Exam: 312-39 Certified SOC Analyst - 100 Questions

Study online at https://quizlet.com/_h52rg5

1.	Bonney's system has been infected by a gruesome malware. What is the primary step that is advisable to Bonney to prevent contain the malware incident from spreading?	B. Turn off the infected machine
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
3.	Which of the following is the correct flow for setting up a Computer Forensics Lab?	A. Planning and budgeting -> Physical location and structural design consideration -> Work area considerations -> Human resource considerations -> Physical security considerations -> Forensics lab licensing
4.	Which of the following directory will contain logs related to printer access?	A. /var/log/cups/Printer_log file
5.	Which of the following command is used to enable logging in iptables?	iptables -A OUTPUT -j LOG
6.	Ray is a SOC Analyst in a company named Queens Tech. One Day, Queens Tech is affected by 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?	D. Absorbing The Attack
7.		B. SQL Injection Attack

	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	
8.	What encoding replaces unusual ASCII characters with "%" followed by the character's two-digit ASCII code expressed in hexadecimal?	D. URL Encoding
9.	Which of the following formula represents risk?	B. Risk = Likelihood x Consequence x Severity
10.	The Syslog message severity levels are labelled from level 0 to level 7. What does level 0 indicate?	B. Notification
11.	Where will you find the reputation IP database, if you want to monitor traffic from known bad IP reputation using OSSIM SIEM?	B. /etc/ossim/siem/server/reputation/data
12.	According to the Risk Table matrix, what will be the risk level when the probability of an attack is very low and the impact of that attack is very high?	C. Low
13.	Which of the following command is used to view iptables logs on Ubuntu and Debian distributions?	$ talif /var/log/kern.log
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

15.	Which of the following formula is used to calculate the EPS of an organization?	A. EPS = number of correlated events / time in seconds
16.	Julie, a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads. What does this mean?	B. DNS Exfiltration Attempt
17.	An organization is implementing and deploying the SIEM with the following capabilities - IN house: Visualization, Alerting, Analytics, Reporting, Retention, Correlation, Aggregation, Collection, and Event Sources.	A. Cloud, MSSP Managed
18.	What is the process of monitoring and capturing all data packets passing through a given network using different tools?	C. Network Sniffing
19.	Which of the following is a report writing tool that can help incident handlers to generate efficient reports on detected incidents during the incident response process?	C. IntelMQ
20.	Which of the following features is used to enable Security Auditing in Windows?	C. Local Group Policy Editor
21.	Which of the following attack can be eradicated by filtering improper XML syntax?	B. SQL Injection Attacks
22.	Which of the following attack can be eradicated by using a safe API to avoid the use of the interpreter entirely?	B. SQL Injection Attacks
23.	Shawn is a security manager working at Lee Inc Solution. His organization wants to develop threat intelligent strategy plan. As part of threat intelligent strat-	C. Threat buy-in

	egy plan, he suggested various components, such as threat intelligence requirement analysis, intelligence and collection planning, asset identification, threat reports, and intelligence buy-in. Which of the following components he should include in the above threat intelligent strategy to make it effective?	
24.	Which of the following can help you eliminate the burden of investigating false positives?	A. Keeping default rules
25.	Which of the following event detection techniques uses User Entity and Behavior Analysis?	C. Anomaly-based detection
26.	Identify the password cracking technique involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.	A. Dictionary Attack
27.	Which of the log storage method arranges event logs in the form of a buffer?	A. FIFO
28.	An organization wants to implement a SIEM deployment architecture. However, 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?	C. Self-hosted, MSSP-managed
29.	Banter is a threat analyst in the 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?	B. Processing and Exploitation
30.		A. Ransomware Attack

	Which of the following attacks causes sudden changes in file extensions or increase in file renames at rapid speed?	
31.	Which of the following security technology is used to attract and trap people who attempt unauthorized or illicit utilization of the host system?	C. Honeypot
32.	Identify the event severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future problem.	B. Warning
33.	Which of the following factors determines the choice of SIEM architecture?	C. DNS Configuration
34.	What does HTTPS status 403 represents?	D. Forbidden Error
35.	Which of the following Windows event is logged every time when a user tries to access the "Registry" key?	D. 4657
36.	Which of the following are responsibilities of SIEM agents?	1. Collecting data from various devices before sending 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.
37.	Sam , a security analyst with INFOSOL INC., while monitoring and analyzing IIS logs, detected an event	A. SQL Injection Attack

	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	
38.	Which of the following framework describes the essential characteristics of an organization's security engineering process that must exist to ensure good security?	C. SSE-CMM
39.	What does Windows event ID 4740 indicate?	A. A user account was locked out
40.	Which of the following is a Threat Intelligence Platform?	A. SolarWinds MS
41.	A type of threat intelligent that find out the information about the attacker by misleading them is known as ____.	C. Operational Intelligence
42.	Chloe, a SOC Analyst with Jake Tech, is checking Linux systems logs. She is investigating logs at /var/log/wtmp. What is Chloe looking at?	D. Login records
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.	A. Tactical/operational threat intelligence
44.		

	Properly applied cyber intelligence to the SOC team help them in identifying TTPs. What does these TTPs refer to?	A. Tactics, Techniques and Procedures
45.	Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?	B. Web Server Logs
46.	Daniel is a member of IRT, which was recently started in a company named Mesh Tech. He wanted to find the purpose and the scope of the planned incident response capabilities. What is he looking for?	D. Incident Response Resources
47.	John, a SOC analyst, was monitoring and analyzing Apache web server logs, identified an event log matching Regex /(.|(%|%25)2E)(.|(%|%25)2E)(V|%\%25)|2F|\\(%|%25)5C)/i. What does this event log indicate?	A. XSS Attack
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?	A. High
49.	Jason, a SOC Analyst with Maximus Tech, was investigating Cisco ASA Firewall Logs and came across the following log query: 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
50.	What is the correct sequence of SOC Workflow?	

		Collect, Ingest, Validate, Report, Respond, Document
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	C. Allow serialization for security-sensitive classes
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/<script>alert("WARNING: The application has encountered an error");</script>. Identify the attack demonstrated in the above scenario.	D. Session Attack
53.	Which of the following formula represents the risk levels?	B. Level of Risk = Consequence x Impact
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

55. Jane, a security analyst, while analyzing IDS logs, detected an event matching Regex (attached). What does this event log indicate?

C. XSS Attack

56. Which of the following Windows Event Id Log will helps you monitor file sharing across the network?

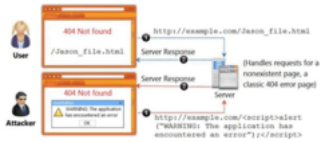
C. 5140

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

B. Strategic Threat Intelligence

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

A. Cross-site Scripting Attack



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

60. Which of the following tools is used to recover from web application incident?

B. Symantec Secure Web GW (Gateway)

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

B. Self-Hosted, MSSP Managed

C. Hybrid Model, Jointly Managed
D. Cloud, Self-Managed

62. Which type of event is recorded when an application driver successfully loads in Windows?

D. Information

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. Identify the attack depicted in the above scenario.

D. Session Fixation Attack

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

D. Operational Threat Intelligence

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

D. ~/Library/Logs

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 Event-

B. index=windows LogName=Security EventCode=4688 NOT (Account_Name=*$) .. .. ..

	Code=4678 NOT (Account_Name=*$) .. .. B. index=windows LogName=Security Event-Code=4688 NOT (Account_Name=*$) .. .. .. C. index=windows LogName=Security Event-Code=3688 NOT (Account_Name=*$) .. .. .. D. index=windows LogName=Security Event-Code=5688 NOT (Account_Name=*$)	
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	B. SystemDrive%\Log-Files\inet-pub\logs\W3SVCN
68.	What does the Security Log ID 4624 of Windows 10 indicate?	C. An account was suc-cessfully logged in
69.	Which of the following is a set of standard guidelines for ongoing development, enhancement, storage, dis-semination and implementation of security standards for account data protection?	C. PCI-DSS
70.	What does the HTTP code 1XX represents?	A. Informational message
71.	In what phase of Lockheed Martin's Cyber Kill Chain Methodology, adversary creates a deliverable mali-cious payload using an exploit and a backdoor?	B. Delivery
72.		D. Reconnaissance Attack

	Identify the attack, where an attacker tries to discover all the possible information about a target network before launching a further attack.	
73.	What does [-n] in the following checkpoint firewall log syntax represents?	A. Speed up the process by not performing IP addresses DNS resolution in the Logfiles
74.	Which of the following attack inundates DHCP servers with fake DHCP requests to exhaust all available IP addresses?	A. DHCP Starvation Attacks
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 he is currently in.	B. Incident Recording and Assignment
76.	Which of the following is the correct flow of the stages in an incident handling and response (IH&R) process?	B. Preparation -> Incident Recording -> Incident Triage -> Containment -> Eradication -> Recovery -> Post-Incident Activities
77.	Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below What does this event log indicate? A. Directory Traversal Attack B. XSS Attack	D. Parameter Tampering Attack 

C. SQL Injection Attack
D. Parameter Tampering Attack

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 were generated by access control list numbered 210. What filter should Peter add to the 'show logging' command to get the required output?	C. show logging | include 210
79.	Identify the attack in which the attacker exploits a target system through publicly known but still unpatched vulnerabilities.	C. Zero-Day Attack
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
81.	Which of the following attack can be eradicated by disabling of "allow_url_fopen and allow_url_include" in the php.ini file?	B. URL Injection Attacks
82.	Which of the following stage executed after identifying the required event sources?	D. Validating the event source against monitoring requirement
83.	Which of the following steps of incident handling and response process focus on limiting the scope and extent of an incident?	A. Containment
84.	Which of the following data source will a SOC Analyst use to monitor connections to the insecure ports?	A. Netstat data
85.		C. Ingress Filtering

	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?	
86.	Which of the following contains the performance measures, and the proper project and time management details?	D. Incident Response Procedures
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?	D. Apache/Web Server logs with IP addresses and Host Name
88.	Which of the following tool can be used to filter web requests associated with the SQL injection attack?	B. UrlScan
89.	Which of the following refers to the discarding of packets at the routing level without informing the source that the data did not reach its intended recipient?	C. Black Hole Filtering
90.	Charline is working as a L2 SOC Analyst. One day, a 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 should her next action according to the SOC workflow?	B. She should contact the network administrator immediately to resolve the problem.
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 ex-	D. Tactical Threat Intelligence

pected to perform the attack on the organization, and the technical capabilities and goals of the attackers along with the attack vectors?

92. If the SIEM generates the following four alerts at the the same time: I. Firewall blocking traffic from getting into the network alerts, II. SQL Injection attempt alerts, III. Data deletion attempts, and IV. Brute force attempt alerts. Which alert should be given least priority per effective alert triaging?

I. Firewall blocking traffic from getting into the network alerts

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

B. Chief Information Security Officer (CISO)

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?

C. OpenDNS

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

C. True Negative Incidents

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

C. Incident Classification

97. Identify the HTTP status codes that represents the server error.
A. 2XX
B. 4XX
C. 1XX
D. 5XX

D. 5XX

98. Jony , a security analyst, while monitoring IIS logs, identified events shown in the figure below
What does this event log indicate?
A. Parameter Tampering Attack
B. XSS Attack
C. Directory Traversal Attack
D. SQL Injection Attack

A. Parameter Tampering Attack

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

B. Bruteforce attack

C. Rainbow Table Attack
D. Birthday Attack

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 forms?	C. XSS Attacks