



Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

NEW QUESTION 1

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 2

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 3

What is the difference between deep packet inspection and stateful inspection?

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

Answer: D

NEW QUESTION 4

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

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

Answer: B

NEW QUESTION 5

Which 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 6

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 7

What is the function of a command and control server?

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

Answer: D

NEW QUESTION 8

Refer to the exhibit.

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

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

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

Answer: D

NEW QUESTION 9

Which attack method intercepts traffic on a switched network?

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

Answer: C

NEW QUESTION 10

Refer to the exhibit.

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

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

What should be interpreted from this packet capture?

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

Answer: B

NEW QUESTION 10

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 15

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 17

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 18

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 22

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

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

Answer: A

NEW QUESTION 27

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 31

Which evasion technique is a function of ransomware?

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

Answer: B

NEW QUESTION 35

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 39

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 40

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 44

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 49

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 54

A malicious file has been identified in a sandbox analysis tool.

Which piece of information is needed to search for additional downloads of this file by other hosts?

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

Answer: D

NEW QUESTION 56

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 60

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

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

Answer: B

NEW QUESTION 64

Which HTTP header field is used in forensics to identify the type of browser used?

- A. referrer
- B. host
- C. user-agent
- D. accept-language

Answer: C

NEW QUESTION 68

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 73

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 75

Which event is user interaction?

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

Answer: D

NEW QUESTION 77

Which access control model does SELinux use?

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

Answer: C

NEW QUESTION 80

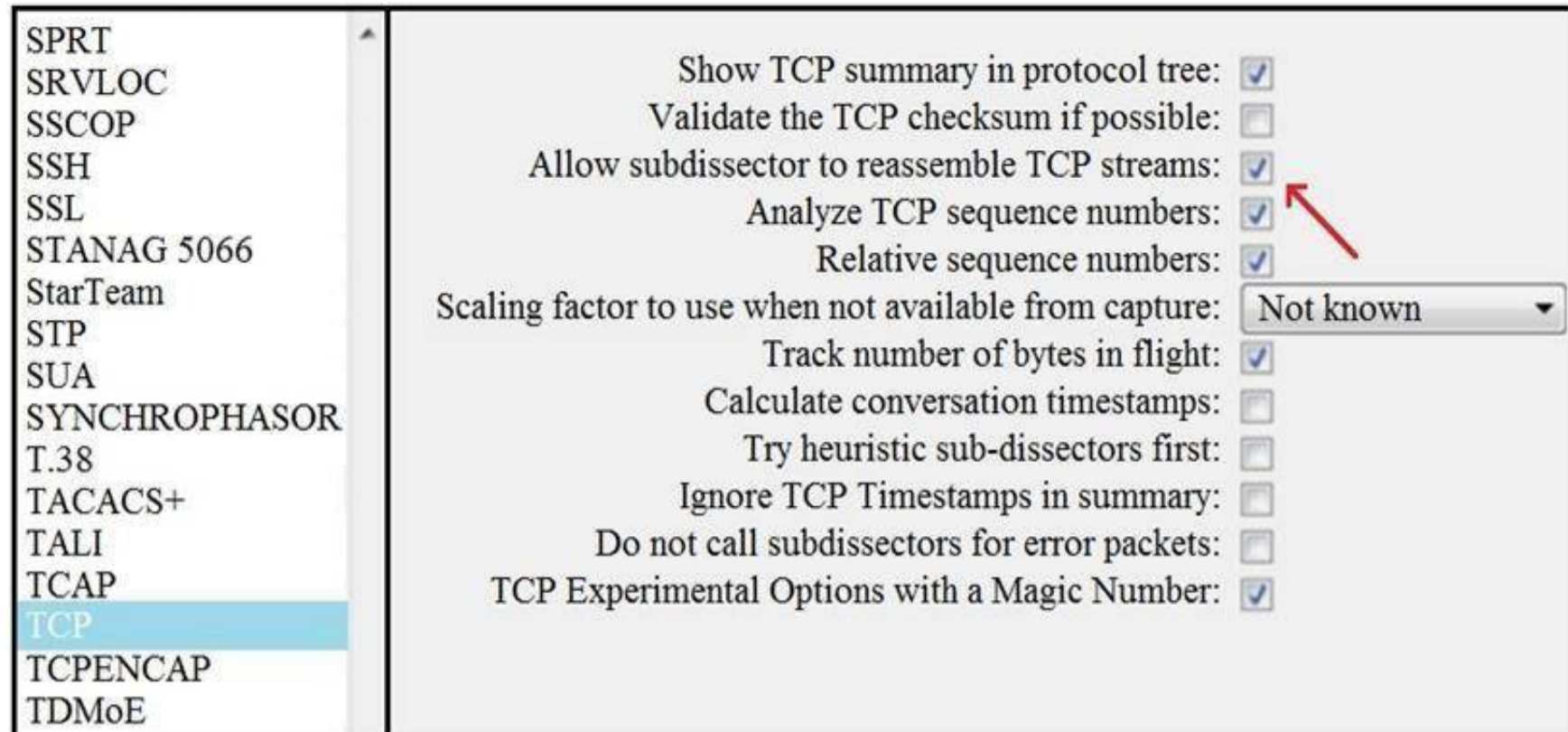
What are two social engineering techniques? (Choose two.)

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

Answer: CE

NEW QUESTION 81

Refer to the exhibit.



The image shows the 'TCP' settings window in Wireshark. On the left is a list of protocols: SPRT, SRVLOC, SSCOP, SSH, SSL, STANAG 5066, StarTeam, STP, SUA, SYNCHROPHASOR, T.38, TACACS+, TALI, TCAP, TCP (highlighted), TCPENCAP, and TDMoE. On the right are various checkboxes and a dropdown menu:

- Show TCP summary in protocol tree: ☒
- Validate the TCP checksum if possible: ☐
- Allow subdissector to reassemble TCP streams: ☒ (indicated by a red arrow)
- Analyze TCP sequence numbers: ☒
- Relative sequence numbers: ☒
- Scaling factor to use when not available from capture: Not known (dropdown menu)
- 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 85

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 90

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 91

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 95

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

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

Answer: DE

NEW QUESTION 97

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 101

Which action prevents buffer overflow attacks?

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

Answer: C

NEW QUESTION 106

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 110

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 112

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 113

.....

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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 2

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 3

What is the difference between deep packet inspection and stateful inspection?

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

Answer: D

NEW QUESTION 4

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

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

Answer: B

NEW QUESTION 5

Which 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 6

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 7

What is the function of a command and control server?

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

Answer: D

NEW QUESTION 8

Refer to the exhibit.

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

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

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

Answer: D

NEW QUESTION 9

Which attack method intercepts traffic on a switched network?

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

Answer: C

NEW QUESTION 10

Refer to the exhibit.

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

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

What should be interpreted from this packet capture?

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

Answer: B

NEW QUESTION 10

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 15

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 17

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 18

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 22

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

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

Answer: A

NEW QUESTION 27

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 31

Which evasion technique is a function of ransomware?

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

Answer: B

NEW QUESTION 35

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 39

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 40

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 44

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 49

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 54

A malicious file has been identified in a sandbox analysis tool.

Which piece of information is needed to search for additional downloads of this file by other hosts?

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

Answer: D

NEW QUESTION 56

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 60

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

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

Answer: B

NEW QUESTION 64

Which HTTP header field is used in forensics to identify the type of browser used?

- A. referrer
- B. host
- C. user-agent
- D. accept-language

Answer: C

NEW QUESTION 68

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 73

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 75

Which event is user interaction?

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

Answer: D

NEW QUESTION 77

Which access control model does SELinux use?

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

Answer: C

NEW QUESTION 80

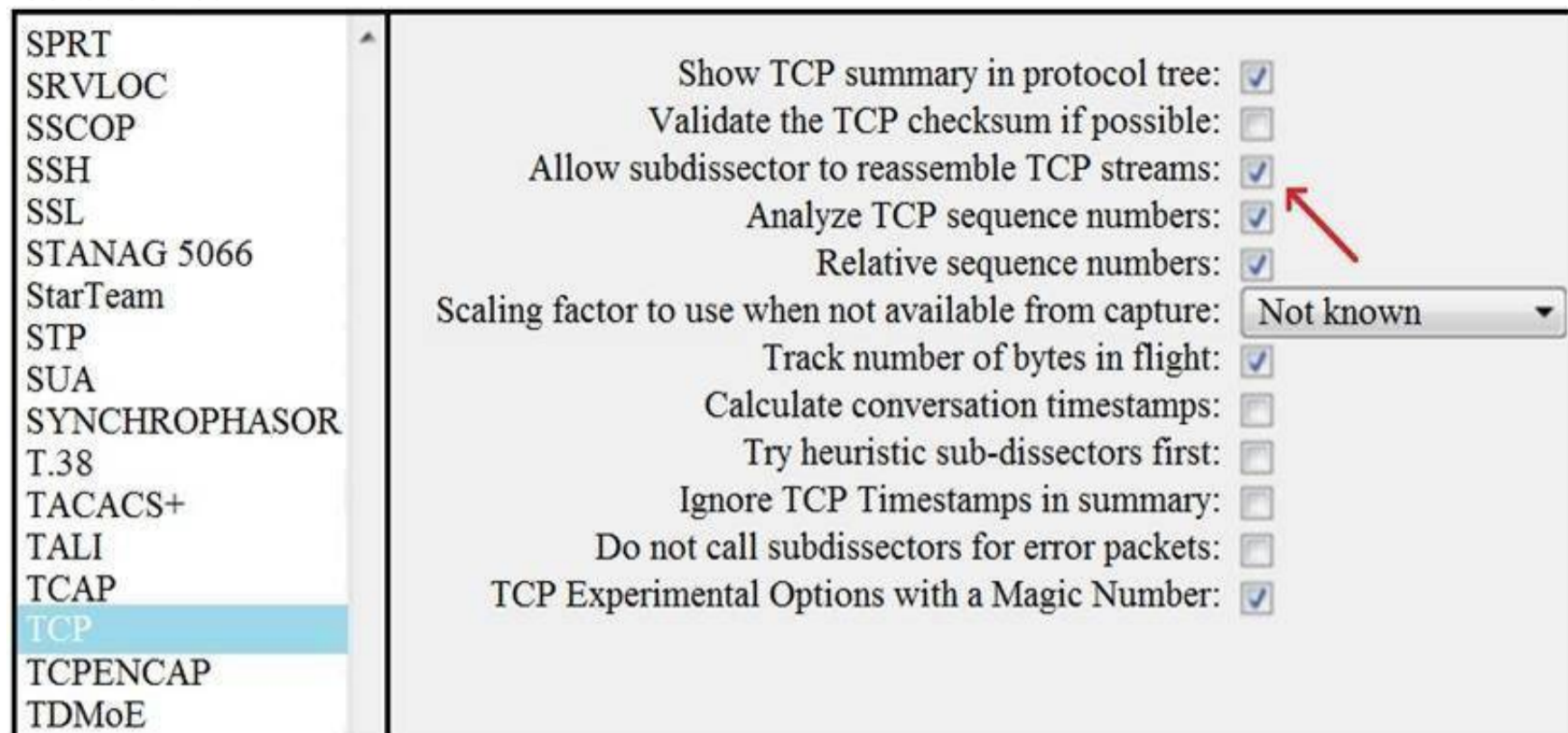
What are two social engineering techniques? (Choose two.)

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

Answer: CE

NEW QUESTION 81

Refer to the exhibit.



The image shows the 'TCP' settings window in Wireshark. On the left, a list of protocols includes SPRT, SRVLOC, SSCOP, SSH, SSL, STANAG 5066, StarTeam, STP, SUA, SYNCHROPHASOR, T.38, TACACS+, TALI, TCAP, TCP (highlighted), TCPENCAP, and TDMoE. On the right, various TCP analysis options are listed with checkboxes or dropdown menus. A red arrow points to the 'Allow subdissector to reassemble TCP streams' checkbox, which is checked.

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

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 85

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 90

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 91

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 95

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

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

Answer: DE

NEW QUESTION 97

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 101

Which action prevents buffer overflow attacks?

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

Answer: C

NEW QUESTION 106

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 110

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 112

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 113

.....

Relate Links

100% Pass Your 200-201 Exam with ExamBible Prep Materials

<https://www.exambible.com/200-201-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>