



Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

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

What is a difference between SIEM and SOAR?

- A. SOAR predicts and prevents security alerts, while SIEM checks attack patterns and applies the mitigation.
- B. SIEM's primary function is to collect and detect anomalies, while SOAR is more focused on security operations automation and response.
- C. SIEM predicts and prevents security alerts, while SOAR checks attack patterns and applies the mitigation.
- D. SOAR's primary function is to collect and detect anomalies, while SIEM is more focused on security operations automation and response.

Answer: B

NEW QUESTION 2

What is a collection of compromised machines that attackers use to carry out a DDoS attack?

- A. subnet
- B. botnet
- C. VLAN
- D. command and control

Answer: B

NEW QUESTION 3

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 4

What describes a buffer overflow attack?

- A. injecting new commands into existing buffers
- B. fetching data from memory buffer registers
- C. overloading a predefined amount of memory
- D. suppressing the buffers in a process

Answer: C

NEW QUESTION 5

Refer to the exhibit.

| | | | |
|-----|------------------|--------------------|-----------|
| TCP | 10.114.248.74:80 | 216.36.50.65:60973 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60974 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60975 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60976 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60977 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60978 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60979 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60980 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60981 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60983 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60984 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60985 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60986 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60987 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60988 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60989 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60990 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60992 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60993 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60994 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60995 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60996 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60997 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60998 | TIME_WAIT |
| TCP | 10.114.248.74:80 | 216.36.50.65:60999 | TIME_WAIT |

An engineer received a ticket about a slowed-down web application The engineer runs the #netstat -an command. How must the engineer interpret the results?

- A. The web application is receiving a common, legitimate traffic
- B. The engineer must gather more data.
- C. The web application server is under a denial-of-service attack.
- D. The server is under a man-in-the-middle attack between the web application and its database

Answer: C

NEW QUESTION 6

Which action should be taken if the system is overwhelmed with alerts when false positives and false negatives are compared?

- A. Modify the settings of the intrusion detection system.
- B. Design criteria for reviewing alerts.
- C. Redefine signature rules.
- D. Adjust the alerts schedule.

Answer: A

Explanation:

Traditional intrusion detection system (IDS) and intrusion prevention system (IPS) devices need to be tuned to avoid false positives and false negatives. Next-generation IPSs do not need the same level of tuning compared to traditional IPSs. Also, you can obtain much deeper reports and functionality, including advanced malware protection and retrospective analysis to see what happened after an attack took place. Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

NEW QUESTION 7

An engineer discovered a breach, identified the threat's entry point, and removed access. The engineer was able to identify the host, the IP address of the threat actor, and the application the threat actor targeted. What is the next step the engineer should take according to the NIST SP 800-61 Incident handling guide?

- A. Recover from the threat.
- B. Analyze the threat.
- C. Identify lessons learned from the threat.
- D. Reduce the probability of similar threats.

Answer: A

Explanation:

Per: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

NEW QUESTION 8

Refer to the exhibit.

| Employee Name | Role |
|---------------|--|
| Employee 1 | Chief Accountant |
| Employee 2 | Head of Managed Cyber Security Services |
| Employee 3 | System Administration |
| Employee 4 | Security Operation Center Analyst |
| Employee 5 | Head of Network & Security Infrastructure Services |
| Employee 6 | Financial Manager |
| Employee 7 | Technical Director |

Which stakeholders must be involved when a company workstation is compromised?

- A. Employee 1 Employee 2, Employee 3, Employee 4, Employee 5, Employee 7
- B. Employee 1, Employee 2, Employee 4, Employee 5
- C. Employee 4, Employee 6, Employee 7
- D. Employee 2, Employee 3, Employee 4, Employee 5

Answer: D

NEW QUESTION 9

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: AE

Explanation:

Cert Guide by Omar Santos, Chapter 9 - Introduction to digital Forensics. "When you collect evidence, you must protect its integrity. This involves making sure that nothing is added to the evidence and that nothing is deleted or destroyed (this is known as evidence preservation)."

NEW QUESTION 10

Which type of verification consists of using tools to compute the message digest of the original and copied data, then comparing the similarity of the digests?

- A. evidence collection order
- B. data integrity
- C. data preservation
- D. volatile data collection

Answer: B

NEW QUESTION 10

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 14

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 18

According to the September 2020 threat intelligence feeds a new malware called Egregor was introduced and used in many attacks. Distribution of Egregor is primarily 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 21

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

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

Answer: A

NEW QUESTION 25

Which technology prevents end-device to end-device IP traceability?

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

Answer: C

NEW QUESTION 29

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 34

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 39

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: D

NEW QUESTION 43

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

Explanation:

According to the Executive Office of the President, Office of Management and Budget (OMB), and the U.S. Department of Commerce, Office of the Chief Information Officer, PII refers to "information which can be used to distinguish or trace an individual's identity."

The following are a few examples:

- An individual's name
- Social security number
- Biological or personal characteristics, such as an image of distinguishing features, fingerprints, Xrays, voice signature, retina scan, and the geometry of the face
- Date and place of birth
- Mother's maiden name
- Credit card numbers
- Bank account numbers
- Driver license number
- Address information, such as email addresses or street addresses, and telephone numbers for businesses or personal use
- Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide Omar Santos

NEW QUESTION 45

Refer to the exhibit.

```
Capturing on 'eth0'
 1 0.000000000 ca:4f:4d:4b:38:5a ? Broadcast ARP 42 Who has 192.168.88.149?
Tell 192.168.88.12
 2 0.000055428 82:69:61:3e:fa:99 ? ca:4f:4d:4b:38:5a ARP 42 192.168.88.149 is at
82:69:61:3e:fa:99
 3 0.000080556 192.168.88.12 ? 192.168.88.149 TCP 74 49098 ? 80 [SYN] Seq=0
Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=65609529 TSecr=0 WS=128
```

What must be interpreted from this packet capture?

- A. IP address 192.168.88.12 is communicating with 192.168.88.149 with a source port 74 to destination port 49098 using TCP protocol
- B. IP address 192.168.88.12 is communicating with 192.168.88.149 with a source port 49098 to destination port 80 using TCP protocol.
- C. IP address 192.168.88.149 is communicating with 192.168.88.12 with a source port 80 to destination port 49098 using TCP protocol.
- D. IP address 192.168.88.149 is communicating with 192.168.88.12 with a source port 49098 to destination port 80 using TCP protocol.

Answer: B

NEW QUESTION 47

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 51

Which metric should be used when evaluating the effectiveness and scope of a Security Operations Center?

- A. The average time the SOC takes to register and assign the incident.
- B. The total incident escalations per week.
- C. The average time the SOC takes to detect and resolve the incident.
- D. The total incident escalations per month.

Answer: C

NEW QUESTION 53

What are two categories of DDoS attacks? (Choose two.)

- A. split brain
- B. scanning
- C. phishing
- D. reflected
- E. direct

Answer: DE

NEW QUESTION 55

Which two elements of the incident response process are stated in NIST SP 800-61 r2? (Choose two.)

- A. detection and analysis
- B. post-incident activity
- C. vulnerability scoring
- D. vulnerability management
- E. risk assessment

Answer: AB

NEW QUESTION 58

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 61

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 external 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 62

An engineer receives a security alert that traffic with a known TOR exit node has occurred on the network. What is the impact of this traffic?

- A. ransomware communicating after infection
- B. users downloading copyrighted content
- C. data exfiltration
- D. user circumvention of the firewall

Answer: D

NEW QUESTION 65

Which are two denial-of-service attacks? (Choose two.)

- A. TCP connections
- B. ping of death
- C. man-in-the-middle
- D. code-red
- E. UDP flooding

Answer: BE

NEW QUESTION 69

What is a difference between SOAR and SIEM?

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

Answer: A

NEW QUESTION 70

Refer to the exhibit.

```
192.168.10.10 -- [01/Dec/2020:11:12:22 -0200] "GET /icons/powered_by_rh.png HTTP/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 -- [01/Dec/2020:11:13:15 -0200] "GET /favicon.ico HTTP/1.1" 404 288 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 -- [01/Dec/2020:11:14:22 -0200] "GET /%27%27;!--%22%3CXSS%3E=&{} HTTP/1.1" 404 310 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
```

What is occurring?

- A. Cross-Site Scripting attack
- B. XML External Entities attack
- C. Insecure Deserialization
- D. Regular GET requests

Answer: A

NEW QUESTION 75

Syslog collecting software is installed on the server. For the log containment, a disk with FAT type partition is used. An engineer determined that log files are being corrupted when the 4 GB file size is exceeded. Which action resolves the issue?

- A. Add space to the existing partition and lower the retention period.
- B. Use FAT32 to exceed the limit of 4 GB.
- C. Use the Ext4 partition because it can hold files up to 16 TB.
- D. Use NTFS partition for log file containment

Answer: D

NEW QUESTION 77

A security engineer notices confidential data being exfiltrated to a domain "Ranso4134-mware31-895" address that is attributed to a known advanced persistent threat group. The engineer discovers that the activity is part of a real attack and not a network misconfiguration. Which category does this event fall under as defined in the Cyber Kill Chain?

- A. reconnaissance
- B. delivery
- C. action on objectives
- D. weaponization

Answer: C

NEW QUESTION 79

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 82

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 83

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 85

Refer to the exhibit.



An engineer is reviewing a Cuckoo report of a file. What must the engineer interpret from the report?

- A. The file will appear legitimate by evading signature-based detection.
- B. The file will not execute its behavior in a sandbox environment to avoid detection.
- C. The file will insert itself into an application and execute when the application is run.
- D. The file will monitor user activity and send the information to an outside source.

Answer: B

NEW QUESTION 89

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

| | |
|---------------|---|
| threat | anything that can exploit a weakness that was not mitigated |
| risk | a gap in security or software that can be utilized by threats |
| vulnerability | possibility for loss and damage of an asset or information |
| exploit | taking advantage of a software flaw to compromise a resource |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Table Description automatically generated

NEW QUESTION 92

What is obtained using NetFlow?

- A. session data
- B. application logs
- C. network downtime report
- D. full packet capture

Answer: A

NEW QUESTION 95

Refer to the exhibit.

```
Error Message%ASA-6-302013: Built {inbound|outbound} TCP
connection_id for interface :real-address /real-port (mapped-
address/mapped-port ) [(idfw_user )] to interface :real-
address /real-port (mapped-address/mapped-port ) [(idfw_user
)] [(user )]
```

During the analysis of a suspicious scanning activity incident, an analyst discovered multiple local TCP connection events Which technology provided these logs?

- A. antivirus
- B. proxy
- C. IDS/IPS
- D. firewall

Answer: D

NEW QUESTION 98

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 103

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 108

What are the two differences between stateful and deep packet inspection? (Choose two)

- A. Stateful inspection is capable of TCP state tracking, and deep packet filtering checks only TCP source and destination ports
- B. Deep packet inspection is capable of malware blocking, and stateful inspection is not
- C. Deep packet inspection operates on Layer 3 and 4. and stateful inspection operates on Layer 3 of the OSI model
- D. Deep packet inspection is capable of TCP state monitoring only, and stateful inspection can inspect TCP and UDP.
- E. Stateful inspection is capable of packet data inspections, and deep packet inspection is not

Answer: AB

NEW QUESTION 112

Refer to the exhibit.

```
Aug 24 2020 09:02:37: %ASA-4-106023: Deny tcp src outside:209.165.200.228/51585 dst  
inside:192.168.150.77/22 by access-group "OUTSIDE" [0x5063b82f, 0x0]
```

An analyst received this alert from the Cisco ASA device, and numerous activity logs were produced. How should this type of evidence be categorized?

- A. indirect
- B. circumstantial
- C. corroborative
- D. best

Answer: C

Explanation:

Indirect=circumstantial so there is no possibility to match A or B (only one answer is needed in this question). For sure it's not a BEST evidence - this FW data inform only of DROPPED traffic. If smth happend inside network, presented evidence could be used to support other evidences or make our narreation stronger but alone it's mean nothing.

NEW QUESTION 114

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 118

A security incident occurred with the potential of impacting business services. Who performs the attack?

- A. malware author
- B. threat actor
- C. bug bounty hunter
- D. direct competitor

Answer: B

NEW QUESTION 122

Which filter allows an engineer to filter traffic in Wireshark to further analyze the PCAP file by only showing the traffic for LAN 10.11.x.x, between workstations and servers without the Internet?

- A. src=10.11.0.0/16 and dst=10.11.0.0/16
- B. ip.src==10.11.0.0/16 and ip.dst==10.11.0.0/16
- C. ip.src=10.11.0.0/16 and ip.dst=10.11.0.0/16
- D. src==10.11.0.0/16 and dst==10.11.0.0/16

Answer: B

NEW QUESTION 123

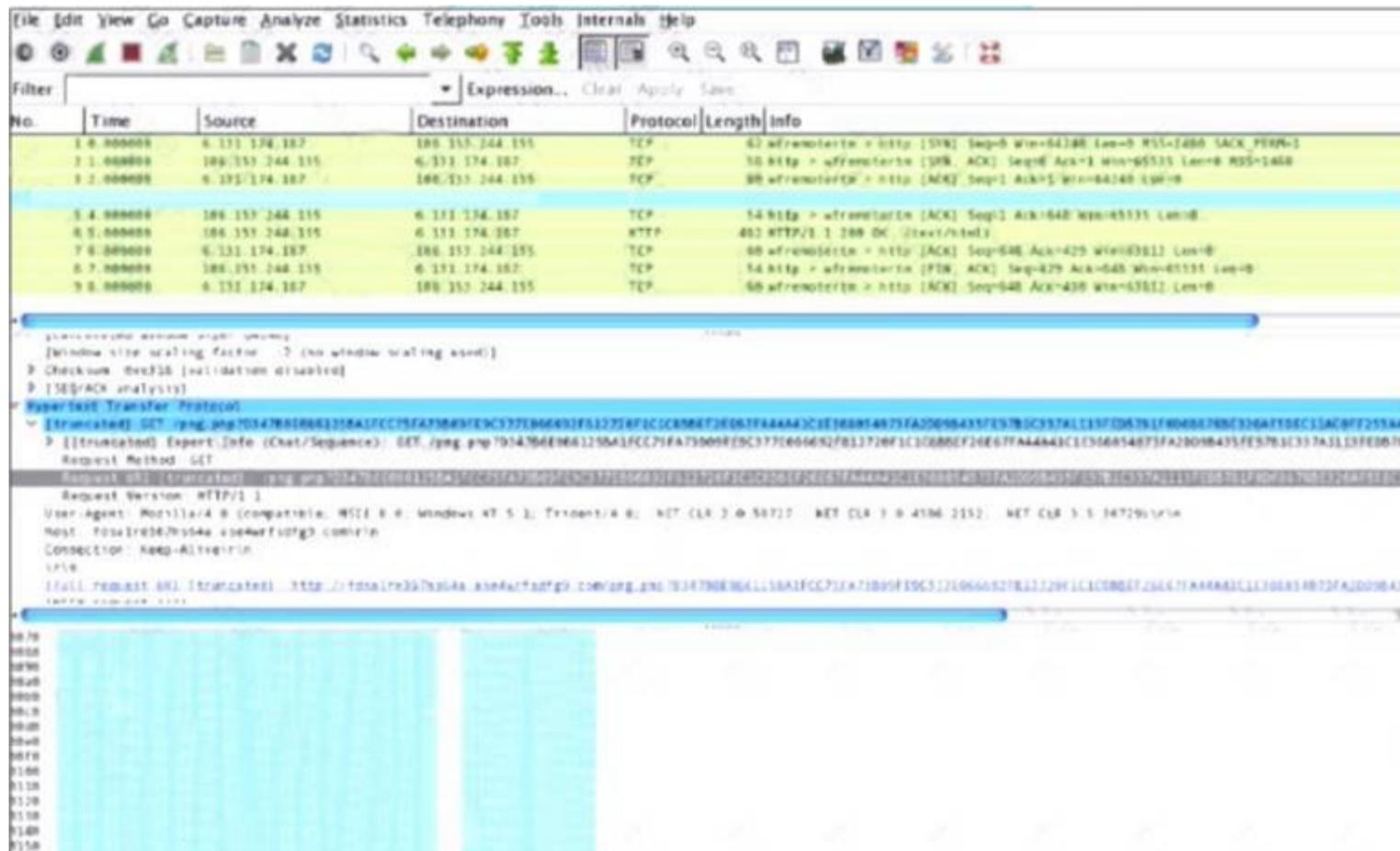
An engineer is addressing a connectivity issue between two servers where the remote server is unable to establish a successful session. Initial checks show that the remote server is not receiving an SYN-ACK while establishing a session by sending the first SYN. What is causing this issue?

- A. incorrect TCP handshake
- B. incorrect UDP handshake
- C. incorrect OSI configuration
- D. incorrect snapplen configuration

Answer: A

NEW QUESTION 128

Refer to the exhibit.



What is shown in this PCAP file?

- A. Timestamps are indicated with error.
- B. The protocol is TCP.
- C. The User-Agent is Mozilla/5.0.
- D. The HTTP GET is encoded.

Answer: D

NEW QUESTION 132

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 134

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 139

Which tool provides a full packet capture from network traffic?

- A. Nagios
- B. CAINE
- C. Hydra
- D. Wireshark

Answer: D

NEW QUESTION 144

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 146

Refer to the exhibit.

```
Mar 07 2020 16:16:48: %ASA-4-106023: Deny tcp src  
outside:10.22.219.221/54602 dst outside:10.22.250.212/504  
by access-group "outside" [0x0, 0x0]
```

Which technology generates this log?

- A. NetFlow
- B. IDS
- C. web proxy
- D. firewall

Answer: D

NEW QUESTION 151

.....

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/>