, the system or application sends log records either on the local disk or over the network.

A. rule-based
B. pull-based
C. push-based
D. signature-based

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81 Which of the following attack can be eradicated by disabling of "allow_url_fopen and allow_url_include" in the php.ini file?

A. File Injection Attacks
B. URL Injection Attacks
C. LDAP Injection Attacks
D. Command Injection Attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82 Which of the following stage executed after identifying the required event sources?

A. Identifying the monitoring Requirements
B. Defining Rule for the Use Case
C. Implementing and Testing the Use Case
D. Validating the event source against monitoring requirement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83 Which of the following steps of incident handling and response process focus on limiting the scope and extent of an incident?

A. Containment
B. Data Collection
C. Eradication
D. Identification

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following technique protects from flooding attacks originated from the valid prefixes (IP addresses) so that they can be traced to its true source?

A. Rate Limiting
B. Egress Filtering
C. Ingress Filtering
D. Throttling

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Reference: http://www.mecs-press.org/ijcnis/ijcnis-v5-n5/IJCNIS-V5-N5-6.pdf (3)

QUESTION 86 Which of the following contains the performance measures, and proper project and time management details?

A. Incident Response Policy
B. Incident Response Tactics
C. Incident Response Process
D. Incident Response Procedures

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
John as a SOC analyst is worried about the amount of Tor traffic hitting the network. He wants to prepare a dashboard in the SIEM to get a graph to identify the locations from where the TOR traffic is coming.

Which of the following data source will he use to prepare the dashboard?

A. DHCP/Logs capable of maintaining IP addresses or hostnames with IPtoName resolution.
B. IIS/Web Server logs with IP addresses and user agent IPtouseragent resolution.
C. DNS/ Web Server logs with IP addresses.
D. Apache/ Web Server logs with IP addresses and Host Name.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
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?

A. Load Balancing
B. Rate Limiting
C. Black Hole Filtering
D. Drop Requests

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Black_hole_(networking)#:~:text=In%20networking%2C%20black%20holes%20refer,not%20reach%20its%20intended%20recipient.

QUESTION 89 Which of the following tool can be used to filter web requests associated with the SQL Injection attack?

A. Nmap
B. UrlScan
C. ZAP proxy
D. Hydra

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Reference: https://aip.scitation.org/doi/pdf/10.1063/1.4982570

QUESTION 90
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
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?

A. Analytical Threat Intelligence
B. Operational Threat Intelligence
C. Strategic Threat Intelligence
D. Tactical Threat Intelligence

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://info-savvy.com/types-of-threat-intelligence/

QUESTION 92 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 alertsIV. Brute-force attempt alerts

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

A. III
B. IV
C. II
D. I

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
InfoSystem LLC, a US-based company, is establishing an in-house SOC. John has been given the responsibility to finalize strategy, policies, and procedures for the SOC.

Identify the job role of John.

A. Security Analyst – L1
B. Chief Information Security Officer (CISO)
C. Security Engineer
D. Security Analyst – L2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.exabeam.com/security-operations-center/security-operations-center-roles-and-responsibilities/

QUESTION 94 Which of the following service provides phishing protection and content filtering to manage the Internet experience on and off your network with the acceptable use or compliance policies?

A. Apility.io
B. Malstrom
C. OpenDNS
D. I-Blocklist

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.spamtitan.com/web-filtering/category/cybersecurity-advice/

QUESTION 95
David is a SOC analyst in Karen Tech. One day an attack is initiated by the intruders but David was not able to find any suspicious events.

This type of incident is categorized into __________?

A. True Positive Incidents
B. False positive Incidents
C. True Negative Incidents
D. False Negative Incidents

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Emmanuel is working as a SOC analyst in a company named Tobey Tech. The manager of Tobey Tech recently recruited an Incident Response Team (IRT) for his company. In the process of collaboration with the IRT, Emmanuel just escalated an incident to the IRT.

What is the first step that the IRT will do to the incident escalated by Emmanuel?

A. Incident Analysis and Validation
B. Incident Recording
C. Incident Classification

D. Incident Prioritization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

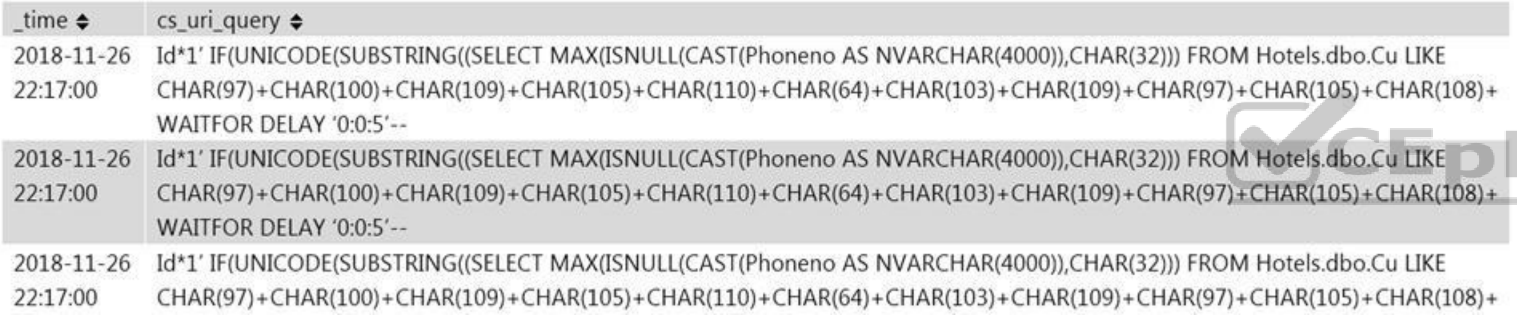
QUESTION 97 Identify the HTTP status codes that represents the server error.

A. 2XX
B. 4XXC. 1XX
D. 5XX

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.tutorialspoint.com/http/http_status_codes.htm

QUESTION 98
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?

A. Parameter Tampering Attack
B. XSS Attack
C. Directory Traversal Attack
D. SQL Injection Attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99 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?

A. Hybrid Attack
B. Bruteforce Attack
C. Rainbow Table Attack
D. Birthday Attack
Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.techrepublic.com/article/brute-force-and-dictionary-attacks-a-cheat-sheet/

QUESTION 100
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?

A. Broken Access Control Attacks
B. Web Services Attacks
C. XSS Attacks
D. Session Management Attacks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://ktflash.gitbooks.io/ceh_v9/content/125_countermeasures.html