

Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals



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

Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

- A. syslog messages
- B. full packet capture
- C. NetFlow
- D. firewall event logs

Answer: C

NEW QUESTION 3

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 4

What is the difference between a threat and a risk?

- A. Threat represents a potential danger that could take advantage of a weakness in a system
- B. Risk represents the known and identified loss or danger in the system
- C. Risk represents the nonintentional interaction with uncertainty in the system
- D. Threat represents a state of being exposed to an attack or a compromise either physically or logically

Answer: A

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

Refer to the exhibit.

```
Mar 6 10:35:34 user sshd[12900]: pam_unix(sshd:auth):authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Mar 6 10:35:36 user sshd[12900]: Failed password for invalid user not_bill from
127.0.0.1 port 38346 ssh2
```

In which Linux log file is this output found?

- A. /var/log/authorization.log
- B. /var/log/dmesg
- C. var/log/var.log
- D. /var/log/auth.log

Answer: D

NEW QUESTION 7

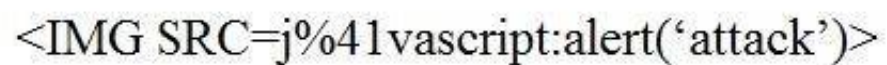
Which category relates to improper use or disclosure of PII data?

- A. legal
- B. compliance
- C. regulated
- D. contractual

Answer: C

NEW QUESTION 8

Refer to the exhibit.



```
<IMG SRC=j%41vascript:alert('attack')>
```

Which kind of attack method is depicted in this string?

- A. cross-site scripting
- B. man-in-the-middle
- C. SQL injection
- D. denial of service

Answer: A

NEW QUESTION 9

An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group. What is the initial event called in the NIST SP800-61?

- A. online assault
- B. precursor
- C. trigger
- D. instigator

Answer: B

NEW QUESTION 10

Which incidence response step includes identifying all hosts affected by an attack'?

- A. post-incident activity
- B. detection and analysis
- C. containment eradication and recovery
- D. preparation

Answer: A

NEW QUESTION 10

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 15

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 20

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 24

An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture the analyst cannot determine the technique and payload used for the communication.

File	Actions	Edit	View	Help
48	41.270348133	185.199.111.153 → 192.168.88.164	TLSv1.2 123	Application Data
49	41.270348165	185.199.111.153 → 192.168.88.164	TLSv1.2 104	Application Data
50	41.270356290	192.168.88.164 → 185.199.111.153	TCP 66 44736 → 443 [ACK]	
Seq=834 Ack=3104 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849				
51	41.270369874	192.168.88.164 → 185.199.111.153	TCP 66 44736 → 443 [ACK]	
Seq=834 Ack=3142 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849				
52	41.270430171	192.168.88.164 → 185.199.111.153	TLSv1.2 104	Application Data
53	41.271767772	185.199.111.153 → 192.168.88.164	TLSv1.2 2854	Application Data
54	41.271767817	185.199.111.153 → 192.168.88.164	TLSv1.2 904	Application Data
55	41.271788996	192.168.88.164 → 185.199.111.153	TCP 66 44736 → 443 [ACK]	
Seq=872 Ack=6768 Win=62592 Len=0 TSval=3947973758 TSecr=2989424849				
56	41.271973293	192.168.88.164 → 185.199.111.153	TLSv1.2 97	Encrypted Alert
57	41.272411701	192.168.88.164 → 185.199.111.153	TCP 66 44736 → 443 [FIN, ACK]	
Seq=903 Ack=6768 Win=64128 Len=0 TSval=3947973759 TSecr=2989424849				
58	41.283301751	185.199.111.153 → 192.168.88.164	TCP 66 443 → 44736 [ACK]	
Seq=6768 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757				
59	41.283301808	185.199.111.153 → 192.168.88.164	TLSv1.2 97	Encrypted Alert
60	41.283321947	192.168.88.164 → 185.199.111.153	TCP 54 44736 → 443 [RST]	
Seq=903 Win=0 Len=0				
61	41.283939151	185.199.111.153 → 192.168.88.164	TCP 66 443 → 44736 [FIN, ACK]	
Seq=6799 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757				
62	41.283945760	192.168.88.164 → 185.199.111.153	TCP 54 44736 → 443 [RST]	
Seq=903 Win=0 Len=0				
63	41.284635561	185.199.111.153 → 192.168.88.164	TCP 66 443 → 44736 [ACK]	
Seq=6800 Ack=904 Win=28160 Len=0 TSval=2989424853 TSecr=3947973759				
64	41.284642324	192.168.88.164 → 185.199.111.153	TCP 54 44736 → 443 [RST]	
Seq=904 Win=0 Len=0				

Which obfuscation technique is the attacker using?

- A. Base64 encoding
- B. transport layer security encryption
- C. SHA-256 hashing
- D. ROT13 encryption

Answer: B

NEW QUESTION 27

How does certificate authority impact a security system?

- A. It authenticates client identity when requesting SSL certificate
- B. It validates domain identity of a SSL certificate
- C. It authenticates domain identity when requesting SSL certificate
- D. It validates client identity when communicating with the server

Answer: B

NEW QUESTION 31

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 33

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.2	10.128.0.2	TCP	54	3341 → 80 [SYN] Seq=0 Win=512 Len=0
2	0.003987	10.128.0.2	10.0.0.2	TCP	58	88 → 3222 [SYN, ACK] Seq=0 Ack=1 Win=29288 Len=0 NSS=1468
3	0.005514	10.128.0.2	10.0.0.2	TCP	58	88 → 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
4	0.008429	10.0.0.2	10.128.0.2	TCP	54	3342 → 80 [SYN] Seq=0 Win=512 Len=0
5	0.010233	10.128.0.2	10.0.0.2	TCP	58	88 → 3220 [SYN, ACK] Seq=0 Ack=1 Win=2988 Len=0 NSS=1468
6	0.014072	10.128.0.2	10.0.0.2	TCP	58	80 → 3342 [SYN, ACK] Seq=0 Ack=1 Win=2900 Len=0 NSS=1460
7	0.016930	10.0.0.2	10.128.0.2	TCP	54	3343 → 88 [SYN] Seq=0 Win=512 Len=0
8	0.022220	10.128.0.2	10.0.0.2	TCP	58	89 → 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
9	0.023496	10.128.0.2	10.0.0.2	TCP	58	89 → 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
10	0.025243	10.0.0.2	10.128.0.2	TCP	54	3344 → 88 [SYN] Seq=0 Win=512 Len=0
11	0.026672	10.128.0.2	10.0.0.2	TCP	58	89 → 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
12	0.028038	10.128.0.2	10.0.0.2	TCP	58	80 → 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
13	0.030523	10.128.0.2	10.0.0.2	TCP	58	88 → 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
 Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)
 Internet Protocol Version 4, Src: 18.0.0.2, Dst: 10.128.0.2
 Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0

Source Port: 3341
 Destination Port: 80
 [Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 0 (relative sequence number)
 [Next sequence number: 0 (relative sequence number)]

Acknowledgement number: 1023350884
 0101 ... = Header Length: 20 bytes (5)

Flags: 0x002 (SYN)
 Windows Size Value: 512
 [Calculated window size: 512]
 Checksum: 0x8d5a [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 [Timestamps]

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 36

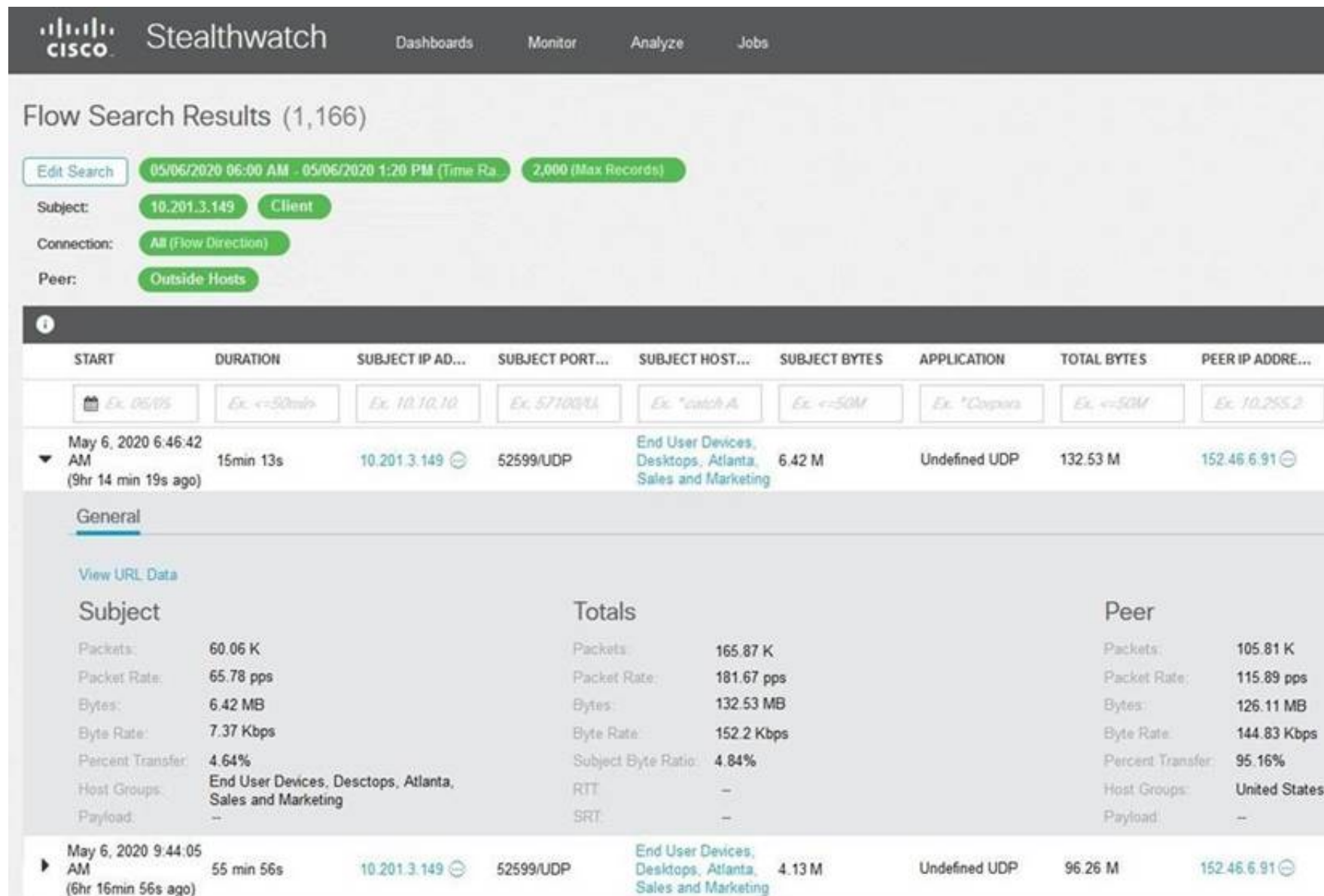
What are two differences in how tampered and untampered disk images affect a security incident? (Choose two.)

- A. Untampered images are used in the security investigation process
- B. Tampered images are used in the security investigation process
- C. The image is tampered if the stored hash and the computed hash match
- D. Tampered images are used in the incident recovery process
- E. The image is untampered if the stored hash and the computed hash match

Answer: BE

NEW QUESTION 38

Refer to the exhibit.



The screenshot shows the Cisco Stealthwatch interface. At the top, there's a navigation bar with 'Dashboards', 'Monitor', 'Analyze', and 'Jobs'. Below it, the 'Flow Search Results (1,166)' section is active. Search filters include: 'Edit Search', '05/06/2020 06:00 AM - 05/06/2020 1:20 PM (Time Ra)', '2,000 (Max Records)', 'Subject: 10.201.3.149 Client', 'Connection: All (Flow Direction)', and 'Peer: Outside Hosts'.

The main table displays flow details. The selected flow is from May 6, 2020, 6:46:42 AM (9hr 14 min 19s ago). It shows a duration of 15min 13s, subject IP 10.201.3.149, subject port 52599/UDP, subject host 'End User Devices, Desktops, Atlanta, Sales and Marketing', subject bytes 6.42 M, application 'Undefined UDP', total bytes 132.53 M, and peer IP 152.46.6.91.

Below the table, the 'General' tab is selected, showing 'View URL Data'. It displays statistics for the Subject, Totals, and Peer:

Subject		Totals		Peer	
Packets:	60.06 K	Packets:	165.87 K	Packets:	105.81 K
Packet Rate:	65.78 pps	Packet Rate:	181.67 pps	Packet Rate:	115.89 pps
Bytes:	6.42 MB	Bytes:	132.53 MB	Bytes:	126.11 MB
Byte Rate:	7.37 Kbps	Byte Rate:	152.2 Kbps	Byte Rate:	144.83 Kbps
Percent Transfer:	4.64%	Subject Byte Ratio:	4.84%	Percent Transfer:	95.16%
Host Groups:	End User Devices, Desktops, Atlanta, Sales and Marketing	RTT:	-	Host Groups:	United States
Payload:	-	SRT:	-	Payload:	-

Below the statistics, another flow entry is visible for May 6, 2020, 9:44:05 AM (6hr 16min 56s ago), showing a duration of 55 min 56s, subject IP 10.201.3.149, subject port 52599/UDP, subject host 'End User Devices, Desktops, Atlanta, Sales and Marketing', subject bytes 4.13 M, application 'Undefined UDP', total bytes 96.26 M, and peer IP 152.46.6.91.

What is the potential threat identified in this Stealthwatch dashboard?

- A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.
- B. Host 152.46.6.91 is being identified as a watchlist country for data transfer.
- C. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.
- D. Host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91.

Answer: D

NEW QUESTION 42

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 46

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 48

Which evasion technique is a function of ransomware?

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

Answer: B

NEW QUESTION 52

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 55

A security engineer has a video of a suspect entering a data center that was captured on the same day that files in the same data center were transferred to a competitor.
Which type of evidence is this?

- A. best evidence
- B. prima facie evidence
- C. indirect evidence
- D. physical evidence

Answer: C

NEW QUESTION 57

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 58

Refer to the exhibit.

File name	CVE-2009-4324 PDF 2009-11-30 note200911.pdf
File size	400918 bytes
File type	PDF document, version 1.6
CRC32	11638A9B
MD5	61baabd6fc12e01ff73ceacc07c84f9a
SHA1	0805d0ae62f5358b9a3f4c1868d552fc3561b17
SHA256	27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
SHA512	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
Ssdeep	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/QR/875+ prahGV6B
PEID	None matched
Yara	<ul style="list-style-type: none">• embedded_pe (Contains an embedded PE32 file)• embedded_win_api (A non-Windows executable contains win32 API)• vmdetect (Possibly employs anti-virtualization techniques)
VirusTotal	Permalink VirusTotal Scan Date: 2013-12-27 06:51:52 Detection Rate: 32/46 (collapse)

An engineer is analyzing this Cuckoo Sandbox report for a PDF file that has been downloaded from an email. What is the state of this file?

- A. The file has an embedded executable and was matched by PEiD threat signatures for further analysis.
- B. The file has an embedded non-Windows executable but no suspicious features are identified.
- C. The file has an embedded Windows 32 executable and the Yara field lists suspicious features for further analysis.
- D. The file was matched by PEiD threat signatures but no suspicious features are identified since the signature list is up to date.

Answer: C

NEW QUESTION 63

Which evasion technique is indicated when an intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources?

- A. resource exhaustion
- B. tunneling
- C. traffic fragmentation
- D. timing attack

Answer: A

NEW QUESTION 68

Which artifact is used to uniquely identify a detected file?

- A. file timestamp
- B. file extension
- C. file size
- D. file hash

Answer: D

NEW QUESTION 69

How does an SSL certificate impact security between the client and the server?

- A. by enabling an authenticated channel between the client and the server
- B. by creating an integrated channel between the client and the server
- C. by enabling an authorized channel between the client and the server
- D. by creating an encrypted channel between the client and the server

Answer: D

NEW QUESTION 70

What do the Security Intelligence Events within the FMC allow an administrator to do?

- A. See if a host is connecting to a known-bad domain.
- B. Check for host-to-server traffic within your network.
- C. View any malicious files that a host has downloaded.
- D. Verify host-to-host traffic within your network.

Answer: A

NEW QUESTION 71

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 74

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 75

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 78

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 80

Which two pieces of information are collected from the IPv4 protocol header? (Choose two.)

- A. UDP port to which the traffic is destined
- B. TCP port from which the traffic was sourced
- C. source IP address of the packet
- D. destination IP address of the packet
- E. UDP port from which the traffic is sourced

Answer: CD

NEW QUESTION 82

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 84

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 vector identifies 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 89

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 93

Refer to the exhibit.

```
$ cuckoo submit --machine cuckoo1 /path/to/binary
```

Which event is occurring?

- A. A binary named "submit" is running on VM cuckoo1.
- B. A binary is being submitted to run on VM cuckoo1
- C. A binary on VM cuckoo1 is being submitted for evaluation
- D. A URL is being evaluated to see if it has a malicious binary

Answer: C

NEW QUESTION 94

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 98

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

- A. total throughput
- B. session duration
- C. running processes

- D. OS fingerprint
- E. listening ports

Answer: DE

NEW QUESTION 100

Which utility blocks a host portscan?

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

Answer: C

NEW QUESTION 104

Which list identifies the information that the client sends to the server in the negotiation phase of the TLS handshake?

- A. ClientStart, ClientKeyExchange, cipher-suites it supports, and suggested compression methods
- B. ClientStart, TLS versions it supports, cipher-suites it supports, and suggested compression methods
- C. ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression methods
- D. ClientHello, ClientKeyExchange, cipher-suites it supports, and suggested compression methods

Answer: C

NEW QUESTION 107

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 108

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 109

What are two social engineering techniques? (Choose two.)

- A. privilege escalation
- B. DDoS attack
- C. phishing
- D. man-in-the-middle
- E. pharming

Answer: CE

NEW QUESTION 113

Refer to the exhibit.

SPRT
 SRVLOC
 SSCOP
 SSH
 SSL
 STANAG 5066
 StarTeam
 STP
 SUA
 SYNCHROPHASOR
 T.38
 TACACS+
 TALI
 TCAP
 TCP
 TCPENCAP
 TDMoE

Show TCP summary in protocol tree: ☒
 Validate the TCP checksum if possible: ☐
 Allow subdissector to reassemble TCP streams: ☒
 Analyze TCP sequence numbers: ☒
 Relative sequence numbers: ☒
 Scaling factor to use when not available from capture: Not known
 Track number of bytes in flight: ☒
 Calculate conversation timestamps: ☐
 Try heuristic sub-dissectors first: ☐
 Ignore TCP Timestamps in summary: ☐
 Do not call subdissectors for error packets: ☐
 TCP Experimental Options with a Magic Number: ☒

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 114

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 119

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 124

Refer to the exhibit.

Date	Flow Start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2020-01-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→ 192.168.0.1:20521	1	82	1

Which type of log is displayed?

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

Answer: B

NEW QUESTION 126

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 128

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 129

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 131

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 134

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 138

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

Risk Assessment	network is compromised
Vulnerability	lack of an access list
Exploit	configuration review
Threat	leakage of confidential information

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Risk Assessment	Threat
Vulnerability	Vulnerability
Exploit	Risk Assessment
Threat	Exploit

NEW QUESTION 142

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 147

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 148

In a SOC environment, what is a vulnerability management metric?

- A. code signing enforcement
- B. full assets scan
- C. internet exposed devices
- D. single factor authentication

Answer: D

NEW QUESTION 152

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

200-201 Practice Exam Features:

- * 200-201 Questions and Answers Updated Frequently
- * 200-201 Practice Questions Verified by Expert Senior Certified Staff
- * 200-201 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 200-201 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 200-201 Practice Test Here](#)