Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

NEW QUESTION 1
Which tool gives the ability to see session data in real time?

A. tcpdstat
B. trafdump
C. tcptrace
D. trafshow

Answer: C

NEW QUESTION 2
Which incidence response step includes identifying all hosts affected by an attack?

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

Answer: D

Explanation:
* 3.3.3 Identifying the Attacking Hosts During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts. Although this information can be important, incident handlers should generally stay focused on containment, eradication, and recovery. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
The response phase, or containment, of incident response, is the point at which the incident response team begins interacting with affected systems and attempts to keep further damage from occurring as a result of the incident.

NEW QUESTION 3
What is an advantage of symmetric over asymmetric encryption?

A. A key is generated on demand according to data type.
B. A one-time encryption key is generated for data transmission
C. It is suited for transmitting large amounts of data.
D. It is a faster encryption mechanism for sessions

Answer: D

NEW QUESTION 4
Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
17	0.011641	10.0.2.15	192.124.249.9	TCP	76	50586–443 [SYN] Seq=0 Win=
18	0.011918	10.0.2.15	192.124.249.9	TCP	76	50588–443 [SYN] Seq=0 Win=
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443–50588 [SYN, ACK] Seq=0
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588–443 [ACK] Seq=1 Ack=
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443–50586 [SYN, ACK] Seq=0
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586–443 [ACK] Seq=1 Ack=
23	0.023212	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
24	0.023373	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443–50588 [ACK] Seq=1 Ack=
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443–50586 [ACK] Seq=1 Ack=
27	0.037413	192.124.249.9	10.0.2.15	TLSv1.2	2792	Server Hello
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586–443 [ACK] Seq=206 Ac

> Frame 23: 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: 50588 (50588), Dst Port: 443 (443), Seq: 1, Ack:1,
> Secure Sockets Layer

```
0000  00 04 00 01 00 06 08 00  27 7a 3c 93 00 00 08 00   ........ *z<.....
0010  45 00 00 f5 eb 3e 40 00  40 06 89 2f 0a 00 02 0f   E....>@. @../....
0020  c0 7c f9 09 c5 9c 01 bb  4d db 7f f7 00 b3 b0 02   .|...... M.......
0030  50 18 72 10 c6 7c 00 00  16 03 01 00 c8 01 00 00   P.r..|.. ........
0040  c4 03 03 d1 08 45 78 b7  2c 90 04 ee 51 16 f1 82   .....Ex. ....Q...
0050  16 43 ec d4 89 60 34 4a  7b 80 a6 d1 72 d5 11 87   .C....4J {...r...
0060  10 57 cc 00 00 1e c0 2b  c0 2f cc a9 cc a8 c0 2c   .W.....+ ./.....,
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   .www.lin 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   pdy/3.2. 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                                     .....
```

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 5
Drag and drop the type of evidence from the left onto the description of that evidence on the right.

direct evidence	log that shows a command and control check-in from verified malware
corroborative evidence	firewall log showing successful communication and threat intelligence stating an IP is known to host malware
indirect evidence	NetFlow-based spike in DNS traffic

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

NEW QUESTION 6
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 7
Refer to the exhibit.

```
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63064 135 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.14 63065 49156 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63066 65386 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63067 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.14 62292 389 0 - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63068 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63069 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.13 62293 389 0 - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63070 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63071 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63072 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63073 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63074 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63075 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63076 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 55053 53 0 - - - - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 50845 53 0 - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP fe80::29ea:1a3c:24d6:fb49 ff02::1:3 57333 5355 0 - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP 10.40.4.252 224.0.0.252 59629 5355 0 - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 58846 5355 0 - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP 10.40.4.182 224.0.0.252 58846 5355 0 - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 137 137 0 - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 63504 5355 0 - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 63504 5355 0 - - - - - - SEND
```

An engineer received an event log file to review. Which technology generated the log?

A. NetFlow
B. proxy
C. firewall
D. IDS/IPS

Answer: C

NEW QUESTION 8
What is the difference between discretionary access control (DAC) and role-based access control (RBAC)?

A. DAC requires explicit authorization for a given user on a given object, and RBAC requires specific conditions.
B. RBAC access is granted when a user meets specific conditions, and in DAC, permissions are applied on user and group levels.
C. RBAC is an extended version of DAC where you can add an extra level of authorization based on time.
D. DAC administrators pass privileges to users and groups, and in RBAC, permissions are applied to specific groups

Answer: A

NEW QUESTION 9
Why is HTTPS traffic difficult to screen?

A. HTTPS is used internally and screening traffic (or external parties is hard due to isolation.
B. The communication is encrypted and the data in transit is secured.
C. Digital certificates secure the session, and the data is sent at random intervals.
D. Traffic is tunneled to a specific destination and is inaccessible to others except for the receiver.

Answer: B

NEW QUESTION 10
What is a benefit of using asymmetric cryptography?

A. decrypts data with one key
B. fast data transfer
C. secure data transfer
D. encrypts data with one key

Answer: C

NEW QUESTION 10
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

Explanation:
CDfs is a virtual file system for Unix-like operating systems; it provides access to data and audio tracks on Compact Discs. When the CDfs driver mounts a Compact Disc, it represents each track as a file. This is consistent with the Unix convention "everything is a file". Source: https://en.wikipedia.org/wiki/CDfs
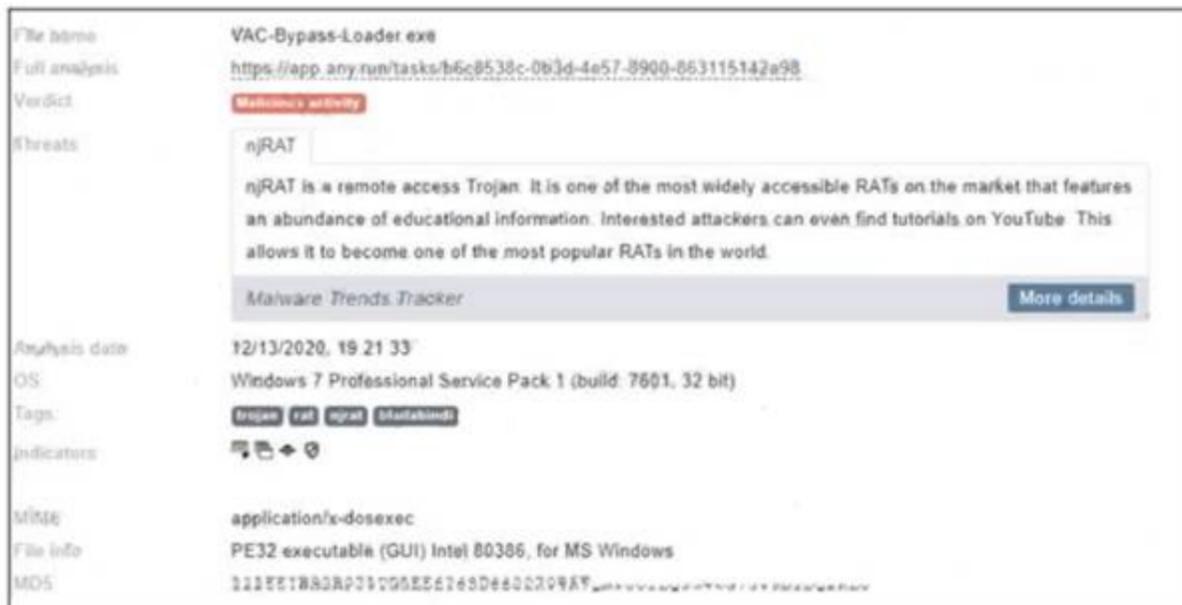
NEW QUESTION 15
What is the difference between mandatory access control (MAC) and discretionary access control (DAC)?

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 20
Refer to the exhibit.

Where is the executable file?

A. info
B. tags
C. MIME
D. name

Answer: C

NEW QUESTION 24
How does agentless monitoring differ from agent-based monitoring?

A. Agentless can access the data via AP
B. while agent-base uses a less efficient method and accesses log data through WMI.
C. Agent-based monitoring is less intrusive in gathering log data, while agentless requires open ports to fetch the logs
D. Agent-based monitoring has a lower initial cost for deployment, while agentless monitoring requires resource-intensive deployment.
E. Agent-based has a possibility to locally filter and transmit only valuable data, while agentless has much higher network utilization

Answer: B

NEW QUESTION 25
What describes the concept of data consistently and readily being accessible for legitimate users?

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

Answer: B

NEW QUESTION 30
An engineer needs to fetch logs from a proxy server and generate actual events according to the data received. Which technology should the engineer use to accomplish this task?

A. Firepower
B. Email Security Appliance
C. Web Security Appliance
D. Stealthwatch

Answer: C

NEW QUESTION 33
Drag and drop the data source from the left onto the data type on the right.

Wireshark		session data
NetFlow		alert data
server log		full packet capture
IPS		transaction data

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Wireshark		NetFlow
NetFlow		IPS
server log		Wireshark
IPS		server log

NEW QUESTION 34
According to the September 2020 threat intelligence feeds a new malware called Egregor was introduced and used in many attacks. Distnbution of Egregor is pnmanly through a Cobalt Strike that has been installed on victim's workstations using RDP exploits Malware exfiltrates the victim's data to a command and control server. The data is used to force victims pay or lose it by publicly releasing it. Which type of attack is described?

A. malware attack
B. ransomware attack
C. whale-phishing
D. insider threat

Answer: B

NEW QUESTION 39
The security team has detected an ongoing spam campaign targeting the organization. The team's approach is to push back the cyber kill chain and mitigate ongoing incidents. At which phase of the cyber kill chain should the security team mitigate this type of attack?

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

Answer: B

NEW QUESTION 43
What does cyber attribution identify in an investigation?

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

Answer: D

Explanation:
https://www.techtarget.com/searchsecurity/definition/cyber-attribution

NEW QUESTION 47
What is rule-based detection when compared to statistical detection?

A. proof of a user's identity
B. proof of a user's action
C. likelihood of user's action
D. falsification of a user's identity

Answer: B

NEW QUESTION 48
Which technology prevents end-device to end-device IP traceability?

A. encryption
B. load balancing
C. NAT/PAT
D. tunneling

Answer: C

NEW QUESTION 49
Which event artifact is used to identify HTTP GET requests for a specific file?

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

Answer: D

NEW QUESTION 54
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 56
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. 81.179.179.69 is sending a packet from port 80 to port 50272 of IP address 192.168.122.100 using UDP protocol.
B. 192.168.122.100 is sending a packet from port 50272 to port 80 of IP address 81.179.179.69 using TCP protocol.
C. 192.168.122.100 is sending a packet from port 80 to port 50272 of IP address 81.179.179.69 using UDP protocol.
D. 81.179.179.69 is sending a packet from port 50272 to port 80 of IP address 192.168.122.100 using TCP UDP protocol.

Answer: B

NEW QUESTION 60
Which event is a vishing attack?

A. obtaining disposed documents from an organization
B. using a vulnerability scanner on a corporate network
C. setting up a rogue access point near a public hotspot
D. impersonating a tech support agent during a phone call

Answer: D

NEW QUESTION 61
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 62
At which layer is deep packet inspection investigated on a firewall?

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

Answer: C

Explanation:
Deep packet inspection is a form of packet filtering usually carried out as a function of your firewall. It is applied at the Open Systems Interconnection's application layer. Deep packet inspection evaluates the contents of a packet that is going through a checkpoint.

NEW QUESTION 64
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: A

Explanation:
HIDS is capable of monitoring the internals of a computing system as well as the network packets on its network interfaces. Host-based firewall is a piece of software running on a single Host that can restrict incoming and outgoing Network activity for that host only.

NEW QUESTION 65
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 69
An engineer is analyzing a recent breach where confidential documents were altered and stolen by the receptionist Further analysis shows that the threat actor connected an externa USB device to bypass security restrictions and steal data The engineer could not find an external USB device Which piece of information must an engineer use for attribution in an investigation?

A. list of security restrictions and privileges boundaries bypassed
B. external USB device
C. receptionist and the actions performed
D. stolen data and its criticality assessment

Answer: C

NEW QUESTION 74
An engineer received an alert affecting the degraded performance of a critical server. Analysis showed a heavy CPU and memory load. What is the next step the engineer should take to investigate this resource usage?

A. Run "ps -d" to decrease the priority state of high load processes to avoid resource exhaustion.
B. Run "ps -u" to find out who executed additional processes that caused a high load on a server.
C. Run "ps -ef" to understand which processes are taking a high amount of resources.
D. Run "ps -m" to capture the existing state of daemons and map required processes to find the gap.

Answer: C

NEW QUESTION 77
What is the principle of defense-in-depth?

A. Agentless and agent-based protection for security are used.
B. Several distinct protective layers are involved.
C. Access control models are involved.
D. Authentication, authorization, and accounting mechanisms are used.

Answer: B

NEW QUESTION 78
Drag and drop the definition from the left onto the phase on the right to classify intrusion events according to the Cyber Kill Chain model.

The threat actor takes actions to violate data integrity and availability.	Exploitation
The targeted environment is taken advantage of triggering the threat actor's code.	Installation
Backdoor is placed on the victim system allowing the threat actor to maintain the persistence.	Command and Control
An outbound connection is established to an Internet-based controller server.	Actions and Objectives

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Exploitation - The targeted Environment is taken advantage of triggering the threat actor's code Installation - Backdoor is placed on the victim system allowing the threat actor to maintain the persistence. Command and Control - An outbound connection is established to an Internet-based controller server. Actions and Objectives - The threat actor takes actions to violate data integrity and availability

NEW QUESTION 83
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 88
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 93
An employee reports that someone has logged into their system and made unapproved changes, files are out of order, and several documents have been placed in the recycle bin. The security specialist reviewed the system logs, found nothing suspicious, and was not able to determine what occurred. The software is up to date; there are no alerts from antivirus and no failed login attempts. What is causing the lack of data visibility needed to detect the attack?

A. The threat actor used a dictionary-based password attack to obtain credentials.
B. The threat actor gained access to the system by known credentials.

C. The threat actor used the teardrop technique to confuse and crash login services.
D. The threat actor used an unknown vulnerability of the operating system that went undetected.

Answer: C

NEW QUESTION 98
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 99
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/antispyware software

Answer: A

NEW QUESTION 101
Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=2987 Ack=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/i/ntpagetag.gif?js=1&ts=147629607552.286&tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=6871 Ack=14979 Win=62480 Len=0

Which packet contains a file that is extractable within Wireshark?

A. 2317
B. 1986
C. 2318
D. 2542

Answer: D

NEW QUESTION 105
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 107
The SOC team has confirmed a potential indicator of compromise on an endpoint. The team has narrowed the executable file's type to a new trojan family.
According to the NIST Computer Security Incident Handling Guide, what is the next step in handling this event?

A. Isolate the infected endpoint from the network.
B. Perform forensics analysis on the infected endpoint.
C. Collect public information on the malware behavior.
D. Prioritize incident handling based on the impact.

Answer: C

NEW QUESTION 109
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 113
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: B

Explanation:
An ARP-based MITM attack is achieved when an attacker poisons the ARP cache of two devices with the MAC address of the attacker's network interface card (NIC). Once the ARP caches have been successfully poisoned, each victim device sends all its packets to the attacker when communicating to the other device and puts the attacker in the middle of the communications path between the two victim devices. It allows an attacker to easily monitor all communication between victim devices. The intent is to intercept and view the information being passed between the two victim devices and potentially introduce sessions and traffic between the two victim devices

NEW QUESTION 116
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 118
Which technology on a host is used to isolate a running application from other applications?

A. sandbox
B. application allow list
C. application block list
D. host-based firewall

Answer: A

NEW QUESTION 119
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 122
Which utility blocks a host portscan?

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

Answer: C

NEW QUESTION 125
What is the difference between a threat and an exploit?

A. A threat is a result of utilizing flow in a system, and an exploit is a result of gaining control over the system.
B. A threat is a potential attack on an asset and an exploit takes advantage of the vulnerability of the asset
C. An exploit is an attack vector, and a threat is a potential path the attack must go through.
D. An exploit is an attack path, and a threat represents a potential vulnerability

Answer: B

NEW QUESTION 130
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 131
When trying to evade IDS/IPS devices, which mechanism allows the user to make the data incomprehensible without a specific key, certificate, or password?

A. fragmentation
B. pivoting
C. encryption
D. stenography

Answer: C

Explanation:
https://techdifferences.com/difference-between-steganography-and-cryptography.html#:~:text=The%20steganog

NEW QUESTION 135
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 137
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: A

Explanation:
You also see the 5-tuple in IPS events, NetFlow records, and other event data. In fact, on the exam you may need to differentiate between a firewall log versus a traditional IPS or IDS event. One of the things to remember is that traditional IDS and IPS use signatures, so an easy way to differentiate is by looking for a signature ID (SigID). If you see a signature ID, then most definitely the event is a traditional IPS or IDS event.

NEW QUESTION 138
What describes the impact of false-positive alerts compared to false-negative alerts?

A. A false negative is alerting for an XSS attac
B. An engineer investigates the alert and discovers that an XSS attack happened A false positive is when an XSS attack happens and no alert is raised
C. A false negative is a legitimate attack triggering a brute-force aler
D. An engineer investigates the alert and finds out someone intended to break into the system A false positive is when no alert and no attack is occurring
E. A false positive is an event alerting for a brute-force attack An engineer investigates the alert and discovers that a legitimate user entered the wrong credential several times A false negative is when a threat actor tries to brute-force attack a system and no alert is raised.
F. A false positive is an event alerting for an SQL injection attack An engineer investigates the alert and discovers that an attack attempt was blocked by IPS A false negative is when the attack gets detected but succeeds and results in a breach.

Answer: C

NEW QUESTION 140
How is NetFlow different from 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 142
What is the virtual address space for a Windows process?

A. physical location of an object in memory
B. set of pages that reside in the physical memory
C. system-level memory protection feature built into the operating system
D. set of virtual memory addresses that can be used

Answer: D

NEW QUESTION 143
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 148
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 149
At a company party a guest asks questions about the company's user account format and password complexity. How is this type of conversation classified?

A. Phishing attack
B. Password Revelation Strategy
C. Piggybacking
D. Social Engineering

Answer: D

NEW QUESTION 151
Refer to the exhibit.

What is the potential threat identified in this Stealthwatch dashboard?

A. A policy violation is active for host 10.10.101.24.
B. A host on the network is sending a DDoS attack to another inside host.
C. There are three active data exfiltration alerts.
D. A policy violation is active for host 10.201.3.149.

Answer: C

Explanation:
"EX" = exfiltration And there are three.
Also the "suspect long flow" and "suspect data heading" suggest, for example, DNS exfiltration
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6 page 177.

NEW QUESTION 153
How does an attack surface differ from an attack vector?

A. An attack vector recognizes the potential outcomes of an attack, and the attack surface is choosing a method of an attack.
B. An attack surface identifies vulnerable parts for an attack, and an attack vector specifies which attacks are feasible to those parts.
C. An attack surface mitigates external vulnerabilities, and an attack vector identifies mitigation techniques and possible workarounds.
D. An attack vector matches components that can be exploited, and an attack surface classifies the potential path for exploitation

Answer: B

NEW QUESTION 155
What is an incident response plan?

A. an organizational approach to events that could lead to asset loss or disruption of operations
B. an organizational approach to security management to ensure a service lifecycle and continuous improvements
C. an organizational approach to disaster recovery and timely restoration of operational services
D. an organizational approach to system backup and data archiving aligned to regulations

Answer: C

NEW QUESTION 157
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.

Which obfuscation technique is the attacker using?

A. Base64 encoding
B. TLS encryption
C. SHA-256 hashing
D. ROT13 encryption

Answer: B

Explanation:
ROT13 is considered weak encryption and is not used with TLS (HTTPS:443). Source: https://en.wikipedia.org/wiki/ROT13

NEW QUESTION 161
What is a difference between data obtained from Tap and SPAN ports?

A. Tap mirrors existing traffic from specified ports, while SPAN presents more structured data for deeper analysis.
B. SPAN passively splits traffic between a network device and the network without altering it, while Tap alters response times.

C. SPAN improves the detection of media errors, while Tap provides direct access to traffic with lowered data visibility.
D. Tap sends traffic from physical layers to the monitoring device, while SPAN provides a copy of network traffic from switch to destination

Answer: D

NEW QUESTION 162
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 164
What is a description of a social engineering attack?

A. fake offer for free music download to trick the user into providing sensitive data
B. package deliberately sent to the wrong receiver to advertise a new product
C. mistakenly received valuable order destined for another person and hidden on purpose
D. email offering last-minute deals on various vacations around the world with a due date and a counter

Answer: D

NEW QUESTION 165
How does statistical detection differ from rule-based detection?

A. Statistical detection involves the evaluation of events, and rule-based detection requires an evaluated set of events to function.
B. Statistical detection defines legitimate data over time, and rule-based detection works on a predefined set of rules
C. Rule-based detection involves the evaluation of events, and statistical detection requires an evaluated set of events to function Rule-based detection defines
D. legitimate data over a period of time, and statistical detection works on a predefined set of rules

Answer: B

NEW QUESTION 167
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 171
What is the impact of encryption?

A. Confidentiality of the data is kept secure and permissions are validated
B. Data is accessible and available to permitted individuals
C. Data is unaltered and its integrity is preserved
D. Data is secure and unreadable without decrypting it
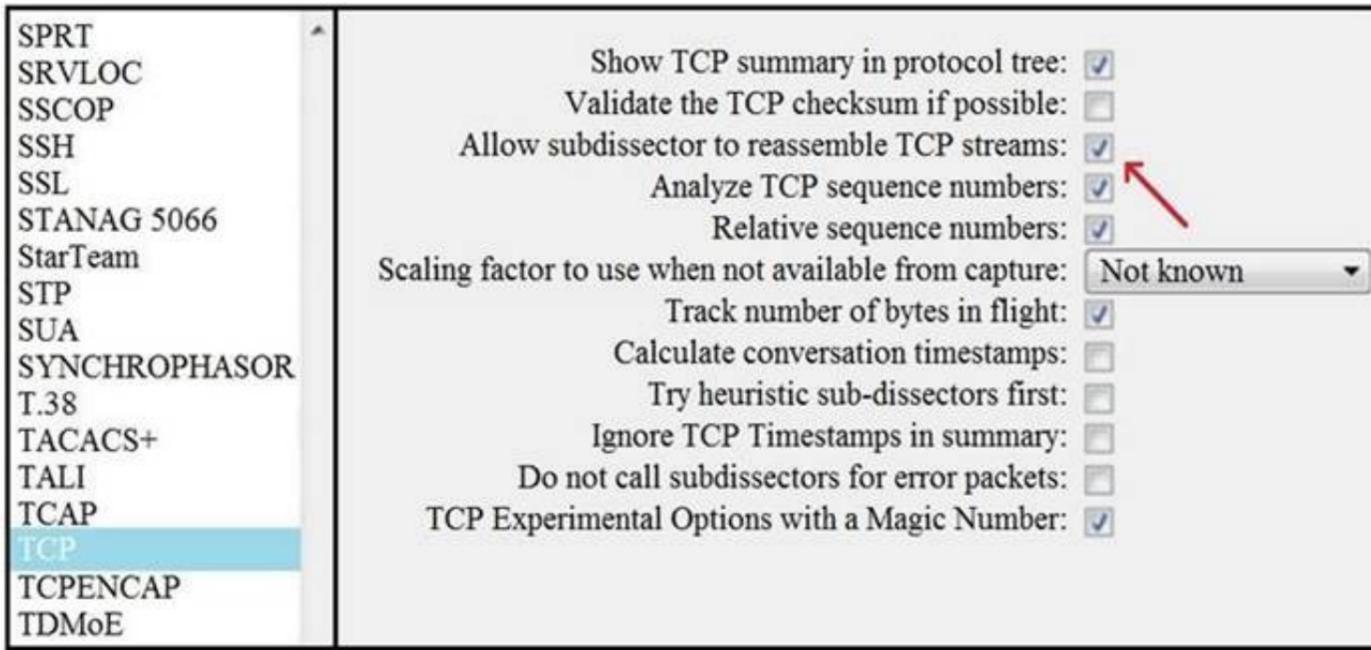
Answer: A

NEW QUESTION 176
A threat actor penetrated an organization's network. Using the 5-tuple approach, which data points should the analyst use to isolate the compromised host in a grouped set of logs?

A. event name, log source, time, source IP, and host name
B. protocol, source IP, source port, destination IP, and destination port
C. event name, log source, time, source IP, and username
D. protocol, log source, source IP, destination IP, and host name
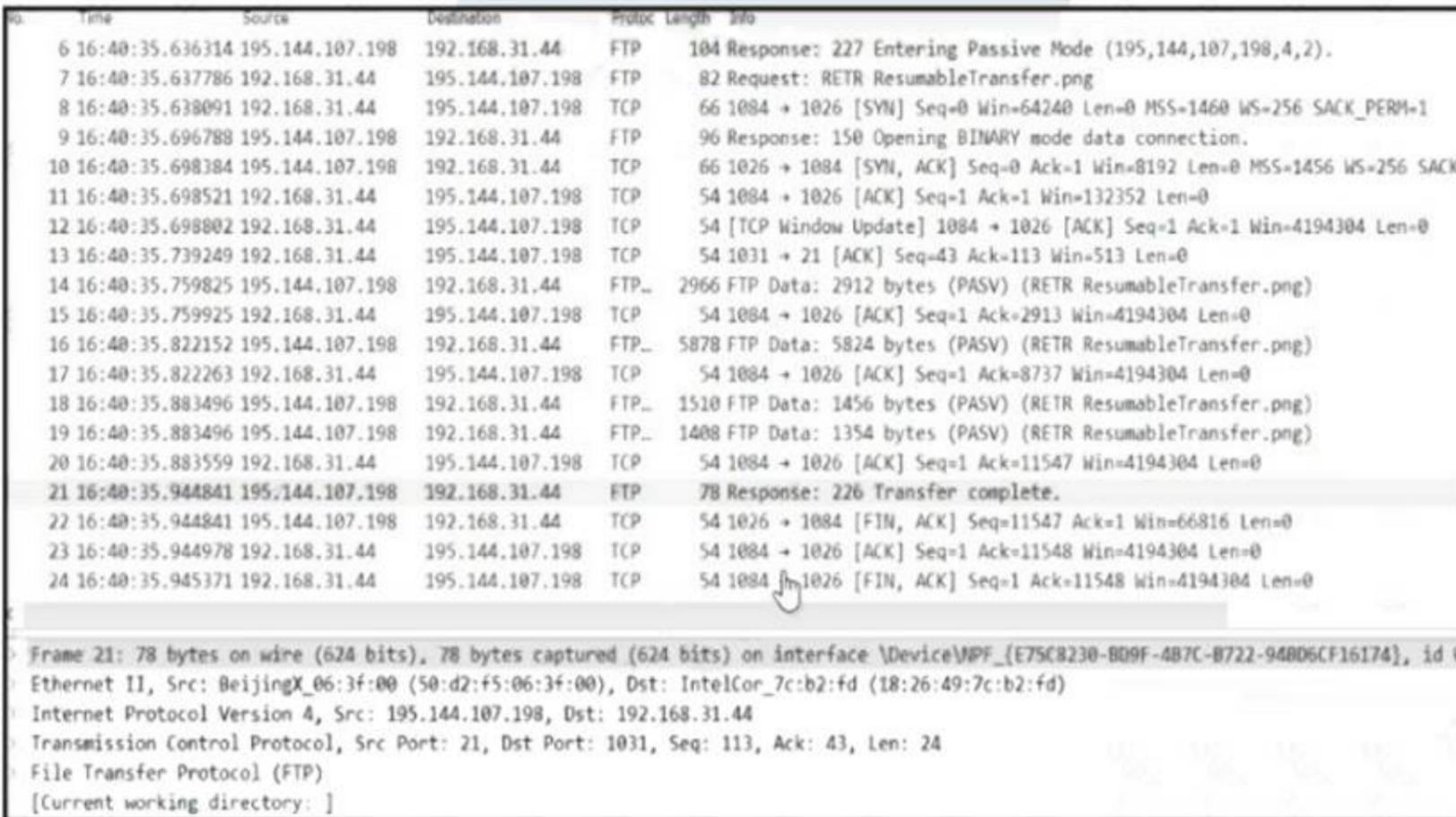
Answer: B

NEW QUESTION 181
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 183
Refer to the exhibit.

Which frame numbers contain a file that is extractable via TCP stream within Wireshark?

A. 7,14, and 21
B. 7 and 21
C. 14,16,18, and 19
D. 7 to 21

Answer: B

NEW QUESTION 184
Refer to the exhibit.

```
ip.addr == 192.168.1.80 and tcp.port==8081 and http.request.full_uri
No.      Time         Source          Destination      Protocol  Length  Info
14   27.405297   192.168.1.83    192.168.1.80     HTTP      335 GET /news.php HTTP/1.1
14   27.423516   192.168.1.80    192.168.1.83     HTTP      12  HTTP/1.0 200 OK  (text/html)
14   27.843983   192.168.1.83    192.168.1.80     HTTP      516 POST /admin/get.php HTTP/1.1
14   27.856474   192.168.1.80    192.168.1.83     HTTP      519 HTTP/1.0 200 OK  (text/html)
14   28.053803   192.168.1.83    192.168.1.80     HTTP      276 POST /news.php HTTP/1.1
15   28.065561   192.168.1.80    192.168.1.83     HTTP      11  HTTP/1.0 200 OK  (text/html)
20   33.245337   192.168.1.83    192.168.1.80     HTTP      259 GET /login/process.php HTTP/1.1
20   33.253440   192.168.1.80    192.168.1.83     HTTP      60  HTTP/1.0 200 OK  (text/html)
23   38.265103   192.168.1.83    192.168.1.80     HTTP      250 GET /news.php HTTP/1.1
23   38.271353   192.168.1.80    192.168.1.83     HTTP      60  HTTP/1.0 200 OK  (text/html)
26   43.291043   192.168.1.83    192.168.1.80     HTTP      259 GET /login/process.php HTTP/1.1
26   43.298364   192.168.1.80    192.168.1.83     HTTP      60  HTTP/1.0 200 OK  (text/html)
30   48.311212   192.168.1.83    192.168.1.80     HTTP      259 GET /login/process.php HTTP/1.1
30   48.322750   192.168.1.80    192.168.1.83     HTTP      340 HTTP/1.0 200 OK  (text/html)
30   48.439913   192.168.1.83    192.168.1.80     HTTP      148 POST /admin/get.php HTTP/1.1
30   48.455743   192.168.1.80    192.168.1.83     HTTP      60  HTTP/1.0 404 NOT FOUND  (text/html)
35   53.482265   192.168.1.83    192.168.1.80     HTTP      255 GET /admin/get.php HTTP/1.1
35   53.491062   192.168.1.80    192.168.1.83     HTTP      60  HTTP/1.0 200 OK  (text/html)
40   58.515011   192.168.1.83    192.168.1.80     HTTP      259 GET /login/process.php HTTP/1.1
40   58.522942   192.168.1.80    192.168.1.83     HTTP      60  HTTP/1.0 200 OK  (text/html)
```

A network administrator is investigating suspicious network activity by analyzing captured traffic. An engineer notices abnormal behavior and discovers that the default user agent is present in the headers of
requests and data being transmitted What is occurring?

A. indicators of denial-of-service attack due to the frequency of requests
B. garbage flood attack attacker is sending garbage binary data to open ports
C. indicators of data exfiltration HTTP requests must be plain text
D. cache bypassing attack: attacker is sending requests for noncacheable content

Answer: D

NEW QUESTION 185
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 188
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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 FirstTry

* 200-201 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 200-201 Practice Test Here