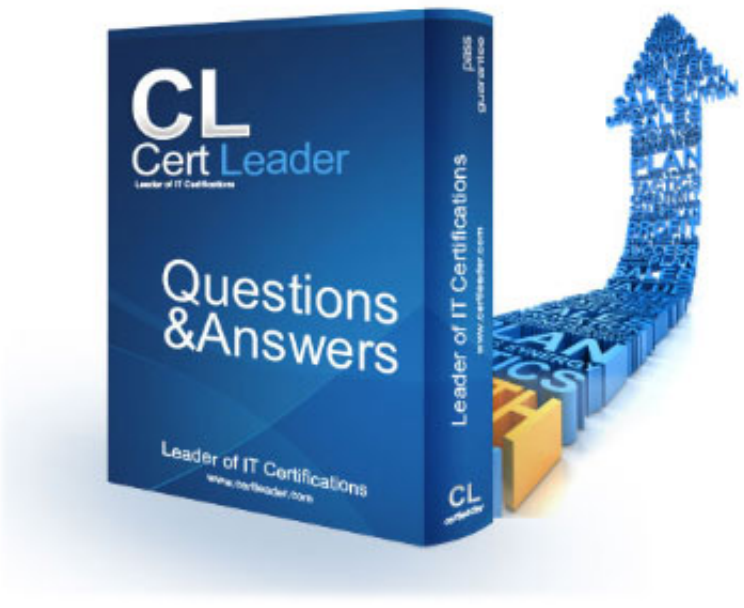
200-201 Dumps

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
Refer to the exhibit.

Top 10 Src IP Addr ordered by flows:

Date first seen	Duration	Src IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2019-11-30 06:45:50.990	1147.332	192.168.12.234	109183	202523	13.1 M	176	96116	68
2019-11-30 06:45:02.928	1192.834	10.10.151.203	62794	219715	25.9 M	184	182294	123
2019-11-30 06:59:24.563	330.110	192.168.28.173	27864	47943	2.2 M	145	55769	48

What information is depicted?

A. IIS data
B. NetFlow data
C. network discovery event
D. IPS event data

Answer: B

NEW QUESTION 3
Which two elements are assets in the role of attribution in an investigation? (Choose two.)

A. context
B. session
C. laptop
D. firewall logs
E. threat actor

Answer: AE

NEW QUESTION 4
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 5
Drag and drop the technology on the left onto the data type the technology provides on the right.

tcpdump	session data
web content filtering	full packet capture
traditional stateful firewall	transaction data
NetFlow	connection event

A. Mastered
B. Not Mastered

Answer: A

Explanation:

tcpdump	web content filtering
web content filtering	tcpdump
traditional stateful firewall	NetFlow
NetFlow	traditional stateful firewall

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 is the function of a command and control server?

A. It enumerates open ports on a network device
B. It drops secondary payload into malware
C. It is used to regain control of the network after a compromise
D. It sends instruction to a compromised system

Answer: D

NEW QUESTION 8
Refer to the exhibit.

```
GET /item.php?id=34' or sleep(10)
```

This request was sent to a web application server driven by a database. Which type of web server attack is represented?

A. parameter manipulation
B. heap memory corruption
C. command injection
D. blind SQL injection

Answer: D

NEW QUESTION 9
Which attack method intercepts traffic on a switched network?

A. denial of service
B. ARP cache poisoning
C. DHCP snooping
D. command and control

Answer: C

NEW QUESTION 10
Refer to the exhibit.

```
- Internet Protocol version 4, Src: 192.168.122.100 (192.168.122.100), Dst:
81.179.179.69 (81.179.179.69)
   Version: 4
   Header Length: 20 bytes
 + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT
(Not ECN-Capable Transport))
   Total Length: 538
   Identification: 0x6bse (27534)
 + Flags: 0x02 (Don't Fragment)
   Fragment offset: 0
   Time to live: 128
   Protocol: TCP (6)
 + Header checksum: 0x000 [Validation disabled]
   Source: 192.168.122.100 (192.168.122.100)
   Destination: 81.179.179.69 (81.179.179.69)
   [Source GeoIP: Unknown]



+ Transmission control protocol. src port: 50272 (50272) Dst Port: 80 (80).
Seq: 419451624. Ack: 970444123. Len: 490
```

What should be interpreted from this packet capture?

A. IP address 179.179.69/50272/192.168.122.100/80/6 is sending a packet from port 80 of IP address 192.168.122.100 that is going to port 50272 of IP address 81.179.179.69 using IP protocol 6.
B. IP address 192.168.122.100/50272/81.179.179.69/80/6 is sending a packet from port 50272 of IP address 192.168.122.100 that is going to port 80 of IP address 81.179.179.69 using IP protocol 6.
C. IP address 192.168.122.100/50272/81.179.179.69/80/6 is sending a packet from port 80 of IP address 192.168.122.100 that is going to port 50272 of IP address 81.179.179.69 using IP protocol 6.7E503B693763E0113BE0CD2E4A16C9C4
D. IP address 179.179.69/50272/192.168.122.100/80/6 is sending a packet from port 50272 of IP address 192.168.122.100 that is going to port 80 of IP address 81.179.179.69 using IP protocol 6.

Answer: B

NEW QUESTION 10
Which regular expression matches "color" and "colour"?

A. colo?ur
B. col[08]+our
C. colou?r
D. col[09]+our

Answer: C

NEW QUESTION 14
What is the difference between mandatory access control (MAC) and discretionary access control (DAC)?

A. MAC is controlled by the discretion of the owner and DAC is controlled by an administrator
B. MAC is the strictest of all levels of control and DAC is object-based access
C. DAC is controlled by the operating system and MAC is controlled by an administrator
D. DAC is the strictest of all levels of control and MAC is object-based access

Answer: B

NEW QUESTION 16
Which security principle is violated by running all processes as root or administrator?

A. principle of least privilege
B. role-based access control
C. separation of duties
D. trusted computing base

Answer: A

NEW QUESTION 17
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 19
Which evasion technique is a function of ransomware?

A. extended sleep calls
B. encryption
C. resource exhaustion
D. encoding

Answer: B

NEW QUESTION 21
Which regex matches only on all lowercase letters?

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

Answer: A

NEW QUESTION 23
An analyst discovers that a legitimate security alert has been dismissed. Which signature caused this impact on network traffic?

A. true negative
B. false negative
C. false positive
D. true positive

Answer: B

NEW QUESTION 24
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

A. integrity
B. confidentiality
C. availability
D. scope

Answer: A

NEW QUESTION 27
Which signature impacts network traffic by causing legitimate traffic to be blocked?

A. false negative
B. true positive
C. true negative
D. false positive

Answer: D

NEW QUESTION 32
Which step in the incident response process researches an attacking host through logs in a SIEM?

A. detection and analysis
B. preparation
C. eradication
D. containment

Answer: A

NEW QUESTION 37
One of the objectives of information security is to protect the CIA of information and systems. What does CIA mean in this context?

A. confidentiality, identity, and authorization
B. confidentiality, integrity, and authorization
C. confidentiality, identity, and availability
D. confidentiality, integrity, and availability

Answer: D

NEW QUESTION 40
An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked

the user to engage with a link in an email. When the fink launched, it infected machines and the intruder was able to access the corporate network.
Which testing method did the intruder use?

A. social engineering
B. eavesdropping
C. piggybacking
D. tailgating

Answer: A

NEW QUESTION 43
The target web application server is running as the root user and is vulnerable to command injection. Which result of a successful attack is true?

A. cross-site scripting
B. cross-site scripting request forgery
C. privilege escalation
D. buffer overflow

Answer: B

NEW QUESTION 45
A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver. Which event category is described?

A. reconnaissance
B. action on objectives
C. installation
D. exploitation

Answer: C

NEW QUESTION 50
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 52
Which NIST IR category stakeholder is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies?

A. CSIRT
B. PSIRT
C. public affairs
D. management

Answer: D

NEW QUESTION 57
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 62
Which two components reduce the attack surface on an endpoint? (Choose two.)

A. secure boot
B. load balancing
C. increased audit log levels
D. restricting USB ports
E. full packet captures at the endpoint

Answer: AD

NEW QUESTION 63
Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

A. NetScout
B. tcpdump
C. SolarWinds
D. netsh

Answer: B

NEW QUESTION 64
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 66
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 67
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 69
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 70
An analyst is investigating an incident in a SOC environment. Which method is used to identify a session from a group of logs?

A. sequence numbers
B. IP identifier
C. 5-tuple
D. timestamps

Answer: C

NEW QUESTION 72
Which event artifact is used to identify HTTP GET requests for a specific file?

A. destination IP address
B. URI
C. HTTP status code
D. TCP ACK

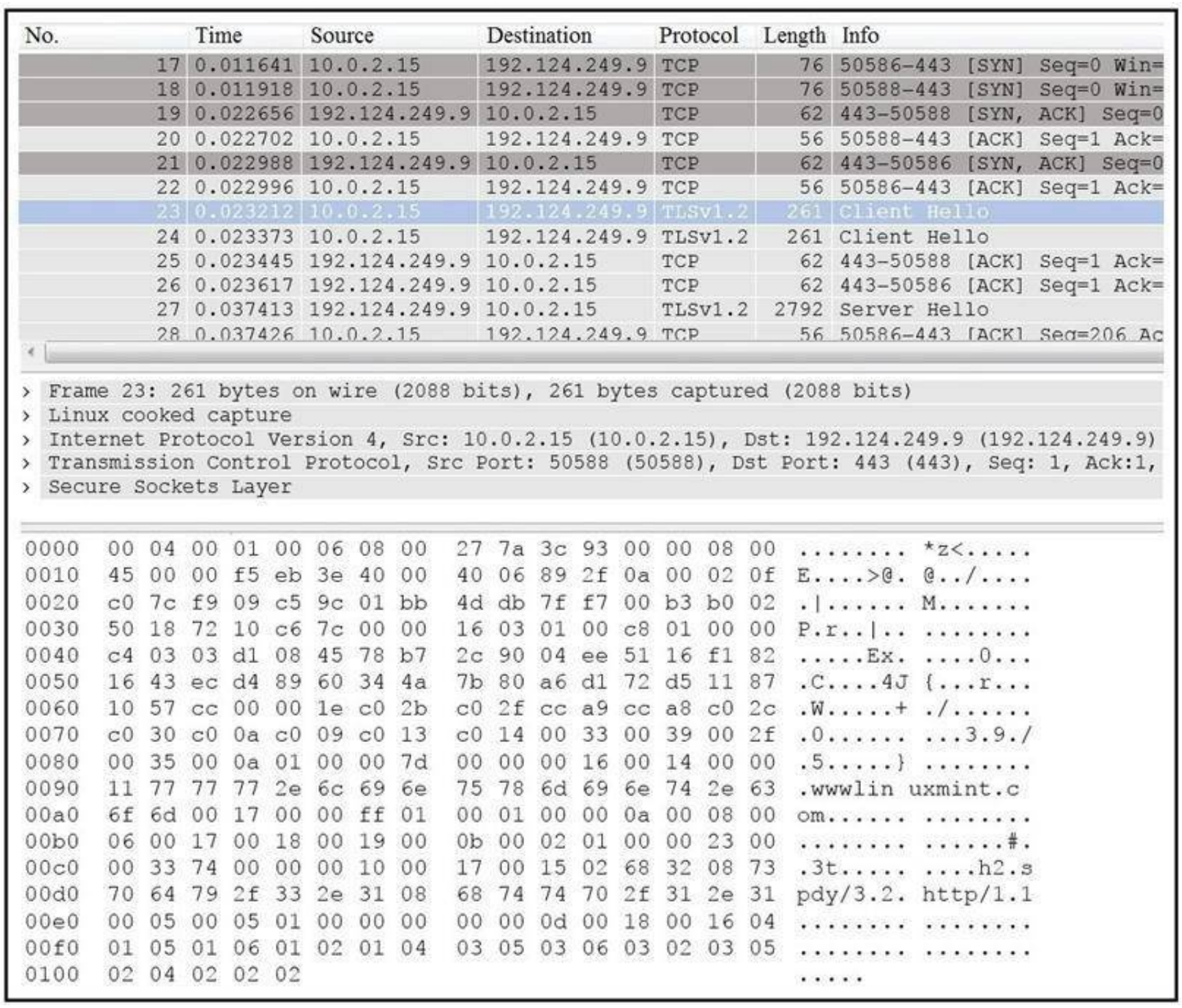
Answer: B

NEW QUESTION 74
Which event is user interaction?

A. gaining root access
B. executing remote code
C. reading and writing file permission
D. opening a malicious file

Answer: D

NEW QUESTION 76
Refer to the exhibit.



Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

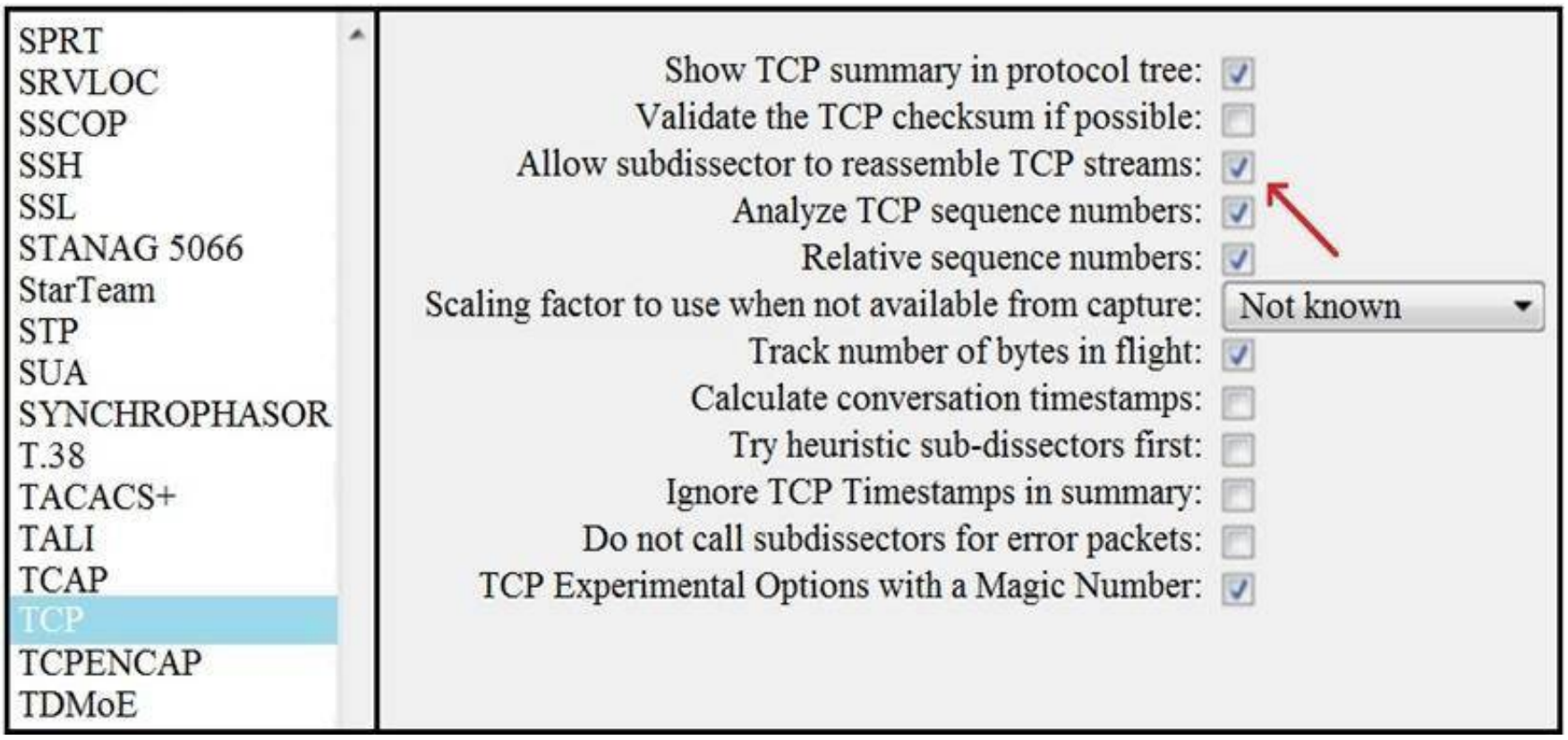
A. Mastered
B. Not Mastered

Answer: A

Explanation:

source address	source address
destination address	source port
source port	destination port
destination port	destination address
Network Protocol	Transport Protocol
Transport Protocol	Network Protocol
Application Protocol	Application Protocol

NEW QUESTION 79
Refer to the exhibit.



What is the expected result when the "Allow subdissector to reassemble TCP streams" feature is enabled?

A. insert TCP subdissectors
B. extract a file from a packet capture
C. disable TCP streams
D. unfragment TCP

Answer: D

NEW QUESTION 81
How does an attacker observe network traffic exchanged between two users?

A. port scanning
B. man-in-the-middle
C. command injection
D. denial of service

Answer: B

NEW QUESTION 86
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 88
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 93
Which two elements are used for profiling a network? (Choose two.)

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

Answer: DE

NEW QUESTION 97
What is a difference between SOAR and SIEM?

A. SOAR platforms are used for threat and vulnerability management, but SIEM applications are not
B. SIEM applications are used for threat and vulnerability management, but SOAR platforms are not
C. SOAR receives information from a single platform and delivers it to a SIEM
D. SIEM receives information from a single platform and delivers it to a SOAR

Answer: A

NEW QUESTION 102
Which action prevents buffer overflow attacks?

A. variable randomization
B. using web based applications
C. input sanitization
D. using a Linux operating system

Answer: C

NEW QUESTION 106
Which type of data consists of connection level, application-specific records generated from network traffic?

A. transaction data
B. location data
C. statistical data
D. alert data

Answer: A

NEW QUESTION 107
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