

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

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

Refer to the exhibit.

Interface: 192.168.1.29 --- 0x11		
Internet Address	Physical Address	Type
192.168.1.10	d8-a7-56-d7-19-ea	dynamic
192.168.1.67	d8-a7-56-d7-19-ea	dynamic
192.168.1.1	01-00-5e-00-00-16	static

What is occurring in this network?

- A. ARP cache poisoning
- B. DNS cache poisoning
- C. MAC address table overflow
- D. MAC flooding attack

Answer: A

NEW QUESTION 5

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 6

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 7

Which process is used when IPS events are removed to improve data integrity?

- A. data availability
- B. data normalization
- C. data signature
- D. data protection

Answer: B

NEW QUESTION 8

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 9

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 10

Drag and drop the access control models from the left onto the correct descriptions on the right.

MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC

NEW QUESTION 10

What is a purpose of a vulnerability management framework?

- A. identifies, removes, and mitigates system vulnerabilities
- B. detects and removes vulnerabilities in source code
- C. conducts vulnerability scans on the network
- D. manages a list of reported vulnerabilities

Answer: A

NEW QUESTION 11

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 16

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 21

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 25

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 29

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 34

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 35

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 39

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 41

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 46

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 47

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 48

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
18	0.011918	10.0.2.15	192.124.249.9	TCP	78	50588→443 [SYN] Seq=1
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443→50588 [SYN, ACK]
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588→443 [ACK] Seq=1
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443→50586 [SYN, ACK]
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586→443 [ACK] Seq=1
23	0.023212	10.0.2.15	192.124.249.9	TCP	261	50588→443 [PSH, ACK]
24	0.023373	10.0.2.15	192.124.249.9	TCP	261	50586→443 [PSH, ACK]
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443→50588 [ACK] Seq=1
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443→50586 [ACK] Seq=1
27	0.037413	192.124.249.9	10.0.2.15	TCP	2792	443→50586 [PSH, ACK]
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586→443 [ACK] Seq=2

> Frame 24: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)

> Linux cooked capture

> Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)

> Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, A

> Data [205 bytes]

Data: 16030100c8010000c403030e06ead078d17676c13ab46ebf...

[Length: 205]

0000	00 04 00 01 00 06 08 00	27 7a 3c 93 00 00 08 00 *z<.....
0010	45 00 00 f5 48 7b 40 00	40 06 2b f3 0a 00 02 0f	E...H{@. @.+.....
0020	c0 7c f9 09 c5 9a 01 bb	0e 1f dc b4 00 b4 aa 02
0030	50 18 72 10 c6 7c 00 00	16 03 01 00 c8 01 00 00	P.r.. ..
0040	c4 03 03 0e 06 ea d0 78	d1 76 76 c1 3a b4 6e bfx.vv.:n..
0050	e6 b8 b8 b2 ba 08 d6 6d	0d 38 fb 91 45 de fc eem .8..E...
0060	8b 6e f8 00 00 1e c0 2b	c0 2f cc a9 cc a8 c0 2c	.n.....+ ./.....
0070	c0 30 c0 0a c0 09 c0 13	c0 14 00 33 00 39 00 2f	.0..... ...3.9./
0080	00 35 00 0a 01 00 00 7d	00 00 00 16 00 14 00 00	.5.....}
0090	11 77 77 77 2e 6c 69 6e	75 78 6d 69 6e 74 2e 63	.wwwlin uxmint.c
00a0	6f 6d 00 17 00 00 ff 01	00 01 00 00 0a 00 08 00	om.....
00b0	06 00 17 00 18 00 19 00	0b 00 02 01 00 00 23 00#.
00c0	00 33 74 00 00 00 10 00	17 00 15 02 68 32 08 73	.3t.....h2.s
00d0	70 64 79 2f 33 2e 31 08	68 74 74 70 2f 31 2e 31	pdv/3.1. http/1.1
00e0	00 05 00 05 01 00 00 00	00 00 0d 00 18 00 16 04
00f0	01 05 01 06 01 02 01 04	03 05 03 06 03 02 03 05
0100	02 04 02 02 02	

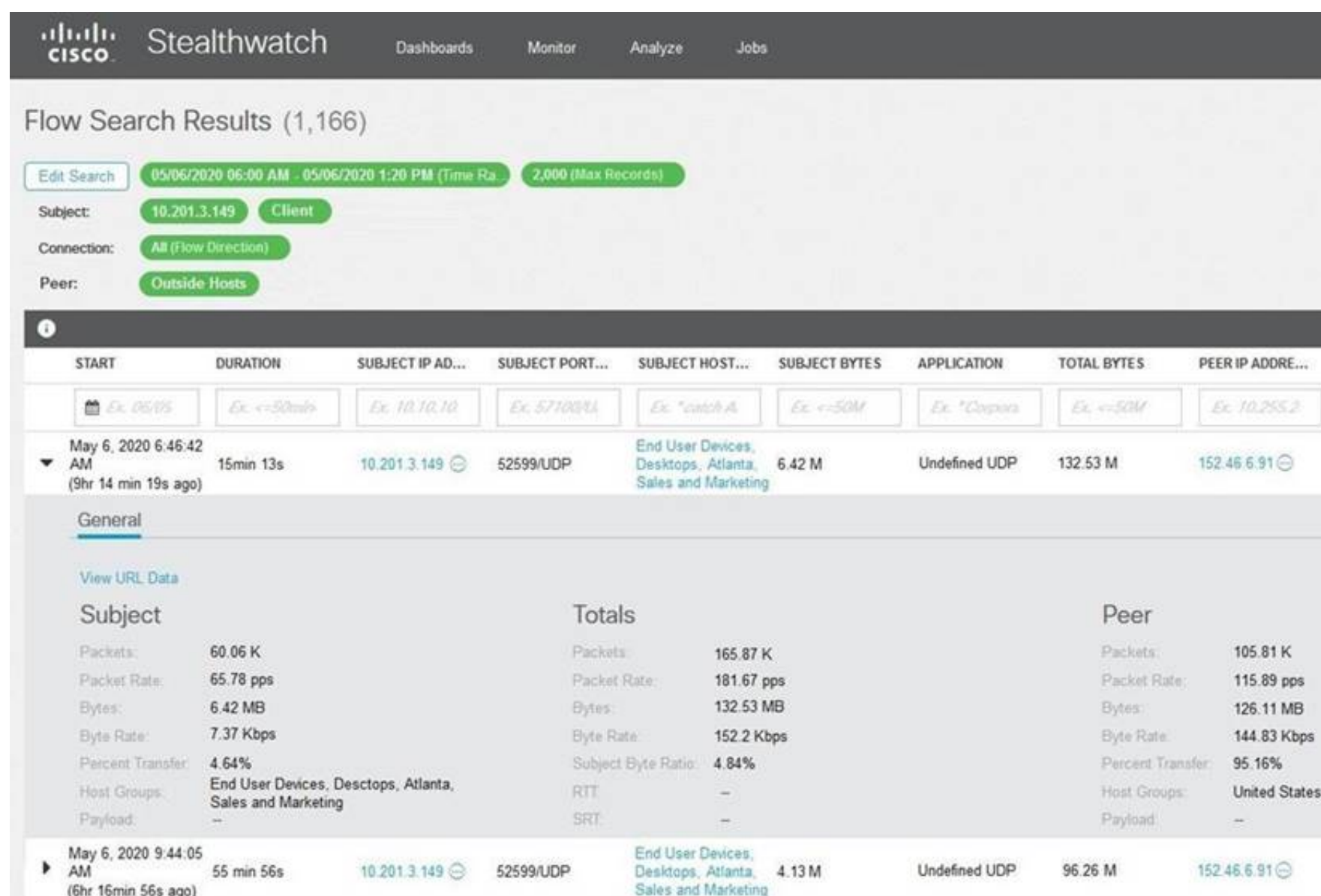
Which application protocol is in this PCAP file?

- A. SSH
- B. TCP
- C. TLS
- D. HTTP

Answer: B

NEW QUESTION 50

Refer to the exhibit.



The screenshot shows the Cisco Stealthwatch interface. At the top, there are navigation tabs: Dashboards, Monitor, Analyze, and Jobs. Below this, the 'Flow Search Results' section shows 1,166 results. The search filters are: Subject: 10.201.3.149, Client; Connection: All (Flow Direction); Peer: Outside Hosts. The search criteria bar shows the time range from 05/06/2020 06:00 AM to 05/06/2020 1:20 PM (Time Range) and a limit of 2,000 (Max Records). Below the search filters, there is a table of search results. The first result is for May 6, 2020 6:46:42 AM, showing 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 address 152.46.6.91. Below the table, there is a 'General' tab with a 'View URL Data' link. The 'General' tab shows three columns: Subject, Totals, and Peer. The Subject column shows: Packets: 60.06 K, Packet Rate: 65.78 pps, Bytes: 6.42 MB, Byte Rate: 7.37 Kbps, Percent Transfer: 4.64%, Host Groups: End User Devices, Desktops, Atlanta, Sales and Marketing, Payload: -. The Totals column shows: Packets: 165.87 K, Packet Rate: 181.67 pps, Bytes: 132.53 MB, Byte Rate: 152.2 Kbps, Subject Byte Ratio: 4.84%, RTT: -, SRT: -. The Peer column shows: Packets: 105.81 K, Packet Rate: 115.89 pps, Bytes: 126.11 MB, Byte Rate: 144.83 Kbps, Percent Transfer: 95.16%, Host Groups: United States, Payload: -. Below the 'General' tab, there is another search result for May 6, 2020 9:44:05 AM, 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 address 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 55

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 57

Which evasion technique is a function of ransomware?

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

Answer: B

NEW QUESTION 61

Which regex matches only on all lowercase letters?

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

Answer: A

NEW QUESTION 62

What are the two characteristics of the full packet captures? (Choose two.)

- A. Identifying network loops and collision domains.
- B. Troubleshooting the cause of security and performance issues.

- C. Reassembling fragmented traffic from raw data.
- D. Detecting common hardware faults and identify faulty assets.
- E. Providing a historical record of a network transaction.

Answer: CE

NEW QUESTION 65

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 67

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 68

While viewing packet capture data, an analyst sees that one IP is sending and receiving traffic for multiple devices by modifying the IP header. Which technology makes this behavior possible?

- A. encapsulation
- B. TOR
- C. tunneling
- D. NAT

Answer: D

NEW QUESTION 70

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 73

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 78

Which event artifact is used to identity HTTP GET requests for a specific file?

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

Answer: D

NEW QUESTION 79

What makes HTTPS traffic difficult to monitor?

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

Answer: D

NEW QUESTION 81

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 86

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 91

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 92

A security engineer deploys an enterprise-wide host/endpoint technology for all of the company's corporate PCs. Management requests the engineer to block a selected set of applications on all PCs.

Which technology should be used to accomplish this task?

- A. application whitelisting/blacklisting
- B. network NGFW
- C. host-based IDS
- D. antivirus/antispysware software

Answer: A

NEW QUESTION 96

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 101

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 106

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 111

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 112

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 117

Which utility blocks a host portscan?

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

Answer: C

NEW QUESTION 120

When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification. Which information is available on the server certificate?

- A. server name, trusted subordinate CA, and private key
- B. trusted subordinate CA, public key, and cipher suites
- C. trusted CA name, cipher suites, and private key
- D. server name, trusted CA, and public key

Answer: D

NEW QUESTION 123

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 124

Which security technology allows only a set of pre-approved applications to run on a system?

- A. application-level blacklisting
- B. host-based IPS
- C. application-level whitelisting
- D. antivirus

Answer: C

NEW QUESTION 129

A SOC analyst is investigating an incident that involves a Linux system that is identifying specific sessions. Which identifier tracks an active program?

- A. application identification number
- B. active process identification number
- C. runtime identification number
- D. process identification number

Answer: D

NEW QUESTION 131

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 136

Which access control model does SELinux use?

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

Answer: C

NEW QUESTION 137

How is attacking a vulnerability categorized?

- A. action on objectives
- B. delivery
- C. exploitation
- D. installation

Answer: C

NEW QUESTION 138

What is personally identifiable information that must be safeguarded from unauthorized access?

- A. date of birth
- B. driver's license number
- C. gender
- D. zip code

Answer: B

NEW QUESTION 142

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 146

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 149

At which layer is deep packet inspection investigated on a firewall?

- A. internet
- B. transport
- C. application
- D. data link

Answer: C

NEW QUESTION 151

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 154

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 155

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 158

Refer to the exhibit.

Overview Analysis Policies Devices Objects													
Content Explorer Connections > Security Intelligence Events Intrusions Files Hosts Users Vulnerabilities Correlation Custom Search													
Security Intelligence Events (switch workflow)													
Security Intelligence with Application Details > Table View of Security Intelligence Events													
Search Constraints (Edit Search Serve Search)													
2018-03-02 07:20:20 - 2018-03-07 13:47:20													
Expanding Disabled Columns													
First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port	ICMP Type
2018-03-07 13:42:01		Sinkhole DNS Block		10.0.10.75		JERILABORDE (DCLOUD-SOC-LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp	
2018-03-07 13:42:01		Sinkhole DNS Block		10.0.0.100		AMPARO GIVENS (DCLOUD-SOC-LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp	
2018-03-07 13:42:01		Sinkhole DNS Block		10.112.10.158		VERNETTA DONNEL (DCLOUD-SOC-LDAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp	

Which two elements in the table are parts of the 5-tuple? (Choose two.)

- A. First Packet
- B. Initiator User
- C. Ingress Security Zone
- D. Source Port

E. Initiator IP

Answer: DE

NEW QUESTION 162

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 164

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 168

.....

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](#)