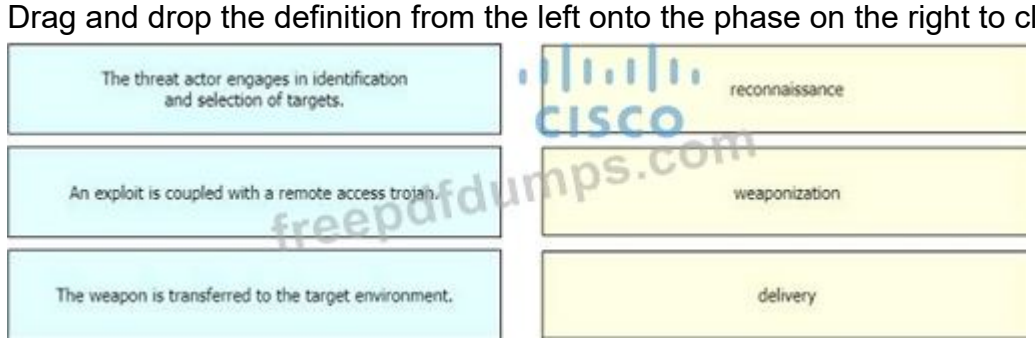
Cisco.200-201.v2025-02-28.q243

Exam Code:	200-201
Exam Name:	Understanding Cisco Cybersecurity Operations Fundamentals
Certification Provider:	Cisco
Free Question Number:	243
Version:	v2025-02-28
# of views:	1276
# of Questions views:	2430
https://www.freepdfdumps.com/Cisco.200-201.v2025-02-28.q243.html	

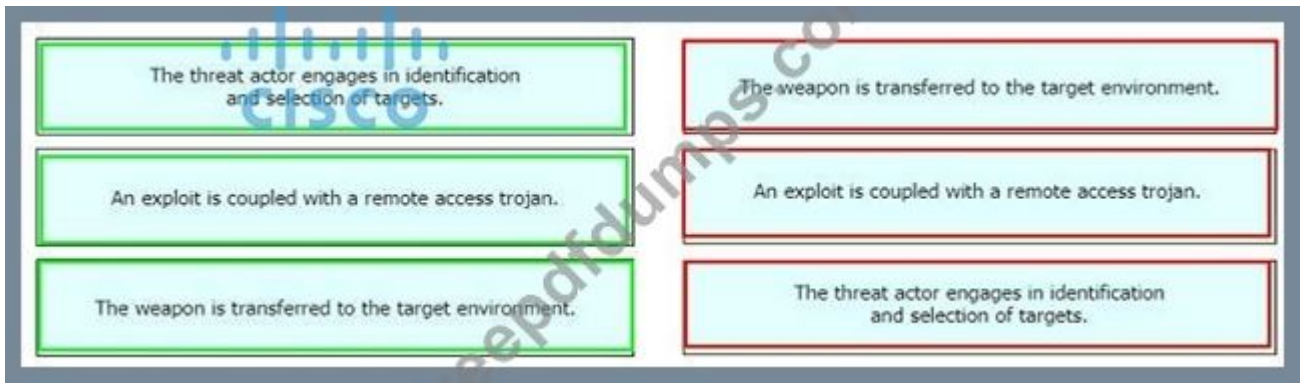
NEW QUESTION: 1
While viewing packet capture data, an analyst sees that one IP is sending and receiving traffic for multiple devices by modifying the IP header.
Which technology makes this behavior possible?
A. encapsulation
B. TOR
C. tunneling
D. NAT
Answer: D (LEAVE A REPLY)
Section: Network Intrusion Analysis

NEW QUESTION: 2
W[^t is vulnerability management?
A. A process to identify and remediate existing weaknesses.
B. A security practice of performing actions rather than acknowledging the threats.
C. A process to recover from service interruptions and restore business-critical applications
D. A security practice focused on clarifying and narrowing intrusion points.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
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.



Answer:



NEW QUESTION: 4

Refer to the exhibit.

```
SELECT * FROM people WHERE username = '' OR '1'='1';
```

Which type of attack is being executed?

A. cross-site scripting

B. cross-site request forgery

C. command injection

D. SQL injection

Answer: D (LEAVE A REPLY)

NEW QUESTION: 5

When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification.

Which information is available on the server certificate?

A. server name, trusted CA, and public key

B. trusted CA name, cipher suites, and private key

C. trusted subordinate CA, public key, and cipher suites

D. server name, trusted subordinate CA, and private key

Answer: (SHOW ANSWER)

When communicating via TLS, part of the handshake process involves presenting a certificate containing the server name, the name of the trusted CA that issued the certificate, and the public key of the server. The client can verify the validity of the certificate and use the public key to encrypt the data sent to the server. Reference:= Cisco Cybersecurity Source Documents

NEW QUESTION: 6

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

A. internet

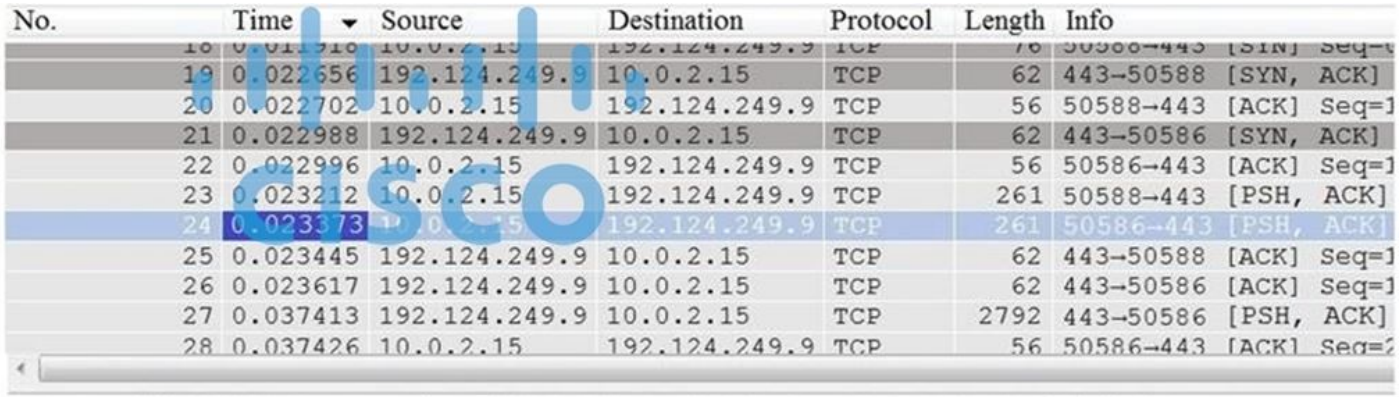
B. transport

C. application

D. data link
Answer: C (LEAVE A REPLY)
Deep packet inspection (DPI) is a sophisticated method of examining the content of data packets as they pass through a network checkpoint, including both the header and the data payload. DPI is typically performed at the application layer of the Open Systems Interconnection (OSI) model. This allows the inspection process to evaluate the actual content of the packets, not just the header information, enabling the identification of various types of threats and the enforcement of network policies1.

NEW QUESTION: 7
What is a difference between signature-based and behavior-based detection?
A. Signature-based identifies behaviors that may be linked to attacks, while behavior-based has a predefined set of rules to match before an alert.
B. Behavior-based identifies behaviors that may be linked to attacks, while signature-based has a predefined set of rules to match before an alert.
C. Behavior-based uses a known vulnerability database, while signature-based intelligently summarizes existing data.
D. Signature-based uses a known vulnerability database, while behavior-based intelligently summarizes existing data.
Answer: B (LEAVE A REPLY)
Behavior-based detection monitors the behavior of programs in real-time. If a piece of software acts similarly to known malware after it's been executed, behavior-based detection can stop it in its tracks. Signature-based detection involves searching for known patterns of data within executable code; if a pattern matches a
"signature" in the system's database that is considered malicious. References: Cisco Cybersecurity Operations Fundamentals

NEW QUESTION: 8
Refer to the exhibit.



Which application protocol is in this PCAP file?

A. SSH

B. HTTP

C. TLS

D. TCP

Answer: B (LEAVE A REPLY)

NEW QUESTION: 9

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: (SHOW ANSWER)

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: 10
A SOC analyst detected connections to known C&C and port scanning activity to main HR database servers from one of the HR endpoints via Cisco StealthWatch. What are the two next steps of the SOC team according to the NISTSP800-61 incident handling process? (Choose two)
A. Isolate affected endpoints and take disk images for analysis
B. Provide security awareness training to HR managers and employees
C. Block connection to this C&C server on the perimeter next-generation firewall
D. Update antivirus signature databases on affected endpoints to block connections to C&C
E. Detect the attack vector and analyze C&C connections
Answer: A,C (LEAVE A REPLY)
According to the NIST SP 800-61 incident handling process, the SOC team should first isolate the affected endpoints to prevent further spread of the attack and take disk images for analysis (A). This helps in preserving evidence for a thorough investigation. The next step would be to block the connection to the C&C server on the perimeter next-generation firewall , which helps to cut off the communication between the compromised endpoint and the attacker's server, thereby mitigating the threat123.
References: The answers are based on the guidelines provided in the NIST SP 800-61 Computer Security Incident Handling Guide, which outlines the steps for incident handling, including detection, analysis, containment, eradication, recovery, and post-incident activities

NEW QUESTION: 11
What is vulnerability management?
A. A security practice focused on clarifying and narrowing intrusion points.
B. A security practice of performing actions rather than acknowledging the threats.
C. A process to identify and remediate existing weaknesses.
D. A process to recover from service interruptions and restore business-critical applications
Answer: C (LEAVE A REPLY)
Vulnerability management is a proactive approach to securing systems by identifying and fixing vulnerabilities before they can be exploited by attackers. It involves scanning systems for known weaknesses, prioritizing and assessing the risks of those vulnerabilities, and applying patches or other remediation measures to mitigate them. Vulnerability management helps reduce the attack surface and prevent potential breaches. Reference:= Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 11.

NEW QUESTION: 12
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: B,D (LEAVE A REPLY)
Profiling a network involves various elements that provide insights into its characteristics and behaviors. Total throughput is crucial as it measures the amount of data passing from a source to a destination in a given period, reflecting the network's capacity and usage patterns1.

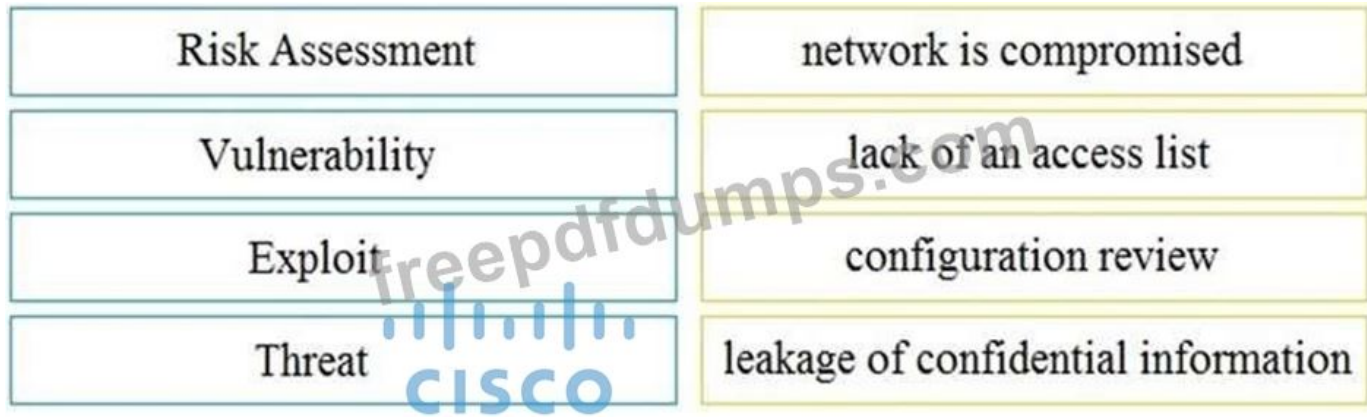
Listening ports are also essential for profiling because they represent the entry points for network services, indicating which services are available and potentially vulnerable1.
References :=
* Network profiling tools and techniques discussed in online resources23.
* Direct explanations of network profile elements

NEW QUESTION: 13
What is indicated by an increase in IPv4 traffic carrying protocol 41 ?
A. additional PPTP traffic due to Windows clients
B. unauthorized peer-to-peer traffic
C. deployment of a GRE network on top of an existing Layer 3 network
D. attempts to tunnel IPv6 traffic through an IPv4 network
Answer: D (LEAVE A REPLY)
Protocol 41 is used to encapsulate IPv6 packets in IPv4 headers for transmission over an IPv4 network. This is one of the methods to implement IPv6 transition mechanisms for hosts and routers that are located on IPv4 networks. An increase in IPv4 traffic carrying protocol 41 may indicate that some hosts or routers are trying to tunnel IPv6 traffic through an IPv4 network, which could be a legitimate or malicious activity depending on the network policy. References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 177; [IPv6 Transition Mechanisms for IPv4 Domains]

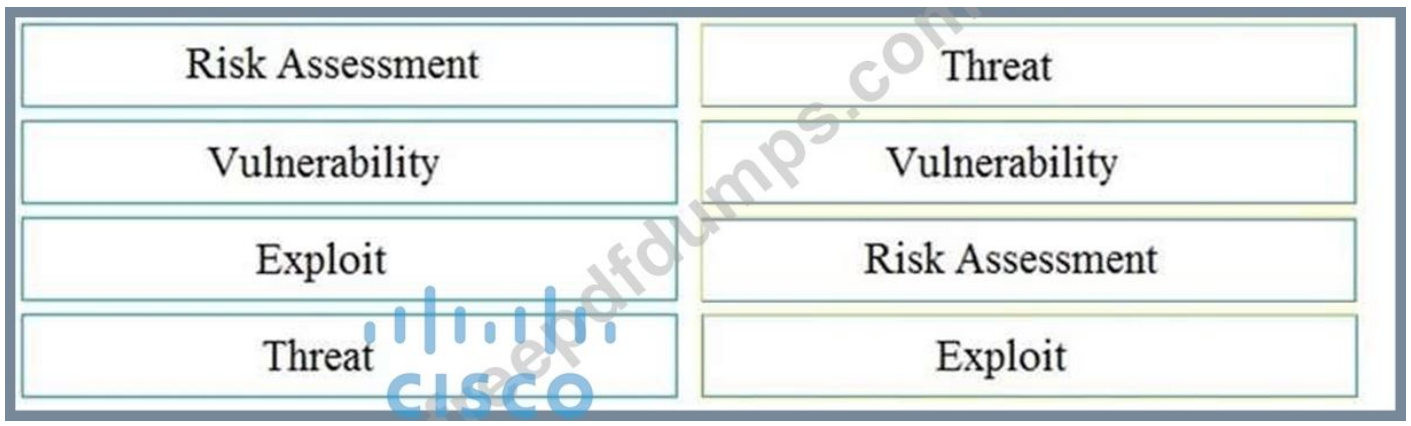
NEW QUESTION: 14
Which type of evidence supports a theory or an assumption that results from initial evidence?
A. probabilistic
B. indirect
C. best
D. corroborative
Answer: D (LEAVE A REPLY)
Corroborative evidence is the type of evidence that supports a theory or an assumption that results from initial evidence. It provides additional support to the initial findings, strengthening the theory or assumption by confirming the same facts or pointing towards the same conclusion with independent pieces of evidence4567.
References := Types of evidence (article) | Lessons | Khan Academy, Evidence: Fundamental Concepts and the Phenomenal Conception, Navigating Scientific Evidence: Types and Definitions, How Courts Work - American Bar Association

NEW QUESTION: 15
Which technology prevents end-device to end-device IP traceability?
A. encryption
B. load balancing
C. NAT/PAT
D. tunneling
Answer: (SHOW ANSWER)
NAT (Network Address Translation) and PAT (Port Address Translation) are technologies that modify the IP address information in packet headers as they pass through a router or firewall, making it difficult to trace the communication back to the originating end-device.

NEW QUESTION: 16
DRAG DROP
Drag and drop the security concept on the left onto the example of that concept on the right.
Select and Place:



Answer:



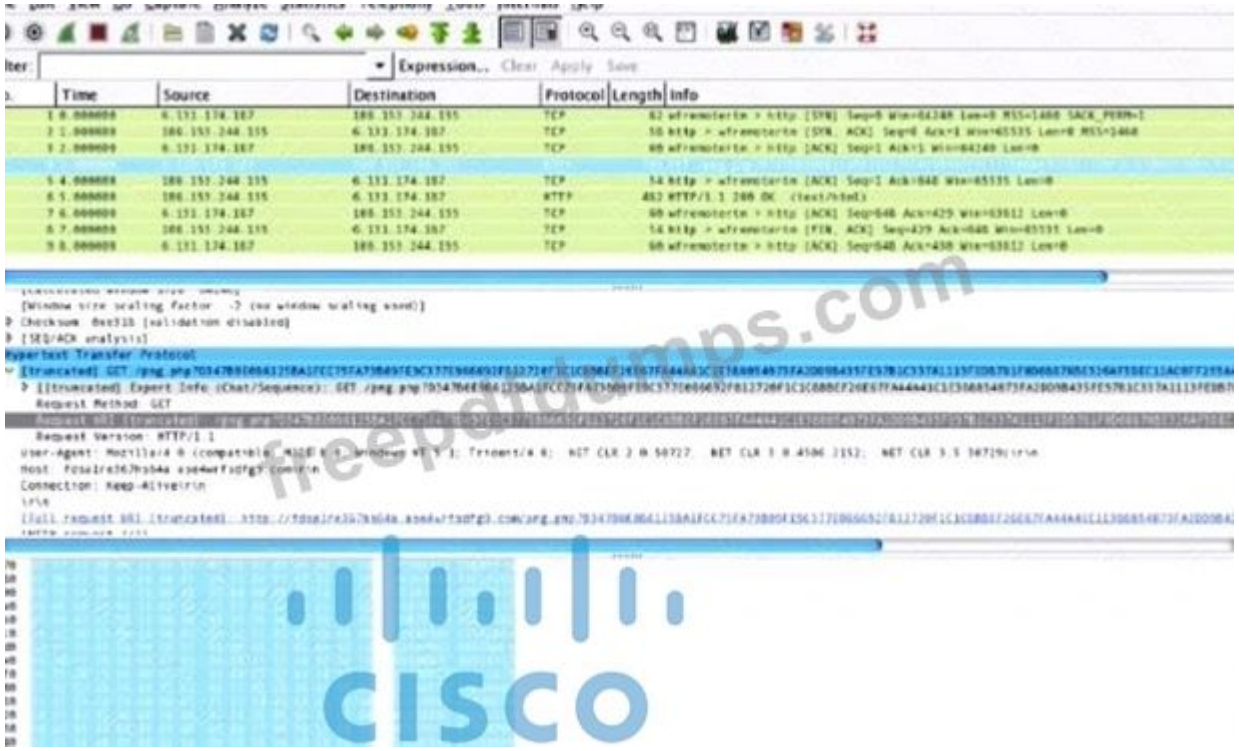
NEW QUESTION: 17
Which regular expression is needed to capture the IP address 192.168.20.232?
A. ^ (?:[0-9]{1,3}\.)'
B. ^ (?:[0-9]{1,3}\.){3}[0-9]{1,3}
C. ^ ([0-9]-{3})
D. ^ (?:[0-9]f1,3}\.){1,4}
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
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 (LEAVE A REPLY)
The Uniform Resource Identifier (URI) is used to identify specific resources on the internet, including files. In the context of HTTP GET requests, the URI specifies the path to the file being requested.

NEW QUESTION: 19
A company receptionist received a threatening call referencing stealing assets and did not take any action assuming it was a social engineering attempt. Within 48 hours, multiple assets were breached, affecting the confidentiality of sensitive information. What is the threat actor in this incident?
A. customer assets that are threatened
B. companyassets that are threatened
C. perpetrators of the attack
D. victims of the attack
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Refer to the exhibit.



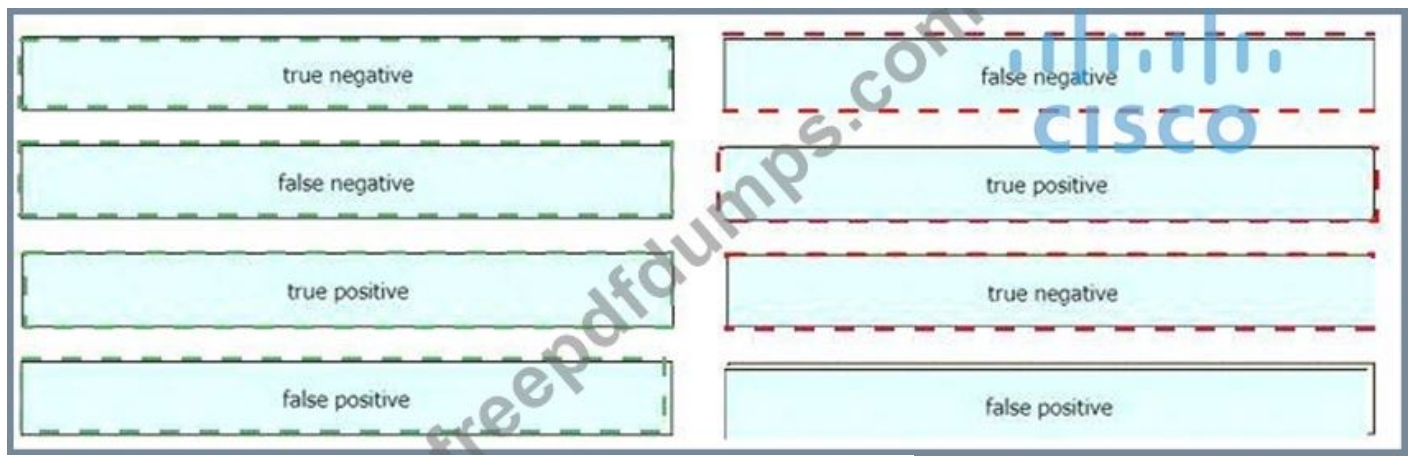
What is shown in this PCAP file?
A. The User-Agent is Mozilla/5.0.
B. The protocol is TCP.
C. The HTTP GET is encoded.
D. Timestamps are indicated with error.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 21

Drag and drop the event term from the left onto the description on the right.

Answer:



NEW QUESTION: 22

Which data type is necessary to get information about source/destination ports?

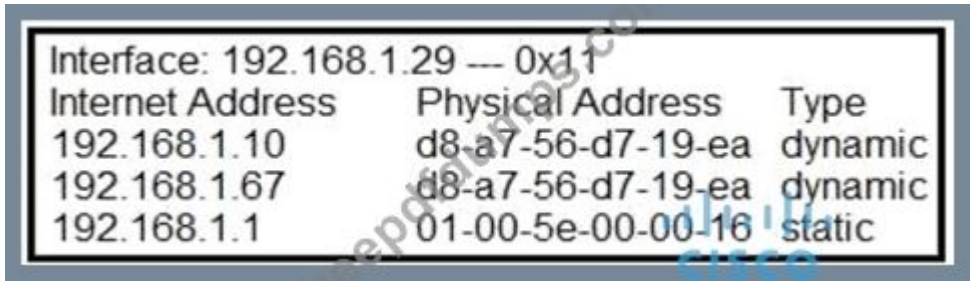
A. statistical data

B. session data

C. connectivity data
D. alert data
Answer: B (LEAVE A REPLY)
Session data is the data type that is necessary to get information about source/destination ports. Session data is the information about connections between hosts, such as IP addresses, ports, protocols, and duration. Session data can be used to identify the services and applications that are being used on the network, as well as the direction and volume of the traffic. Session data can also help to detect anomalous or malicious behavior, such as port scanning, brute force attacks, or data exfiltration. Session data can be collected from various sources, such as firewalls, routers, switches, or network monitoring tools. Reference:
Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 2: Security Monitoring, Lesson 2.2: Data Sources, Topic 2.2.2: Session Data (https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fundamentals-cbrops-v1-0/CSCU-LP-CBROPS-V1-028093.html) Cisco Certified CyberOps Associate Certification Guide, Chapter 3: Data Sources, Section 3.2: Session Data (https://www.ciscopress.com/store/cisco-certified-cyberops-associate-certification-guide-9780136807834) Reference:
https://www.ibm.com/docs/en/networkmanager/4.2.0?topic=relationships-connectivity-data

NEW QUESTION: 23
A company is using several network applications that require high availability and responsiveness, such that milliseconds of latency on network traffic is not acceptable. An engineer needs to analyze the network and identify ways to improve traffic movement to minimize delays. Which information must the engineer obtain for this analysis?
A. total throughput on the interface of the router and NetFlow records
B. output of routing protocol authentication failures and ports used
C. running processes on the applications and their total network usage
D. deep packet captures of each application flow and duration
Answer: A (LEAVE A REPLY)
For high availability and responsiveness, especially where milliseconds of latency are critical, an engineer must analyze the network's performance in detail. Total throughput on the interface of the router will provide information on the bandwidth and traffic load, which is essential for understanding if the network can handle the current and projected traffic without delays. NetFlow records are crucial for this analysis as they provide data about the traffic flow across the network, which helps in identifying patterns, peak usage times, and types of traffic. This information is vital for making informed decisions to optimize traffic movement and minimize latency123.
Reference:
Cisco's guide on Network Traffic Analysis1.
Cisco's white paper on Network Security Policy: Best Practices2.
Cisco's documentation on Implementation of High Availability

NEW QUESTION: 24
Refer to the exhibit.



What is occurring in this network?

A. DNS cache poisoning

B. ARP cache poisoning

C. MAC flooding attack

D. MAC address table overflow

Answer: B (LEAVE A REPLY)

NEW QUESTION: 25

A user received an email attachment named "Hr405-report2609-empl094.exe" but did not run it. Which category of the cyber kill chain should be assigned to this type of event?

A. installation

B. reconnaissance

C. weaponization

D. delivery

Answer: D (LEAVE A REPLY)

Delivery is the fourth phase of the cyber kill chain, which is a model to describe the stages of a cyberattack. Delivery refers to the transmission of the weaponized payload to the target system, such as via email attachments, web links, USB drives, or network connections. Delivery does not necessarily imply successful installation or execution of the payload, which are subsequent phases of the kill chain.
Reference:= Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 31.

NEW QUESTION: 26

Which attack represents the evasion technique of resource exhaustion?

A. SQL injection

B. man-in-the-middle

C. bluesnarfing

D. denial-of-service

Answer: (SHOW ANSWER)

A denial-of-service attack represents the evasion technique of resource exhaustion, where the attacker overwhelms a system's resources, making the system unusable and unable to handle legitimate requests. Reference:= Cisco Cybersecurity Source Documents

NEW QUESTION: 27

What is a difference between inline traffic interrogation and traffic mirroring?

A. Inline inspection acts on the original traffic data flow

B. Traffic mirroring passes live traffic to a tool for blocking

C. Traffic mirroring inspects live traffic for analysis and mitigation

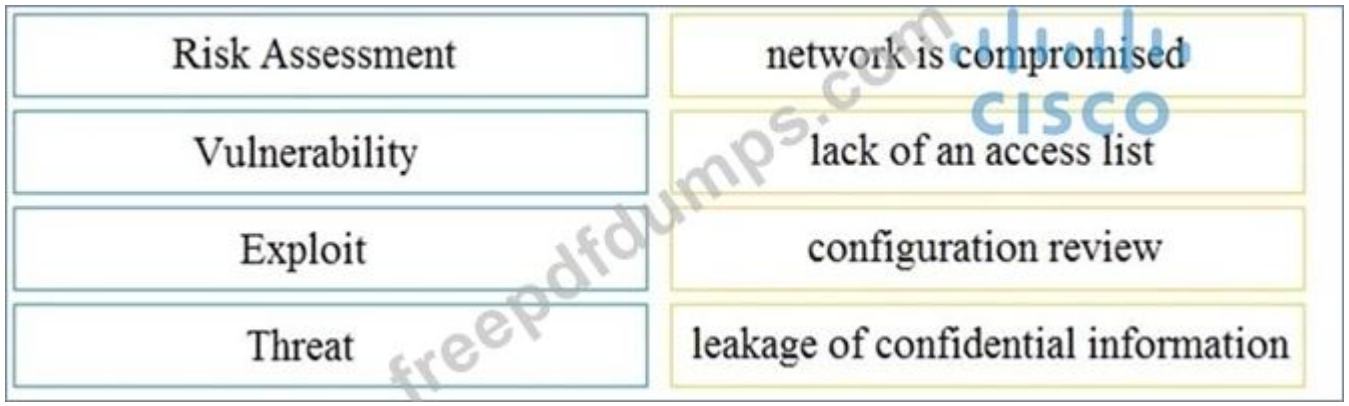
D. Inline traffic copies packets for analysis and security

Answer: (SHOW ANSWER)

Section: Network Intrusion Analysis

NEW QUESTION: 28

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



Answer:

NEW QUESTION: 29

Refer to the exhibit.

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

Which kind of attack method is depicted in this string?

A. cross-site scripting

B. man-in-the-middle

C. SQL injection

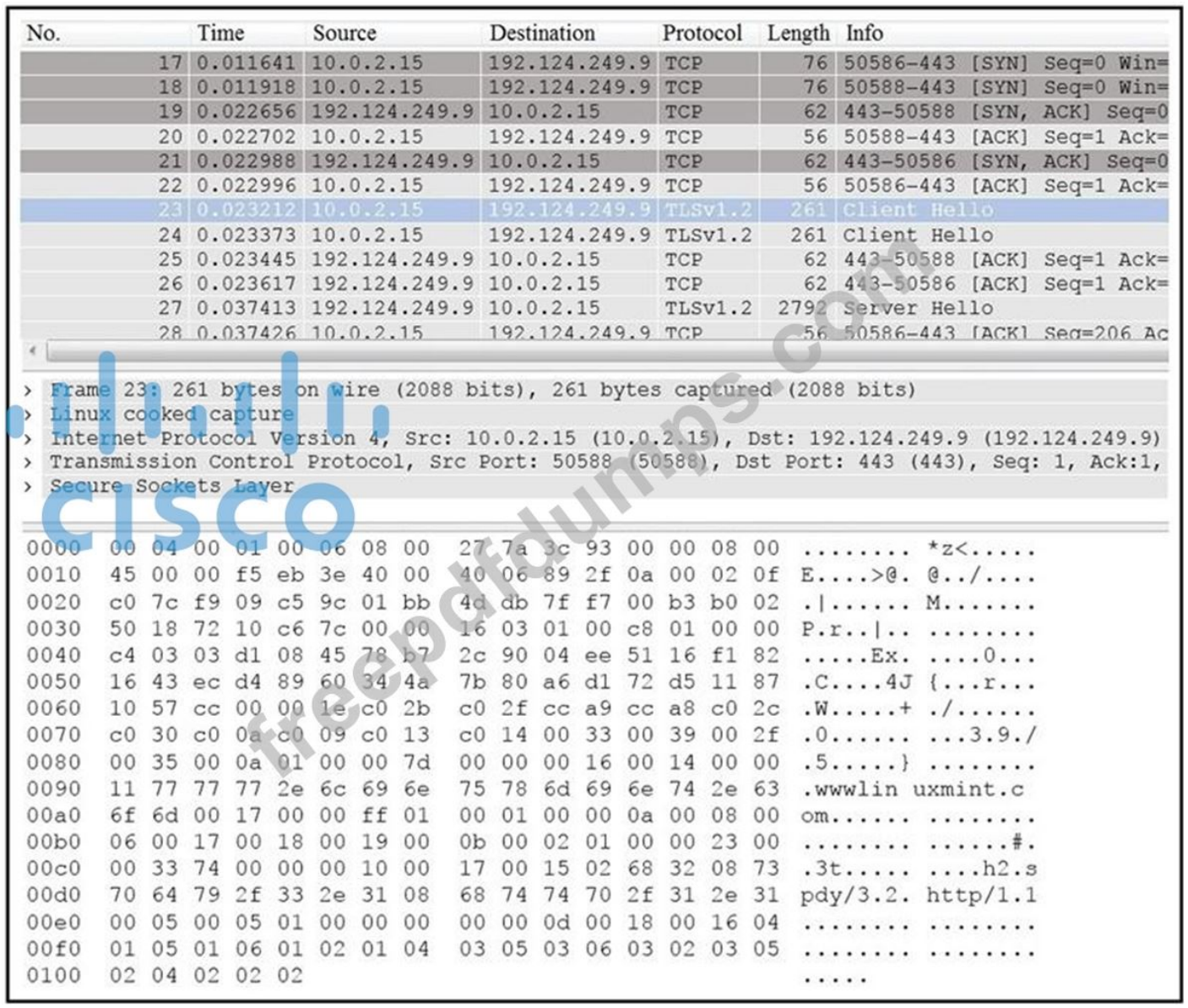
D. denial of service

Answer: (SHOW ANSWER)

* The image shows a piece of code within a bordered rectangular area.
* It is a string of HTML code that appears to be an example of an attack, specifically "<IMG SRC=j%41vascript:alert('attack')>".
* The code suggests an attempt to execute JavaScript within an image source attribute, indicative of a cross-site scripting attack.

NEW QUESTION: 30

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

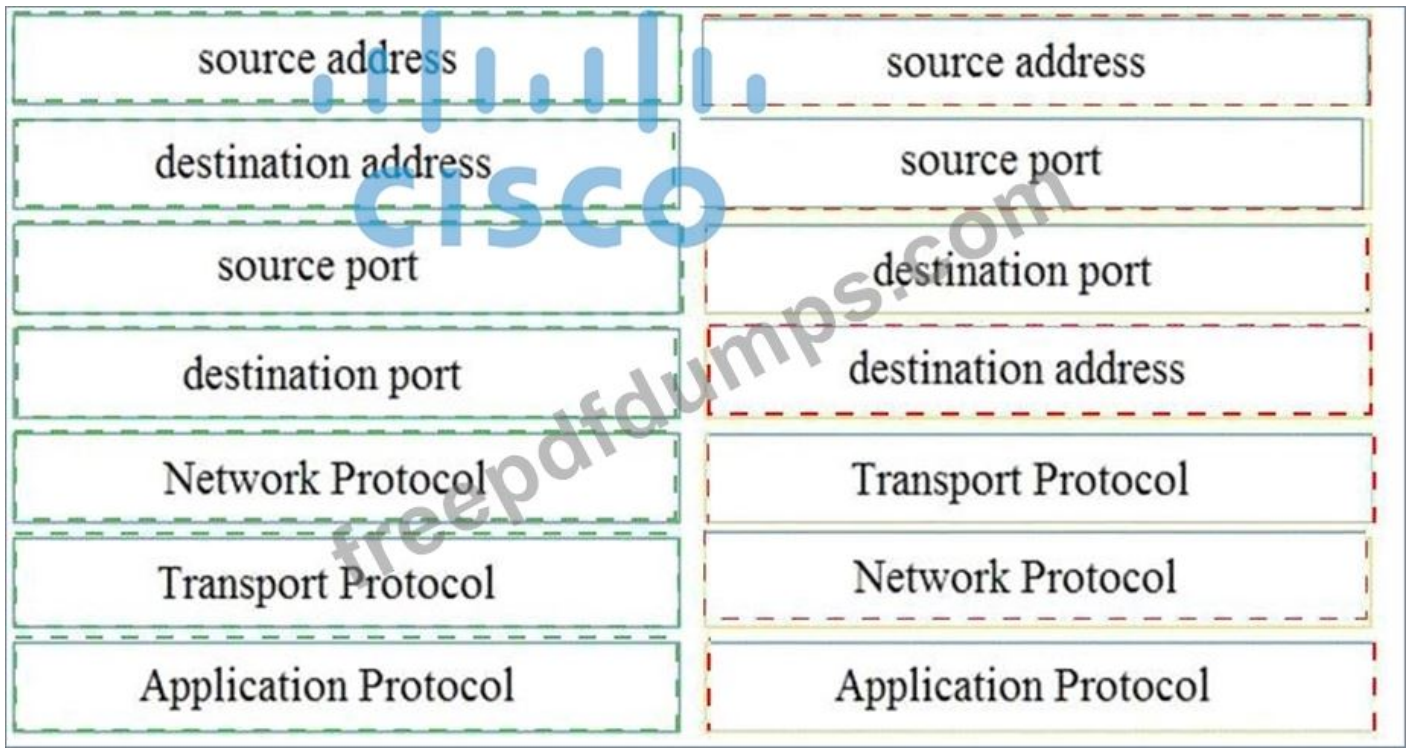
```
> Frame 23: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)
> Transmission Control Protocol, Src Port: 50588 (50588), Dst Port: 443 (443), Seq: 1, Ack:1,
> Secure Sockets Layer
```

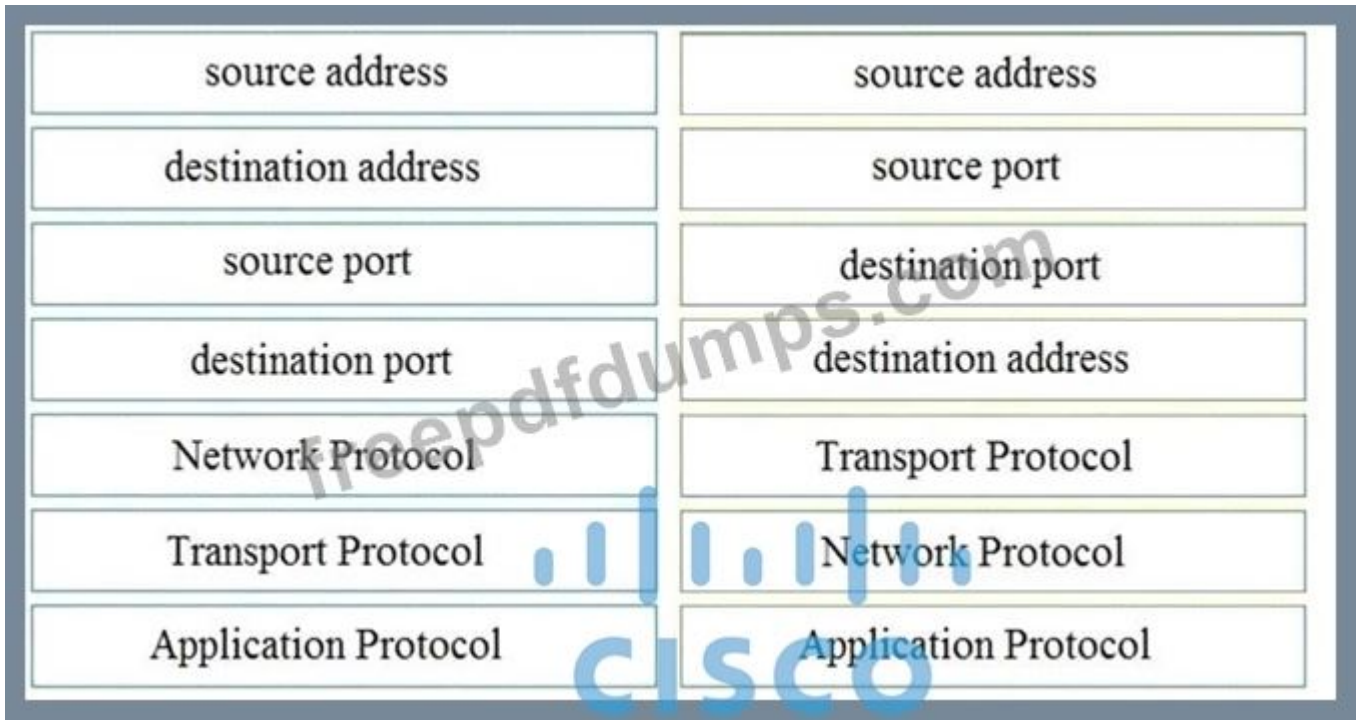
```
0000  00 04 00 01 00 06 08 00  27 7a 3c 93 00 00 08 00  ........ *z<.....
0010  45 00 00 f5 eb 3e 40 00  40 06 89 2f 0a 00 02 0f  E....>@. @../....
0020  c0 7c f9 09 c5 9c 01 bb  4d db 7f f7 00 b3 b0 02  .|...... M.......
0030  50 18 72 10 c6 7c 00 00  16 03 01 00 c8 01 00 00  P.r..|.. ........
0040  c4 03 03 d1 08 45 78 b7  2c 90 04 ee 51 16 f1 82  .....Ex. ....0...
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  .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  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

Answer:





NEW QUESTION: 31
Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)
A. detection and analysis
B. post-incident activity
C. vulnerability management
D. risk assessment
E. vulnerability scoring
Answer: A,B (LEAVE A REPLY)
Section: Security Policies and Procedures
Explanation/Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NEW QUESTION: 32
What are two differences between tampered disk images and untampered disk images'? (Choose two.)
A. Tampered Images are used in a security investigation process
B. Untampered images can be used as law enforcement evidence.
C. The image is untampered if the existing stored hash matches the computed one
D. The image is tampered if the stored hash and the computed hash are identical

E. Tampered images are used as an element for the root cause analysis report

Answer: (SHOW ANSWER)

An untampered disk image is one that has not been altered since its creation. This is verified by comparing the stored hash of the image at the time of creation with a newly computed hash; if they match, the image is considered untampered. Tampered images, on the other hand, may be used during the root cause analysis process to understand how and what was altered12. References: The differences between tampered and untampered disk images are discussed in cybersecurity literature, including Cisco's certification guides, which explain the importance of hash matching for verifying the integrity of disk images

NEW QUESTION: 33

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 mitigates external vulnerabilities, and an attack vector identifies mitigation techniques and possible workarounds.

C. An attack vector matches components that can be exploited, and an attack surface classifies the potential path for exploitation

D. An attack surface identifies vulnerable parts for an attack, and an attack vector specifies which attacks are feasible to those parts.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 34

What is sliding window anomaly detection?

A. Detect changes in operations and management processes.

B. Identify uncommon patterns that do not fit usual behavior.

C. Define response times for requests for owned applications.

D. Apply lowest privilege/permission level to software

Answer: B (LEAVE A REPLY)

Sliding window anomaly detection is a technique used in cybersecurity to identify unusual patterns or behaviors that deviate from the norm. It involves analyzing segments of data over a period of time, referred to as a 'window,' and comparing them against typical patterns. Anomalies are detected when observed behaviors significantly differ from expected patterns, indicating potential security incidents or issues that require further investigation. Reference:: An adaptive sliding window for anomaly detection of time series in wireless sensor networks

NEW QUESTION: 35

What is the impact of false positive alerts on business compared to true positive?

A. True positives affect security as no alarm is raised when an attack has taken place, while false positives are alerts raised appropriately to detect and further mitigate them.

B. True-positive alerts are blocked by mistake as potential attacks, while False-positives are actual attacks Identified as harmless.

C. False-positive alerts are detected by confusion as potential attacks, while true positives are attack attempts identified appropriately.

D. False positives alerts are manually ignored signatures to avoid warnings that are already acknowledged, while true positives are warnings that are not yet acknowledged.

Answer: C (LEAVE A REPLY)

False-positive alerts are alerts that are triggered by benign or normal network traffic and are mistakenly identified as malicious. False positives can have a negative impact on business as they may consume the resources and time of the security team that need to analyze and verify them. True-positive alerts are alerts that correctly identify malicious traffic or activity and require proper incident response procedures. True positives can help the security team to quickly detect and mitigate threats and minimize the damage to the organization.

References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 92;
[Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide], page 98

NEW QUESTION: 36
Which type of data consists of connection level, application-specific records generated from network traffic?
A. transaction data
B. location data
C. statistical data
D. alert data
Answer: A (LEAVE A REPLY)
Section: Security Monitoring
Explanation/Reference:

NEW QUESTION: 37
What is the difference between indicator of attack (IoA) and indicators of compromise (IoC)?
A. IoA is the evidence that a security breach has occurred, and IoC allows organizations to act before the vulnerability can be exploited.
B. IoA refers to the individual responsible for the security breach, and IoC refers to the resulting loss.
C. IoC refers to the individual responsible for the security breach, and IoA refers to the resulting loss.
D. IoC is the evidence that a security breach has occurred, and IoA allows organizations to act before the vulnerability can be exploited.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 38
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 192.168.88.149 is communicating with 192.168.88.12 with a source port 49098 to destination port 80 using TCP protocol.
B. 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.
C. 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.
D. 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
Answer: C (LEAVE A REPLY)

NEW QUESTION: 39
An engineer needs to have visibility on TCP bandwidth usage, response time, and latency, combined with deep packet inspection to identify unknown software by its network traffic flow. Which two features of Cisco Application Visibility and Control should the engineer use to accomplish this goal? (Choose two.)

A. management and reporting
B. traffic filtering
C. adaptive AVC
D. metrics collection and exporting
E. application recognition
Answer: D,E (LEAVE A REPLY)
Cisco Application Visibility and Control (AVC) provides features like metrics collection and exporting (D) for visibility on TCP bandwidth usage, response time, and latency. Application recognition (E) combined with deep packet inspection helps in identifying unknown software by its network traffic flow. References := Cisco CyberOps Associate - Module 2: Security Concepts

NEW QUESTION: 40
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. running processes of the server
D. open ports of an email server
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification.
Which information is available on the server certificate?
A. server name, trusted subordinate CA, and private key
B. trusted subordinate CA, public key, and cipher suites
C. trusted CA name, cipher suites, and private key
D. server name, trusted CA, and public key
Answer: D (LEAVE A REPLY)
When communicating via TLS, part of the handshake process involves presenting a certificate containing the server name, the name of the trusted CA that issued the certificate, and the public key of the server. The client can verify the validity of the certificate and use the public key to encrypt the data sent to the server. References := Cisco Cybersecurity Source Documents

NEW QUESTION: 42
What is a difference between an inline and a tap mode traffic monitoring?
A. Inline monitors traffic without examining other devices, while a tap mode tags traffic and examines the data from monitoring devices.
B. Tap mode monitors traffic direction, while inline mode keeps packet data as it passes through the monitoring devices.
C. Tap mode monitors packets and their content with the highest speed, while the inline mode draws a packet path for analysis.
D. Inline mode monitors traffic path, examining any traffic at a wire speed, while a tap mode monitors traffic as it crosses the network.
Answer: D (LEAVE A REPLY)
Inline mode is used for monitoring the traffic path and can examine any traffic at wire speed. This means that it can analyze data packets as they pass through in real-time. On the other hand, tap mode is used for monitoring traffic as it traverses across the network but does not have the capability to examine data at wire speed like inline mode. References: The information can be referenced from Cisco's official documentation on cybersecurity operations and fundamentals.

NEW QUESTION: 43

```
C:\>nmap -p U:53,67-68,T:21-25,80,135 192.168.233.128
Starting Nmap 7.70 ( https://nmap.org ) at 2018-07-21 13:11 GMT Summer Time
Nmap scan report for 192.168.233.128
Host is up (0.0011s latency).

PORT    STATE    SERVICE
21/tcp  filtered ftp
22/tcp  filtered ssh
23/tcp  filtered telnet
24/tcp  filtered priv-mail
25/tcp  filtered smtp
80/tcp  filtered http

MAC Address: 00:0C:29:62:6A:81 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 22.87 seconds
```

Refer to the exhibit. An attacker scanned the server using Nmap. What did the attacker obtain from this scan?
A. Identified a firewall device preventing the pert state from being returned.
B. Identified open SMB ports on the server
C. Gathered information on processes running on the server
D. Gathered a list of Active Directory users
Answer: (SHOW ANSWER)
The Nmap scan results show that several ports, including ftp (21/tcp), ssh (22/tcp), telnet (23/tcp), smtp (25/tcp), and http (80/tcp), are listed as "filtered". This typically indicates that a firewall is filtering the traffic to these ports, making it impossible to determine whether they are open without further investigation.
However, the question specifically asks about SMB ports, which are not shown in the provided Nmap scan results. Therefore, based on the information given, we cannot confirm that the attacker identified open SMB ports on the server. The correct answer would require additional evidence not present in the scan results.
References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course materials and official Cisco documentation provide insights into interpreting Nmap scan results and identifying port states. These resources can be found at the Cisco Learning Network Store and Cisco's official training and certifications webpage

NEW QUESTION: 44

How is attacking a vulnerability categorized?
A. delivery
B. installation
C. exploitation
D. action on objectives
Answer: (SHOW ANSWER)

NEW QUESTION: 45
A SOC analyst is investigating an incident that involves a Linux system that is identifying specific sessions. Which identifier tracks an active program?
A. application identification number
B. active process identification number
C. runtime identification number
D. process identification number
Answer: (SHOW ANSWER)
In the context of Linux systems, each active program is tracked using a process identification number (PID). The PID is a unique number that the system uses to refer to a specific process, which is an instance of an executed program. This allows the system and the SOC analyst to monitor and manage different processes, including those initiated by users, the system itself, or by applications.

NEW QUESTION: 46
An engineer received a flood of phishing emails from HR with the source address HRjacobm@companycom.
What is the threat actor in this scenario?
A. HR
B. receiver
C. phishing email
D. sender
Answer: D (LEAVE A REPLY)

NEW QUESTION: 47
Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
27336	245.7615440	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27337	245.7615820	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27338	245.7616210	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27340	245.7616680	192.168.154.129	192.168.154.131	FTP	78	Request: PASS binkley
27343	245.7617170	192.168.154.129	192.168.154.131	FTP	84	Request: PASS bloomcounty
27344	245.7617400	192.168.154.131	192.168.154.129	FTP	100	Response: 331 Please specify the password.
27345	245.7617580	192.168.154.129	192.168.154.131	FTP	78	Request: PASS brown
27346	245.7617890	192.168.154.131	192.168.154.129	FTP	100	Response: 331 Please specify the password.
27347	245.7618140	192.168.154.129	192.168.154.131	FTP	78	Request: PASS bloom
27348	245.7618360	192.168.154.131	192.168.154.129	FTP	100	Response: 331 Please specify the password.
27349	245.7618550	192.168.154.129	192.168.154.131	FTP	80	Request: PASS blondie
27350	245.7618920	192.168.154.129	192.168.154.131	FTP	77	Request: PASS capp
27351	245.7653470	192.168.154.129	192.168.154.131	FTP	79	Request: PASS caucas
27352	245.7692450	192.168.154.129	192.168.154.131	FTP	80	Request: PASS cerebus
27353	245.7693080	192.168.154.129	192.168.154.131	FTP	81	Request: PASS catwoman
27355	245.7771480	192.168.154.131	192.168.154.129	FTP	88	Response: 530 Login incorrect.

An analyst was given a PCAP file, which is associated with a recent intrusion event in the company FTP server Which display filters should the analyst use to filter the FTP traffic?

A. dstport == FTP

B. tcp.port==21

C. tcpport = FTP

D. dstport = 21

Answer: B (LEAVE A REPLY)

The correct display filter for analyzing FTP traffic in a PCAP file is "tcp.port==21". This filter will show all TCP packets where the port number is 21, which is the standard port for FTP control messages.

NEW QUESTION: 48

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

A. UDP port to which the traffic is destined

B. TCP port from which the traffic was sourced

C. destination IP address of the packet

D. UDP port from which the traffic is sourced

E. source IP address of the packet

Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 49

An engineer is working with the compliance teams to identify the data passing through the network. During analysis, the engineer informs the compliance team that external penmeter data flows contain records, writings, and artwork Internal segregated network flows contain the customer choices by gender, addresses, and product preferences by age. The engineer must identify protected dat a. Which two types of data must be identified'? (Choose two.)

A. SOX

B. PII

C. PHI

D. PCI

E. copyright

Answer: (SHOW ANSWER)

Protected data refers to any information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. In the scenario described, the engineer must identify data that is considered protected under privacy laws

and regulations. Personal Identifiable Information (PII) and Protected Health Information (PHI) are two types of data that are considered protected. PII includes any data that could potentially identify a specific individual, such as addresses and gender. PHI refers to any information about health status, provision of health care, or payment for health care that can be linked to an individual. This is what makes both PII and PHI crucial to be identified and protected in compliance with data protection regulations.

NEW QUESTION: 50
Which type of evidence supports a theory or an assumption that results from initial evidence?
A. probabilistic
B. indirect
C. best
D. corroborative
Answer: D (LEAVE A REPLY)
Corroborative evidence is the type of evidence that supports a theory or an assumption that results from initial evidence. It provides additional support to the initial findings, strengthening the theory or assumption by confirming the same facts or pointing towards the same conclusion with independent pieces of evidence4567.

NEW QUESTION: 51
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: C,E (LEAVE A REPLY)
In the context of cybersecurity, an asset is anything that has value to the organization, its business operations and their continuity, including data and physical devices. In the role of attribution in an investigation, which is the process of associating an action or event with a particular individual or entity, certain assets are particularly relevant. A laptop can be an asset because it may contain data or clues that can help trace the origin of a cyber attack. Similarly, identifying the threat actor (E) is crucial for attribution, as it involves understanding who is behind the attack and their motives, which can be essential for preventing future attacks and for legal proceedings.

NEW QUESTION: 52
Refer to the exhibit.

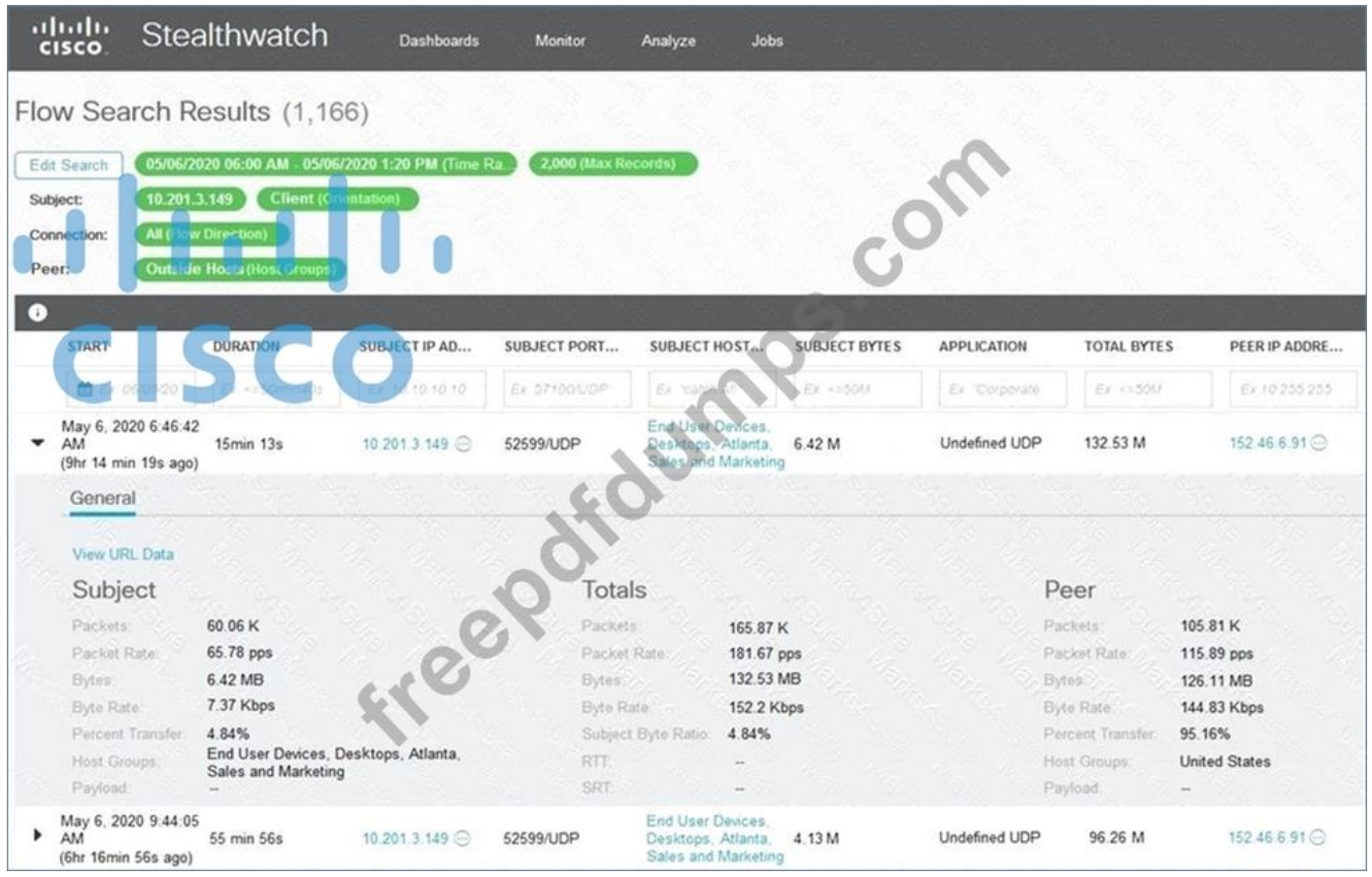
```
# nmap -sV 172.18.104.139

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 an email server
B. open port of an FTP server
C. running processes of the server
D. open ports of a web server
Answer: (SHOW ANSWER)

NEW QUESTION: 53
Refer to the exhibit.



What is the potential threat identified in this Stealthwatch dashboard?
A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.
B. Host 152.46.6.91 is being identified as a watchlist country for data transfer.
C. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.
D. Host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91.
Answer: D (LEAVE A REPLY)
The exhibit shows a Stealthwatch dashboard displaying information on alarming hosts, alarms by type, and today's alarms. On the left side under "Top Alarming Hosts," there are five host IP addresses listed with their respective categories indicating different types of alerts including 'Data Hoarding' and 'Exfiltration.' In
"Alarms by Type" section at center top part of image shows bar graphs representing various alarm types including 'Crypto Violation' with their respective counts. On right side under "Today's Alarms," there's a table showing the details of each alarm such as the host IP, the alarm type, the severity, and the time. The potential threat identified in this dashboard is that host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91, which is a sign of data exfiltration. Data exfiltration is the unauthorized transfer of data from a compromised system to an external destination, such as a command and control server or a malicious actor. This can result in data loss,

breach of confidentiality, and damage to the organization's reputation and assets. References := Cisco Cybersecurity Operations Fundamentals - Module 7: Network and Host Forensics

NEW QUESTION: 54
An engineer is working on a ticket for an incident from the incident management team A week ago. an external web application was targeted by a DDoS attack Server resources were exhausted and after two hours it crashed. An engineer was able to identify the attacker and technique used Three hours after the attack, the server was restored and the engineer recommended implementing mitigation by Blackhole filtering and transferred the incident ticket back to the IR team According to NIST SP800-61, at which phase of the incident response did the engineer finish work?
A. preparation
B. post-incident activity
C. containment eradication and recovery
D. detection and analysis
Answer: C (LEAVE A REPLY)
According to NIST SP800-61, the incident response phase called "Containment, Eradication, and Recovery" involves containing the incident, eradicating the threat, and recovering from the incident2. In the scenario described, the engineer worked on containing the DDoS attack by identifying the attacker and the technique used, which is part of the containment process. The recommendation to implement Blackhole filtering is part of the eradication process, where measures are taken to prevent the attack from happening again. Finally, restoring the server is part of the recovery process, where normal operations are resumed. Therefore, the engineer finished work during the "Containment, Eradication, and Recovery" phase. Reference:: NIST SP800-61 Computer Security Incident Handling Guide2.

NEW QUESTION: 55
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. NetFlow
C. sys
D. proxy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 56
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

Answer:

MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC

NEW QUESTION: 57

Refer to the exhibit.

```
192.168.10.10 – – [01/Dec/2020:11:12:22 -0200] "GET /icons/powered_by_rh.png HTT
P/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-U
S; 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 2
88 "-" "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 within the exhibit?

A. cross-site scripting attack

B. XML External Entities attack

C. regular GET requests

D. insecure deserialization

Answer: (SHOW ANSWER)

NEW QUESTION: 58

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

A. Tap sends traffic from physical layers to the monitoring device, while SPAN provides a copy of network traffic from switch to destination

B. SPAN passively splits traffic between a network device and the network without altering it, while Tap alters response times.

C. Tap mirrors existing traffic from specified ports, while SPAN presents more structured data for deeper analysis.

D. SPAN improves the detection of media errors, while Tap provides direct access to traffic with lowered data visibility.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 59
Refer to the exhibit.

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any ( msg:"BROWSER-
CHROME Google Chrome XSSAuditor filter security policy bypass attempt";
flow:to_client,established; file_data; content:"<iframe",nocase; content:"srcdoc",within
20,nocase; content:"<script>",within 10,nocase;
pcre:"/<iframe[^>]*?srcdoc\s?=\s?[\x22\x27]<script>/smi"; metadata:policy max-detect-
ips drop; service:http; reference:bugtraq,65066;
reference:url,googlechromereleases.blogspot.ca/2014/01/stable-channel-update.html;
classtype:attempted-user; sid:30252; rev:3; )
```


A company's user HTTP connection to a malicious site was blocked according to configured policy What is the source technology used for this measure'?
A. network application control
B. firewall
C. IPS
D. web proxy
Answer: D (LEAVE A REPLY)
A web proxy is the technology used to block a user's HTTP connection to a malicious site according to configured policy. It acts as an intermediary between users and the internet, enforcing security policies and preventing access to harmful sites by inspecting and managing web traffic.

NEW QUESTION: 60
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 (LEAVE A REPLY)
A botnet is a network of compromised computers controlled by an attacker. Botnets are often used to carry out Distributed Denial of Service (DDoS) attacks, where the compromised machines are directed to flood a target with traffic, rendering it inaccessible. References: Cisco Cybersecurity Operations Fundamentals, Module 1:
Security Concepts, Lesson 1.3: Common Network Application Operations and Attacks, Topic 1.3.4:
Denial-of-Service Attacks

NEW QUESTION: 61
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?
A. availability
B. confidentiality

C. scope
D. integrity
Answer: D (LEAVE A REPLY)
The integrity metric in CVSS refers to the unauthorized modification or destruction of information. In this case, an attack that changes a destination bank account number with another one directly affects the accuracy and reliability of data, thus compromising its integrity.
References := Cisco Cybersecurity

NEW QUESTION: 62
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 (LEAVE A REPLY)
Section: Security Concepts

NEW QUESTION: 63
Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?
A. NetScout
B. tcpdump
C. SolarWinds
D. netsh
Answer: B (LEAVE A REPLY)
tcpdump is an open-source packet capture tool that uses the libpcap library to capture network traffic on Linux and Mac OS X operating systems. It can display the contents of packets in various formats, filter packets based on criteria, and save packets to a file. tcpdump is a command-line tool that can be run on a terminal or a remote shell1 Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Module 2: Security Monitoring

NEW QUESTION: 64
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 (LEAVE A REPLY)
Social engineering is the practice of manipulating or deceiving people into performing actions or divulging information that can compromise the security of the organization. Asking questions about the company's user account format and password complexity at a party is an example of social engineering, as the guest may be trying to gather information that can be used to launch a cyberattack. References := Cisco Cybersecurity Operations Fundamentals - Module 6: Security Incident Investigations

NEW QUESTION: 65
An engineer runs a suspicious file in a sandbox analysis tool to see the outcome. The analysis report shows that outbound callouts were made post infection.
Which two pieces of information from the analysis report are needed to investigate the callouts? (Choose two.)
A. signatures
B. host IP addresses
C. file size
D. dropped files
E. domain names
Answer: B,E (LEAVE A REPLY)
To investigate the callouts made post infection, it's essential to know where the callouts were made to (domain names) and from which host IP addresses they originated. This information can help trace back the source and destination, aiding in understanding the nature of the callouts. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Working_with_Indicators_of_Compromise.html

NEW QUESTION: 66
An analyst received a ticket regarding a degraded processing capability for one of the HR department's servers. On the same day, an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?
A. Recovery
B. Detection
C. Eradication
D. Analysis
Answer: D (LEAVE A REPLY)
According to the NIST Incident Handling Guide, the analysis phase is the next phase of this investigation.
The analysis phase involves examining the evidence and determining the impact, scope, and cause of the incident. The analyst should also identify the attacker's methods, tools, and objectives, as well as any indicators of compromise or malicious activity. The analysis phase may also involve collecting additional data, such as logs, network traffic, or malware samples, to support the investigation. The analysis phase is crucial for developing an effective response and recovery strategy, as well as preventing or mitigating future incidents. References:
* NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide, Section 3.2.4, Analysis (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)
* Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 5: Security Incident Response, Lesson 5.2: Incident Response Process, Topic 5.2.3: Analysis Phase (https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operatio

NEW QUESTION: 67
What is the relationship between a vulnerability and a threat?
A. A threat exploits a vulnerability
B. A vulnerability is a calculation of the potential loss caused by a threat
C. A vulnerability exploits a threat
D. A threat is a calculation of the potential loss caused by a vulnerability
Answer: A (LEAVE A REPLY)
A vulnerability refers to a weakness or flaw in a system that can be exploited by threats (such as hackers or malware) to gain unauthorized access, cause damage, etc. Threats exploit these vulnerabilities to impact the confidentiality, integrity, or availability of information and systems. Reference: Cisco Cybersecurity Associate

NEW QUESTION: 68
Which type of data must an engineer capture to analyze payload and header information?
A. frame check sequence
B. alert data
C. full packet
D. session logs
Answer: C (LEAVE A REPLY)
To analyze both payload and header information, an engineer must capture the full packet data. This includes all protocol and payload information for the traffic, allowing for a comprehensive analysis of the data being transmitted5678. Reference:: Full packet capture is a common practice in network monitoring and security, as it provides detailed insights into the data transmitted over the network, including both payload and header information

NEW QUESTION: 69
An engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. Which command will accomplish this goal?
A. nmap --top-ports 192.168.1.0/24
B. nmap -sP 192.168.1.0/24
C. nmap -sL 192.168.1.0/24
D. nmap -sV 192.168.1.0/24
Answer: B (LEAVE A REPLY)
Explanation
https://explainshell.com/explain?cmd=nmap+-sP

NEW QUESTION: 70
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: (SHOW ANSWER)
The file that is extractable via TCP stream within Wireshark is the one that has the Content-Type header set to application/octet-stream, which indicates binary data. This header is present in frames 7, 14, and 21, which are part of the same TCP stream. The other frames have different Content-Type headers, such as text/html or image/jpeg, which are not extractable as binary files. Reference:= Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 3: Network Intrusion Analysis, Lesson 3.2: Analyze Data from Common TCP/IP Protocols, Topic 3.2.3: HTTP

NEW QUESTION: 71
An engineer is working with the compliance teams to identify the data passing through the network. During analysis, the engineer informs the compliance team that external penmeter data flows contain records, writings, and artwork Internal segregated network flows contain the customer choices by gender, addresses, and product preferences by age. The engineer must identify protected data. Which two types of data must be identified'? (Choose two.)
A. SOX
B. PII
C. PHI
D. PCI
E. copyright
Answer: (SHOW ANSWER)
Protected data refers to any information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. In the scenario described, the engineer must identify data that is considered protected under privacy laws and regulations. Personal Identifiable Information (PII) and Protected Health Information (PHI) are two types of data that are considered protected.
PII includes any data that could potentially identify a specific individual, such as addresses and gender. PHI refers to any information about health status, provision of health care, or payment for health care that can be linked to an individual. This is what makes both PII and PHI crucial to be identified and protected in compliance with data protection regulations.
References: The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course provides insights into identifying protected data and the importance of safeguarding it within a network1.

NEW QUESTION: 72
What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?
A. least privilege
B. need to know
C. integrity validation
D. due diligence
Answer: A (LEAVE A REPLY)
The principle of least privilege states that users and processes should be granted only the minimum permissions necessary to perform their specific role or function within an organization. This reduces the attack surface and limits the potential damage of a compromised account or process. References:
* Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 1: Security Concepts, Lesson 1.2: Security Principles

* Cisco Certified CyberOps Associate Overview, Exam Topics, 1.1 Explain the CIA triad

NEW QUESTION: 73
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: (SHOW ANSWER)
The "ps" command is used to display information about the processes running on a system. The "-ef" option shows the full format listing, which includes the process ID, the user, the CPU and memory usage, the command name, and other details. This can help the engineer identify which processes are consuming the most resources and causing the degraded performance of the server. The other options are either invalid or irrelevant, as they do not provide the necessary information or perform the required action. Reference:= Cisco Cybersecurity

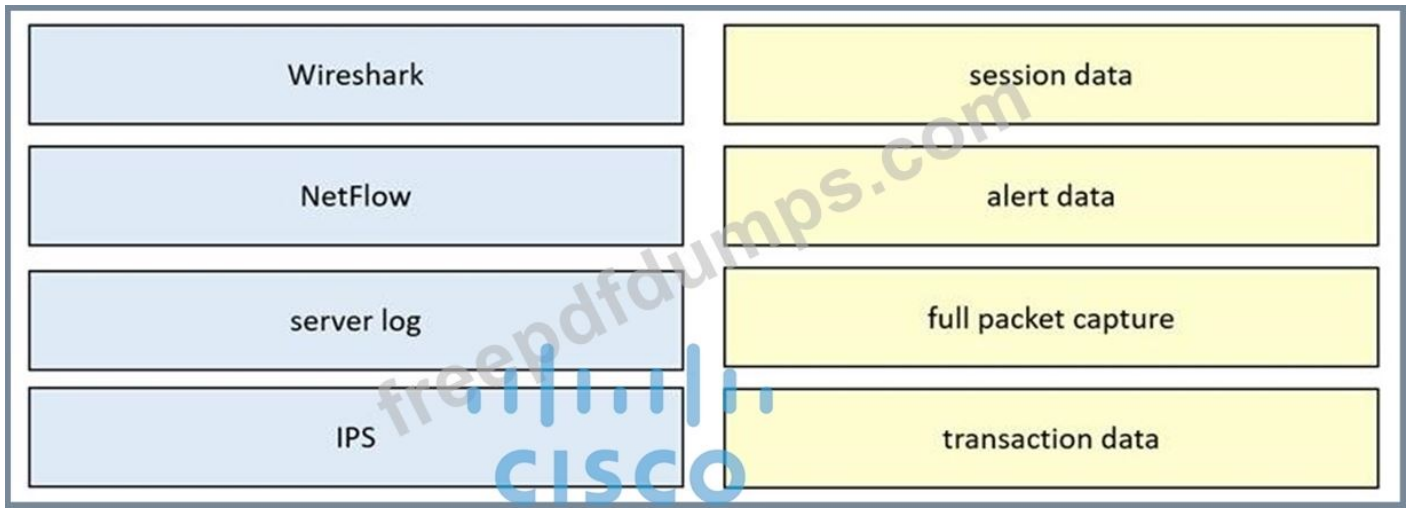
NEW QUESTION: 74
How is SQL injection prevented?
A. Address space layout randomization
B. Validate and sanitize user input
C. ...in the web server as a nonprivileged user
D. ...cost profiling
Answer: B (LEAVE A REPLY)
SQL injection is a type of injection attack where malicious SQL statements are inserted into an entry field for execution.
The primary way to prevent SQL injection is by validating and sanitizing user input. This involves checking the input for malicious content and ensuring it adheres to expected patterns.
Prepared statements (parameterized queries) are also highly effective, as they treat user input as data rather than executable code.
Implementing these practices ensures that any input received from users does not manipulate SQL queries in a harmful way.
Reference:
OWASP SQL Injection Prevention Cheat Sheet
Best Practices for Input Validation and Sanitization
Secure Coding Guidelines

NEW QUESTION: 75
An automotive company provides new types of engines and special brakes for rally sports cars. The company has a database of inventions and patents for their engines and technical information Customers can access the database through the company's website after they register and identify themselves. Which type of protected data is accessed by customers?
A. IP data
B. PII data
C. PSI data
D. PHI data
Answer: A (LEAVE A REPLY)

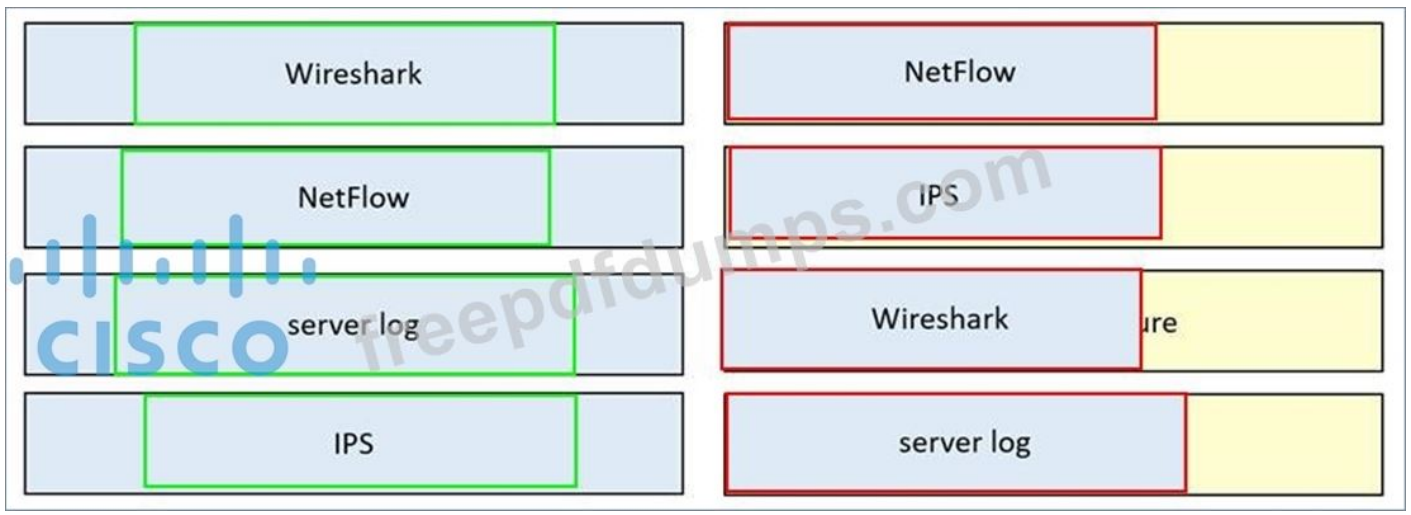
IP data stands for Intellectual Property data, which is any data that represents the creations of the mind, such as inventions, patents, designs, or artistic works. IP data is protected by law and has commercial value for its owners. In this case, the automotive company has a database of IP data for their engines and technical information, which customers can access after they register and identify themselves.
References := Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.2: Data Protection, Topic 1.2.1: Data Types

NEW QUESTION: 76
An engineer must investigate suspicious connections. Data has been gathered using a tcpdump command on a Linux device and saved as sandboxmatware2022-12-22.pcaps file. The engineer is trying to open the tcpdump in the Wireshark tool. What is the expected result?
A. The tool does not support Linux.
B. The file is opened.
C. The file has an incorrect extension.
D. The file does not support the"-" character.
Answer: B (LEAVE A REPLY)
Wireshark is a widely used network protocol analyzer that supports various capture file formats, including those generated by tcpdump. The .pcap extension is a standard format for packet capture files and is fully supported by Wireshark.
The file extension or the inclusion of characters such as "-" in the file name does not impact Wireshark's ability to open and read the file.
When the engineer opens the sandboxmatware2022-12-22.pcaps file in Wireshark, the tool will read the packet capture data, allowing for detailed analysis of network traffic.
Reference:
Cisco Cybersecurity Operations Fundamentals
Wireshark User Guide
tcpdump and libpcap Documentation

NEW QUESTION: 77
Drag and drop the data source from the left onto the data type on the right.



Answer:



NEW QUESTION: 78

Refer to the exhibit.

Which kind of attack method is depicted in this string?

A. cross-site scripting

B. man-in-the-middle

C. SQL injection

D. denial of service

Answer: A (LEAVE A REPLY)

The image shows a piece of code within a bordered rectangular area.

It is a string of HTML code that appears to be an example of an attack, specifically "<IMG SRC=j%41vascript:alert('attack')>".

The code suggests an attempt to execute JavaScript within an image source attribute, indicative of a cross-site scripting attack.

NEW QUESTION: 79

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: (SHOW ANSWER)
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: 80
What is personally identifiable information that must be safeguarded from unauthorized access?
A. zip code
B. date of birth
C. driver's license number
D. gender
Answer: C (LEAVE A REPLY)

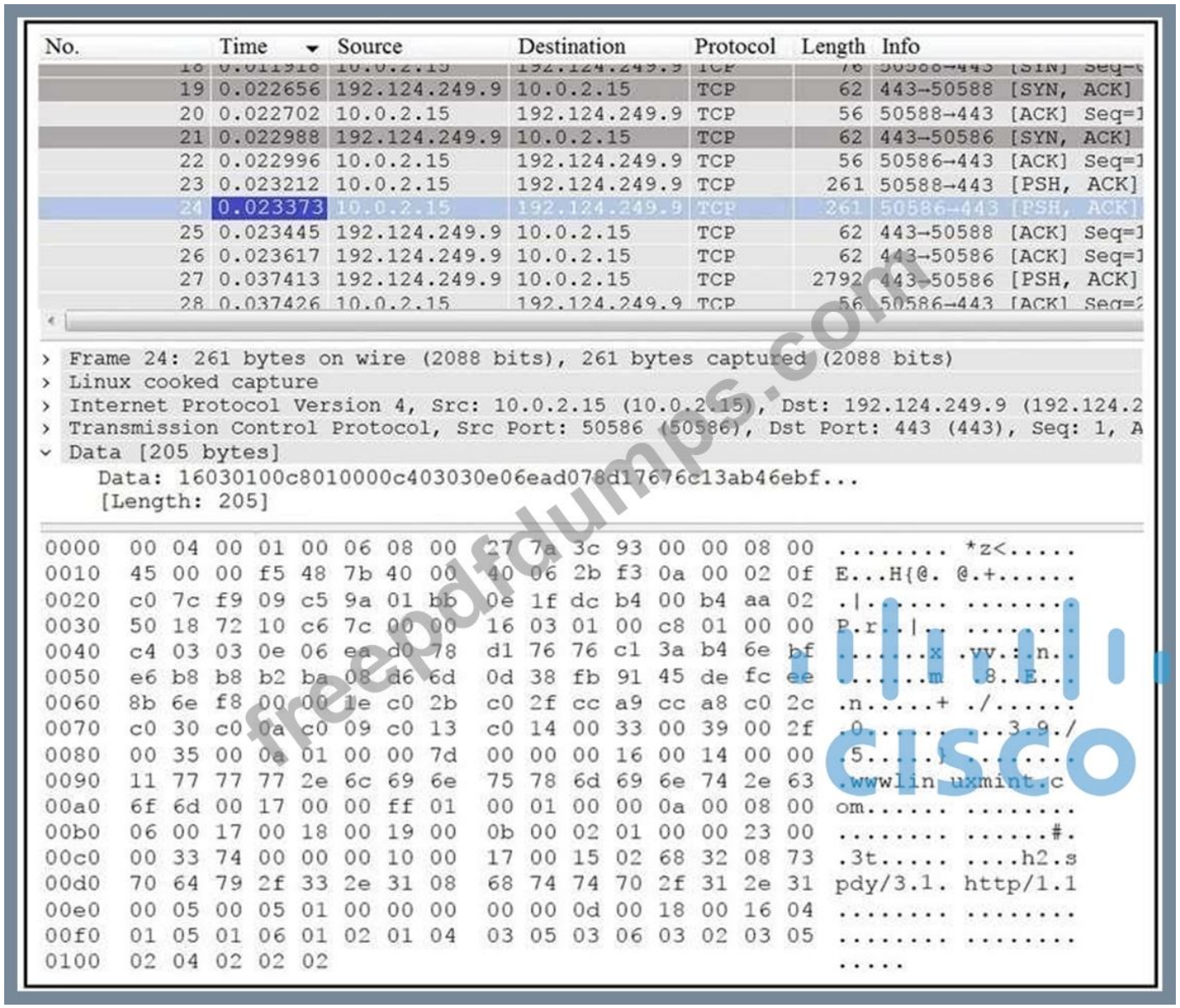
NEW QUESTION: 81
An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture, the analyst cannot determine the technique and payload used for the communication.

Which obfuscation technique is the attacker using?
A. TLS encryption
B. Base64 encoding
C. ROT13 encryption

D. SHA-256 hashing

Answer: A (LEAVE A REPLY)

NEW QUESTION: 82



Refer to the exhibit. Which application protocol is in this PCAP file?

A. SSH

B. HTTP

C. TLS

D. TCP

Answer: D (LEAVE A REPLY)

NEW QUESTION: 83

Refer to the exhibit.

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 (LEAVE A REPLY)
The /var/log/auth.log file contains information about authentication and authorization events on a Linux system, such as successful and failed logins, sudo commands, and SSH sessions. The output in the exhibit shows a failed login attempt from a user named "root" using SSH.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide_24_new_chapter_01101.html

NEW QUESTION: 84
Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)
A. post-incident activity
B. detection and analysis
C. risk assessment
D. vulnerability management
E. vulnerability scoring
Answer: (SHOW ANSWER)

NEW QUESTION: 85
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. data exfiltration
C. users downloading copyrighted content
D. user circumvention of the firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 86
What is a description of a social engineering attack?
A. package deliberately sent to the wrong receiver to advertise a new product
B. email offering last-minute deals on various vacations around the world with a due date and a counter
C. mistakenly received valuable order destined for another person and hidden on purpose
D. fake offer for free music download to trick the user into providing sensitive data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 87

```
File     Actions     Edit     View     Help

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


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. SHA-256 hashing
B. ROT13 encryption
C. Base64 encoding
D. transport layer security encryption
Answer: (SHOW ANSWER)

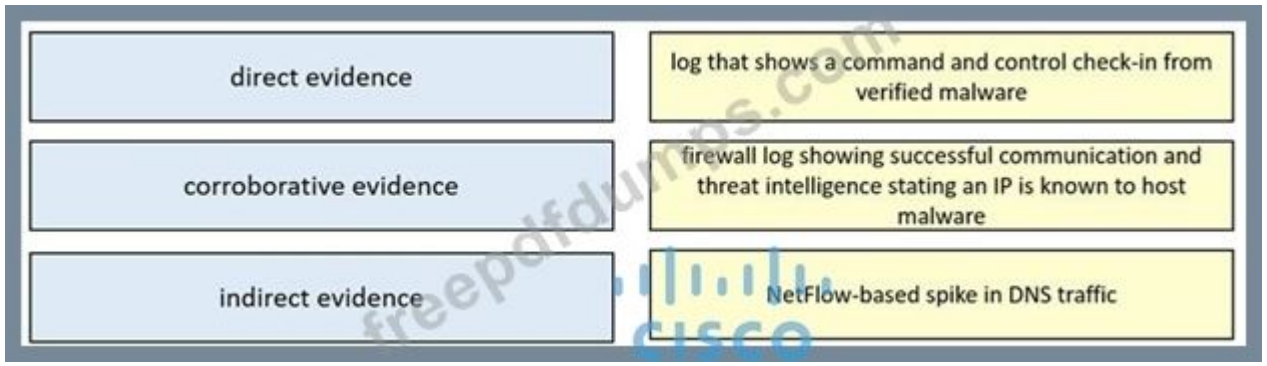
NEW QUESTION: 88
What are two differences in how tampered and untampered disk images affect a security incident? (Choose two.)

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

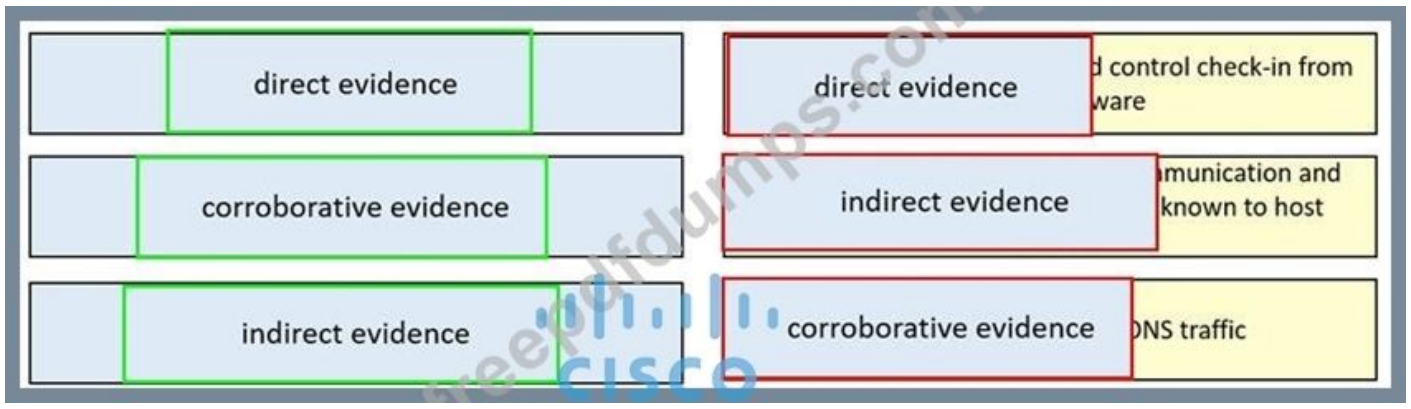
NEW QUESTION: 89
Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

A. dictionary
B. man-in-the-middle
C. replay
D. known-plaintext
Answer: B (LEAVE A REPLY)

NEW QUESTION: 90
Drag and drop the type of evidence from the left onto the description of that evidence on the right.



Answer:



NEW QUESTION: 91

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

Refer to the exhibit. Which event is occurring?
A. A binary is being submitted to run on VM cuckoo1
B. A binary on VM cuckoo1 is being submitted for evaluation
C. A URL is being evaluated to see if it has a malicious binary
D. A binary named "submit" is running on VM cuckoo1.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 92
Refer to the exhibit.
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 (LEAVE A REPLY)
The logs indicating multiple local TCP connection events are typically provided by a firewall. Firewalls are responsible for monitoring and controlling incoming and outgoing network traffic based on predetermined security rules, and they generate logs that detail such events, which can be used for further analysis and incident response. Reference:= Cisco Cybersecurity Operations Fundamentals

NEW QUESTION: 93
Which regular expression is needed to capture the IP address 192.168.20.232?
A. ^ (?:[0-9]{1,3}\.){3}[0-9]{1,3}
B. ^ (?:[0-9]f1,3}\.){1,4}
C. ^ (?:[0-9]{1,3}\.)'
D. ^ ([0-9]-{3})
Answer: A (LEAVE A REPLY)
The regular expression ^ (?:[0-9]{1,3}.){3}[0-9]{1,3} is needed to capture the IP address 192.168.20.232. This regex matches any string that starts with three groups of one to three digits followed by a dot, and ends with one group of one to three digits. The IP address 192.168.20.232 matches this pattern exactly. The other options are either invalid or do not match the IP address format. Reference:= Cisco Cybersecurity Operations Fundamentals, Module 5: Security Policies and Procedures, Lesson 5.3: Data and Event Analysis, Topic 5.3.2: Regular Expressions

NEW QUESTION: 94
An engineer must compare NIST vs ISO frameworks The engineer deeded to compare as readable documentation and also to watch a comparison video review. Using Windows 10 OS. the engineer started a browser and searched for a NIST document and then opened a new tab in the same browser and searched for an ISO document for comparison The engineer tried to watch the video, but there 'was an audio problem with OS so the engineer had to troubleshoot it At first the engineer started CMD and looked fee a driver path then locked for a corresponding registry in the registry editor The engineer enabled "Audiosrv" in task manager and put it on auto start and the problem was solved Which two components of the OS did the engineer touch? (Choose two)
A. process and thread
B. PowerShell logs
C. permissions
D. MBR
E. service

Answer: (SHOW ANSWER)

NEW QUESTION: 95
What are two differences between tampered disk images and untampered disk images'? (Choose two.)
A. Tampered Images are used in a security investigation process
B. Untampered images can be used as law enforcement evidence.
C. The image is untampered if the existing stored hash matches the computed one
D. The image is tampered if the stored hash and the computed hash are identical
E. Tampered images are used as an element for the root cause analysis report
Answer: C,E (LEAVE A REPLY)
An untampered disk image is one that has not been altered since its creation. This is verified by comparing the stored hash of the image at the time of creation with a newly computed hash; if they match, the image is considered untampered. Tampered images, on the other hand, may be used during the root cause analysis process to understand how and what was altered12. Reference:: The differences between tampered and untampered disk images are discussed in cybersecurity literature, including Cisco's certification guides, which explain the importance of hash matching for verifying the integrity of disk images

NEW QUESTION: 96
Which security model assumes an attacker within and outside of the network and enforces strict verification before connecting to any system or resource within the organization?
A. Biba
B. Object-capability
C. Take-Grant
D. Zero Trust
Answer: D (LEAVE A REPLY)
Explanation
Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

NEW QUESTION: 97
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: (SHOW ANSWER)
When a system is overwhelmed with alerts, designing criteria for reviewing alerts can help prioritize and manage them more effectively. This approach allows for a structured review process that can distinguish between false positives, false negatives, and legitimate alerts, reducing the overall number of alerts that require attention3.

NEW QUESTION: 98
What is rule-based detection when compared to statistical detection?

A. proof of a user's action
B. falsification of a user's identity
C. proof of a user's identity
D. likelihood of user's action
Answer: A (LEAVE A REPLY)

NEW QUESTION: 99
What is an advantage of symmetric over asymmetric encryption?
A. A one-time encryption key is generated for data transmission
B. It is a faster encryption mechanism for sessions
C. It is suited for transmitting large amounts of data.
D. A key is generated on demand according to data type.
Answer: C (LEAVE A REPLY)

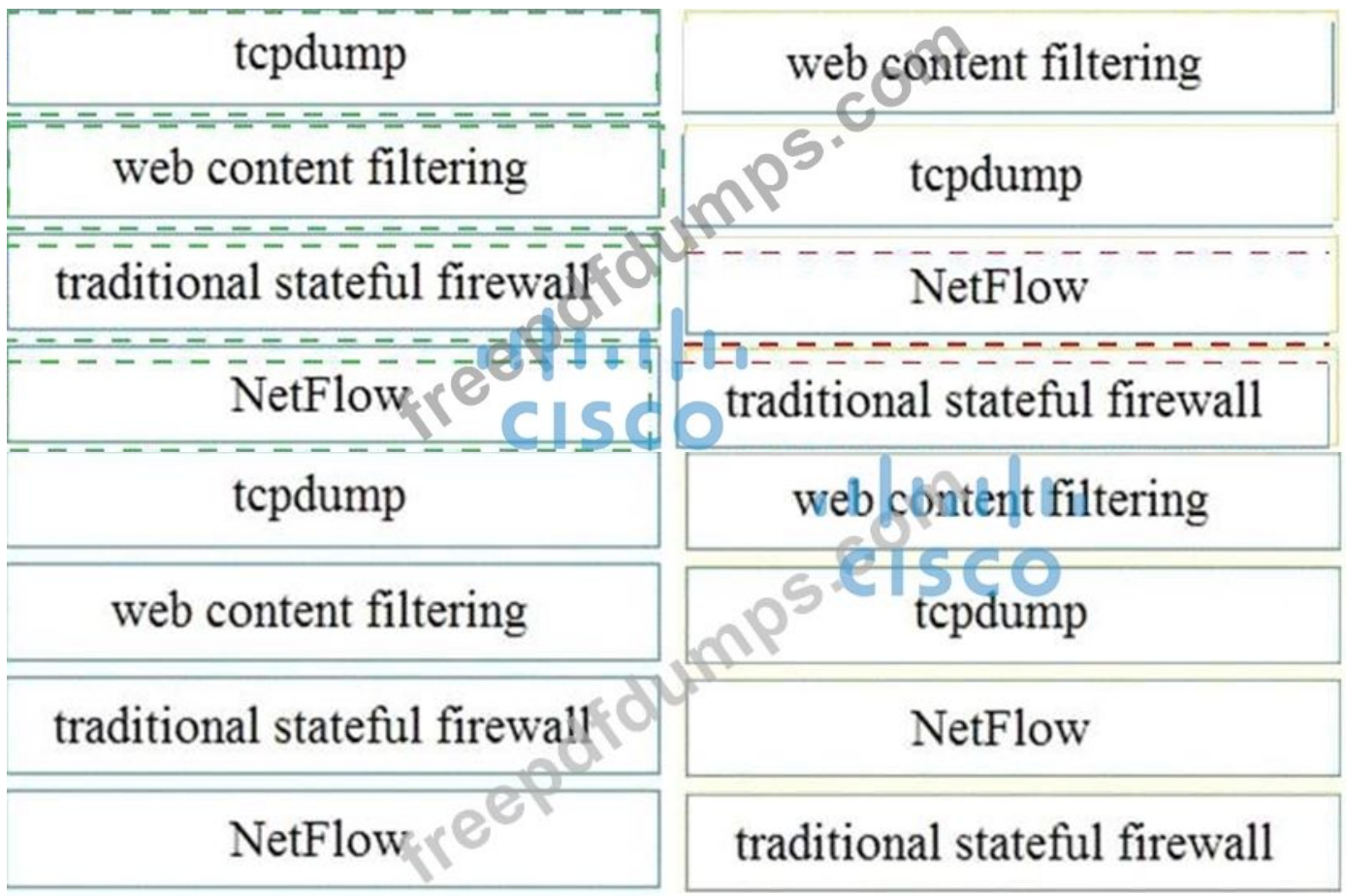
NEW QUESTION: 100
A security engineer notices confidential data being exfiltrated to a domain "Ranso4134-mware31-895" address that is attributed to a known advanced persistent threat group The engineer discovers that the activity is part of a real attack and not a network misconfiguration. Which category does this event fall under as defined in the Cyber Kill Chain?
A. reconnaissance
B. delivery
C. action on objectives
D. weaponization
Answer: (SHOW ANSWER)
The event described falls under the 'action on objectives' category of the Cyber Kill Chain. This stage occurs after the attacker has established a foothold within the network and begins to execute their intended actions, such as data exfiltration. References: The Cyber Kill Chain framework outlines the stages of a cyberattack, with 'action on objectives' being the final step where attackers achieve their primary goal, such as data theft

NEW QUESTION: 101
After a large influx of network traffic to externally facing devices, a security engineer begins investigating what appears to be a denial of service attack When the packet capture data is reviewed, the engineer notices that the traffic is a single SYN packet to each port Which type of attack is occurring?
A. traffic fragmentation
B. port scanning
C. host profiling
D. SYN flood
Answer: B (LEAVE A REPLY)
The scenario described is indicative of a port scanning attack. Port scanning is a method used by attackers to discover open ports on network devices. A single SYN packet sent to each port is a technique known as SYN scanning or half-open scanning, where the attacker sends a SYN message (as if they are going to initiate a TCP connection) to every port on the server, looking for positive responses which

indicate an open port. This type of scanning is less intrusive and harder to detect because it never completes the TCP three-way handshake1.
References: Cisco community resources on Denial of Service (DoS) attacks

NEW QUESTION: 102
Drag and drop the technology on the left onto the data type the technology provides on the right.

Answer:



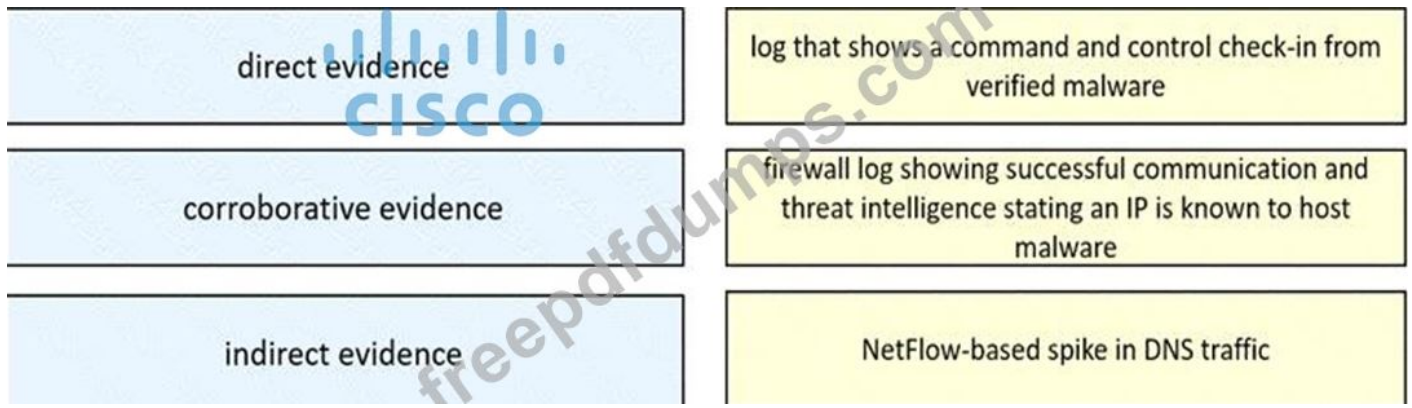
NEW QUESTION: 103
What are two social engineering techniques? (Choose two.)
A. privilege escalation
B. DDoS attack

C. phishing
D. man-in-the-middle
E. pharming
Answer: C,E (LEAVE A REPLY)
Social engineering techniques often involve manipulating individuals into divulging confidential information or performing actions that compromise security. Phishing involves sending fraudulent messages (often emails) that appear to be from reputable sources with the goal of stealing sensitive data or installing malware.
Pharming redirects the traffic of a legitimate website to another fraudulent website without the user's knowledge, aiming to collect the user's credentials. References := Cisco Cybersecurity Source Documents

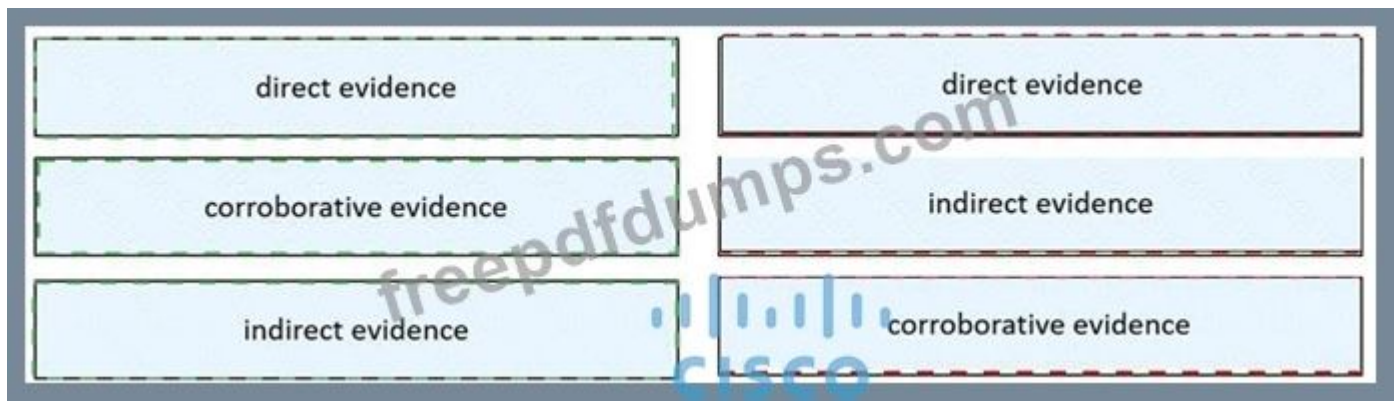
NEW QUESTION: 104
What is the difference between statistical detection and rule-based detection models?
A. Rule-based detection involves the collection of data in relation to the behavior of legitimate users over a period of time
B. Statistical detection defines legitimate data of users over a period of time and rule-based detection defines it on an IF/THEN basis
C. Statistical detection involves the evaluation of an object on its intended actions before it executes that behavior
D. Rule-based detection defines legitimate data of users over a period of time and statistical detection defines it on an IF/THEN basis
Answer: (SHOW ANSWER)
Statistical detection involves collecting data over time to define what is considered normal behavior or legitimate data for users or systems. It then uses statistical analysis to identify abnormal behavior that could indicate a security incident. Rule-based detection uses predefined rules or patterns that are based on known threats or vulnerabilities - it operates on an IF/THEN basis where if certain conditions are met then an alert is triggered. References := Cisco Cybersecurity Operations Fundamentals

NEW QUESTION: 105
An organization is cooperating with several third-party companies. Data exchange is on an unsecured channel using port 80 Internal employees use the FTP service to upload and download sensitive data An engineer must ensure confidentiality while preserving the integrity of the communication. Which technology must the engineer implement in this scenario'?
A. web application firewall
B. CA server
C. RADIUS server
D. 509 certificates are used in conjunction with secure data transfer protocols to ensure the confidentiality and integrity of communication. They are part of a public key infrastructure (PKI) that authenticates the identity of entities and encrypts data in transit. Reference:: Implementing X.509 certificates along with secure data transfer protocols like SFTP, HTTPS, FTPS, and IPSec can help secure data sharing with third-party companies
E. X 509 certificates
Answer: E (LEAVE A REPLY)

NEW QUESTION: 106
Drag and drop the type of evidence from the left onto the description of that evidence on the right.

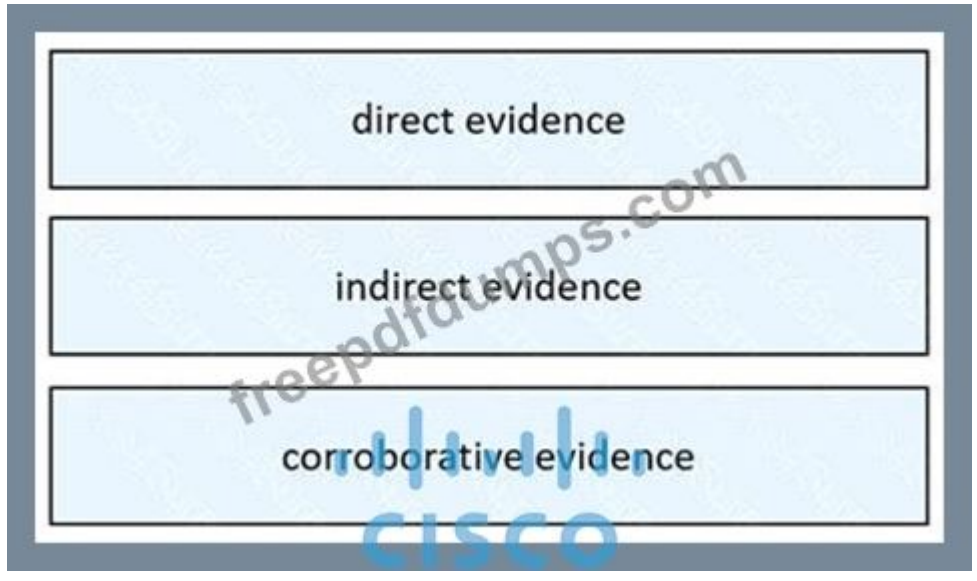


Answer:



Explanation:

Graphical user interface, application Description automatically generated



NEW QUESTION: 107

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 tile size is exceeded. Which action resolves the issue?

A. Use the Ext4 partition because it can hold files up to 16 TB.

B. Add space to the existing partition and lower the retention penod.

C. Use FAT32 to exceed the limit of 4 GB.

D. Use NTFS partition for log file containment

Answer: D (LEAVE A REPLY)

NEW QUESTION: 108

Refer to the exhibit.

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 (LEAVE A REPLY)

The packet capture exhibit shows that the source IP address is 192.168.122.100 and it is sending a packet from source port 50272 to destination port 80 of destination IP address 81.179.179.69 using TCP protocol. The TCP protocol is indicated by the Protocol field which has the value 6. The source and destination ports are indicated by the SrcPort and DstPort fields respectively. The source and destination IP addresses are indicated by the SrcAddr and DstAddr fields respectively. Reference:= Cisco Cybersecurity Operations Fundamentals - Module 3: Network Data and Event Analysis

NEW QUESTION: 109

Why should an engineer use a full packet capture to investigate a security breach?

A. It reconstructs the event allowing the engineer to identify the root cause by seeing what took place during the breach

B. It provides the full TCP streams for the engineer to follow the metadata to identify the incoming threat.

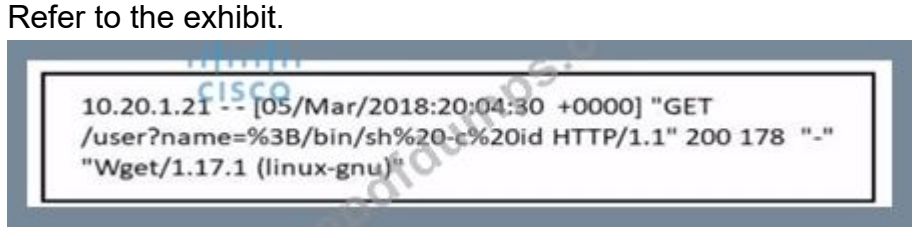
C. It captures the TCP flags set within each packet for the engineer to focus on suspicious packets to identify malicious activity

D. It collects metadata for the engineer to analyze, including IP traffic packet data that is sorted, parsed, and indexed.

Answer: (SHOW ANSWER)

NEW QUESTION: 110

Refer to the exhibit.



Which attack is being attempted against a web application?

A. SQL injection

B. man-in-the-middle

C. command injection

D. denial of service

Answer: C (LEAVE A REPLY)
The exhibit shows an HTTP GET request with a parameter that includes ; /bin/sh -c id.
This indicates a command injection attempt, where the attacker is trying to execute shell commands on the server.
Command injection vulnerabilities allow an attacker to execute arbitrary commands on the host operating system via a vulnerable application.
The use of /bin/sh and the -c flag is typical in command injection exploits to run shell commands, such as id, which returns user identity information.
Reference:
OWASP Command Injection
Analyzing HTTP Requests for Injection Attacks
Web Application Security Testing Guidelines

NEW QUESTION: 111
Which regex matches only on all lowercase letters?
A. [a-z]+
B. [^a-z]+
C. a-z+
D. a*z+
Answer: (SHOW ANSWER)
The regex [a-z]+ matches one or more lowercase letters from a to z. The plus sign (+) indicates that the preceding character set [a-z] can appear one or more times, thus matching strings of only lowercase letters1.

NEW QUESTION: 112
An engineer must configure network systems to detect command-and-control communications by decrypting ingress and egress perimeter traffic and allowing network security devices to detect malicious outbound communications. Which technology must be used to accomplish this task?
A. digital certificates
B. signatures
C. cipher suite
D. static IP addresses
Answer: (SHOW ANSWER)

NEW QUESTION: 113
Refer to the exhibit.

What is occurring?

A. ARP flood

B. DNS amplification

C. ARP poisoning

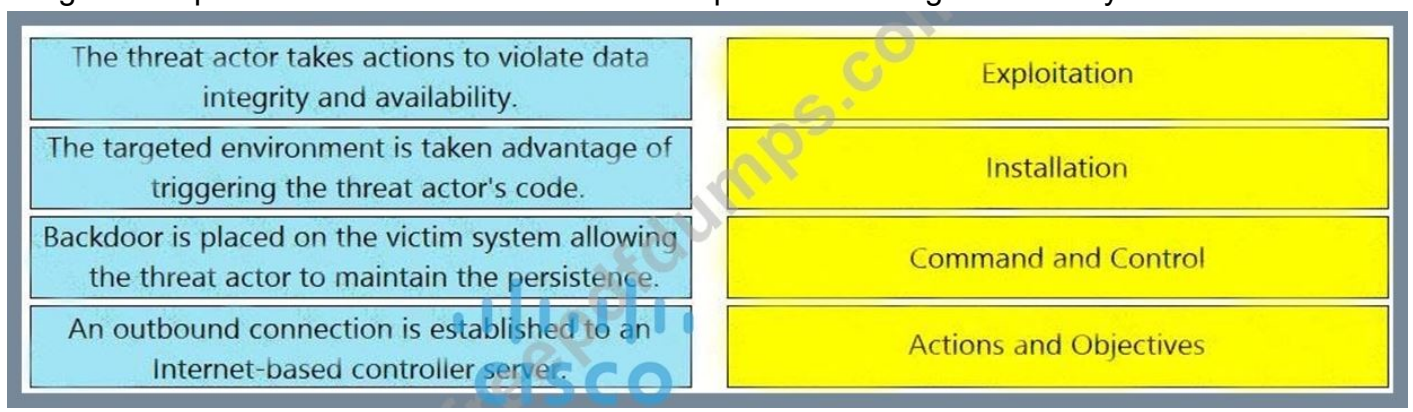
D. DNS tunneling

Answer: B (LEAVE A REPLY)

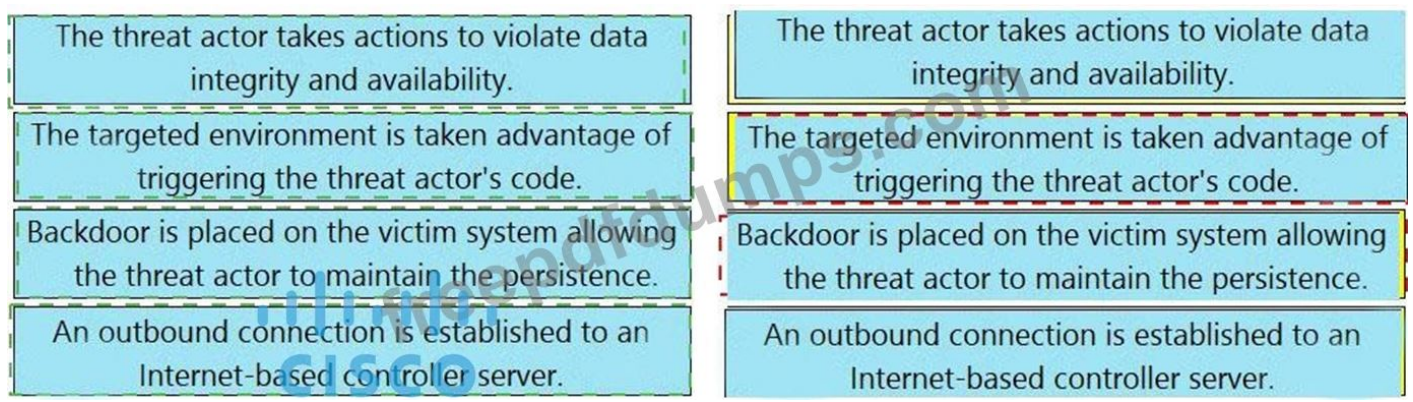
DNS amplification is a type of Distributed Denial of Service (DDoS) attack where an attacker uses publicly accessible open DNS servers to flood a target with DNS response traffic. The goal is to overwhelm the target with traffic, causing a denial of service.

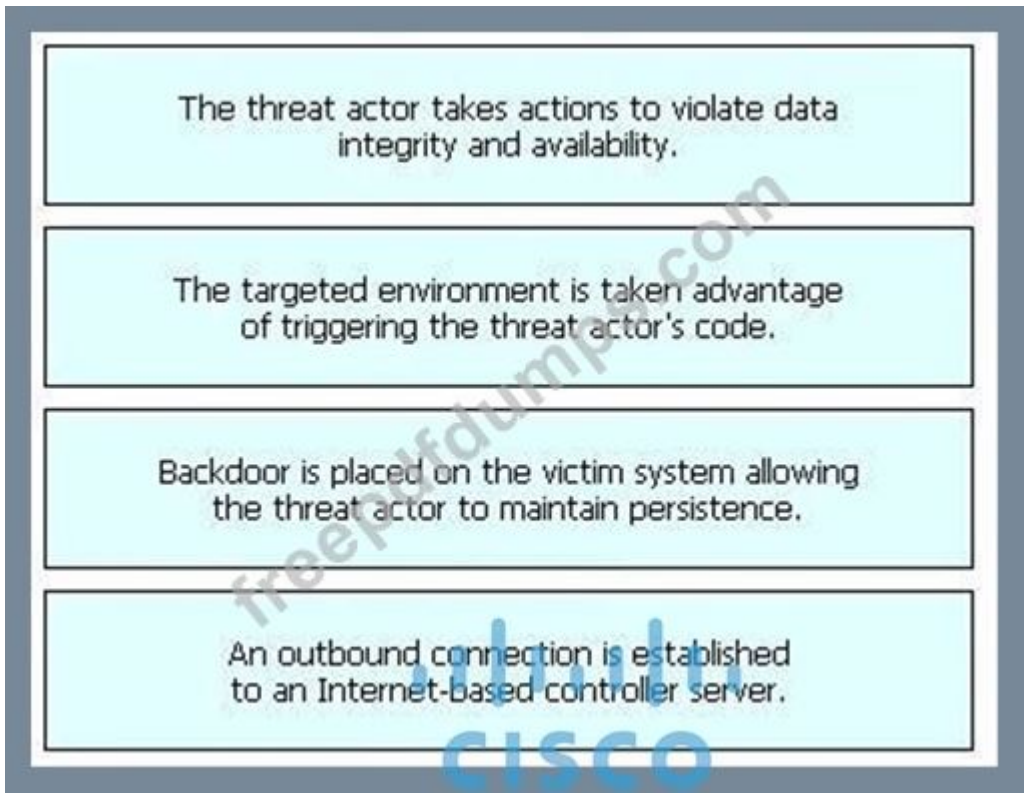
NEW QUESTION: 114

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.



Answer:





NEW QUESTION: 115
Refer to the exhibit.
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: C (LEAVE A REPLY)
The packet capture shows that IP address 192.168.88.149, using source port 80 (common for HTTP traffic), initiated communication with IP address 192.168.88.12 at destination port 49098, using the TCP protocol, indicating a typical client-server interaction over the web.

NEW QUESTION: 116
Which action should be taken if the system is overwhelmed with alerts when false positives and false negatives are compared?
A. Design criteria for reviewing alerts.
B. Adjust the alerts schedule.
C. Modify the settings of the intrusion detection system.
D. Redefine signature rules.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 117
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/auth.log

B. /var/log/authorization.log

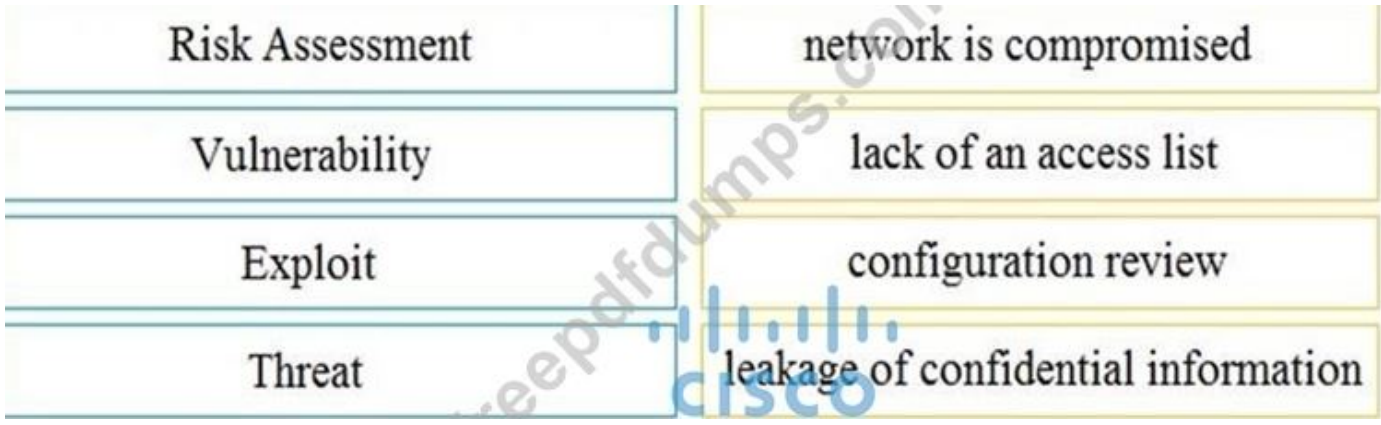
C. /var/log/dmesg

D. var/log/var.log

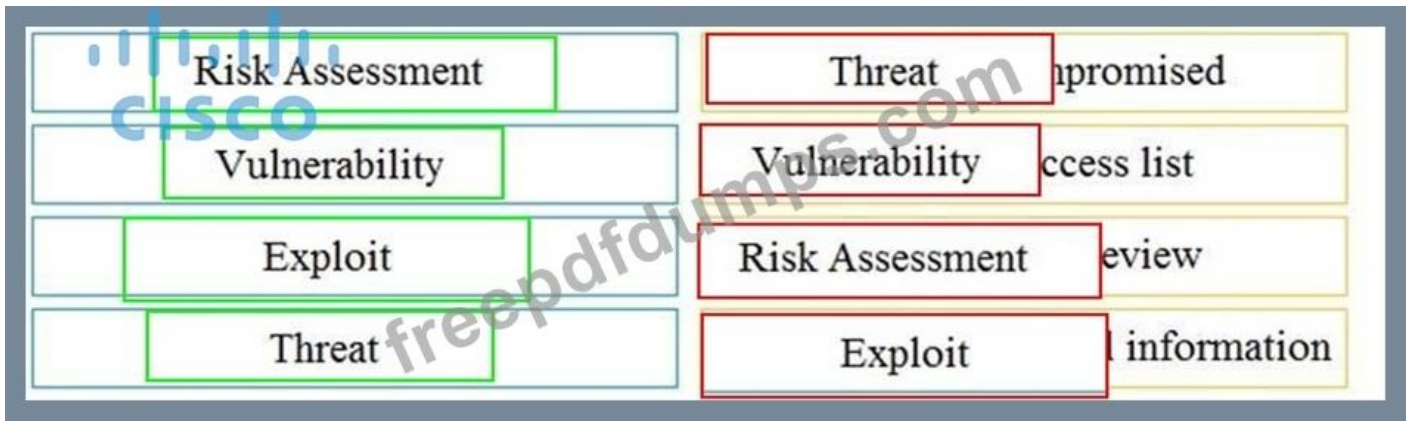
Answer: A (LEAVE A REPLY)

NEW QUESTION: 118

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



Answer:



NEW QUESTION: 119

A company receptionist received a threatening call referencing stealing assets and did not take any action assuming it was a social engineering attempt. Within 48 hours, multiple assets were breached, affecting the confidentiality of sensitive information. What is the threat actor in this incident?

A. company assets that are threatened

B. customer assets that are threatened

C. perpetrators of the attack

D. victims of the attack
Answer: C (LEAVE A REPLY)
In this scenario, the threat actor refers to the individuals or entities responsible for the attack that resulted in a breach of assets and sensitive information. The receptionist received a threatening call but did not take action, leading to an actual breach within 48 hours. Reference: The explanation is inferred from general cybersecurity knowledge as specific details are not provided in the Cisco Cybersecurity documents linked.

NEW QUESTION: 120
What is the difference between inline traffic interrogation (TAPS) and traffic mirroring (SPAN)?
A. SPAN results in more efficient traffic analysis, and TAPS is considerably slower due to latency caused by mirroring.
B. TAPS replicates the traffic to preserve integrity, and SPAN modifies packets before sending them to other analysis tools
C. TAPS interrogation is more complex because traffic mirroring applies additional tags to data and SPAN does not alter integrity and provides full duplex network.
D. SPAN ports filter out physical layer errors, making some types of analyses more difficult, and TAPS receives all packets, including physical errors.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 121
Which data type is necessary to get information about source/destination ports?
A. statistical data
B. session data
C. connectivity data
D. alert data
Answer: B (LEAVE A REPLY)
Explanation
Session data provides information about the five tuples; source IP address/port number, destination IP address/port number and the protocol
What is Connectivity Data? According to IBM - Connectivity data defines how entities are connected in the network. It includes connections between different devices, and VLAN-related connections within the same device https://www.ibm.com/docs/en/networkmanager/4.2.0?topic=relationships-connectivity-data

NEW QUESTION: 122
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

A suspicious IP address is tagged by Threat Intelligence as a brute-force attempt source After the attacker produces many of failed login entries, it successfully compromises the account. Which stakeholder is responsible for the incident response detection step?

A. employee 5

B. employee 3

C. employee 4

D. employee 2

Answer: C (LEAVE A REPLY)

In the context of incident response, the detection step involves identifying potential security incidents. The Security Operation Center (SOC) Analyst, which in this case is Employee 4, is typically responsible for monitoring and analyzing security alerts to detect suspicious activities such as brute-force attempts. Therefore, Employee 4 would be the stakeholder responsible for the incident response detection step.
References: The role of a SOC Analyst in incident response is outlined in cybersecurity frameworks and best practices, which describe the responsibilities of various stakeholders in detecting and responding to security incidents.

NEW QUESTION: 123

An employee received an email from a colleague's address asking for the password for the domain controller.
The employee noticed a missing letter within the sender's address. What does this incident describe?

A. brute-force attack

B. insider attack

C. shoulder surfing

D. social engineering

Answer: (SHOW ANSWER)

Social engineering is a tactic used by attackers to manipulate individuals into divulging confidential information, such as passwords. In this scenario, the attacker is impersonating a colleague by using a similar email address with a missing letter, attempting to trick the employee into revealing sensitive information.
References: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course and materials provide insights into various types of cybersecurity threats, including social engineering, and how to recognize and respond to them.

NEW QUESTION: 124

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 (LEAVE A REPLY)

NEW QUESTION: 125

What is the practice of giving an employee access to only the resources needed to accomplish their job?

A. principle of least privilege

B. organizational separation

C. separation of duties

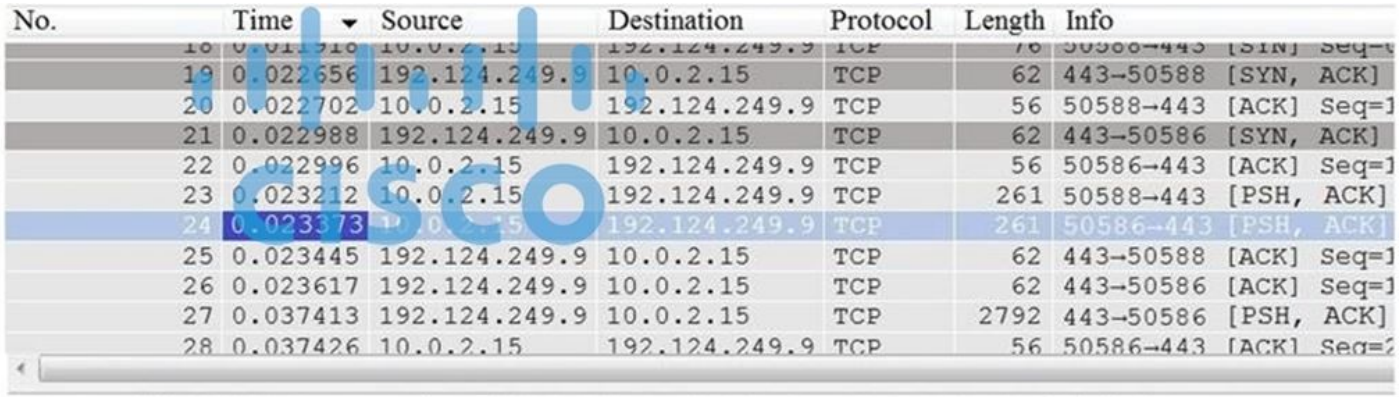
D. need to know principle

Answer: (SHOW ANSWER)

Section: Security Concepts

NEW QUESTION: 126

Refer to the exhibit.



No.	Time	Source	Destination	Protocol	Length	Info
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 (192.124.2
> Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, A
v 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 bf  .......x .vv.:.n..
0050  e6 b8 b8 b2 ba 08 d6 6d  0d 38 fb 91 45 de fc ee  .......m  .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  pdy/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. HTTP

B. SSH

C. TCP

D. TLS

Answer: (SHOW ANSWER)

NEW QUESTION: 127

What is a difference between tampered and untampered disk images?

A. Untampered images are deliberately altered to preserve as evidence.

B. Tampered images have the same stored and computed hash.

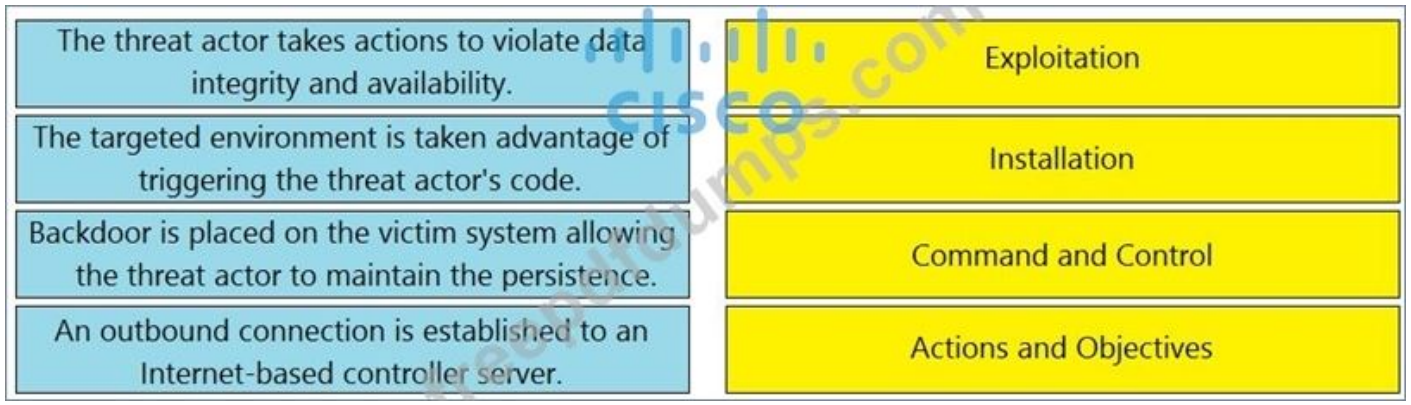
C. Untampered images are used for forensic investigations.

D. Tampered images are used as evidence.

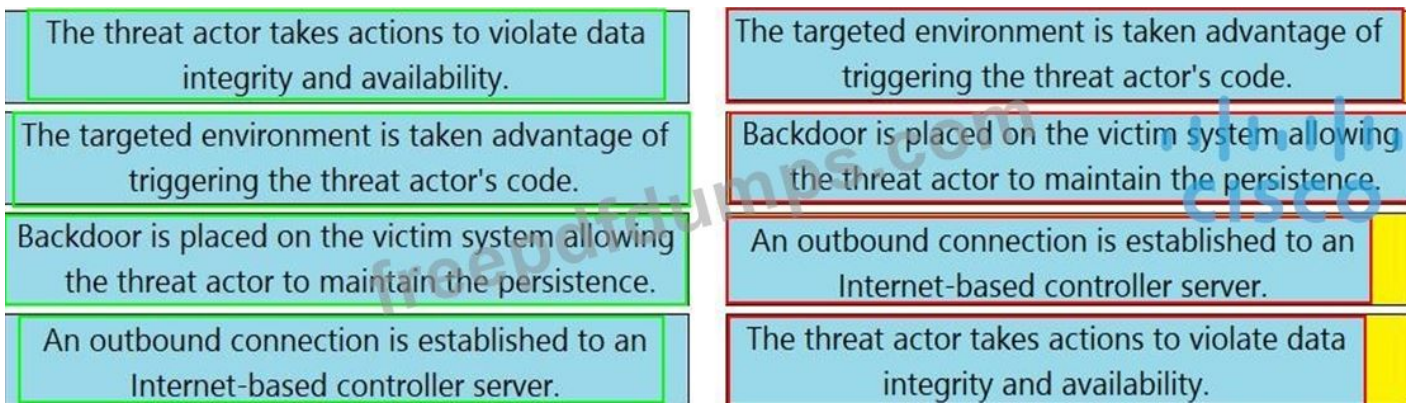
Answer: D (LEAVE A REPLY)

NEW QUESTION: 128

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.



Answer:



NEW QUESTION: 129

What is a difference between tampered and untampered disk images?

A. Tampered images have the same stored and computed hash.

B. Tampered images are used as evidence.

C. Untampered images are used for forensic investigations.

D. Untampered images are deliberately altered to preserve as evidence

Answer: C (LEAVE A REPLY)

Tampered images are disk images that have been modified or altered in some way after they were captured from the original source. Tampered images may have different stored and computed hash values, which indicate that the integrity of the image has been compromised. Tampered images are not reliable or valid sources of evidence for forensic investigations, as they may contain false or misleading information.

Untampered images are disk images that have not been changed or manipulated after they were acquired from the original source. Untampered images have the same stored and computed hash values, which verify that the image is an exact copy of the original disk. Untampered images are used for forensic investigations, as they preserve the original state and content of the disk and provide accurate and trustworthy evidence. References:

* Contrasting tampered and untampered disk images
* What is a difference between tampered and untampered disk images?

NEW QUESTION: 130

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: B (LEAVE A REPLY)

The lack of data visibility needed to detect the attack is caused by the threat actor gaining access to the system by known credentials. This means that the threat actor either obtained the employee's username and password through phishing, social engineering, or other means, or used a compromised account that had legitimate access to the system. This would explain why there were no suspicious logs, alerts, or failed login attempts, as the threat actor appeared to be a normal user. Reference: https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fundamentals-cbrops-v1-0/CSCU-LP-CBROPS-V1-028093.html (Module 2, Lesson 2.1.2)

NEW QUESTION: 131

Which type of evidence supports a theory or an assumption that results from initial evidence?

A. probabilistic

B. indirect

C. corroborative

D. best

Answer: (SHOW ANSWER)

NEW QUESTION: 132

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

A. legal

B. compliance

C. regulated

D. contractual

Answer: (SHOW ANSWER)

Section: Security Policies and Procedures

NEW QUESTION: 133

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. piggybacking

B. tailgating

C. eavesdropping

D. social engineering

Answer: D (LEAVE A REPLY)

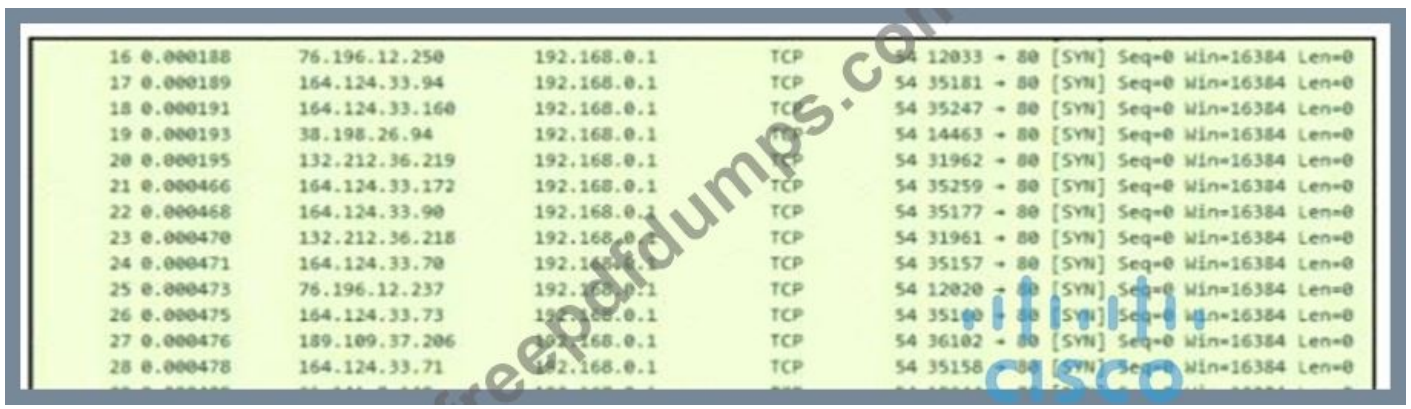
NEW QUESTION: 134
A security engineer notices confidential data being exfiltrated to a domain "Ranso4134-mware31-895" address that is attributed to a known advanced persistent threat group The engineer discovers that the activity is part of a real attack and not a network misconfiguration. Which category does this event fall under as defined in the Cyber Kill Chain?
A. reconnaissance
B. delivery
C. action on objectives
D. weaponization
Answer: C (LEAVE A REPLY)
The event described falls under the 'action on objectives' category of the Cyber Kill Chain. This stage occurs after the attacker has established a foothold within the network and begins to execute their intended actions, such as data exfiltration. Reference:: The Cyber Kill Chain framework outlines the stages of a cyberattack, with 'action on objectives' being the final step where attackers achieve their primary goal, such as data theft

NEW QUESTION: 135
At which layer is deep packet inspection investigated on a firewall?
A. internet
B. transport
C. application
D. data link
Answer: C (LEAVE A REPLY)
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: 136
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 (LEAVE A REPLY)
Defense-in-depth is a security strategy where multiple layers of defense are placed throughout an information technology (IT) system. It addresses physical, technical, and administrative controls to provide redundancy and ensure that if one layer fails, others will be in place to thwart an attack. Reference: Cisco Tech Roles - CyberOps Engineer

NEW QUESTION: 137

Refer to the exhibit.



16 0.000188	76.196.12.250	192.168.0.1	TCP	54 12033 → 80 [SYN] Seq=0 Win=16384 Len=0
17 0.000189	164.124.33.94	192.168.0.1	TCP	54 35181 → 80 [SYN] Seq=0 Win=16384 Len=0
18 0.000191	164.124.33.160	192.168.0.1	TCP	54 35247 → 80 [SYN] Seq=0 Win=16384 Len=0
19 0.000193	38.198.26.94	192.168.0.1	TCP	54 14463 → 80 [SYN] Seq=0 Win=16384 Len=0
20 0.000195	132.212.36.219	192.168.0.1	TCP	54 31962 → 80 [SYN] Seq=0 Win=16384 Len=0
21 0.000466	164.124.33.172	192.168.0.1	TCP	54 35259 → 80 [SYN] Seq=0 Win=16384 Len=0
22 0.000468	164.124.33.90	192.168.0.1	TCP	54 35177 → 80 [SYN] Seq=0 Win=16384 Len=0
23 0.000470	132.212.36.218	192.168.0.1	TCP	54 31961 → 80 [SYN] Seq=0 Win=16384 Len=0
24 0.000471	164.124.33.70	192.168.0.1	TCP	54 35157 → 80 [SYN] Seq=0 Win=16384 Len=0
25 0.000473	76.196.12.237	192.168.0.1	TCP	54 12020 → 80 [SYN] Seq=0 Win=16384 Len=0
26 0.000475	164.124.33.73	192.168.0.1	TCP	54 35180 → 80 [SYN] Seq=0 Win=16384 Len=0
27 0.000476	189.109.37.206	192.168.0.1	TCP	54 36102 → 80 [SYN] Seq=0 Win=16384 Len=0
28 0.000478	164.124.33.71	192.168.0.1	TCP	54 35158 → 80 [SYN] Seq=0 Win=16384 Len=0

Which application-level protocol is being targeted?

A. TCP

B. HTTP

C. HTTPS

D. FTP

Answer: B (LEAVE A REPLY)

NEW QUESTION: 138

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

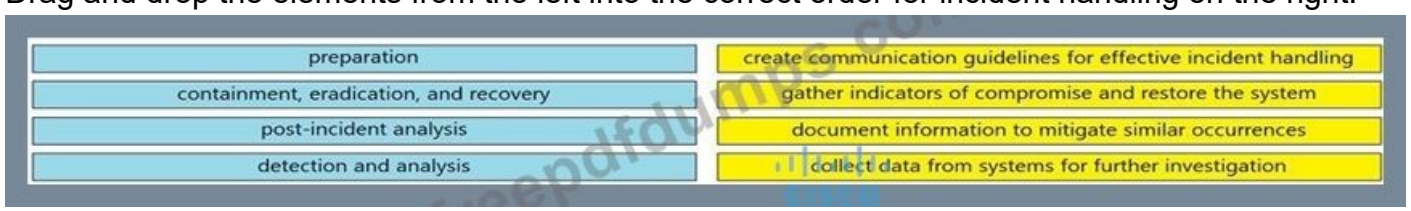
Answer: A (LEAVE A REPLY)

Explanation

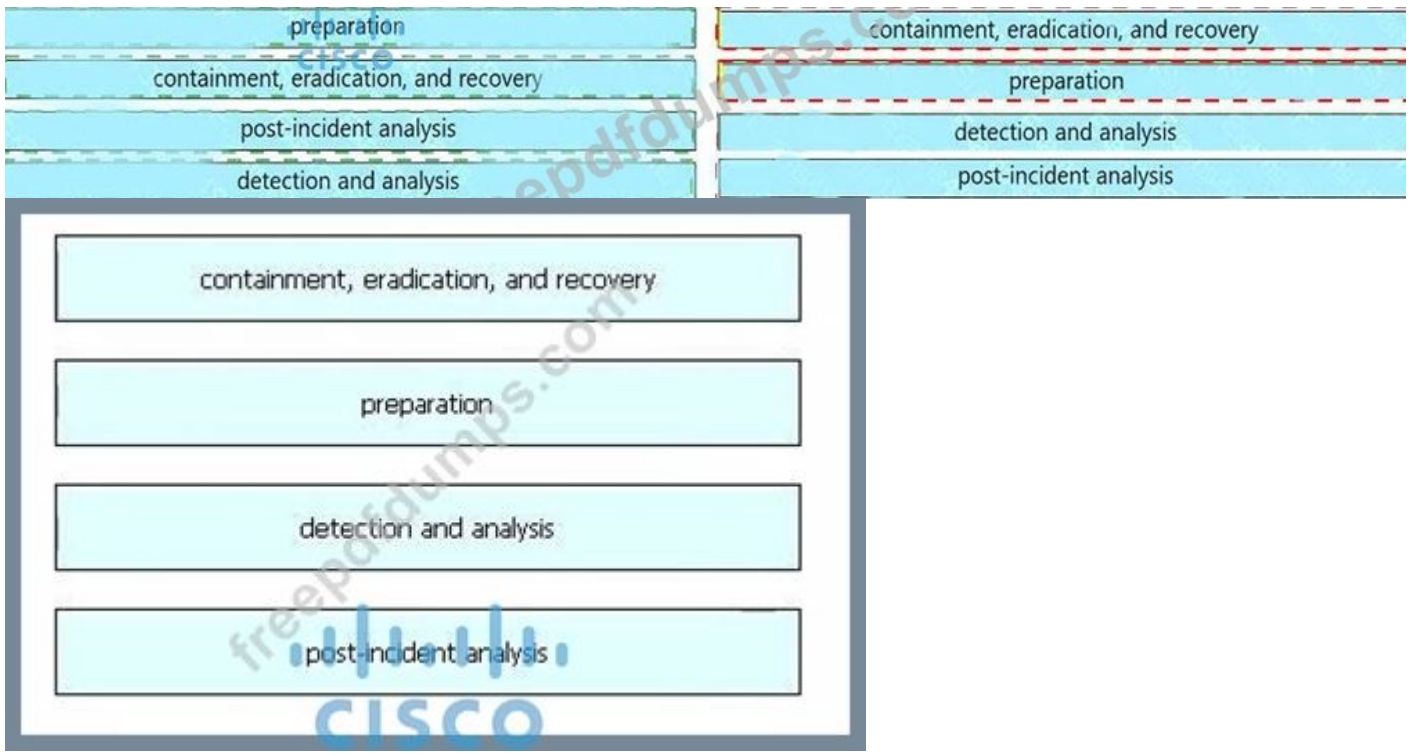
HIDS is capable of monitoring the internals of a computing system as well as the network packets on its network interfaces. Host-based firewall is a piece of software running on a single Host that can restrict incoming and outgoing Network activity for that host only.

NEW QUESTION: 139

Drag and drop the elements from the left into the correct order for incident handling on the right.



Answer:



NEW QUESTION: 140
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 (LEAVE A REPLY)

NEW QUESTION: 141
What is the dataflow set in the NetFlow flow-record format?
A. Dataflow set is a collection of HEX records.
B. Dataflow set provides basic information about the packet such as the NetFlow version
C. Dataflow set is a collection of binary patterns
D. Dataflow set is a collection of data records.
Answer: (SHOW ANSWER)
In the NetFlow flow-record format, a dataflow set is a collection of data records that follow the template FlowSet in an export packet. Each data record corresponds to a flow and contains values for the fields defined in the template FlowSet. This allows for efficient organization and retrieval of flow information by NetFlow collectors.
References:
* Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)
* NetFlow Version 9 Flow-Record Format Documentation

NEW QUESTION: 142

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 (LEAVE A REPLY)

Defense-in-depth is a security strategy where multiple layers of defense are placed throughout an information technology (IT) system. It addresses physical, technical, and administrative controls to provide redundancy and ensure that if one layer fails, others will be in place to thwart an attack. References: Cisco Tech Roles - CyberOps Engineer

NEW QUESTION: 143

Refer to the exhibit.

```
root@:~# cat access-logs/access_130603.txt | grep '192.168.1.91' | cut -d "\"" -f 2 |
uniq -c
    1 GET /portal.php?mode=addevent&date=2018-05-01 HTTP/1.1
    1 GET /blog/?attachment_id=2910 HTTP/1.1
    1 GET /blog/?attachment_id=2998&feed=rss2 HTTP/1.1
    1 GET /blog/?attachment_id=3156 HTTP/1.1
```

What is depicted in the exhibit?

A. UNIX-based syslog

B. Apache logs

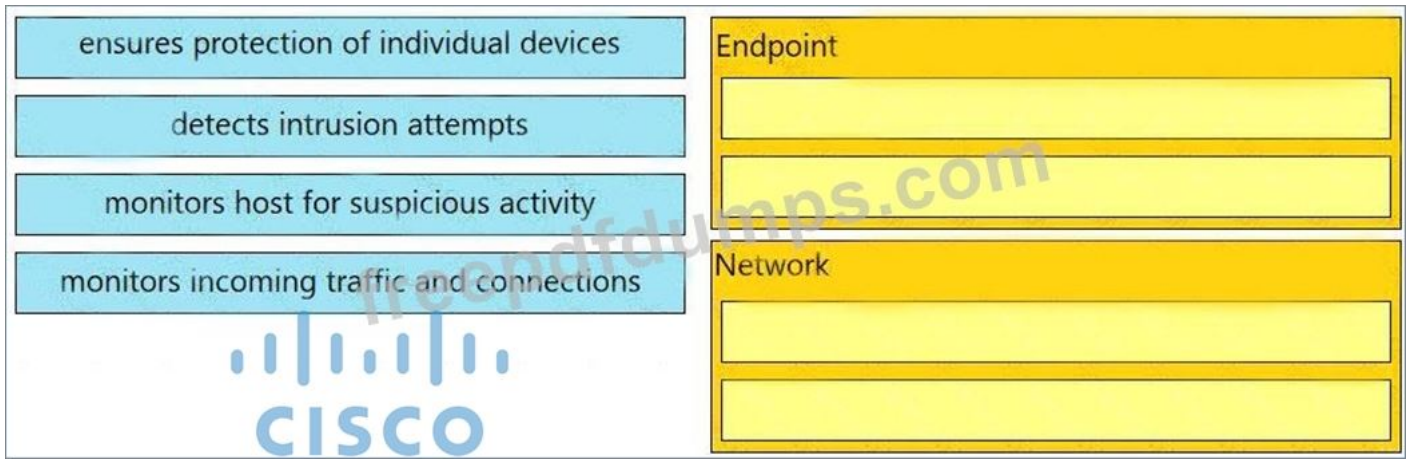
C. IIS logs

D. Windows Event logs

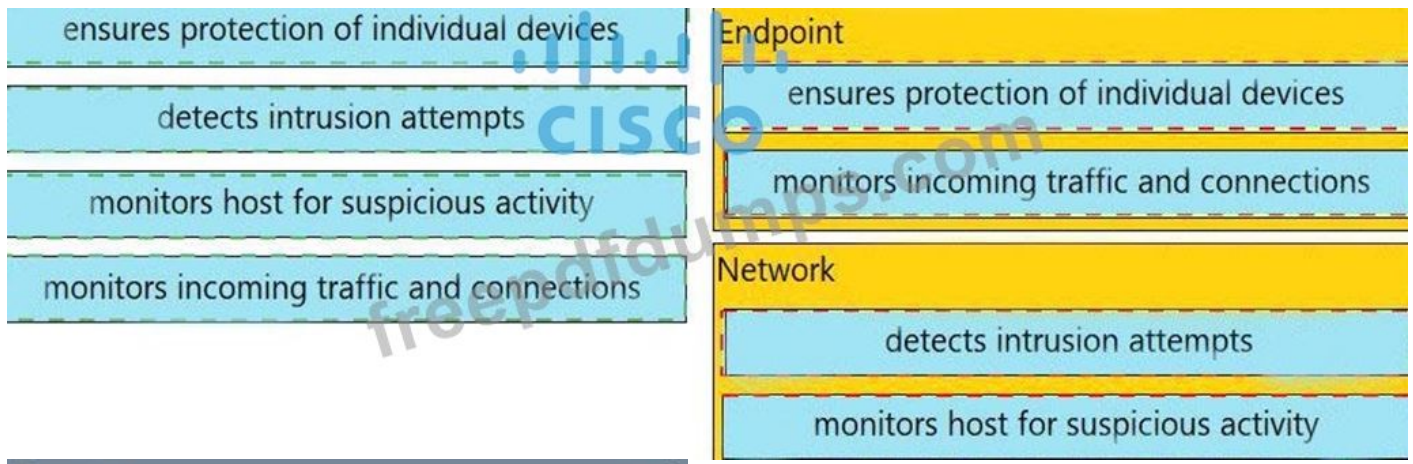
Answer: (SHOW ANSWER)

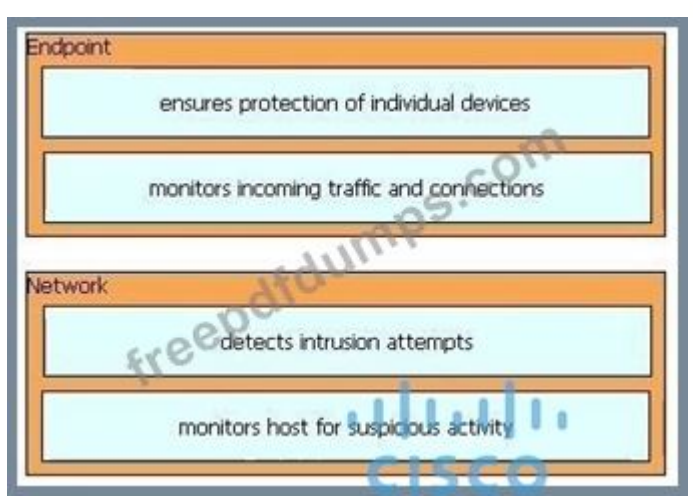
NEW QUESTION: 144

Drag and drop the uses on the left onto the type of security system on the right.



Answer:

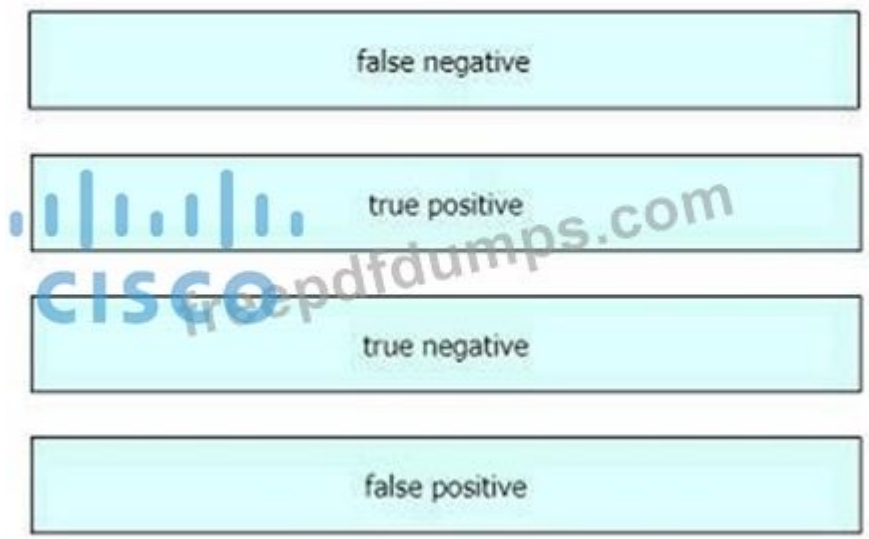




NEW QUESTION: 145
A threat actor penetrated an organization's network. Using the 5-tuple approach, which data points should the analyst use to isolate the compromised host in a grouped set of logs?
A. protocol, source IP, source port, destination IP, and destination port
B. event name, log source, time, source IP, and username
C. event name, log source, time, source IP, and host name
D. protocol, log source, source IP, destination IP, and host name
Answer: A (LEAVE A REPLY)

NEW QUESTION: 146
Drag and drop the event term from the left onto the description on the right.

Answer:



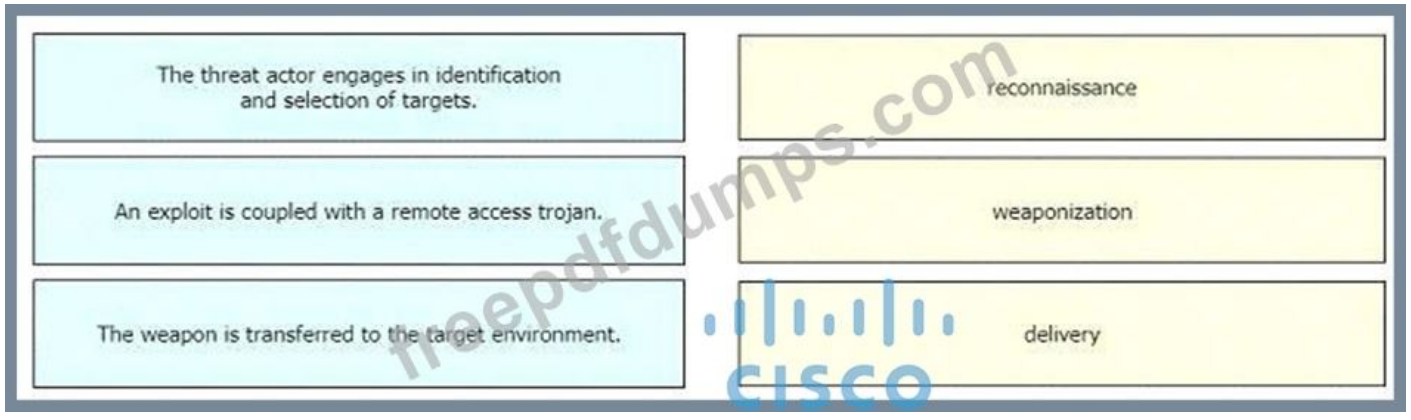
NEW QUESTION: 147
An analyst is investigating an incident in a SOC environment.
Which method is used to identify a session from a group of logs?
A. sequence numbers
B. IP identifier
C. 5-tuple
D. timestamps
Answer: (SHOW ANSWER)
Section: Security Concepts

NEW QUESTION: 148
Which two compliance frameworks require that data be encrypted when it is transmitted over a public network?
(Choose two.)
A. HIPAA
B. SOX
C. COBIT
D. PCI

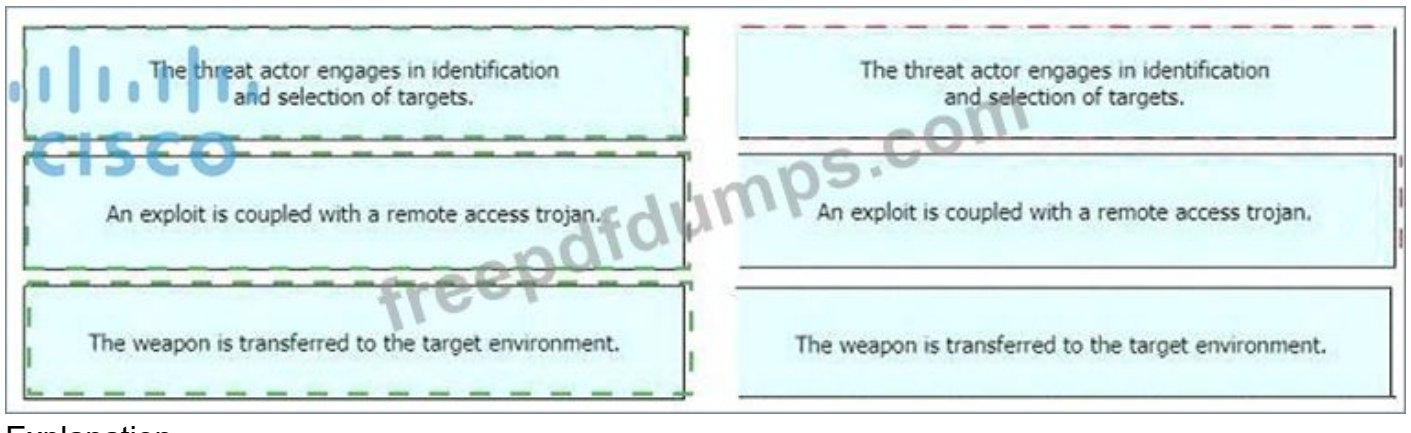
E. GLBA
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 149
A security analyst notices a sudden surge of incoming traffic and detects unknown packets from unknown senders After further investigation, the analyst learns that customers claim that they cannot access company servers According to NIST SP800-61, in which phase of the incident response process is the analyst?
A. post-incident activity
B. detection and analysis
C. preparation
D. containment, eradication, and recovery
Answer: B (LEAVE A REPLY)
The analyst is in the detection and analysis phase of the incident response process according to NIST SP800-61. In this phase, events are detected and analyzed to determine whether they constitute incidents that require a response. It involves monitoring security events or data collection, correlation, and analysis of log entries and network flow data, among others. The goal is to identify incidents quickly so that appropriate actions can be taken. References := NIST SP800-61, Computer Security Incident Handling Guide, Section 3.2: Detection and Analysis

NEW QUESTION: 150
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.



Answer:



Explanation
Delivery: This step involves transmitting the weapon to the target.

Weaponization: In this step, the intruder creates a malware weapon like a virus, worm or such in order to exploit the vulnerabilities of the target. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as the zero-day exploits) or it can focus on a combination of different vulnerabilities.
Reconnaissance: In this step, the attacker / intruder chooses their target. Then they conduct an in-depth research on this target to identify its vulnerabilities that can be exploited.

NEW QUESTION: 151
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: (SHOW ANSWER)
Section: Security Monitoring

NEW QUESTION: 152
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: (SHOW ANSWER)
Section: Security Policies and Procedures

NEW QUESTION: 153
Refer to the exhibit. Where is the executable file?
A. info
B. tags
C. MIME
D. name
Answer: D (LEAVE A REPLY)
The executable file is identified in the "name" section of the exhibit, which lists the file name "VAC-Bypass-Loader.exe". This indicates that the file is an executable, as denoted by the ".exe" extension commonly associated with executable files in Windows operating systems.

NEW QUESTION: 154
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 tile size is exceeded. Which action resolves the issue?
A. Add space to the existing partition and lower the retention penod.
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: B (LEAVE A REPLY)
FAT is a file system that organizes and stores data on a disk. However, FAT has a limitation of 4 GB for the maximum file size, which means that any file larger than that will be corrupted. To resolve this issue, the engineer can use FAT32, which is an improved version of FAT that supports files up to 32 GB. Alternatively, the engineer can use other file systems that have higher file size limits, such as Ext4 or NTFS.
Reference:= Cisco Cybersecurity Operations Fundamentals, Module 5: Security Policies and Procedures, Lesson 5.1: Data Retention, Topic 5.1.1: Data Retention Policies and Procedures

NEW QUESTION: 155
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: (SHOW ANSWER)
Host-based antivirus protection is also known as agent-based. Agent-based antivirus runs on every protected machine. Agentless antivirus protection performs scans on hosts from a centralized system. Agentless systems have become popular for virtualized environments in which multiple OS instances are running on a host simultaneously. Agent-based antivirus running in each virtualized system can be a serious drain on system resources. Agentless antivirus for virtual hosts involves the use of a special security virtual appliance that performs optimized scanning tasks on the virtual hosts. An example of this is VMware's vShield.

NEW QUESTION: 156
What is a benefit of agent-based protection when compared to agentless protection?
A. It provides a centralized platform
B. It manages numerous devices simultaneously
C. It lowers maintenance costs
D. It collects and detects all traffic locally
Answer: (SHOW ANSWER)

NEW QUESTION: 157
According to the NIST SP 800-86. which two types of data are considered volatile? (Choose two.)
A. free space
B. login sessions
C. dump files

D. temporary files
E. swap files
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 158
What is the difference between the ACK flag and the RST flag?
A. The RST flag approves the connection, and the ACK flag terminates spontaneous connections.
B. The ACK flag confirms the received segment, and the RST flag terminates the connection.
C. The RST flag approves the connection, and the ACK flag indicates that a packet needs to be resent
D. The ACK flag marks the connection as reliable, and the RST flag indicates the failure within TCP Handshake
Answer: (SHOW ANSWER)
In TCP/IP networking, the ACK flag is used to acknowledge the receipt of a packet. It's a way to confirm that the previous packets have been received and that the connection is proceeding as expected. The RST flag, on the other hand, is used to reset the connection. It is sent if a segment arrives which is not intended for the current connection, or if a connection request is to be denied. Essentially, the ACK flag is about maintaining the established connection, while the RST flag is about aborting connections that are not valid or are no longer needed123.

NEW QUESTION: 159
Which action matches the weaponization step of the Cyber Kill Chain Model?
A. Develop a specific malware to exploit a vulnerable server, i
B. Match a known script to a vulnerability.
C. Construct a trojan and deliver I! to the victim.
D. Scan open services and ports on a server.
Answer: (SHOW ANSWER)
The weaponization step in the Cyber Kill Chain Model involves the creation or use of a specific weapon (malware, exploit) designed to leverage a vulnerability.
This phase follows the reconnaissance phase where the attacker gathers information and precedes the delivery phase where the weapon is delivered to the target.
Developing specific malware to exploit a vulnerable server is a precise example of weaponization.
Reference:
Lockheed Martin Cyber Kill Chain Model
Understanding the Weaponization Phase in Cyber Attacks
Steps in the Cyber Kill Chain

NEW QUESTION: 160
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: (SHOW ANSWER)

Encryption allows the user to make the data incomprehensible without a specific key, certificate, or password.
Encryption is a method of transforming data into a format that only authorized parties can access. Encryption can be used to protect data in transit or at rest from unauthorized access or modification. References:
https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fund (Module 4, Lesson 4.1.1)

NEW QUESTION: 161
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: (SHOW ANSWER)
Data integrity verification involves using tools to compute the message digest of data. A message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula. This digest, which serves as a unique identifier, can be used to verify the integrity of copied data by comparing it to the original data's digest. If the digests match, it means the data has not been altered, ensuring its integrity.
References: The concept of data integrity and the use of message digests are fundamental security concepts taught in the Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course. This course covers the essential skills and knowledge needed to monitor alerts and breaches, and to understand and follow established procedures for response to alerts converted to incidents

NEW QUESTION: 162
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: (SHOW ANSWER)
SIEM (Security Information and Event Management) systems are solutions that provide real-time analysis of security alerts generated by applications and network hardware. They collect, store, analyze, and report on log data for incident response, forensics, and regulatory compliance. On the other hand, SOAR (Security Orchestration Automation and Response) platforms allow organizations to collect data about security threats from multiple sources and respond to low-level security events without human assistance. References: Cisco Cybersecurity Operations Fundamentals

NEW QUESTION: 163
A user received a malicious attachment but did not run it.
Which category classifies the intrusion?
A. reconnaissance
B. weaponization
C. installation
D. delivery

Answer: D (LEAVE A REPLY)

NEW QUESTION: 164
Which technology should be used to implement a solution that makes routing decisions based on HTTP header, uniform resource identifier, and SSL session ID attributes?
A. AWS
B. IIS
C. Load balancer
D. Proxy server
Answer: C (LEAVE A REPLY)
Load Balancing: HTTP(S) load balancing is one of the oldest forms of load balancing. This form of load balancing relies on layer 7, which means it operates in the application layer. This allows routing decisions based on attributes like HTTP header, uniform resource identifier, SSL session ID, and HTML form data.
Load balancing applies to layers 4-7 in the seven-layer Open System Interconnection (OSI) model. Its capabilities are: L4. Directing traffic based on network data and transport layer protocols, e.g., IP address and TCP port. L7. Adds content switching to load balancing, allowing routing decisions depending on characteristics such as HTTP header, uniform resource identifier, SSL session ID, and HTML form data.
GSLB. Global Server Load Balancing expands L4 and L7 capabilities to servers in different sites

NEW QUESTION: 165
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 (LEAVE A REPLY)
Section: Security Monitoring

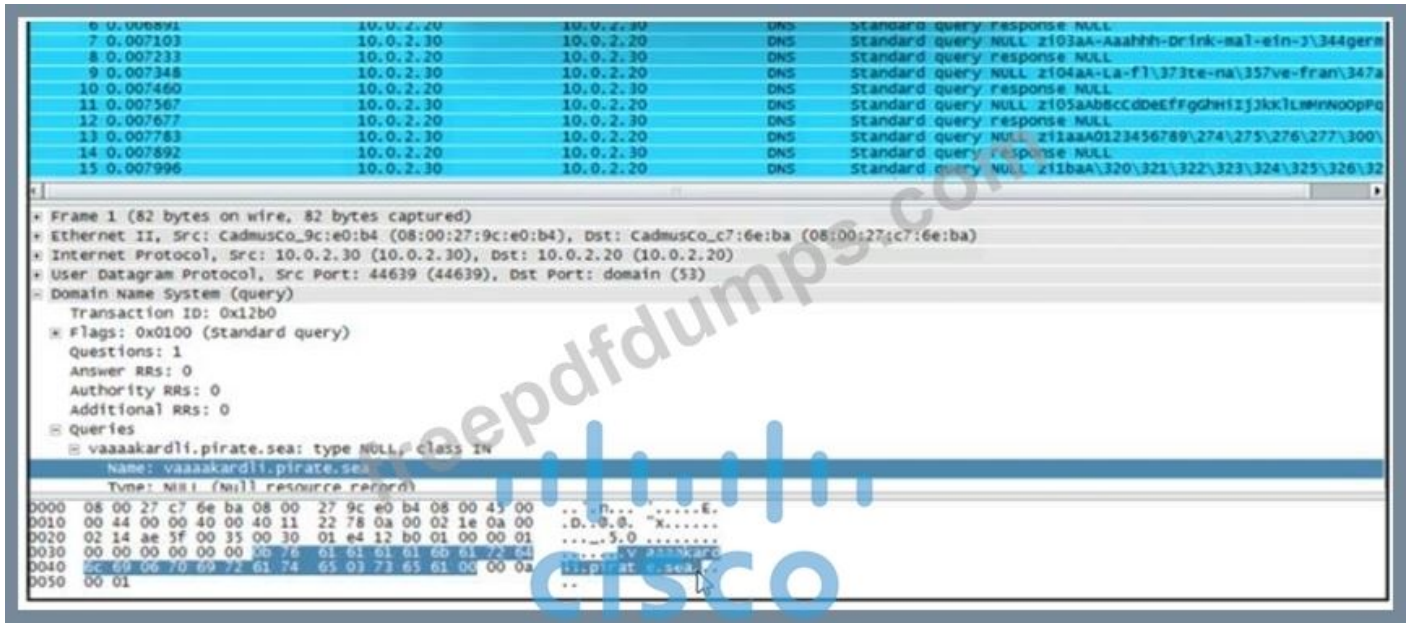
NEW QUESTION: 166
Which step in the incident response process researches an attacking host through logs in a SIEM?
A. detection and analysis
B. preparation
C. eradication
D. containment
Answer: A (LEAVE A REPLY)
Preparation --> Detection and Analysis --> Containment, Erradicaion and Recovery --> Post-Incident Activity Detection and Analysis --> Profile networks and systems, Understand normal behaviors, Create a log retention policy, Perform event correlation. Maintain and use a knowledge base of information.Use Internet search engines for research. Run packet sniffers to collect additional data. Filter the data. Seek assistance from others.

Keep all host clocks synchronized. Know the different types of attacks and attack vectors. Develop processes and procedures to recognize the signs of an incident. Understand the sources of precursors and indicators.
Create appropriate incident documentation capabilities and processes. Create processes to effectively prioritize security incidents. Create processes to effectively communicate incident information (internal and external communications).
Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

NEW QUESTION: 167
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: A (LEAVE A REPLY)
CDFS stands for Compact Disc File System, which is a file system used by Mac OS to store data on CDs.
CDFS is also known as ISO 9660, which is a standard format for data interchange on optical discs. CDFS allows files to be accessed by different operating systems, such as Windows, Linux, and Mac OS. Therefore, an ISO file that is stored in CDFS format is data from a CD copied using Mac-based system. References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 4: Network Intrusion Analysis, Lesson 4.4: File Type Analysis, Topic 4.4.1: File Systems, page 4-40.

NEW QUESTION: 168
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: (SHOW ANSWER)
After a breach has been discovered and the immediate threat has been addressed by identifying and removing the threat's access, the next step according to the NIST SP 800-61 Incident Handling Guide is to recover from the threat. This involves restoring systems to normal operation, confirming that the systems are functioning normally, and applying patches or other remediation measures to prevent similar breaches in the future1.
Reference:
Understanding NIST SP 800-61: The Computer Security Incident Handling Guide

NEW QUESTION: 169
Refer to the exhibit.



What is occurring?
A. DNS tunneling
B. ARP poisoning
C. ARP flood
D. DNS amplification
Answer: A (LEAVE A REPLY)

NEW QUESTION: 170
Refer to the exhibit.
An analyst was given a PCAP file, which is associated with a recent intrusion event in the company FTP server Which display filters should the analyst use to filter the FTP traffic?
A. dstport == FTP
B. tcp.port==21
C. tcpport = FTP
D. dstport = 21
Answer: B (LEAVE A REPLY)
The correct display filter for analyzing FTP traffic in a PCAP file is "tcp.port==21". This filter will show all TCP packets where the port number is 21, which is the standard port for FTP control messages.

NEW QUESTION: 171
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

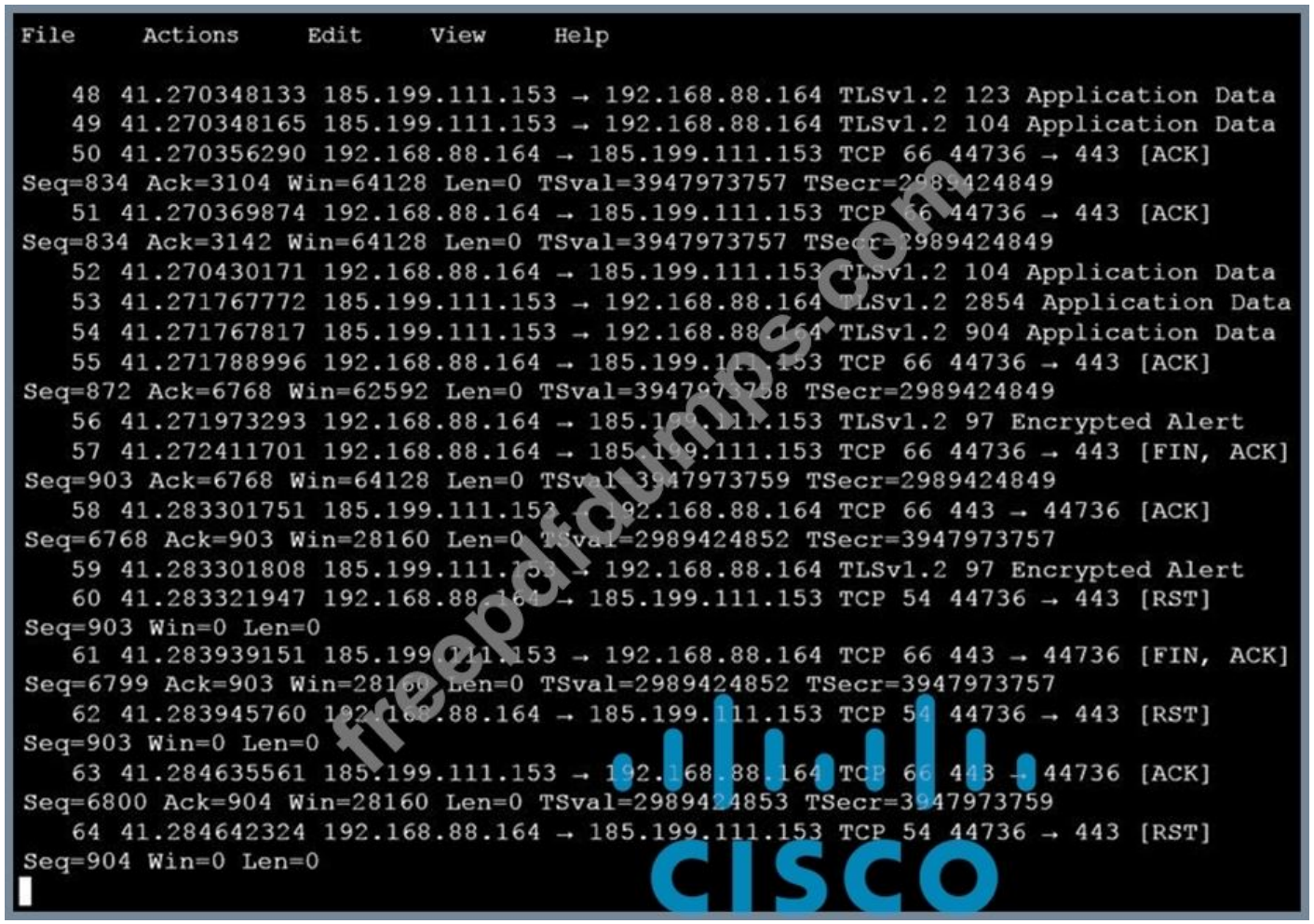
D. instigator
Answer: B (LEAVE A REPLY)
A precursor is a sign that a cyber-attack is about to occur on a system or network. An indicator is the actual alerts that are generated as an attack is happening. Therefore, as a security professional, it's important to know where you can find both precursor and indicator sources of information.
The following are common sources of precursor and indicator information:
* Security Information and Event Management (SIEM)
* Anti-virus and anti-spam software
* File integrity checking applications/software
* Logs from various sources (operating systems, devices, and applications)
* People who report a security incident
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NEW QUESTION: 172
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 insert itself into an application and execute when the application is run.
B. The file will not execute its behavior in a sandbox environment to avoid detection.
C. The file will monitor user activity and send the information to an outside source.
D. The file will appear legitimate by evading signature-based detection.
Answer: (SHOW ANSWER)

NEW QUESTION: 173
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. Email Security Appliance
B. Stealthwatch
C. Web Security Appliance
D. Firepower
Answer: (SHOW ANSWER)

NEW QUESTION: 174
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. transport layer security encryption

C. SHA-256 hashing

D. ROT13 encryption

Answer: B (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 175

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 (LEAVE A REPLY)

User interaction is any event that requires the user to perform an action that enables or facilitates a cyberattack. Opening a malicious file is an example of user interaction, as it can trigger the execution of malicious code or malware that can compromise the system or network. Gaining root access, executing remote code, and reading and writing file permissions are not user interactions, but rather actions that can be

performed by an attacker after exploiting a vulnerability or bypassing security controls. Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, More than 99% of cyberattacks rely on human interaction

NEW QUESTION: 176
Which evasion technique is a function of ransomware?
A. extended sleep calls
B. encryption
C. resource exhaustion
D. encoding
Answer: B (LEAVE A REPLY)
Section: Security Concepts

NEW QUESTION: 177
Refer to the exhibit.

```
root@:~# cat access-logs/access_130603.txt | grep '192.168.1.91' | cut -d "\"" -f 2 |
uniq -c
    1 GET /portal.php?mode=addevent&date=2018-05-01 HTTP/1.1
    1 GET /blog/?attachment_id=2910 HTTP/1.1
    1 GET /blog/?attachment_id=2998&feed=rss2 HTTP/1.1
    1 GET /blog/?attachment_id=3156 HTTP/1.1
```

What is depicted in the exhibit?
A. Windows Event logs
B. Apache logs
C. IIS logs
D. UNIX-based syslog
Answer: (SHOW ANSWER)

NEW QUESTION: 178
Which utility blocks a host portscan?
A. sandboxing
B. antimalware
C. HIDS
D. host-based firewall
Answer: D (LEAVE A REPLY)

NEW QUESTION: 179
Which data type is necessary to get information about source/destination ports?
A. statistical data
B. session data
C. connectivity data

D. alert data

Answer: B (LEAVE A REPLY)

Session data provides information about the five tuples; source IP address/port number, destination IP address/port number and the protocol What is Connectivity Data? According to IBM - Connectivity data defines how entities are connected in the network. It includes connections between different devices, and VLAN-related connections within the same devicehttps://www.ibm.com/docs/en/networkmanager/4.2.0?topic=relationships-connectivity-data

NEW QUESTION: 180

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 (LEAVE A REPLY)

Cyber attribution identifies the threat actors of an attack in an investigation. Threat actors are the individuals, groups, organizations, or states that are responsible for conducting or sponsoring a cyberattack. Threat actors can have different motives, such as financial gain, espionage, sabotage, activism, or warfare. Cyber attribution can help investigators to determine the identity, location, affiliation, and motivation of the threat actors, as well as to hold them accountable and impose sanctions or legal actions. References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 5: Security Policies and Procedures, Lesson
5.2: Incident Response, Topic 5.2.3: Cyber Attribution, page 5-14.

NEW QUESTION: 181

Which two measures are used by the defense-m-depth strategy? (Choose two)

A. Bridge the single connection into multiple.

B. Divide the network into parts

C. Split packets into pieces.

D. Reduce the load on network devices.

E. Implement the patch management process

Answer: (SHOW ANSWER)

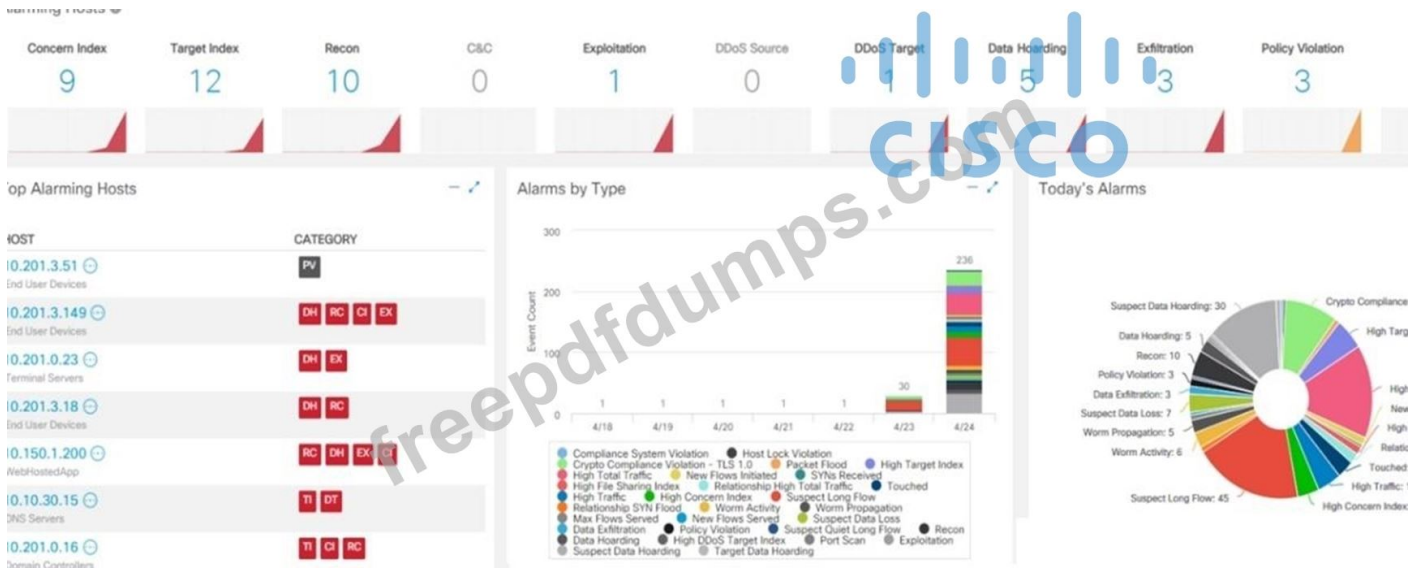
The defense-in-depth strategy is a layered approach to security that includes multiple defensive measures to protect against threats. Dividing the network into parts (B) helps isolate potential breaches, making it harder for an attacker to move laterally across the network. Implementing the patch management process (E) ensures that systems are up-to-date with the latest security patches, reducing vulnerabilities that attackers could exploit.

References: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course

NEW QUESTION: 182
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 (LEAVE A REPLY)
The Cuckoo report indicates that the file has been identified by Yara rules as being capable of detecting a sandbox environment, which is a security mechanism for isolating and analyzing suspicious code. The presence of the "vmdetect" and "anti_dog" Yara rules suggests that the file may have mechanisms to avoid executing its malicious behavior when it detects that it is being analyzed in a sandbox. This is a common evasion technique used by malware to prevent detection and analysis by security researchers or automated systems.
References: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) and other Cisco cybersecurity resources discuss malware analysis and the use of sandbox environments to safely execute and study potential malware. These resources also cover the topic of evasion techniques used by malware to avoid detection.

NEW QUESTION: 183
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 (LEAVE A REPLY)

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: 184

A user received a targeted spear-phishing email and identified it as suspicious before opening the content. To which category of the Cyber Kill Chain model does to this type of event belong?

A. delivery

B. exploitation

C. weaponization

D. reconnaissance

Answer: (SHOW ANSWER)

NEW QUESTION: 185

Refer to the exhibit.

A suspicious IP address is tagged by Threat Intelligence as a brute-force attempt source After the attacker produces many of failed login entries, it successfully compromises the account. Which stakeholder is responsible for the incident response detection step?

A. employee 5

B. employee 3

C. employee 4

D. employee 2

Answer: C (LEAVE A REPLY)

In the context of incident response, the detection step involves identifying potential security incidents. The Security Operation Center (SOC) Analyst, which in this case is Employee 4, is typically responsible for monitoring and analyzing security alerts to detect suspicious activities such as brute-force attempts. Therefore, Employee 4 would be the stakeholder responsible for the incident response detection step.

Reference: The role of a SOC Analyst in incident response is outlined in cybersecurity frameworks and best practices, which describe the responsibilities of various stakeholders in detecting and responding to security incidents.

NEW QUESTION: 186

According to CVSS, what is a description of the attack vector score?

A. It depends on how far away the attacker is located and the vulnerable component

B. It depends on how many physical and logical manipulations are possible on a vulnerable component

C. The metric score will be larger when it is easier to physically touch or manipulate the vulnerable component

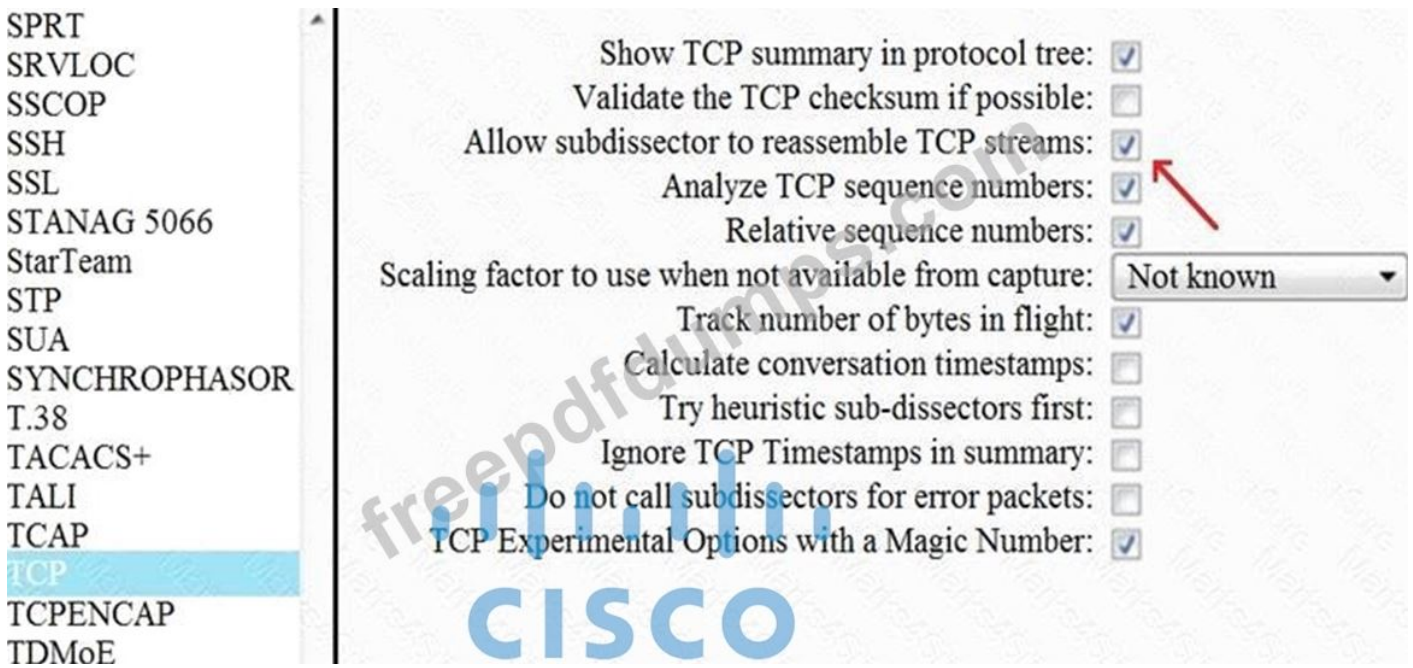
D. The metric score will be larger when a remote attack is more likely.
Answer: (SHOW ANSWER)

NEW QUESTION: 187
Refer to the exhibit. What does this output indicate?
A. HTTPS ports are open on the server.
B. SMB ports are closed on the server.
C. FTP ports are open on the server.
D. Email ports are closed on the server.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 188
Which incidence response step includes identifying all hosts affected by an attack'?
A. containment eradication and recovery
B. detection and analysis
C. post-incident activity
D. preparation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 189
Refer to the exhibit.
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: (SHOW ANSWER)
When a company workstation is compromised, the stakeholders that must be involved are the ones who are responsible for the security incident response process. According to the table, these are Employee 4 (Security Operation Center Analyst), Employee 6 (Head of Network and Security Infrastructure Services), and Employee 7 (Technical Director). The other employees have different roles that are not directly related to the incident response process, such as accounting, financial management, or system administration. Reference:= Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 1: Security Concepts, Lesson 1.4: Security Monitoring, Topic 1.4.1: Security Operations Center

NEW QUESTION: 190
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 (LEAVE A REPLY)

NEW QUESTION: 191

Which evasion method involves performing actions slower than normal to prevent detection?

A. traffic fragmentation

B. tunneling

C. timing attack

D. resource exhaustion

Answer: D (LEAVE A REPLY)

NEW QUESTION: 192

Which vulnerability type is used to read, write, or erase information from a database?

A. SQL injection

B. buffer overflow

C. cross-site request forgery

D. cross-site scripting

Answer: (SHOW ANSWER)

NEW QUESTION: 193

Drag and drop the elements from the left into the correct order for incident handling on the right.

Answer:

NEW QUESTION: 194
What is the relationship between a vulnerability and a threat?
A. A threat exploits a vulnerability
B. A vulnerability is a calculation of the potential loss caused by a threat
C. A vulnerability exploits a threat
D. A threat is a calculation of the potential loss caused by a vulnerability
Answer: A (LEAVE A REPLY)
A vulnerability refers to a weakness or flaw in a system that can be exploited by threats (such as hackers or malware) to gain unauthorized access, cause damage, etc. Threats exploit these vulnerabilities to impact the confidentiality, integrity, or availability of information and systems. References: Cisco Cybersecurity Associate

NEW QUESTION: 195
Refer to the exhibit.
Which technology generates this log?
A. NetFlow
B. IDS
C. web proxy
D. firewall
Answer: D (LEAVE A REPLY)

The log in the exhibit is generated by a firewall. It shows a deny action taken on TCP traffic, specifying the source and destination addresses and ports, which is characteristic of firewall logs. Firewalls are designed to control incoming and outgoing network traffic based on predetermined security rules, and this log entry reflects the enforcement of such a rule.
Reference:
Cisco's official documentation on firewall technologies and their log formats.

NEW QUESTION: 196
What is a difference between SI EM and SOAR security systems?
A. SIEM combines data collecting, standardization, case management, and analytics for a defense-in-depth concept, and SOAR collects security data antivirus logs, firewall logs, and hashes of downloaded files
B. SOAR collects and stores security data at a central point and then converts it into actionable intelligence, and SIEM enables SOC teams to automate and orchestrate manual tasks
C. SIEM raises alerts in the event of detecting any suspicious activity, and SOAR automates investigation path workflows and reduces time spent on alerts
D. SOAR ingests numerous types of logs and event data infrastructure components and SIEM can fetch data from endpoint security software and external threat intelligence feeds
Answer: C (LEAVE A REPLY)

NEW QUESTION: 197
Refer to the exhibit.

```
alert tcp !$HOME_NET any -> $HOME_NET 80 (flags: s; msg:"Attempt to access server is
made with TCP packets"; classtype:attempted-dos; sid:1000990; rev:1;)
```

What is the outcome of the command?
A. TCP rule that detects TCP packets with the SYN flag in an external FTP server
B. TCP rule that detects TCP packets with a SYN flag in the internal network
C. TCP rule that detects TCP packets with a ACK flag in the internal network
D. TCP rule that detects TCP packets with the ACK flag in an external FTP server
Answer: (SHOW ANSWER)
The command in the exhibit is a Snort rule that is configured to alert on TCP packets with the SYN flag set, where the source is not the home network (!$HOME_NET) and the destination is within the home network ($HOME_NET) on port 80. This rule is designed to detect potential SYN flood attacks targeting the internal network's web server on port 80.

NEW QUESTION: 198
What is the difference between vulnerability and risk?

A. A vulnerability is a sum of possible malicious entry points, and a risk represents the possibility of the unauthorized entry itself.
B. A vulnerability represents a flaw in a security that can be exploited, and the risk is the potential damage it might cause.
C. A risk is a potential threat that an exploit applies to, and a vulnerability represents the threat itself
D. A risk is potential threat that adversaries use to infiltrate the network, and a vulnerability is an exploit
Answer: B (LEAVE A REPLY)

NEW QUESTION: 199
Which two elements are used for profiling a network? (Choose two.)
A. listening ports
B. OS fingerprint
C. total throughput
D. running processes
E. session duration
Answer: (SHOW ANSWER)

NEW QUESTION: 200
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 DVD copied using Windows system
B. data from a CD copied using Linux system
C. data from a CD copied using Windows
D. data from a CD copied using Mac-based system
Answer: B (LEAVE A REPLY)

NEW QUESTION: 201
Which type of data must an engineer capture to analyze payload and header information?
A. alert data
B. session logs
C. full packet
D. frame check sequence
Answer: (SHOW ANSWER)

NEW QUESTION: 202
Which attack method is being used when an attacker tries to compromise a network with an authentication system that uses only 4-digit numeric passwords and no username?
A. SQL injection
B. dictionary
C. replay
D. cross-site scripting
Answer: (SHOW ANSWER)
A dictionary attack is a method used to break into a password-protected computer or server by systematically entering every word in a dictionary as a password. In the context of an authentication system that uses only

4-digit numeric passwords, a dictionary attack would involve trying all possible combinations of 4-digit numbers until the correct one is found. References: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course materials discuss various attack methods, including dictionary attacks, and how they can be used to compromise networks

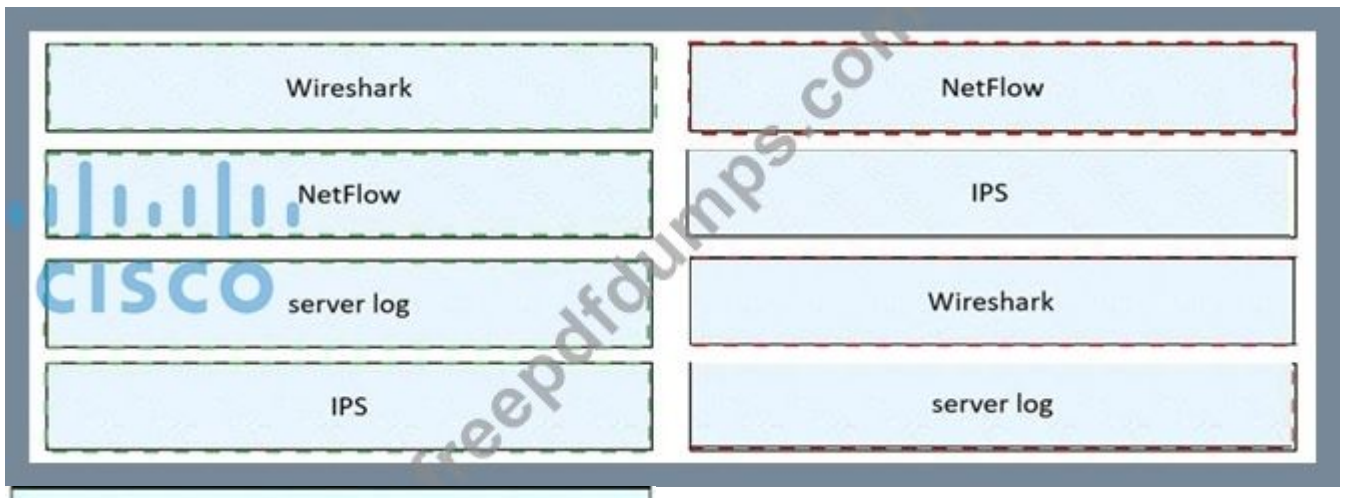
NEW QUESTION: 203
Why is encryption challenging to security monitoring?
A. Encryption analysis is used by attackers to monitor VPN tunnels.
B. Encryption is used by threat actors as a method of evasion and obfuscation.
C. Encryption introduces additional processing requirements by the CPU.
D. Encryption introduces larger packet sizes to analyze and store.
Answer: (SHOW ANSWER)
Encryption is challenging to security monitoring because it can be used by threat actors as a method of evasion and obfuscation. Encryption can prevent security devices from inspecting the content or payload of the network traffic, making it difficult to detect malicious activity or signatures. Encryption can also hide the source and destination of the traffic, making it hard to trace the origin or destination of the attack.
References:
https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fund (Module 4, Lesson 4.1.1)

NEW QUESTION: 204
A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver. Which event category is described?
A. reconnaissance
B. action on objectives
C. installation
D. exploitation
Answer: (SHOW ANSWER)
This event category is exploitation because the HTTP requests contain PHP code that attempts to execute commands on the web server and create a backdoor. Exploitation is the phase of the attack where the threat actor gains access to the target system and executes malicious code. Reference: https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fundamentals-cbrops-v1-0/CSCU-LP-CBROPS-V1-028093.html (Module 2, Lesson 2.1.3)

NEW QUESTION: 205
What is obtained using NetFlow?
A. session data
B. application logs
C. network downtime report
D. full packet capture
Answer: A (LEAVE A REPLY)
NetFlow is a network protocol developed by Cisco for collecting IP traffic information and monitoring network flow. It provides valuable data about the network sessions occurring within the network, such as source and destination IP addresses, port numbers, and protocols used. This session data is useful for understanding traffic patterns, volume, and usage.
References: Cisco's training and certification materials on NetFlow would discuss how it is used to obtain session data for network analysis.

NEW QUESTION: 206
Drag and drop the data source from the left onto the data type on the right.

Answer:



NEW QUESTION: 207
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=1476292607552.286&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

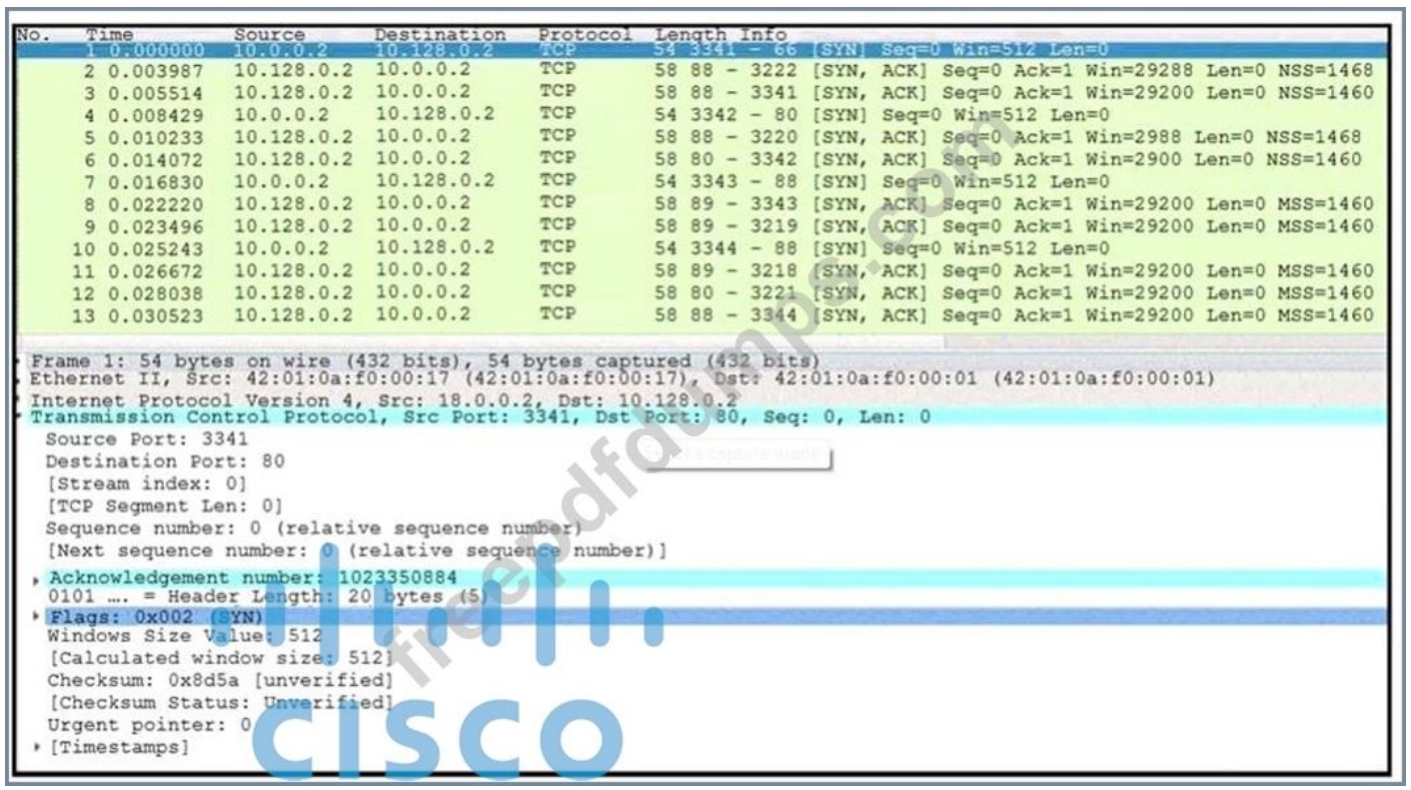
D. 2542

Answer: (SHOW ANSWER)

Packet number 2318 is the one that contains a file that is extractable within Wireshark. This can be determined by the information provided in the packet details, which typically includes an HTTP GET request indicating the retrieval of a file, such as an image or document1.

NEW QUESTION: 208

Refer to the exhibit.



What is occurring in this network traffic?

A. flood of SYN packets coming from a single source IP to a single destination IP

B. high rate of SYN packets being sent from a multiple source towards a single destination IP

C. high rate of SYN packets being sent from a single source IP towards multiple destination IPs

D. flood of ACK packets coming from a single source IP to multiple destination IPs

Answer: A (LEAVE A REPLY)

NEW QUESTION: 209

Which classification of cross-site scripting attack executes the payload without storing it for repeated use?

A. stored

B. reflective

C. DOM

D. CSRF

Answer: B (LEAVE A REPLY)

Reflective XSS, also known as Non-Persistent XSS, occurs when an attacker sends a malicious script to a user through a web application, and the script is executed immediately in the user's browser without being stored on the server. This type of attack is typically carried out by including the malicious script in a URL, which is then sent to the victim. When the victim clicks on the link, the script runs in their browser, reflecting the attacker's actions without storing the payload for repeated use12. Reference:: OWASP Foundation's documentation on Cross-Site Scripting (XSS) provides detailed information on the different types of XSS attacks, including Reflective XSS

NEW QUESTION: 210

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 snaplen configuration

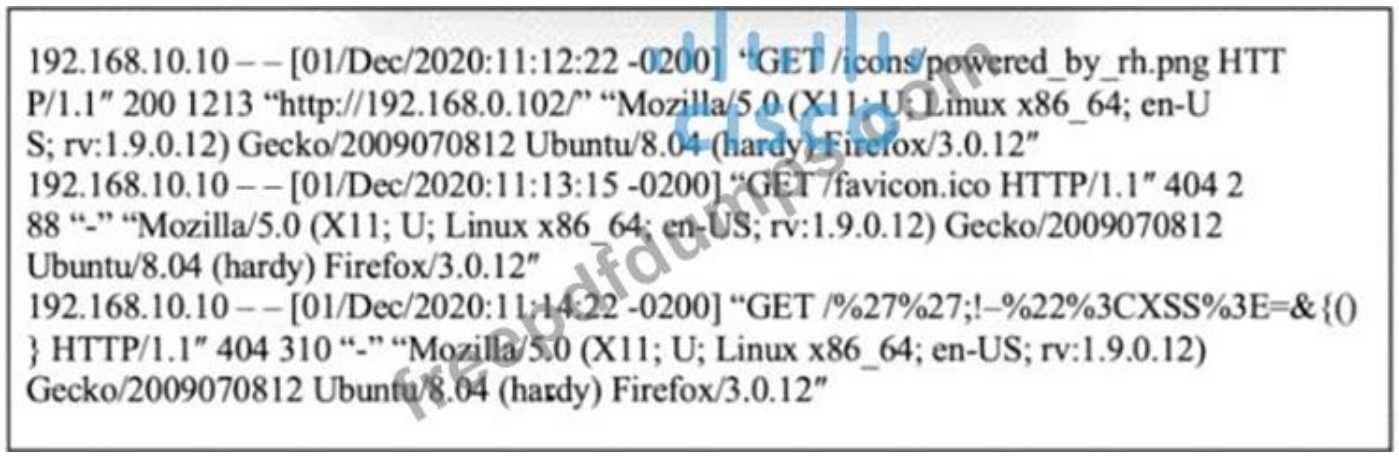
Answer: A (LEAVE A REPLY)

A TCP handshake is a three-way exchange of messages between a client and a server to establish a TCP connection. The client initiates the handshake by sending a SYN packet with a sequence number to the server.

The server responds with a SYN-ACK packet with its own sequence number and an acknowledgment number that is the client's sequence number plus one. The client completes the handshake by sending an ACK packet with an acknowledgment number that is the server's sequence number plus one. If the remote server is not receiving an SYN-ACK packet from the local server, it means that the TCP handshake is not completed and the connection is not established. This could be caused by various factors, such as network congestion, firewall rules, packet filtering, or misconfiguration of the TCP parameters on either end. References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 177; TCP 3-Way Handshake Process
- GeeksforGeeks

NEW QUESTION: 211

Refer to the exhibit.



What is occurring?

A. Insecure Deserialization

B. Cross-Site Scripting attack

C. XML External Entitles attack

D. Regular GET requests

Answer: (SHOW ANSWER)

NEW QUESTION: 212

Which regular expression matches "color" and "colour"?

A. colo?ur

B. col[08]+our

C. colou?r

D. col[09]+our

Answer: (SHOW ANSWER)

The regular expression that matches both "color" and "colour" is colo?ur. In this expression, the ? denotes that the preceding character u is optional, meaning it may appear zero or one time. This allows the expression to match both the American spelling "color" and the British spelling "colour".

References := Understanding regular expressions is fundamental in various computing tasks, including cybersecurity operations. The Cisco Cybersecurity Operations Fundamentals (CBROPS) material covers the use of regular expressions for searching through logs and data, which is a critical skill for a cybersecurity analyst.

NEW QUESTION: 213

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: C (LEAVE A REPLY)
Traffic with a known TOR exit node is often associated with data exfiltration, where sensitive information is transferred from within the network to an external location. TOR networks are used to anonymize the traffic, making it difficult to trace back to the source. References := Cisco Cybersecurity Operations Fundamentals - Module 2: Security Monitoring

NEW QUESTION: 214
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. running processes of the server
C. open ports of an email server
D. open port of an FTP server
Answer: C (LEAVE A REPLY)

NEW QUESTION: 215
What is a scareware attack?
A. using the spoofed email addresses to trick people into providing login credentials
B. overwhelming a targeted website with fake traffic
C. gaming access to your computer and encrypting data stored on it
D. inserting malicious code that causes popup windows with flashing colors
Answer: (SHOW ANSWER)
Scareware is a type of malware attack that tricks users into believing their computer is infected with a virus, prompting them to download and pay for fake antivirus software. The attack often uses popup windows with flashing colors (D) to create a sense of urgency and scare the user into taking immediate action.
References: Cisco Certified CyberOps Associate certification materials

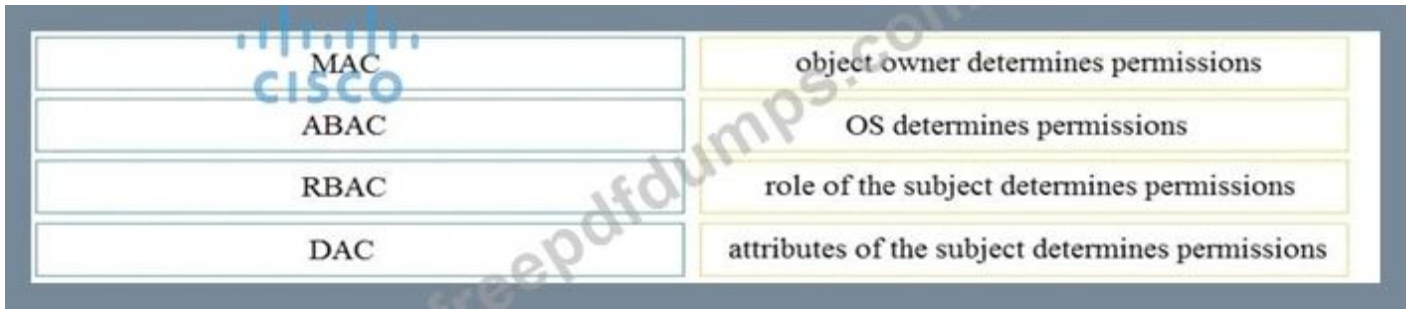
NEW QUESTION: 216
During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?
A. examination

B. collection
C. investigation
D. reporting
Answer: (SHOW ANSWER)

NEW QUESTION: 217
What is the communication channel established from a compromised machine back to the attacker?
A. command and control
B. IDS evasion
C. port scanning
D. man-in-the-middle
Answer: A (LEAVE A REPLY)

NEW QUESTION: 218
An analyst is using the SIEM platform and must extract a custom property from a Cisco device and capture the phrase, "File: Clean." Which regex must the analyst import?
A. File: Clean (.*)
B. ^File: Clean$
C. File: Clean
D. ^Parent File Clean$
Answer: D (LEAVE A REPLY)

NEW QUESTION: 219
Drag and drop the access control models from the left onto the correct descriptions on the right.



Answer:

MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC

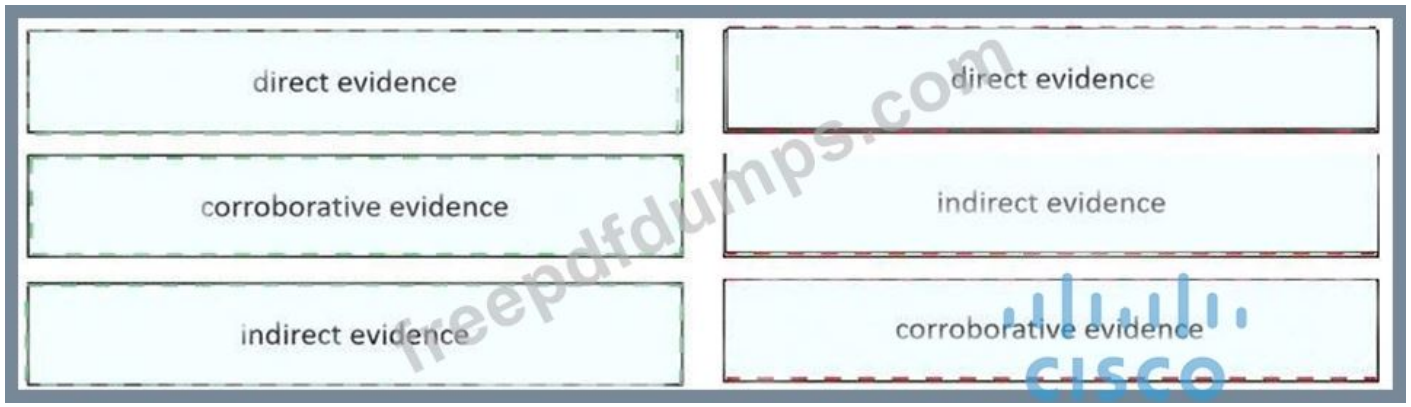
NEW QUESTION: 220
Which type of attack is a blank email with the subject "price deduction" that contains a malicious attachment?
A. integrity violation
B. smishing
C. phishing attack
D. man-in-the-middle attack
Answer: (SHOW ANSWER)

NEW QUESTION: 221
Refer to the exhibit.
Which application protocol is in this PCAP file?
A. SSH
B. TCP
C. TLS
D. HTTP
Answer: (SHOW ANSWER)
The PCAP file in the exhibit shows a Transmission Control Protocol (TCP) communication between two IP addresses. In the data section of the packet capture, "pdy/3.1... http/1" is visible, indicating that HTTP (Hypertext Transfer Protocol) is being used as the application protocol for this communication.

NEW QUESTION: 222
Drag and drop the type of evidence from the left onto the description of that evidence on the right.

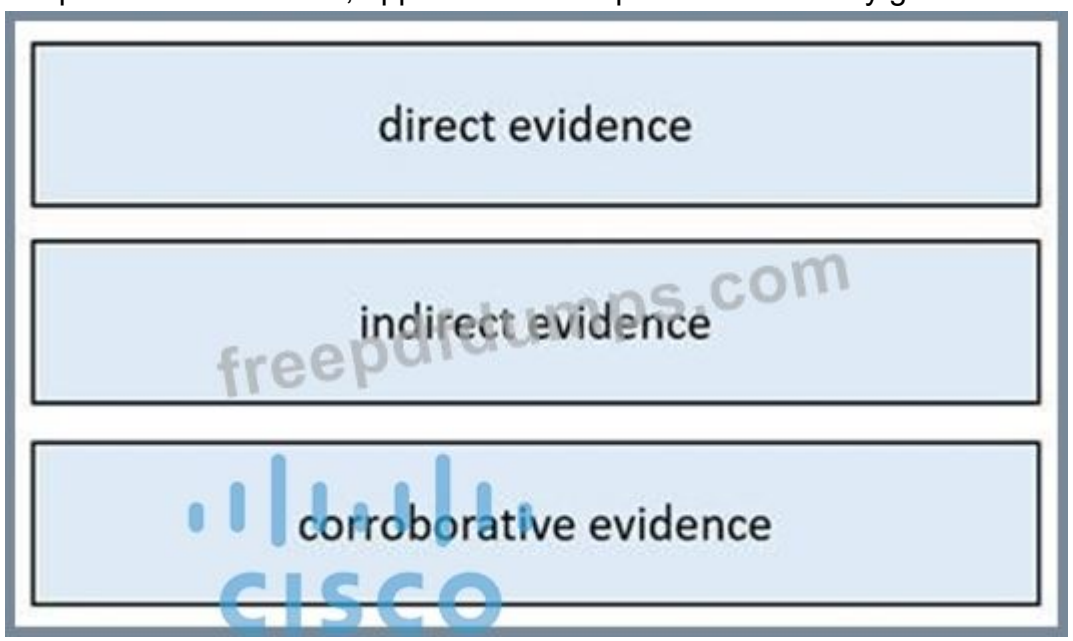
direct evidence	log that shows a command and control check-in from verified malware
corroborative evidence	firewall log showing successful communication and threat intelligence stating an IP is known to host malware
indirect evidence	NetFlow-based spike in DNS traffic

Answer:



Explanation

Graphical user interface, application Description automatically generated



NEW QUESTION: 223

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 (LEAVE A REPLY)

https://techdifferences.com/difference-between-steganography-and-cryptography.html#:~:text=The%20steganography%20and%20cryptography%20are,the%20structure%20of%20the%20message.

NEW QUESTION: 224

Which technique is a low-bandwidth attack?

A. social engineering

B. session hijacking

C. evasion

D. phishing
Answer: D (LEAVE A REPLY)
Phishing is considered a low-bandwidth attack because it does not require the use of significant network resources. Instead, it relies on social engineering to deceive individuals into providing sensitive information or clicking on malicious links, often through email or other communication methods1.

NEW QUESTION: 225
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 (LEAVE A REPLY)
Section: Network Intrusion Analysis
Explanation/Reference:

NEW QUESTION: 226
An engineer runs a suspicious file in a sandbox analysis tool to see the outcome. The analysis report shows that outbound callouts were made post infection.
Which two pieces of information from the analysis report are needed to investigate the callouts? (Choose two.)
A. domain names
B. signatures
C. host IP addresses
D. dropped files
E. file size
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 227
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: (SHOW ANSWER)

A buffer overflow attack occurs when more data is written to a buffer than it is designed to hold. This excess data can overwrite adjacent memory locations, leading to the execution of malicious code or crashing the system. Buffer overflows are a common vulnerability that attackers exploit to gain unauthorized access to systems.

NEW QUESTION: 228
Refer to the exhibit.

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 (LEAVE A REPLY)

NEW QUESTION: 229
Which list identifies the information that the client sends to the server in the negotiation phase of the TLS handshake?
A. ClientStart, ClientKeyExchange, cipher-suites it supports, and suggested compression methods
B. ClientStart, TLS versions it supports, cipher-suites it supports, and suggested compression methods
C. ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression methods
D. ClientHello, ClientKeyExchange, cipher-suites it supports, and suggested compression methods
Answer: C (LEAVE A REPLY)
During the negotiation phase of the TLS handshake, the client sends a "ClientHello" message to the server which includes information about TLS versions it supports, cipher-suites it supports and suggested compression methods. This initiates communication protocols for secure connection. Reference:= Cisco Cybersecurity source documents or study guide

NEW QUESTION: 230
What are two differences between tampered disk images and untampered disk images'? (Choose two.)
A. Untampered images can be used as law enforcement evidence.
B. The image is tampered if the stored hash and the computed hash are identical
C. Tampered Images are used in a security investigation process
D. Tampered images are used as an element for the root cause analysis report
E. The image is untampered if the existing stored hash matches the computed one
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 231
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: (SHOW ANSWER)
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: 232
Refer to the exhibit.
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: B (LEAVE A REPLY)
The #netstat -an command output typically displays a list of all open ports and associated connections. If the web application is slowed down, the engineer would look for unusual patterns such as an excessive number of connections to the web server which could indicate a denial-of-service attack. However, without specific details from the #netstat -an output, it's not possible to determine the exact cause of the issue. Therefore, the engineer would need to gather more data, possibly including checking server logs, resource usage, and network traffic patterns to diagnose the problem accurately.

NEW QUESTION: 233
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. 1986

B. 2318

C. 2542

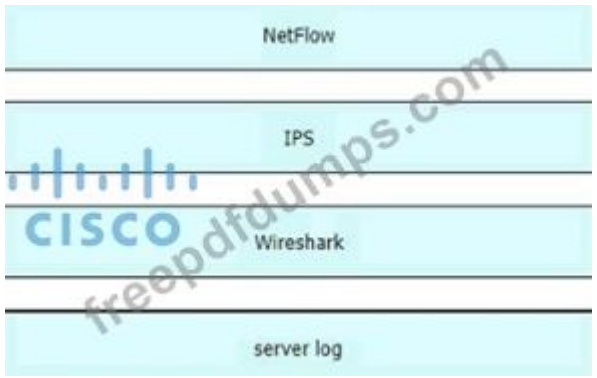
D. 2317

Answer: C (LEAVE A REPLY)

NEW QUESTION: 234

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

Answer:



NEW QUESTION: 235
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: C (LEAVE A REPLY)
Explanation
Host-based antivirus protection is also known as agent-based. Agent-based antivirus runs on every protected machine. Agentless antivirus protection performs scans on hosts from a centralized system. Agentless systems have become popular for virtualized environments in which multiple OS instances are running on a host simultaneously. Agent-based antivirus running in each virtualized system can be a serious drain on system resources. Agentless antivirus for virtual hosts involves the use of a special security virtual appliance that performs optimized scanning tasks on the virtual hosts. An example of this is VMware's vShield.

NEW QUESTION: 236
Refer to the exhibit.

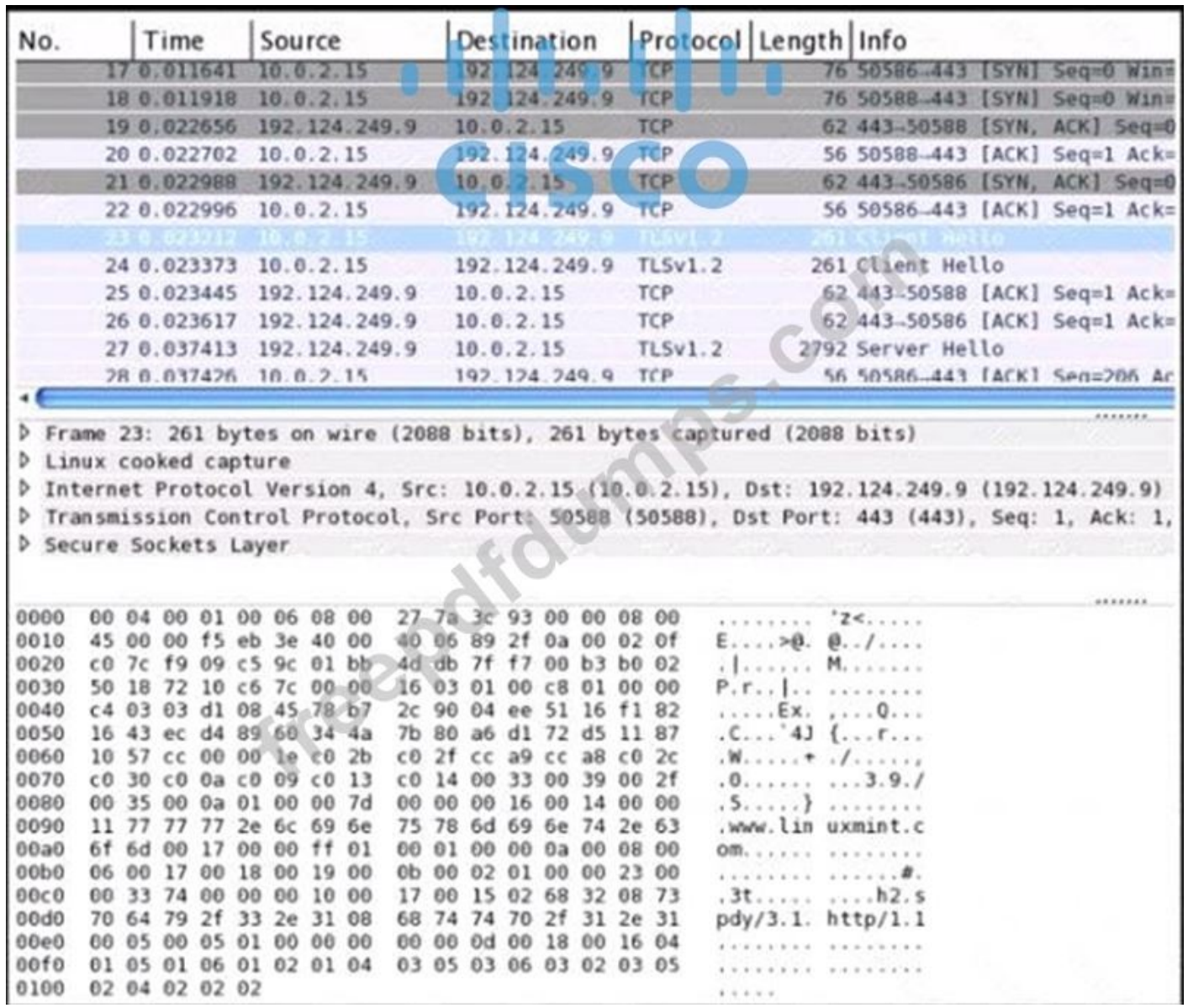
```
Mar 07 2020 16:16:48: %ASA-4-106023: Deny tcp src
outside:10.22.219.221/54602 dst outside:10.22.250.212/504
by access-group "outside" [0x0, 0x0]
```

Which technology generates this log?
A. NetFlow
B. firewall
C. IDS
D. web proxy
Answer: (SHOW ANSWER)

NEW QUESTION: 237
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: A,B (LEAVE A REPLY)
A: Stateful inspection tracks the state of network connections, such as TCP streams, to determine if a packet is part of an established connection.
B: Deep packet inspection examines the data part (payload) of a packet and can identify, block, or reroute packets with specific types of malware. Stateful inspection does not inspect the payload for malware.

NEW QUESTION: 238



Refer to the exhibit Drag and drop the element names from the left onto the corresponding pieces of the PCAP file on the right.

Answer:

NEW QUESTION: 239

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

A. split brain

B. scanning
C. phishing
D. reflected
E. direct
Answer: D,E (LEAVE A REPLY)
DDoS attacks are divided into two categories: reflected and direct. Reflected attacks use a third-party system to amplify the attack traffic and send it to the target. For example, an attacker can send a spoofed request to a DNS server, which will reply with a large amount of data to the target's IP address. Direct attacks send the attack traffic directly from the attacker's system or a botnet to the target. For example, an attacker can send a large number of SYN packets to the target's port, exhausting its resources. References := Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.3: Common Network Application Operations and Attacks, Topic 1.3.4: Denial-of-Service Attacks

NEW QUESTION: 240
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: (SHOW ANSWER)
The exhibit displays a sys log which is used in computer systems for messaging logs. It provides messaging tracking services from different devices like routers, switches etc., which helps in tracking and identifying potential issues. References := Cisco Cybersecurity source documents or study guide

NEW QUESTION: 241
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. IDS/IPS

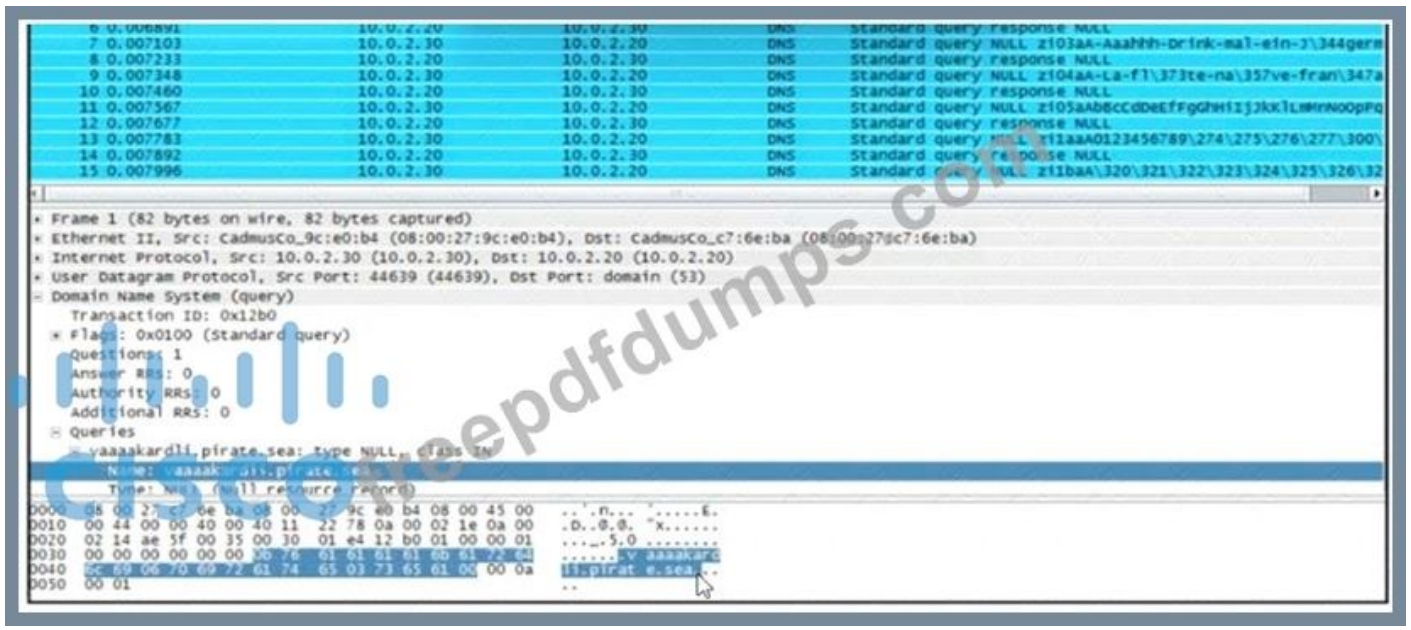
C. firewall

D. proxy

Answer: C (LEAVE A REPLY)

NEW QUESTION: 242

Refer to the exhibit.



What is occurring?

A. ARP poisoning

B. DNS tunneling

C. DNS amplification

D. ARP flood

Answer: (SHOW ANSWER)

NEW QUESTION: 243

Refer to the exhibit.

```
10.44.101.23 - - [20/Nov/2017:14:18:06 -0500] "GET / HTTP/1.1"
200 1254 "-" "Mozilla/5.0(X11; Ubuntu; Linux x86_64; rv:54.0)
Gecko/20100101 Firefox/54.0"
```

What does the message indicate?

A. a successful access attempt was made to retrieve the password file

B. a successful access attempt was made to retrieve the root of the website

C. a denied access attempt was made to retrieve the password file

D. an access attempt was made from the Mosaic web browser

Answer: B (LEAVE A REPLY)