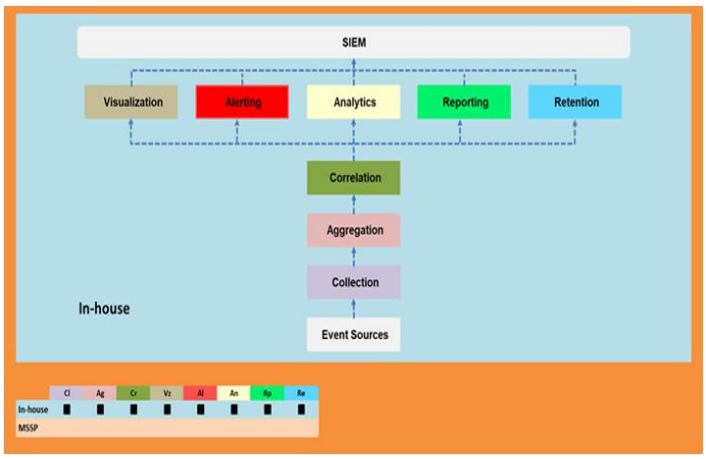
1) An organization is implementing and deploying the SIEM with following capabilities. What kind of SIEM deployment architecture the organization is planning to implement?



- Cloud, MSSP Managed
- Self-hosted, Self-Managed
- Self-hosted, MSSP Managed.

2) Which of the following directory will contain logs related to printer access?

- /var/log/cups/accesslog file
- /var/log/cups/Printeraccess_log file
- /var/log/cups/access_log file
- /var/log/cups/Printer_log file

3) What does the HTTP status codes 1XX represents?

4XX • Client error
3XX • Redirection
2XX • Success
1XX • Informational message

5XX represents server error

4) What is the process of monitoring and capturing all data packets passing through a given network using different tools?

- DNS Footprinting
- Port Scanning
- Network Scanning
- Network Sniffing

Module 02 Page 70

5) 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]

Module 03 Page 291

- 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)
- Display both the date and the time for each log record

6) 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

- Extreme
- Medium
- Low
- High

Module 06 Page 722

7) 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?

Module 04 Page 536

- index=windows LogName=Security EventCode=4678 NOT (Account_Name=*$) .. ..
- index=windows LogName=Security EventCode=5688 NOT (Account_Name=*$) ... ...
- index=windows LogName=Security EventCode=3688 NOT (Account_Name=*$) .. ..
- index=windows LogName=Security EventCode=4688 NOT (Account_Name=*$) .. ..

8) Identify the HTTP status codes that represents the server error.

- 1XX
- 4XX
- 2XX
- 5XX

9) 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?

p-448

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

10) What type of event is recorded when an application driver loads successfully in Windows?

Glossary Page 891

- Success Audit
- Error
- Warning
- Information

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

- Call Organizational Disciplinary Team
- Set a Forensic lab
- Send it to the nearby police station
- Create a Chain of Custody Document

Module 06 Page 748

12) Identify the attack, where an attacker tries to discover all the possible information about a target network before launching a further attack.

- Man-In-Middle Attack
- Ransomware Attack
- DoS Attack
- Reconnaissance Attack

Module 02 Page 65

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

Module 04 Page 449

What does this event log indicate?

- Parameter Tampering Attack
- XSS Attack
- SQL injection Attack
- Directory Traversal Attack

14) Identify the attack in which the attacker exploits a target system through publicly known but still unpatched vulnerabilities.

- Slow DoS Attack
- Zero-Day Attack
- DNS Poisoning Attack
- DHCP Starvation

15) Which of the log storage method arranges event logs in the form of a circular buffer?

Wrapping method: In this method, event logs are arranged in the form of a circular buffer.

Module 03 Page 222

- non-wrapping
- wrapping
- LIFO
- FIFO

16) 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?

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

17) 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? Module 03 Page 304

- SystemDrive%\inetpub\logs\LogFiles\W3SVCN
- SystemDrive%\inetpub\ LogFiles\logs\W3SVCN
- SystemDrive%\LogFiles\inetpub\logs\W3SVCN
- %SystemDrive%\LogFiles\logs\W3SVCN

18) What does HTTPS Status code 403 represents? Module 04 Page 455

404 • Not Found Error
401 • Unauthorized Error
403 • Forbidden Error
500 • Internal Server Error

19) Which of the following Windows event is logged every time when a user tries to access the "Registry" key? Module 04 Page 505

- 4663
- 4656
- 4660
- 4657

20) Which of the following attack inundates DHCP servers with fake DHCP requests to exhaust all available IP addresses? Module 02 Page 81

- DHCP Cache Poisoning
- DHCP Spoofing Attack
- DHCP Starvation Attacks
- DHCP Port Stealing

21) Properly applied cyber threat intelligence to the SOC team help them in discovering TTPs. What does these TTPs refer to?

- Tactics, Threats, and Procedures
- Tactics, Techniques, and Procedures
- Targets, Threats, and Process
- Tactics, Targets, and Process

22) 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? Module 04 Page 560

- I
- IV
- III
- II

23) 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?

- False Negative Incidents
- True Negative Incidents
- False positive Incidents
- True Positive Incidents

24) 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?

- Incident Analysis and Validation Module 06 Page 663
- Incident Prioritization
- Incident Recording
- Incident Classification

25) Which of the following command is used to view iptables logs on Ubuntu and Debian distributions? Module 03 Page 281

- $ tailf /var/log/kern.log
- # tailf /var/log/sys/messages

- $ tailf /var/log/sys/kern.log
- # tailf /var/log/messages

26) Which of the following can help you eliminate the burden of investigating false positives?

Module 04 Page 562

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

27) Which of the following formula represents the risk?

Module 06 Page 719

- Risk = Likelihood x Impact x Asset Value
- Risk = Likelihood x Consequence x Severity
- Risk = Likelihood x Impact x Severity
- Risk = Likelihood x Severity x Asset Value

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

Module 06 Page 742

- Eradication
- Containment
- Data Collection
- Identification

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

- /Library/Logs/Sync
- /var/log/cups/access_log
- ~/Library/Logs
- /private/var/log

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

- Hydra
- ZAP proxy
- Nmap
- UrlScan

31) 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?

Module 04 Page 431

- Hybrid Model, Jointly Managed
- Cloud, Self-Managed
- Self-hosted, Self-Managed
- Self-hosted, MSSP Managed

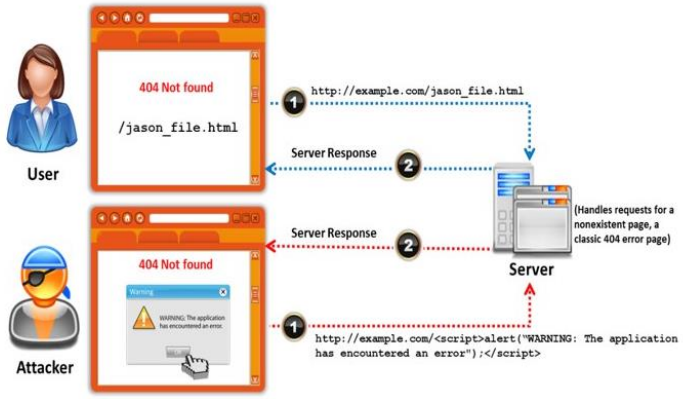
32) Which of the following stage executed after identifying the required event sources?

Module 04 Page 406

- Defining Rule for the Use Case
- Validating the event source against monitoring requirement
- Implementing and Testing the Use Case
- Identifying the monitoring Requirements

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

pag 114



- Session Attack
- Cross-site Scripting Attack
- Denial-of-Service Attack
- SQL Injection Attack

34) 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.

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

35) 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?

- Black Hole Filtering

page 795

- Rate Limiting

- Drop Requests
- Load Balancing

36) 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?

page 582

- Analytical Threat Intelligence
- Operational Threat Intelligence
- Strategic Threat Intelligence
- Tactical Threat Intelligence

37) 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

page 809

- Apility.io
- OpenDNS
- Malstrom
- I-Blocklist

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

page 193

- Exploitation
- Delivery
- Reconnaissance
- Weaponization

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

page 457

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

40) 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?

- Understand the security permissions given to serialization and deserialization
- Deserialization of trusted data must cross a trust boundary

page 826

- Validate untrusted input, which is to be serialized to ensure that serialized data contain only trusted classes
- Allow serialization for security-sensitive classes

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

page 888

- Threat trending Intelligence
- Detection Threat Intelligence
- Operational Intelligence
- Counter Intelligence

42) 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?

page 765

- IntelMQ
- MagicTree
- threat_note
- Malstrom

43) Which of the following formula is used to calculate the EPS of the organization?

page 414

- EPS = number of security events / time in seconds
- EPS = number of normalized events / time in seconds
- EPS = number of correlated events / time in seconds
- EPS = average number of correlated events / time in seconds

44) The Syslog message severity levels are labelled from level 0 to level 7. What does level 0 indicate?

Module 03 Page 246

- Notification
- Alert
- Debugging
- Emergency

45) 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?

Module 05 Page 610

- Analysis and Production
- Dissemination and Integration
- Collection
- Processing and Exploitation

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

- Information

page 230

- Error
- Warning
- Failure

47) Which of the following attack can be eradicated by disabling of "allow_url_fopen and allow_url_include" in the php.ini file

- LDAP Injection Attacks
- Command Injection Attacks
- File Injection Attacks
- URL Injection Attacks

page 815

48) 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?

- Login records
- Error log
- General message and system-related stuff
- System boot log

p-241

49) 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.

- Session Fixation Attack
- SQL Injection Attack
- Denial-of-Service Attack
- Parameter Tampering Attack

p- 120

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

- 4624
- 4625
- 7045
- 5140

p-542

51) 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?

- Web Services Attacks
- Session Management Attacks

p-824

- XSS Attacks
- Broken Access Control Attacks

52) 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?

p-722

- Medium
- Low
- High
- Extreme

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

- Firewall
- De-Militarized Zone (DMZ)
- Honeypot
- Intrusion Detection System

p-701

54) What does the Security Log Event ID 4624 of Windows 10 indicate?

- An account was successfully logged on
- Service added to the endpoint
- A share was assessed
- New process executed

p-539

55) 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?

- Operational Threat Intelligence
- Strategic Threat Intelligence
- Technical Threat Intelligence
- Tactical Threat Intelligence

p-583

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

- Eradication
- Systems Recovery
- Evidence Handling
- Evidence Gathering

p-667

57) 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?

p-671

- Incident Response Resources
- Incident Response Mission
- Incident Response Intelligence
- Incident Response Vision

58) Which of the following formula represents the risk levels?

- Level of risk = Consequence x Severity
- Level of risk = Consequence x Likelihood
- Level of risk = Consequence x Impact
- Level of risk = Consequence x Asset Value

page 721

59) 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?

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

p 423

60) 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?

- show logging | access 210
- show logging | forward 210
- show logging | include 210
- show logging | route 210

p 299

61) 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?

- Rainbow Table Attack
- Birthday Attack
- Hybrid Attack
- Bruteforce Attack

p -73

62) 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

p- 122

- Denial-of-Service Attack
- Form Tampering Attack
- Directory Traversal Attack
- SQL Injection Attack

63) John as a SOC analyst is worried about the amount of Tor traffic hitting the network. He wants to prepare a dashborad 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?

p 488

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

64) 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?

p 227

- Level
- Keywords
- Task Category
- Source

65) 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)|>)/I.
What does this event log indicates?

p-446

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

66) 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 component he should include in the above threat intelligent strategy plan to make it effective?

p-590

- Threat boosting
- Threat trending
- Threat buy-in

- Threat pivoting

67) Which of the following attack can be eradicated by filtering improper XML syntax?

- CAPTCHA Attacks
- Web Services Attacks
- SQL Injection Attacks
- Insufficient Logging and Monitoring Attacks

68) Which of the following Windows features is used to enable Security Auditing in Windows?

- Windows Defender
- Bitlocker
- Windows Firewall
- Local Group Policy Editor

69) Juliea a SOC analyst, while monitoring logs, noticed large TXT , NULL payloads. What does this indicate?

- DNS Exfiltration Attempt p-520
- Covering Tracks Attempt
- Concurrent VPN Connections Attempt
- DHCP Starvation Attempt

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

- Planning and budgeting → Physical location and structural design considerations → Forensics lab licensing → Work area considerations → Human resource considerations → Physical security recommendations
- Planning and budgeting → Forensics lab licensing → Physical location and structural design considerations → Work area considerations → Physical security recommendations → Human resource considerations p-687
- Planning and budgeting → Physical location and structural design considerations → Work area considerations → Human resource considerations → Physical security recommendations → Forensics lab licensing
- Planning and budgeting → Physical location and structural design considerations→ Forensics lab licensing → Human resource considerations → Work area considerations → Physical security recommendations

71) What is the correct sequence of SOC Workflow?

- Collect, Ingest, Document, Validate, Report, Respond p-18
- Collect, Ingest, Validate, Document, Report, Respond
- Collect, Ingest, Validate, Report, Respond, Document

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

72) 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. p 114

- Denial-of-Service Attack
- SQL Injection Attack
- Cross-site Scripting Attack
- Session Attack

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

- Heuristic-based detection
- Rule-based detection
- Anomaly-based detection
- Signature-based detection

p 438

74) 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?

- DARPA
- PCI-DSS
- FISMA
- HIPAA

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

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

76) 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.

p-23

- Security Engineer
- Security Analyst—L2
- Chief Information Security Officer (CISO)
- Security Analyst—L1

77) 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?

- She should immediately contact the network administrator to solve the problem
- She should communicate this incident to the media immediately
- She should immediately escalate this issue to the management
- She should formally raise a ticket and forward it to the IRT

p-710

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

- signature-based
- rule-based
- push-based
- pull-based

p-210

79) Which of the following factors determine the choice of SIEM architecture?

- DHCP Configuration
- Network Topology
- DNS Configuration
- SMTP Configuration

Module 04 Page 419

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

- SSE-CMM
- COBIT
- ITIL
- SOC-CMM

p-38

81) 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.

- 1 & 2 p 374-375
- 2 & 3
- 3 & 1
- 1 & 4

82) Which of the following command is used to enable logging in iptables?

- $ iptables -A INPUT -j LOG
- $ iptables -A OUTPUT -j LOG p-280
- $ iptables -B INPUT -j LOG
- $ iptables -B OUTPUT -j LOG

83) Which of the following contains the performance measures, and proper project and time management details?

- Incident Response Process
- Incident Response Policy
- Incident Response Tactics
- Incident Response Procedures

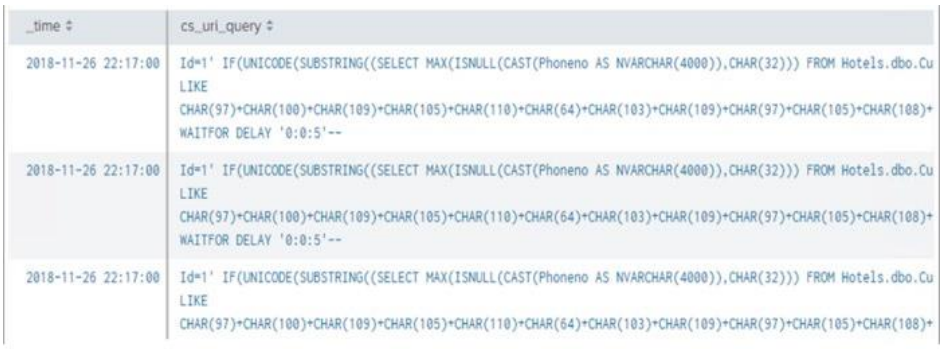
84) Which encoding replaces unusual ASCII characters with "%" followed by the character's two-digit ASCII code expressed in hexadecimal?

- Base64 Encoding
- UTF Encoding
- Unicode Encoding p-834
- URL Encoding

85) Which of the following attack can be eradicated by using a safe API to avoid the use of the interpreter entirely? p-815

- SQL Injection Attacks
- Command Injection Attacks
- LDAP Injection Attacks
- File Injection Attacks

86) 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)+

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

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

- IIS Data
- DNS Data
- Netstat Data
- DHCP Data

88) Which of the following tool is used to recover from web application incident?

- Proxy Workbench
- Symantec Secure Web Gateway
- CrowdStrike Falcon™ Orchestrator
- Smoothwall SWG

p-842

89) 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?

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

p-444

90) 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?

- Absorbing the Attack
- Diverting the Traffic

- Blocking the Attacks
- Degrading the Services

91) Which of the following is a Threat Intelligence Platform?

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

p-618

92) 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?

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

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

- DHCP starvation Attack
- DoS Attack
- File Injection Attack
- Ransomware Attack

94) What does Windows event ID 4740 indicate?

- A user account was enabled.
- A user account was disabled.
- A user account was created.
- A user account was locked out.

p-502

95) 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

- 1 and 3
- 3 and 4

- 2 and 3
- 1 and 2

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

p - 461

- /etc/siem/ossim/server/reputation.data
- /etc/ossim/server/reputation.data
- /etc/ossim/reputation
- /etc/ossim/siem/server/reputation/data

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

- Rainbow Table Attack
- Dictionary Attack

p-74

- Bruteforce Attack
- Syllable Attack

98) 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?

- Throttling
- Egress Filtering

p-795

- Ingress Filtering
- Rate Limiting

99) 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?

- Operational Threat Intelligence
- Tactical Threat Intelligence

p-582

- Strategic Threat Intelligence
- Functional Threat Intelligence

QUESTION 100

Byron, a new network administrator at FBI, would like to ensure that Windows PCs there are up-to-date and have less
internal security flaws. What can he do?

A. Centrally assign Windows PC group policies
B. Dedicate a partition on HDD and format the disk using NTFS
C. Download and install latest patches and enable Windows Automatic Updates
D. Install antivirus software and turn off unnecessary services

Answer: D