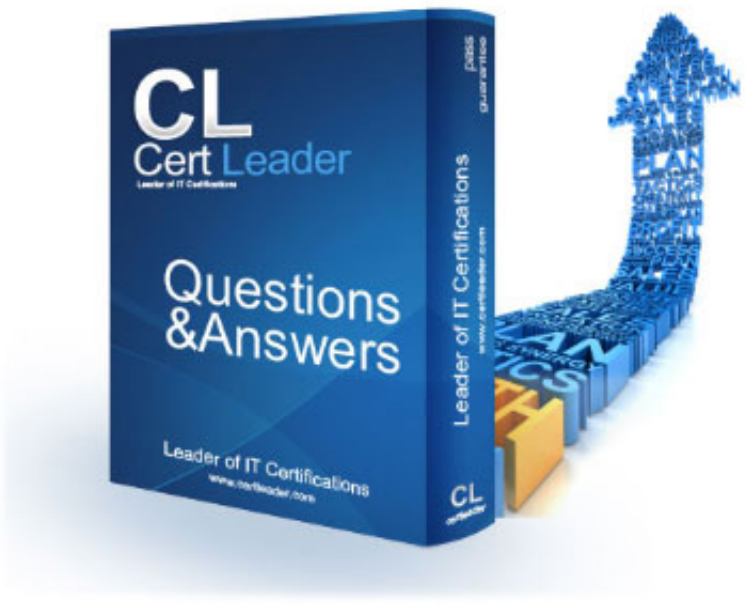
200-201 Dumps

Understanding Cisco Cybersecurity Operations Fundamentals

https://www.certleader.com/200-201-dumps.html



NEW QUESTION 1
During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?

A. examination
B. investigation
C. collection
D. reporting

Answer: C

NEW QUESTION 2
What is the difference between deep packet inspection and stateful inspection?

A. Deep packet inspection is more secure than stateful inspection on Layer 4
B. Stateful inspection verifies contents at Layer 4 and deep packet inspection verifies connection at Layer 7
C. Stateful inspection is more secure than deep packet inspection on Layer 7
D. Deep packet inspection allows visibility on Layer 7 and stateful inspection allows visibility on Layer 4

Answer: D

NEW QUESTION 3
You have identified a malicious file in a sandbox analysis tool. Which piece of file information from the analysis is needed to search for additional downloads of this file by other hosts?

A. file name
B. file hash value
C. file type
D. file size

Answer: B

NEW QUESTION 4
What is a benefit of agent-based protection when compared to agentless protection?

A. It lowers maintenance costs
B. It provides a centralized platform
C. It collects and detects all traffic locally
D. It manages numerous devices simultaneously

Answer: B

NEW QUESTION 5
Which type of evidence supports a theory or an assumption that results from initial evidence?

A. probabilistic
B. indirect
C. best
D. corroborative

Answer: D

NEW QUESTION 6
A user received a malicious attachment but did not run it. Which category classifies the intrusion?

A. weaponization
B. reconnaissance
C. installation
D. delivery

Answer: D

NEW QUESTION 7
What does an attacker use to determine which network ports are listening on a potential target device?

A. man-in-the-middle
B. port scanning
C. SQL injection
D. ping sweep

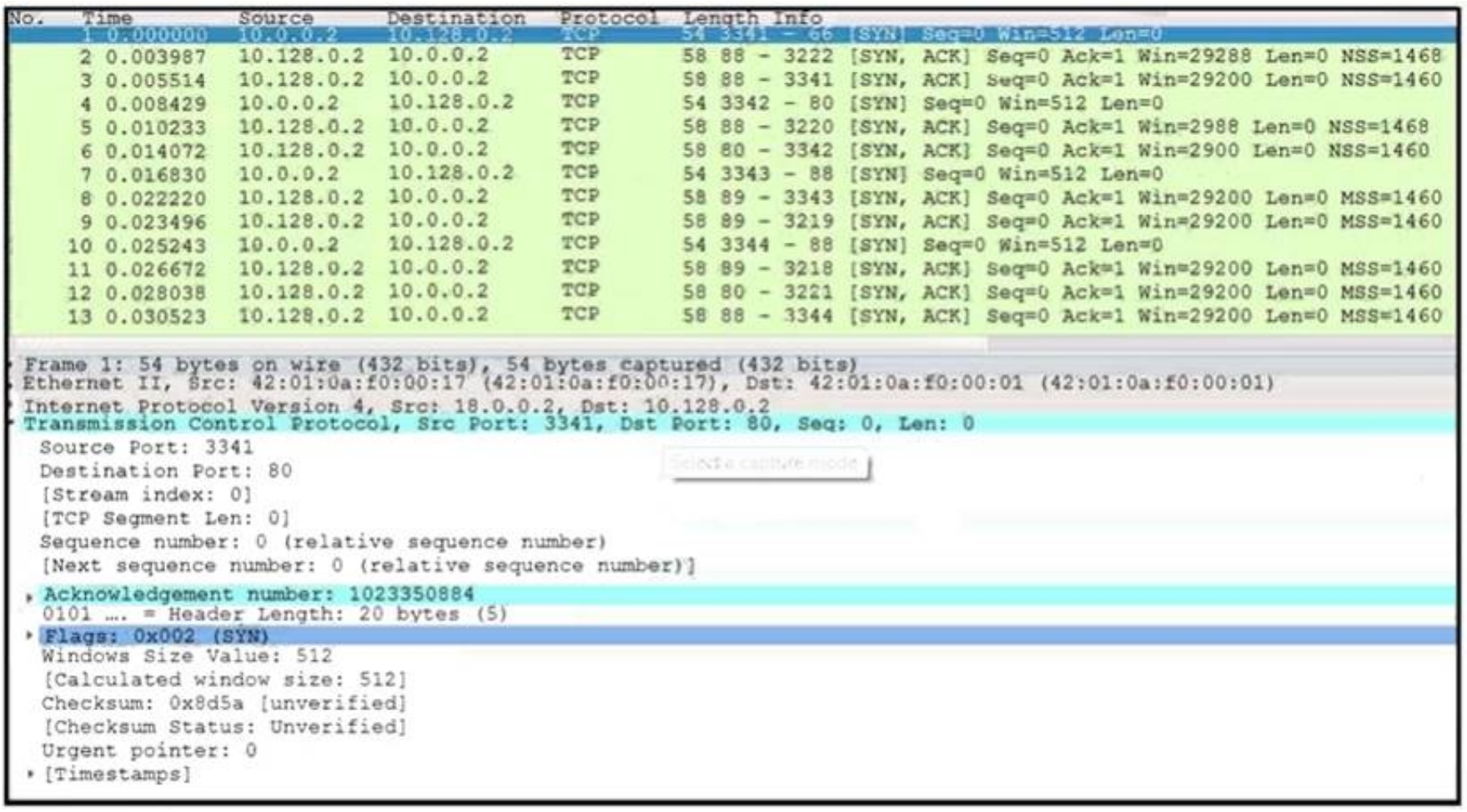
Answer: B

NEW QUESTION 8
Which type of data collection requires the largest amount of storage space?

A. alert data
B. transaction data
C. session data
D. full packet capture

Answer: D

NEW QUESTION 9
Refer to the exhibit.



What is occurring in this network traffic?

A. high rate of SYN packets being sent from a multiple source towards a single destination IP
B. high rate of SYN packets being sent from a single source IP towards multiple destination IPs
C. flood of ACK packets coming from a single source IP to multiple destination IPs
D. flood of SYN packets coming from a single source IP to a single destination IP

Answer: D

NEW QUESTION 10
What is a difference between inline traffic interrogation and traffic mirroring?

A. Inline inspection acts on the original traffic data flow
B. Traffic mirroring passes live traffic to a tool for blocking
C. Traffic mirroring inspects live traffic for analysis and mitigation
D. Inline traffic copies packets for analysis and security

Answer: B

NEW QUESTION 10
What is the practice of giving an employee access to only the resources needed to accomplish their job?

A. principle of least privilege
B. organizational separation
C. separation of duties
D. need to know principle

Answer: A

NEW QUESTION 14
Which metric is used to capture the level of access needed to launch a successful attack?

A. privileges required
B. user interaction
C. attack complexity
D. attack vector

Answer: A

NEW QUESTION 18
What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

A. least privilege
B. need to know
C. integrity validation
D. due diligence

Answer: A

NEW QUESTION 22
Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?

A. decision making
B. rapid response
C. data mining
D. due diligence

Answer: A

NEW QUESTION 26
Which regex matches only on all lowercase letters?

A. [az]+
B. [^az]+
C. az+
D. a*z+

Answer: A

NEW QUESTION 28
Which system monitors local system operation and local network access for violations of a security policy?

A. host-based intrusion detection
B. systems-based sandboxing
C. host-based firewall
D. antivirus

Answer: C

NEW QUESTION 30
What makes HTTPS traffic difficult to monitor?

A. SSL interception
B. packet header size
C. signature detection time
D. encryption

Answer: D

NEW QUESTION 33
What causes events on a Windows system to show Event Code 4625 in the log messages?

A. The system detected an XSS attack
B. Someone is trying a brute force attack on the network
C. Another device is gaining root access to the system
D. A privileged user successfully logged into the system

Answer: B

NEW QUESTION 35
A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?

A. CD data copy prepared in Windows
B. CD data copy prepared in Mac-based system
C. CD data copy prepared in Linux system
D. CD data copy prepared in Android-based system

Answer: A

NEW QUESTION 36
Refer to the exhibit.

Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2020	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	*

Which type of log is displayed?

A. IDS
B. proxy
C. NetFlow
D. sys

Answer: D

NEW QUESTION 39
What is an attack surface as compared to a vulnerability?

A. any potential danger to an asset
B. the sum of all paths for data into and out of the application
C. an exploitable weakness in a system or its design
D. the individuals who perform an attack

Answer: B

NEW QUESTION 42
An offline audit log contains the source IP address of a session suspected to have exploited a vulnerability resulting in system compromise.
Which kind of evidence is this IP address?

A. best evidence
B. corroborative evidence
C. indirect evidence
D. forensic evidence

Answer: B

NEW QUESTION 47
What does cyber attribution identify in an investigation?

A. exploit of an attack
B. threat actors of an attack
C. vulnerabilities exploited
D. cause of an attack

Answer: B

NEW QUESTION 48
What is the difference between an attack vector and attack surface?

A. An attack surface identifies vulnerabilities that require user input or validation; and an attack vectoridentifies vulnerabilities that are independent of user actions.
B. An attack vector identifies components that can be exploited; and an attack surface identifies the potential path an attack can take to penetrate the network.
C. An attack surface recognizes which network parts are vulnerable to an attack; and an attack vector identifies which attacks are possible with these vulnerabilities.
D. An attack vector identifies the potential outcomes of an attack; and an attack surface launches an attack using several methods against the identified vulnerabilities.

Answer: C

NEW QUESTION 51
An investigator is examining a copy of an ISO file that is stored in CDFS format. What type of evidence is this file?

A. data from a CD copied using Mac-based system
B. data from a CD copied using Linux system
C. data from a DVD copied using Windows system
D. data from a CD copied using Windows

Answer: B

NEW QUESTION 52
Refer to the exhibit.

```
# nmap -sV 172.18.104.139

Starting Nmap 7.01 ( https://nmap.org ) at 2020-03-07 11:36 EST
Nmap scan report for 172.18.104.139
Host is up (0.000018s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
25/tcp  open  smtp     Postfix smtpd
110/tcp open  pop3     Dovecot pop3d
143/tcp open  imap     Dovecot imapd
Service Info: Host:   172.18.108.139; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

What does the output indicate about the server with the IP address 172.18.104.139?

A. open ports of a web server
B. open port of an FTP server
C. open ports of an email server
D. running processes of the server

Answer: C

NEW QUESTION 54
What is the difference between the ACK flag and the RST flag in the NetFlow log session?

A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the data for the payload is complete
B. The ACK flag confirms the beginning of the TCP connection, and the RST flag responds when the data for the payload is complete
C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection
D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

Answer: D

NEW QUESTION 59
Which two elements are used for profiling a network? (Choose two.)

A. total throughout
B. session duration
C. running processes
D. OS fingerprint
E. listening ports

Answer: DE

NEW QUESTION 61
Which utility blocks a host portscan?

A. HIDS
B. sandboxing
C. host-based firewall
D. antimalware

Answer: C

NEW QUESTION 66
Which security principle requires more than one person is required to perform a critical task?

A. least privilege
B. need to know
C. separation of duties
D. due diligence

Answer: C

NEW QUESTION 71
Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

A. known-plaintext
B. replay
C. dictionary
D. man-in-the-middle

Answer: D

NEW QUESTION 76
A network engineer discovers that a foreign government hacked one of the defense contractors in their home country and stole intellectual property. What is the threat agent in this situation?

A. the intellectual property that was stolen
B. the defense contractor who stored the intellectual property
C. the method used to conduct the attack
D. the foreign government that conducted the attack

Answer: D

NEW QUESTION 77
A system administrator is ensuring that specific registry information is accurate.
Which type of configuration information does the HKEY_LOCAL_MACHINE hive contain?

A. file extension associations
B. hardware, software, and security settings for the system
C. currently logged in users, including folders and control panel settings
D. all users on the system, including visual settings

Answer: B

NEW QUESTION 78
What is an example of social engineering attacks?

A. receiving an unexpected email from an unknown person with an uncharacteristic attachment from someone in the same company
B. receiving an email from human resources requesting a visit to their secure website to update contact information
C. sending a verbal request to an administrator who knows how to change an account password
D. receiving an invitation to the department's weekly WebEx meeting

Answer: B

NEW QUESTION 81
Which access control model does SELinux use?

A. RBAC
B. DAC
C. MAC
D. ABAC

Answer: C

NEW QUESTION 84
Which attack is the network vulnerable to when a stream cipher like RC4 is used twice with the same key?

A. forgery attack
B. plaintext-only attack
C. ciphertext-only attack
D. meet-in-the-middle attack

Answer: C

NEW QUESTION 87
An analyst is exploring the functionality of different operating systems.
What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?

A. queries Linux devices that have Microsoft Services for Linux installed
B. deploys Windows Operating Systems in an automated fashion
C. is an efficient tool for working with Active Directory
D. has a Common Information Model, which describes installed hardware and software

Answer: D

NEW QUESTION 90
An analyst received an alert on their desktop computer showing that an attack was successful on the host. After investigating, the analyst discovered that no mitigation action occurred during the attack. What is the reason for this discrepancy?

A. The computer has a HIPS installed on it.
B. The computer has a NIPS installed on it.
C. The computer has a HIDS installed on it.
D. The computer has a NIDS installed on it.

Answer: C

NEW QUESTION 92
Which two compliance frameworks require that data be encrypted when it is transmitted over a public network?
(Choose two.)

A. PCI
B. GLBA
C. HIPAA
D. SOX
E. COBIT

Answer: AC

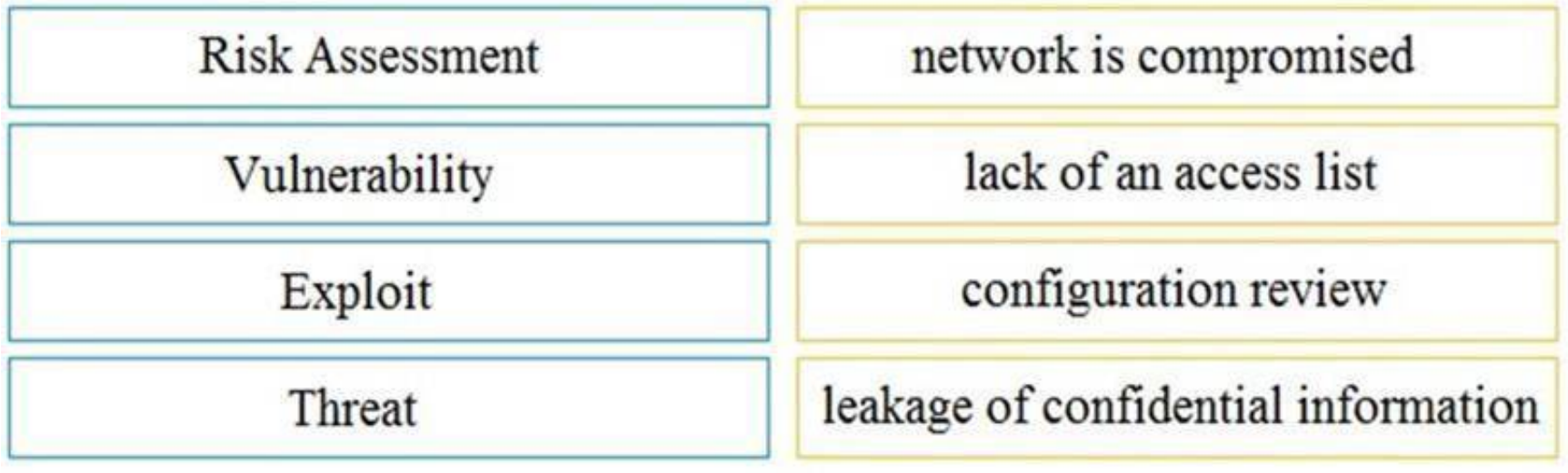
NEW QUESTION 95
How is NetFlow different than traffic mirroring?

A. NetFlow collects metadata and traffic mirroring clones data

B. Traffic mirroring impacts switch performance and NetFlow does not
C. Traffic mirroring costs less to operate than NetFlow
D. NetFlow generates more data than traffic mirroring

Answer: A

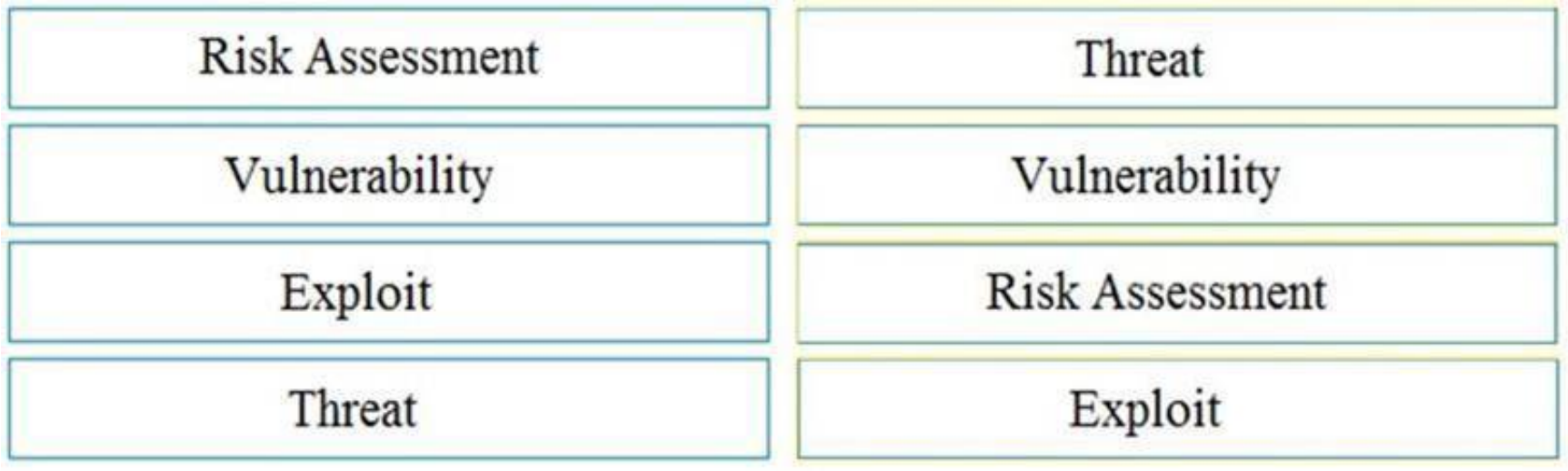
NEW QUESTION 99
Drag and drop the security concept on the left onto the example of that concept on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 100
Why is encryption challenging to security monitoring?

A. Encryption analysis is used by attackers to monitor VPN tunnels.
B. Encryption is used by threat actors as a method of evasion and obfuscation.
C. Encryption introduces additional processing requirements by the CPU.
D. Encryption introduces larger packet sizes to analyze and store.

Answer: B

NEW QUESTION 103
Which IETF standard technology is useful to detect and analyze a potential security incident by recording session flows that occurs between hosts?

A. SFlow
B. NetFlow
C. NFlow
D. IPFIX

Answer: D

NEW QUESTION 108
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 200-201 Exam with Our Prep Materials Via below:

https://www.certleader.com/200-201-dumps.html