Cisco.200-201.v2022-08-16.q164

Exam Code:	200-201
Exam Name:	Understanding Cisco Cybersecurity Operations Fundamentals
Certification Provider:	Cisco
Free Question Number:	164
Version:	v2022-08-16
# of views:	2739
# of Questions views:	1640
https://www.freeqas.com/qa/Cisco/200-201/Cisco.200-201.v2022-08-16.q164.html	

NEW QUESTION: 1

Which attack method intercepts traffic on a switched network?

A. denial of service

B. ARP cache poisoning

C. DHCP snooping

D. command and control

Answer: C (LEAVE A REPLY)

Section: Security Concepts

NEW QUESTION: 2

Refer to the exhibit.

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

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 web application server is under a denial-of-service attack.
C. The engineer must gather more data.
D. The server is under a man-in-the-middle attack between the web application and its database
Answer: (SHOW ANSWER)

NEW QUESTION: 3
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. transport layer security encryption
B. ROT13 encryption
C. Base64 encoding
D. SHA-256 hashing
Answer: A (LEAVE A REPLY)

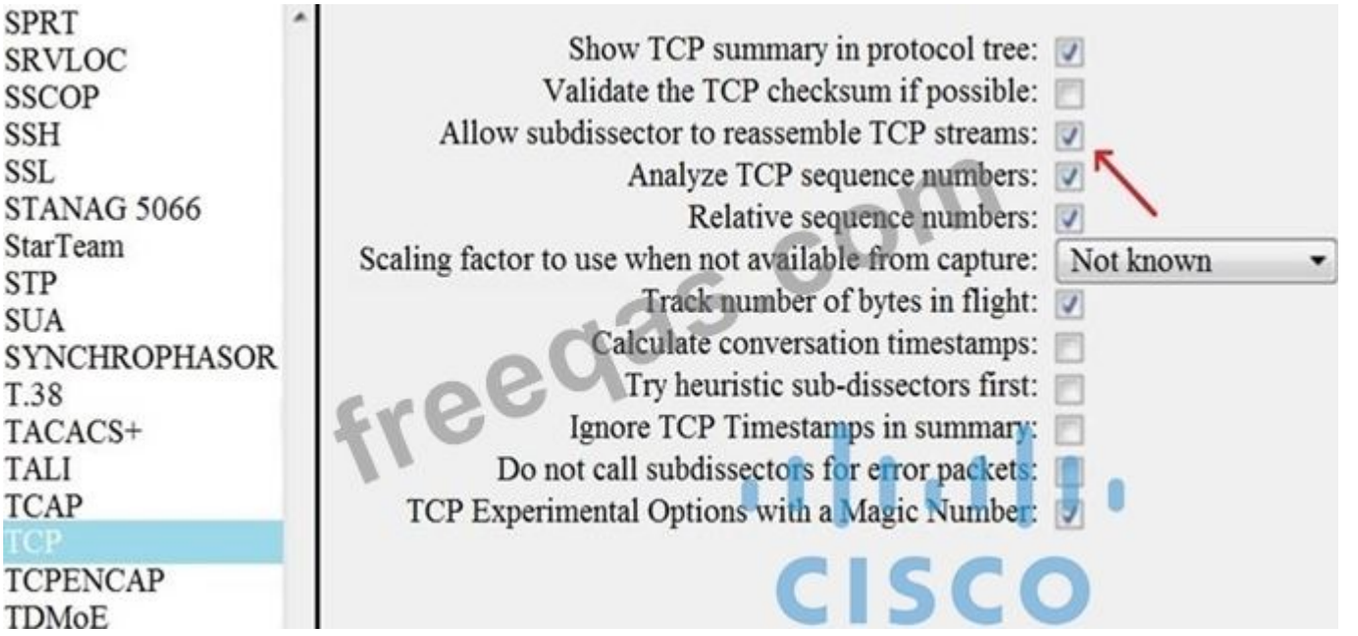
NEW QUESTION: 4
What are two differences in how tampered and untampered disk images affect a security incident? (Choose two.)

A. Untampered images are used in the security investigation process
B. Tampered images are used in the incident recovery process
C. Tampered images are used in the security investigation process
D. The image is untampered if the stored hash and the computed hash match
E. The image is tampered if the stored hash and the computed hash match
Answer: A,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. trusted subordinate CA, public key, and cipher suites
B. server name, trusted subordinate CA, and private key
C. trusted CA name, cipher suites, and private key
D. server name, trusted CA, and public key
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6
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. source IP address of the packet
D. destination IP address of the packet
E. UDP port from which the traffic is sourced
Answer: C,D (LEAVE A REPLY)
Section: Network Intrusion Analysis

NEW QUESTION: 7
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. disable TCP streams

C. extract a file from a packet capture

D. unfragment TCP

Answer: D (LEAVE A REPLY)

NEW QUESTION: 8

At a company party a guest asks

How is this type of conversation classified?

A. Social Engineering

B. Password Revelation Strategy

C. Piggybacking

D. Phishing attack

Answer: (SHOW ANSWER)

NEW QUESTION: 9

Which signature impacts network traffic by causing legitimate traffic to be blocked?

A. false negative

B. false positive

C. true positive

D. true negative

Answer: B (LEAVE A REPLY)

NEW QUESTION: 10

An engineer needs to fetch logs from a proxy server and generate actual events according to the data received.
Which technology should the engineer use to accomplish this task?
A. Web Security Appliance
B. Firepower
C. Stealthwatch
D. Email Security Appliance
Answer: C (LEAVE A REPLY)

NEW QUESTION: 11
An analyst is investigating an incident in a SOC environment. Which method is used to identify a session from a group of logs?
A. IP identifier
B. sequence numbers
C. 5-tuple
D. timestamps
Answer: (SHOW ANSWER)

NEW QUESTION: 12
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: B (LEAVE A REPLY)
Section: Network Intrusion Analysis

NEW QUESTION: 13
What is the difference between deep packet inspection and stateful inspection?
A. Deep packet inspection allows visibility on Layer 7 and stateful inspection allows visibility on Layer 4
B. Stateful inspection verifies contents at Layer 4 and deep packet inspection verifies connection at Layer 7
C. Stateful inspection is more secure than deep packet inspection on Layer 7
D. Deep packet inspection is more secure than stateful inspection on Layer 4
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
What do the Security Intelligence Events within the FMC allow an administrator to do?
A. View any malicious files that a host has downloaded.
B. See if a host is connecting to a known-bad domain.

C. Check for host-to-server traffic within your network.
D. Verify host-to-host traffic within your network.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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: A (LEAVE A REPLY)
Inline traffic interrogation analyzes traffic in real time and has the ability to prevent certain traffic from being forwarded Traffic mirroring doesn't pass the live traffic instead it copies traffic from one or more source ports and sends the copied traffic to one or more destinations for analysis by a network analyzer or other monitoring device

NEW QUESTION: 16
What is an incident response plan?
A. an organizational approach to security management to ensure a service lifecycle and continuous improvements
B. an organizational approach to system backup and data archiving aligned to regulations
C. an organizational approach to disaster recovery and timely restoration of operational services
D. an organizational approach to events that could lead to asset loss or disruption of operations
Answer: (SHOW ANSWER)

NEW QUESTION: 17
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: 18
Refer to the exhibit.

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

NEW QUESTION: 19
An engineer needs to fetch logs from a proxy server and generate actual events according to the data received.
Which technology should the engineer use to accomplish this task?
A. Firepower
B. Web Security Appliance
C. Stealthwatch
D. Email Security Appliance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
How does an attacker observe network traffic exchanged between two users?
A. command injection
B. man-in-the-middle
C. port scanning
D. denial of service
Answer: B (LEAVE A REPLY)

NEW QUESTION: 21

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 -sV 192.168.1.0/24

C. nmap -sP 192.168.1.0/24

D. nmap -sL 192.168.1.0/24

Answer: D (LEAVE A REPLY)

NEW QUESTION: 22

Refer to the exhibit.

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

A. Initiator User

B. Initiator IP

C. Ingress Security Zone

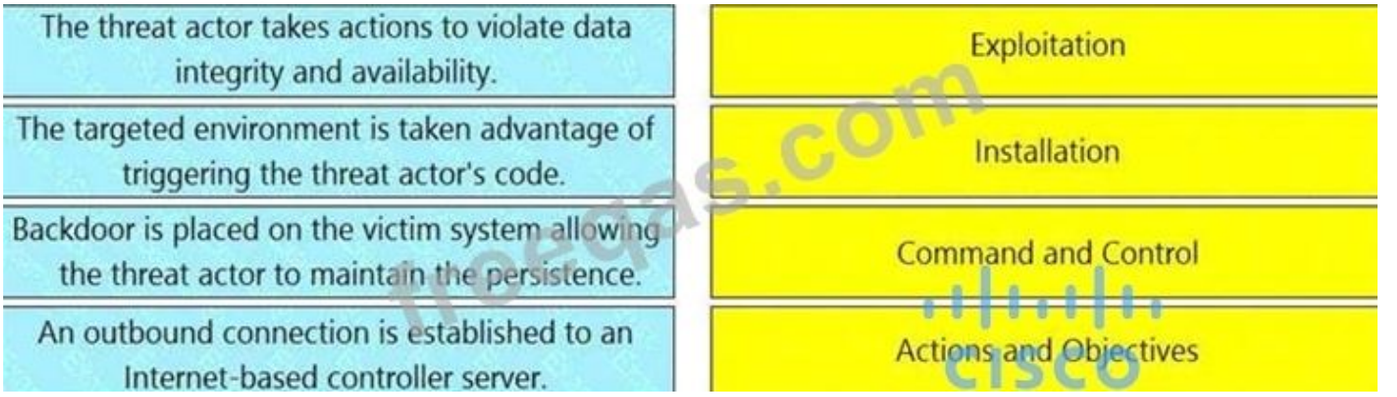
D. Source Port

E. First Packet

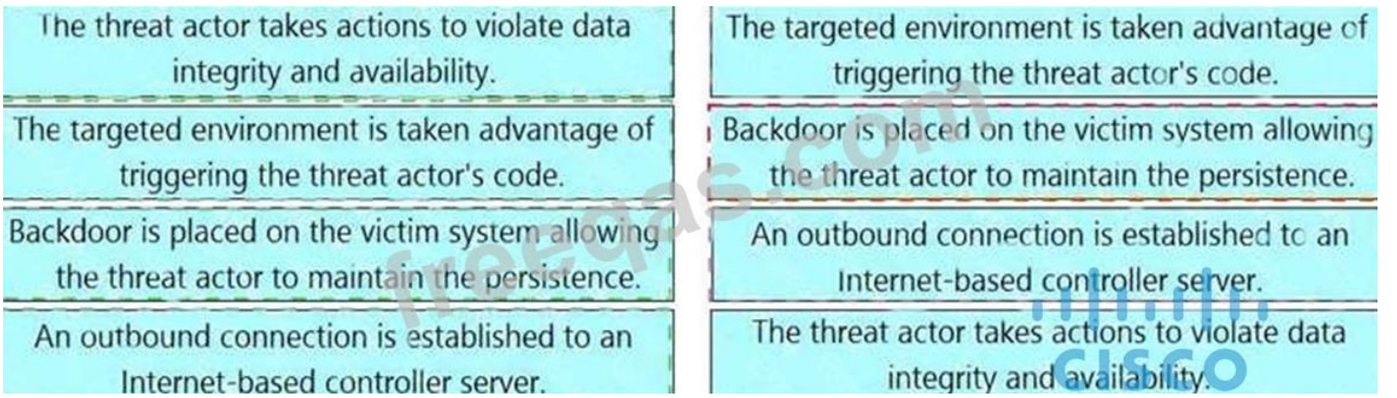
Answer: (SHOW ANSWER)

NEW QUESTION: 23

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

Exploitation - The targeted Environment is taken advantage of triggering the threat actor's code

Installation - Backdoor is placed on the victim system allowing the threat actor to maintain the persistence.

Command and Control - An outbound connection is established to an Internet-based controller server.

Actions and Objectives - The threat actor takes actions to violate data integrity and availability

NEW QUESTION: 24

What does cyber attribution identity 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)

Explanation/Reference:

NEW QUESTION: 25

Which signature impacts network traffic by causing legitimate traffic to be blocked?

A. false negative

B. true positive

C. true negative

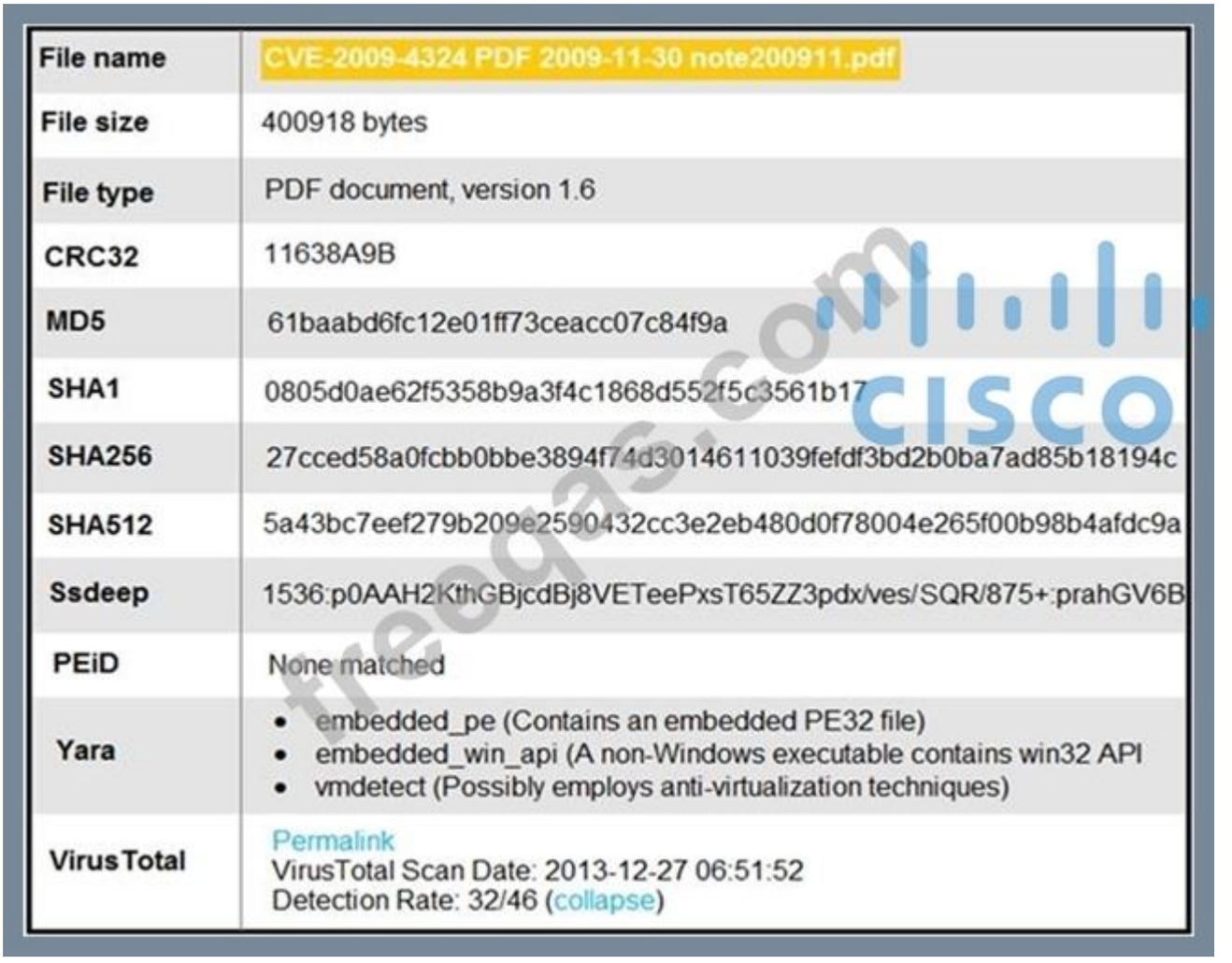
D. false positive

Answer: D (LEAVE A REPLY)

Section: Network Intrusion Analysis

NEW QUESTION: 26

Refer to the exhibit.



File name	CVE-2009-4324 PDF 2009-11-30 note200911.pdf
File size	400918 bytes
File type	PDF document, version 1.6
CRC32	11638A9B
MD5	61baabd6fc12e01ff73ceacc07c84f9a
SHA1	0805d0ae62f5358b9a3f4c1868d552f5c3561b17
SHA256	27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
SHA512	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
Ssdeep	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/SQR/875+:prahGV6B
PEiD	None matched
Yara	• embedded_pe (Contains an embedded PE32 file) • embedded_win_api (A non-Windows executable contains win32 API • vmdetect (Possibly employs anti-virtualization techniques)
VirusTotal	Permalink VirusTotal Scan Date: 2013-12-27 06:51:52 Detection Rate: 32/46 (collapse)

An engineer is analyzing this Cuckoo Sandbox report for a PDF file that has been downloaded from an email.

What is the state of this file?

A. The file has an embedded Windows 32 executable and the Yara field lists suspicious features for further analysis.

B. The file has an embedded executable and was matched by PEiD threat signatures for further analysis.

C. The file has an embedded non-Windows executable but no suspicious features are identified.

D. The file was matched by PEiD threat signatures but no suspicious features are identified since the signature list is up to date.

Answer: (SHOW ANSWER)

NEW QUESTION: 27

An engineer needs to 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 should be used to accomplish the task?

A. cipher suite

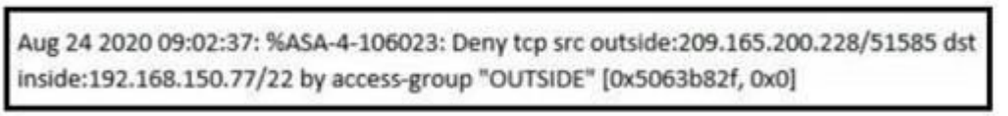
B. static IP addresses

C. signatures

D. digital certificates
Answer: (SHOW ANSWER)

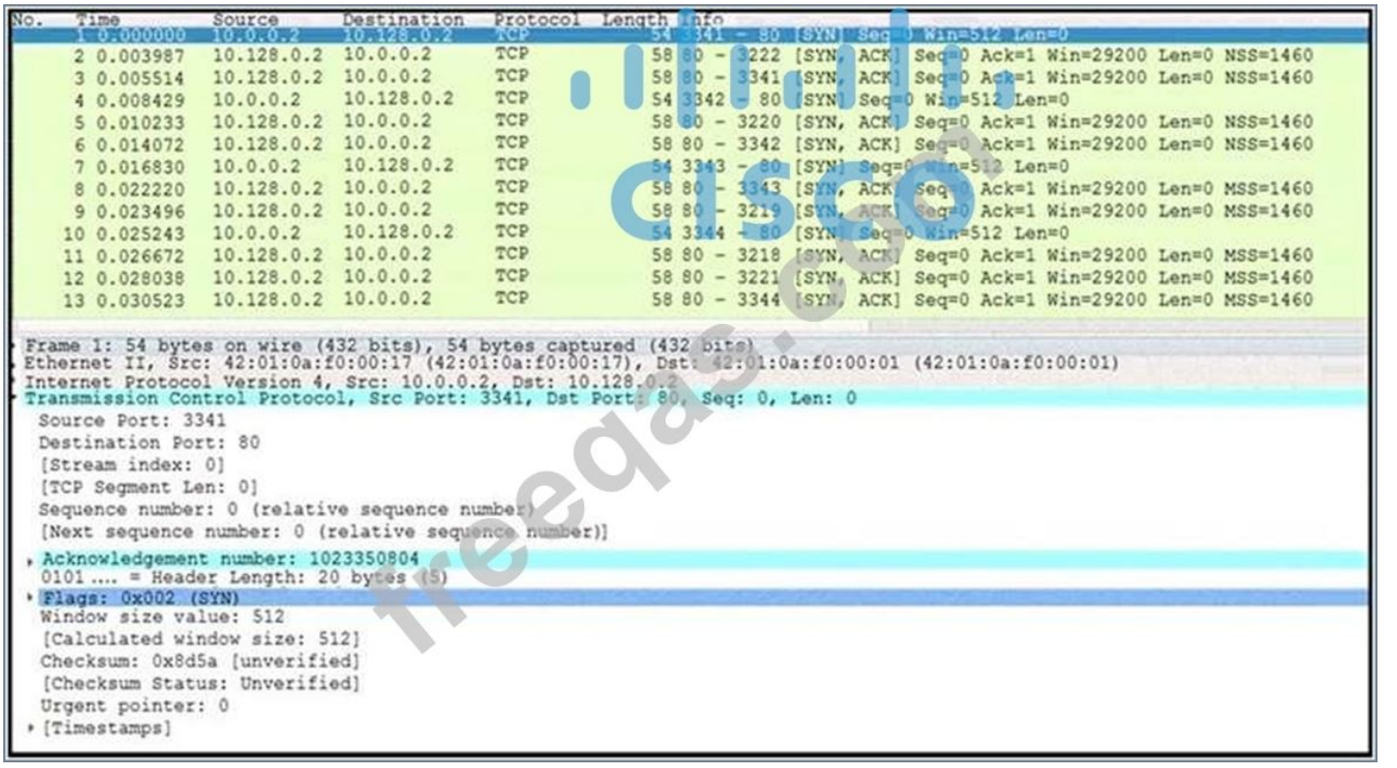
NEW QUESTION: 28
An analyst is using the SIEM platform and must extract a custom property from a Cisco device and capture the phrase, "File: Clean." Which regex must the analyst import?
A. File: Clean (.*)
B. ^File: Clean$
C. ^Parent File Clean$
D. File: Clean
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
Refer to the exhibit.



An analyst received this alert from the Cisco ASA device, and numerous activity logs were produced. How should this type of evidence be categorized?
A. indirect
B. circumstantial
C. corroborative
D. best
Answer: C (LEAVE A REPLY)
Explanation
Indirect=circumstantail so there is no posibility to match A or B (only one answer is needed in this question).
For suer it's not a BEST evidence - this FW data inform only of DROPPED traffic. If smth happend inside network, presented evidence could be used to support other evidences or make our narreation stronger but alone it's mean nothing.

NEW QUESTION: 30
Refer to the exhibit.



What is occurring in this network traffic?

A. High rate of SYN packets being sent from a multiple source towards a single destination IP.

B. High rate of ACK packets being sent from a single source IP towards multiple destination IPs.

C. Flood of SYN packets coming from a single source IP to a single destination IP.

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

Answer: (SHOW ANSWER)

NEW QUESTION: 31

Refer to the exhibit.

What is depicted in the exhibit?

A. IIS logs

B. UNIX-based syslog

C. Apache logs

D. Windows Event logs

Answer: B (LEAVE A REPLY)

NEW QUESTION: 32
Which type of evidence supports a theory or an assumption that results from initial evidence?
A. probabilistic
B. indirect
C. best
D. corroborative
Answer: (SHOW ANSWER)
Section: Security Policies and Procedures

NEW QUESTION: 33
Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2?
(Choose two.)
A. risk assessment
B. detection and analysis
C. vulnerability management
D. post-incident activity
E. vulnerability scoring
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 34
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. preparation
B. post-incident activity
C. containment, eradication, and recovery
D. detection and analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 35
A user received a malicious attachment but did not run it.

Which category classifies the intrusion?

A. weaponization

B. reconnaissance

C. installation

D. delivery

Answer: (SHOW ANSWER)

Section: Security Concepts

NEW QUESTION: 36

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

Which technology should be used to accomplish this task?

A. application whitelisting/blacklisting

B. host-based IDS

C. network NGFW

D. antivirus/antispyware software

Answer: A (LEAVE A REPLY)

NEW QUESTION: 37

Refer to the exhibit.

Which type of attack is being executed?

A. command injection

B. SQL injection

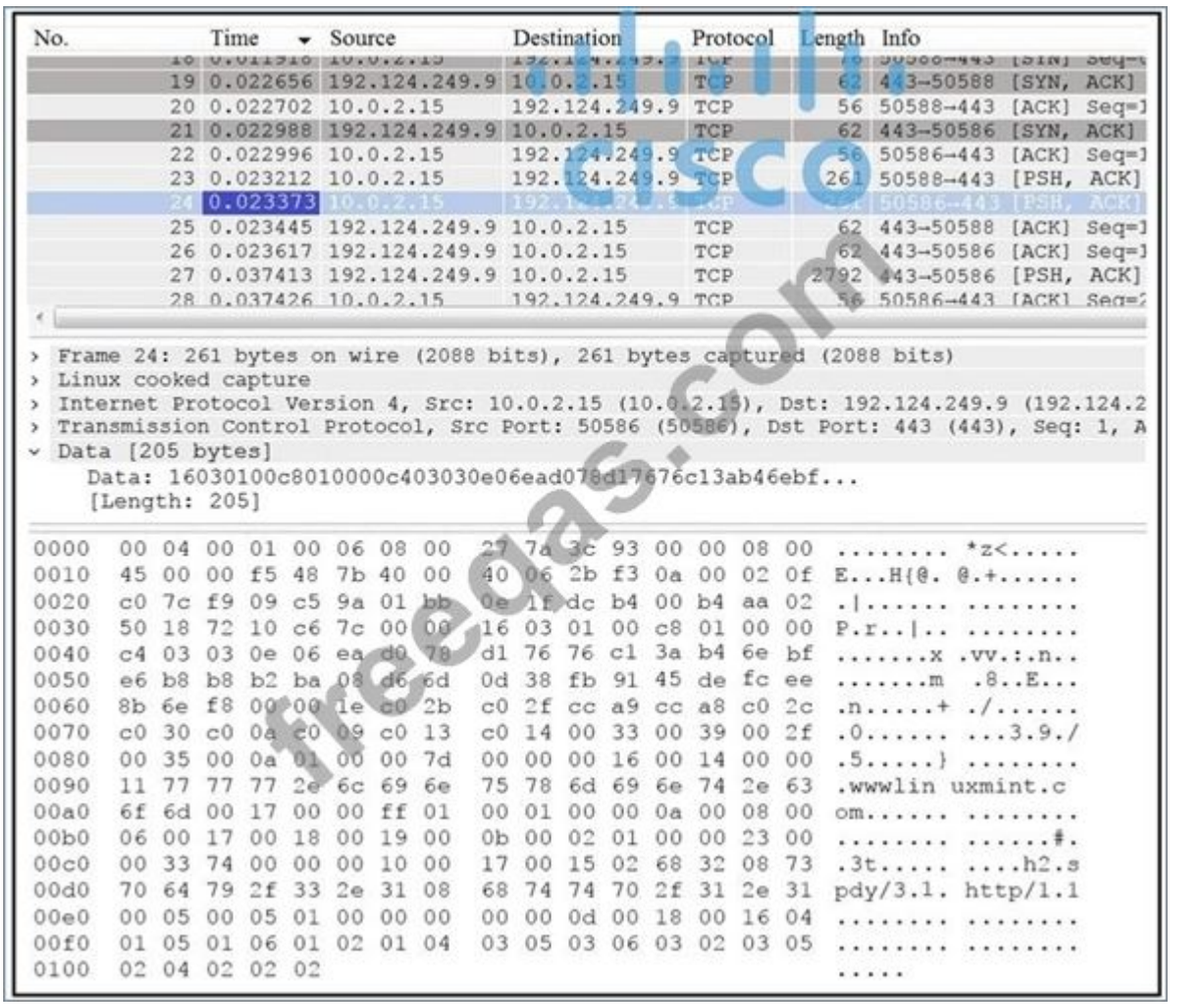
C. cross-site scripting

D. cross-site request forgery

Answer: B (LEAVE A REPLY)

NEW QUESTION: 38

Refer to the exhibit.



Which application protocol is in this PCAP file?

A. TLS

B. HTTP

C. SSH

D. TCP

Answer: B (LEAVE A REPLY)

NEW QUESTION: 39

What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?

A. Tapping interrogation replicates signals to a separate port for analyzing traffic

B. Tapping interrogations detect and block malicious traffic

C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies

D. Inline interrogation detects malicious traffic but does not block the traffic

Answer: A (LEAVE A REPLY)

Explanation

A network TAP is a simple device that connects directly to the cabling infrastructure to split or copy packets for use in analysis, security, or general network management

NEW QUESTION: 40
What ate two denial-of-service (DoS) attacks? (Choose two)
A. teardrop
B. man-in-the-middle
C. phishing
D. SYN flood
E. port scan
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 41
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. delivery
B. weaponization
C. action on objectives
D. reconnaissance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
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: 43
A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?
A. CD data copy prepared in Linux system
B. CD data copy prepared in Windows
C. CD data copy prepared in Android-based system
D. CD data copy prepared in Mac-based system

Answer: A (LEAVE A REPLY)

NEW QUESTION: 44
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. instigator
B. precursor
C. trigger
D. online assault
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
Drag and drop the event term from the left onto the description on the right.

Answer:

NEW QUESTION: 46

```
$ 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 binary named "submit" is running on VM cuckoo1.

D. A URL is being evaluated to see if it has a malicious binary

Answer: (SHOW ANSWER)

NEW QUESTION: 47

Which NIST IR category stakeholder is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies?

A. PSIRT

B. CSIRT

C. management

D. public affairs

Answer: (SHOW ANSWER)

NEW QUESTION: 48

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: 49

One of the objectives of information security is to protect the CIA of information and systems. What does CIA mean in this context?

A. confidentiality, integrity, and authorization

B. confidentiality, identity, and availability

C. confidentiality, identity, and authorization

D. confidentiality, integrity, and availability

Answer: (SHOW ANSWER)

NEW QUESTION: 50

Refer to the exhibit. An attacker scanned the server using Nmap. What did the attacker obtain from this scan?

A. Gathered a list of Active Directory users

B. Gathered information on processes running on the server

C. Identified a firewall device preventing the pert state from being returned.

D. Identified open SMB ports on the server

Answer: B (LEAVE A REPLY)

NEW QUESTION: 51

Refer to the exhibit.

What is occurring in this network?

A. ARP cache poisoning

B. MAC flooding attack

C. DNS cache poisoning

D. MAC address table overflow

Answer: A (LEAVE A REPLY)

NEW QUESTION: 52

What is the difference between indicator of attack (IoA) and indicators of compromise (IoC)?

A. IoC refers to the individual responsible for the security breach, and IoA refers to the resulting loss.

B. IoA is the evidence that a security breach has occurred, and IoC allows organizations to act before the vulnerability can be exploited.

C. IoC is the evidence that a security breach has occurred, and IoA allows organizations to act before the vulnerability can be exploited.

D. IoA refers to the individual responsible for the security breach, and IoC refers to the resulting loss.

Answer: (SHOW ANSWER)

NEW QUESTION: 53

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

A. Source Port

B. Initiator User

C. Ingress Security Zone

D. First Packet

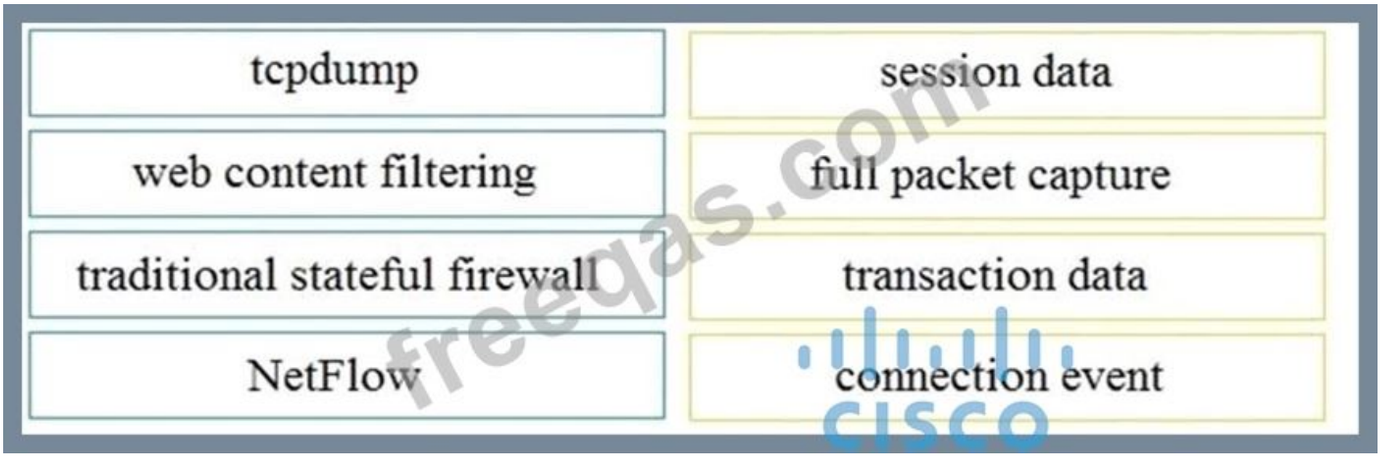
E. Initiator IP

Answer: (SHOW ANSWER)

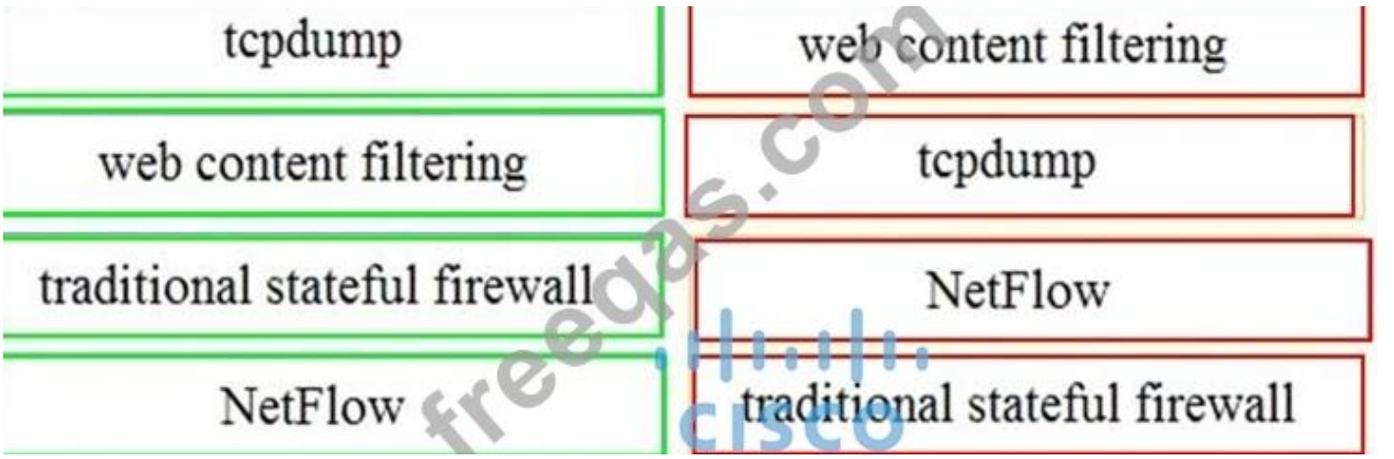
NEW QUESTION: 54
How does an SSL certificate impact security between the client and the server?
A. by creating an integrated channel between the client and the server
B. by enabling an authenticated channel between the client and the server
C. by enabling an authorized channel between the client and the server
D. by creating an encrypted channel between the client and the server
Section: (none)
Explanation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 55
What is an example of social engineering attacks?
A. receiving an unexpected email from an unknown person with an uncharacteristic attachment from someone in the same company
B. receiving an invitation to the department's weekly WebEx meeting
C. receiving an email from human resources requesting a visit to their secure website to update contact information
D. sending a verbal request to an administrator who knows how to change an account password
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Drag and drop the technology on the left onto the data type the technology provides on the right.

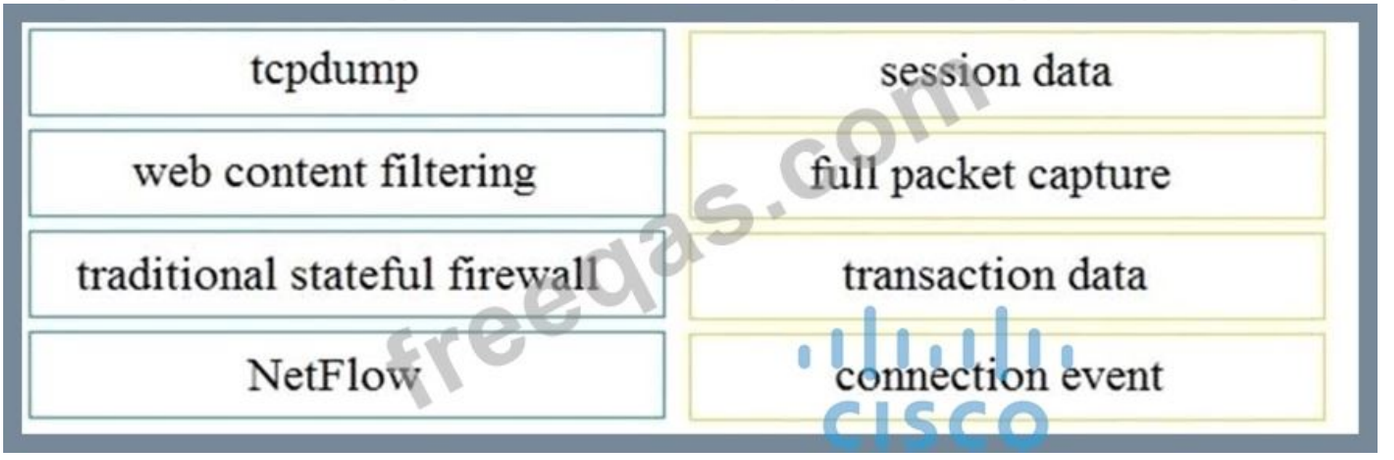


Answer:

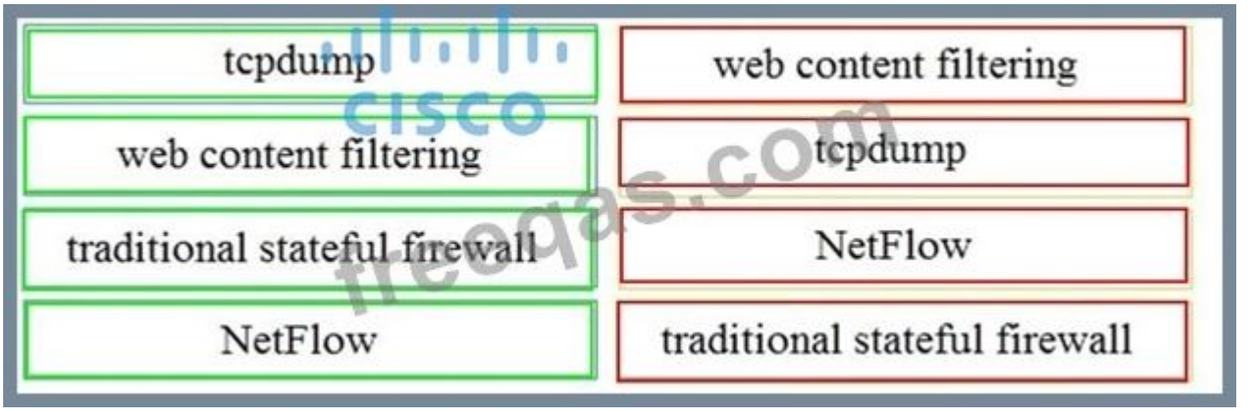


NEW QUESTION: 57
What is a difference between SIEM and SOAR?
A. SOAR's primary function is to collect and detect anomalies, while SIEM is more focused on security operations automation and response.
B. SOAR predicts and prevents security alerts, while SIEM checks attack patterns and applies the mitigation.
C. SIEM predicts and prevents security alerts, while SOAR checks attack patterns and applies the mitigation.
D. SIEM's primary function is to collect and detect anomalies, while SOAR is more focused on security operations automation and response.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 58
Drag and drop the technology on the left onto the data type the technology provides on the right.

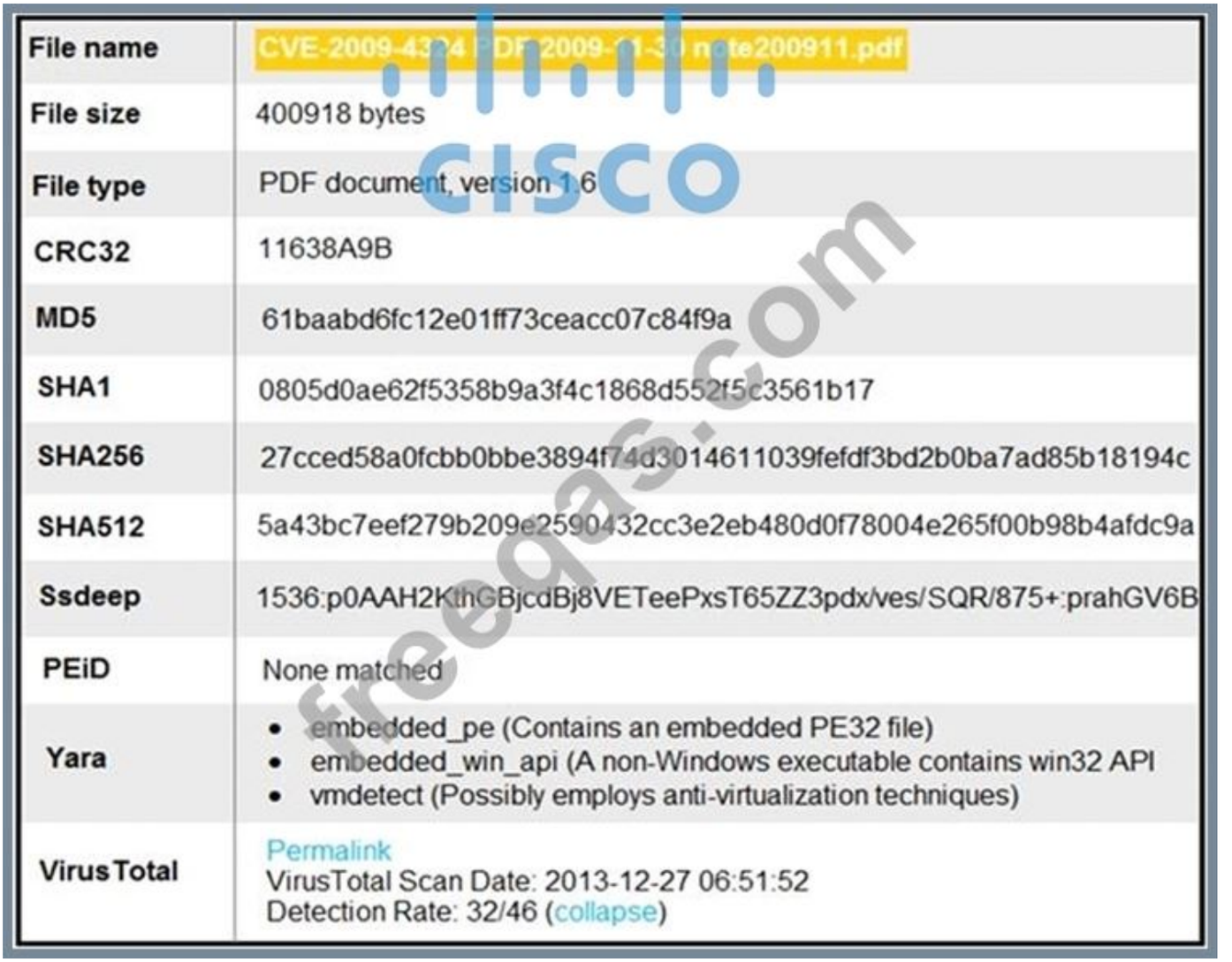


Answer:



NEW QUESTION: 59
How does certificate authority impact a security system?
A. It validates client identity when communicating with the server
B. It validates domain identity of a SSL certificate
C. It authenticates domain identity when requesting SSL certificate
D. It authenticates client identity when requesting SSL certificate
Answer: (SHOW ANSWER)

NEW QUESTION: 60
Refer to the exhibit.



File name	CVE-2009-4324 PDF 2009-11-30 note200911.pdf
File size	400918 bytes
File type	PDF document, version 1.6
CRC32	11638A9B
MD5	61baabd6fc12e01ff73ceacc07c84f9a
SHA1	0805d0ae62f5358b9a3f4c1868d552f5c3561b17
SHA256	27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
SHA512	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
Ssdeep	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/SQR/875+:prahGV6B
PEiD	None matched
Yara	• embedded_pe (Contains an embedded PE32 file) • embedded_win_api (A non-Windows executable contains win32 API • vmdetect (Possibly employs anti-virtualization techniques)
VirusTotal	Permalink VirusTotal Scan Date: 2013-12-27 06:51:52 Detection Rate: 32/46 (collapse)

An engineer is analyzing this Cuckoo Sandbox report for a PDF file that has been downloaded from an email. What is the state of this file?

A. The file was matched by PEiD threat signatures but no suspicious features are identified since the signature list is up to date.

B. The file has an embedded non-Windows executable but no suspicious features are identified.

C. The file has an embedded Windows 32 executable and the Yara field lists suspicious features for further analysis.

D. The file has an embedded executable and was matched by PEiD threat signatures for further analysis.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 61

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

A. HTTP status code

B. destination IP address

C. URI

D. TCP ACK

Answer: C (LEAVE A REPLY)

NEW QUESTION: 62
What should an engineer use to aid the trusted exchange of public keys between user tom0411976943 and dan1968754032?
A. trusted certificate authorities
B. registration authority data
C. central key management server
D. web of trust
Answer: (SHOW ANSWER)

NEW QUESTION: 63
What is the difference between a threat and a risk?
A. Threat represents a potential danger that could take advantage of a weakness in a system
B. Risk represents the known and identified loss or danger in the system
C. Risk represents the nonintentional interaction with uncertainty in the system
D. Threat represents a state of being exposed to an attack or a compromise, either physically or logically.
Answer: A (LEAVE A REPLY)
Explanation
A threat is any potential danger to an asset. If a vulnerability exists but has not yet been exploited-or, more importantly, it is not yet publicly known-the threat is latent and not yet realized.

NEW QUESTION: 64
What is a difference between signature-based and behavior-based detection?
A. Behavior-based uses a known vulnerability database, while signature-based intelligently summarizes existing data.
B. Signature-based uses a known vulnerability database, while behavior-based intelligently summarizes existing data.
C. Behavior-based identifies behaviors that may be linked to attacks, while signature-based has a predefined set of rules to match before an alert.
D. Signature-based identifies behaviors that may be linked to attacks, while behavior-based has a predefined set of rules to match before an alert.

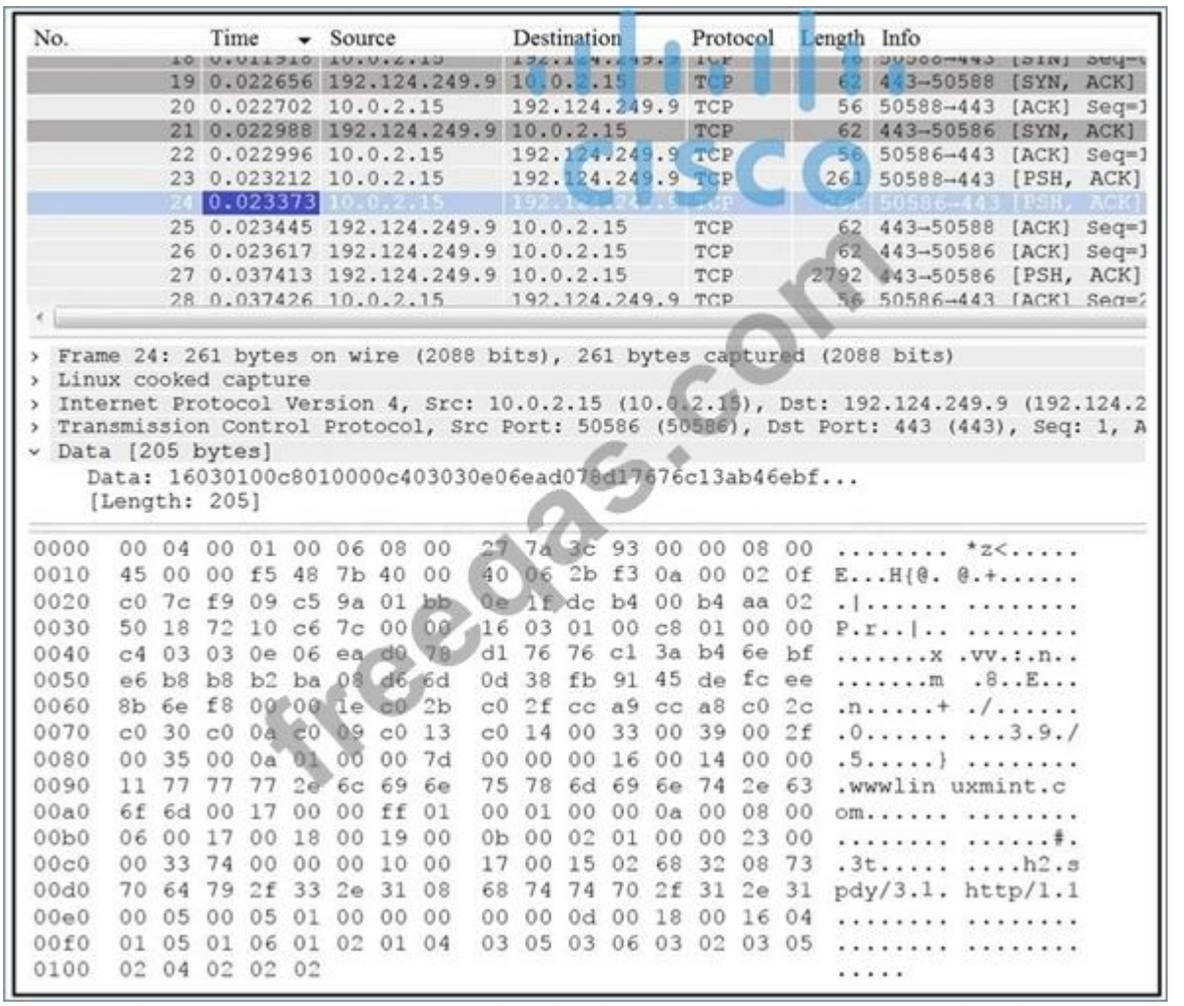
Answer: (SHOW ANSWER)

NEW QUESTION: 65
An engineer is investigating a case of the unauthorized usage of the "Tcpdump" tool. The analysis revealed that a malicious insider attempted to sniff traffic on a specific interface. What type of information did the malicious insider attempt to obtain?
A. all information and data within the datagram
B. tagged protocols being used on the network
C. tagged ports being used on the network
D. all firewall alerts and resulting mitigations
Answer: C (LEAVE A REPLY)

NEW QUESTION: 66
A malicious file has been identified in a sandbox analysis tool.

Which piece of information is needed to search for additional downloads of this file by other hosts?
A. file hash value
B. file size
C. file type
D. file name
Answer: A (LEAVE A REPLY)

NEW QUESTION: 67
Refer to the exhibit.



Which application protocol is in this PCAP file?

A. TLS

B. TCP

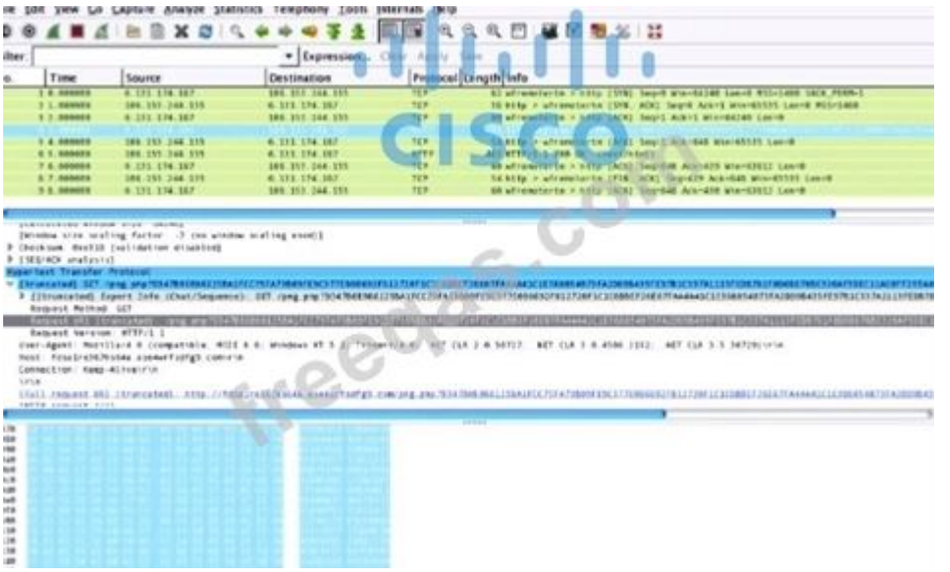
C. SSH

D. HTTP

Answer: B (LEAVE A REPLY)

NEW QUESTION: 68

Refer to the exhibit.



What is shown in this PCAP file?

A. The protocol is TCP.

B. Timestamps are indicated with error.

C. The User-Agent is Mozilla/5.0.

D. The HTTP GET is encoded.

Answer: (SHOW ANSWER)

NEW QUESTION: 69

Refer to the exhibit.

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

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

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

A. NetFlow

B. proxy

C. IDS/IPS

D. firewall

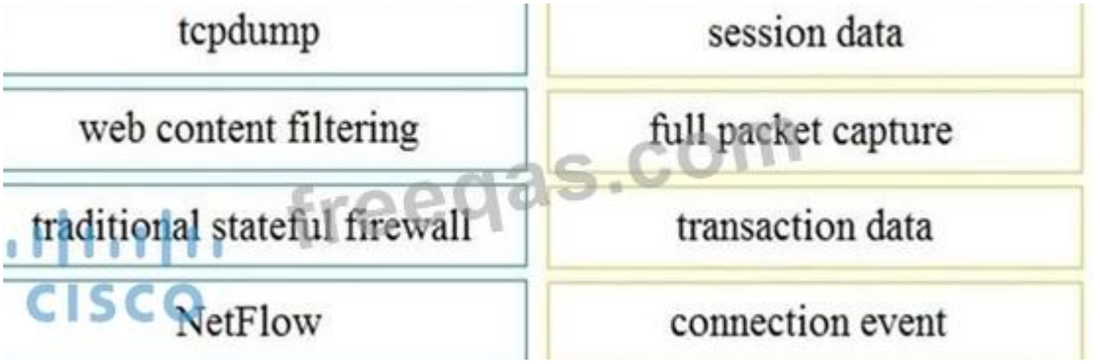
Answer: D (LEAVE A REPLY)

NEW QUESTION: 70

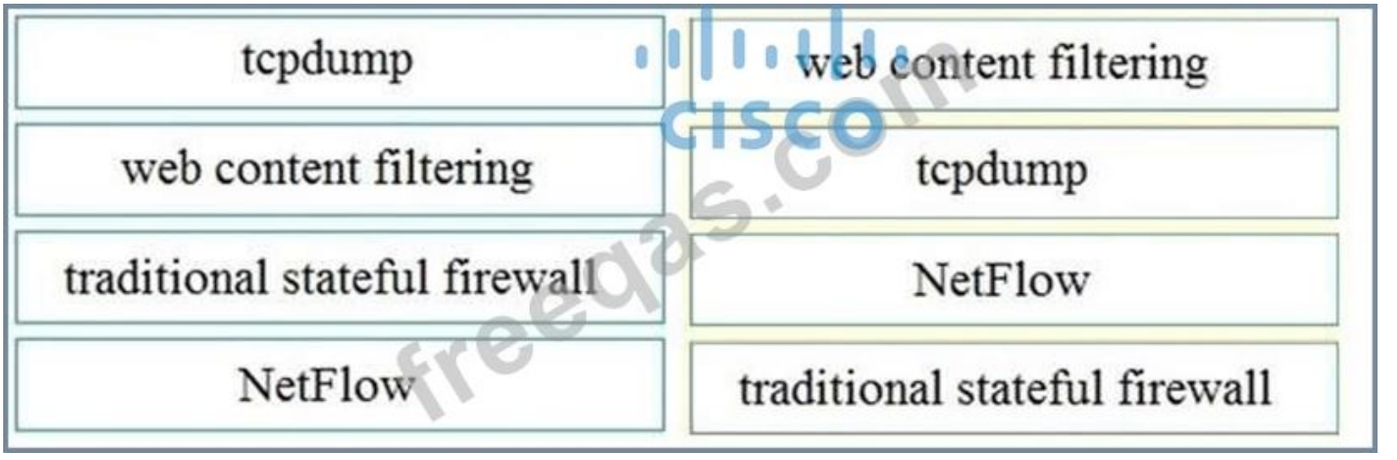
DRAG DROP

Drag and drop the technology on the left onto the data type the technology provides on the right.

Select and Place:



Answer:



NEW QUESTION: 71

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 Linux system

B. data from a DVD copied using Windows system

C. data from a CD copied using Windows

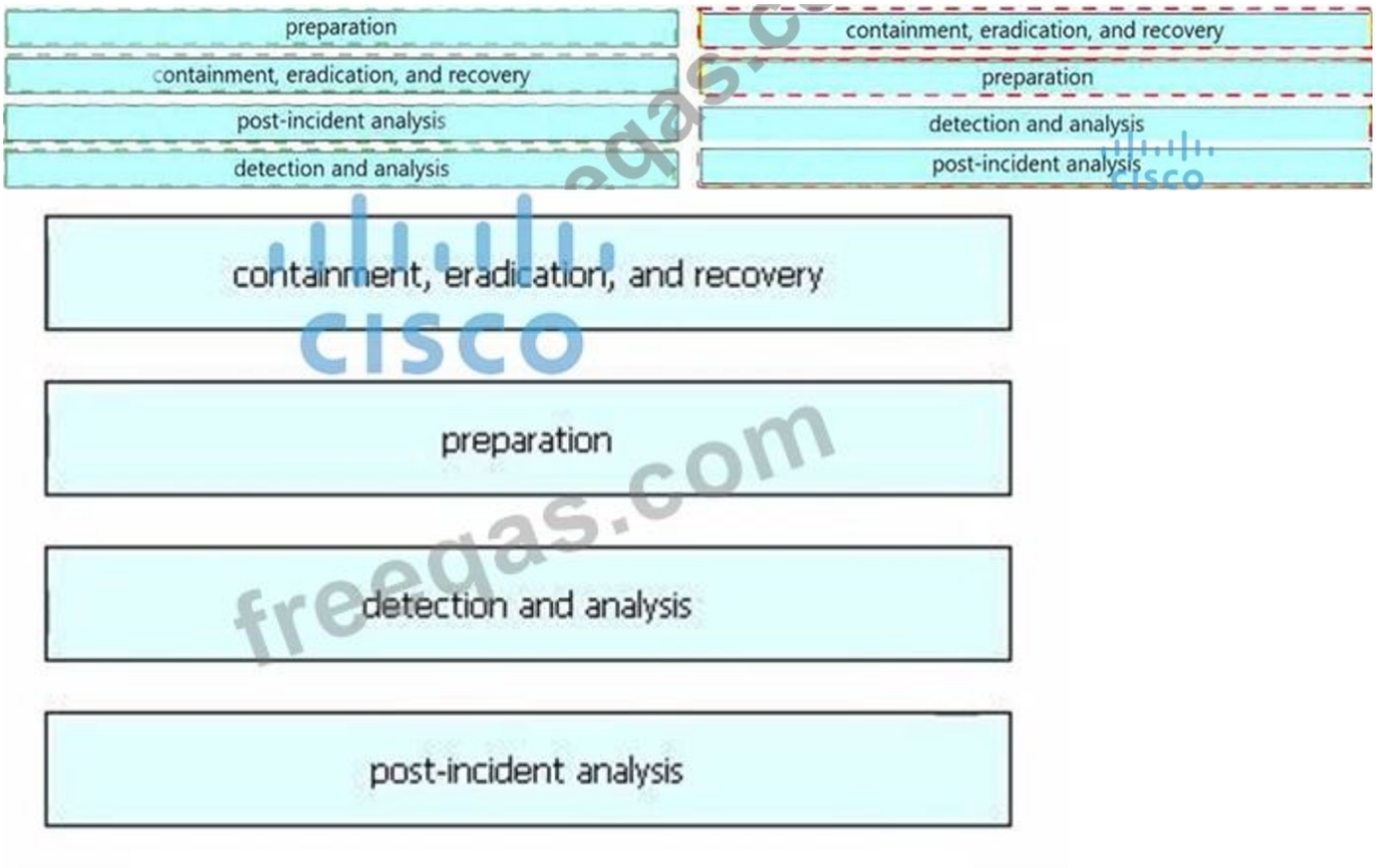
D. data from a CD copied using Mac-based system

Answer: A (LEAVE A REPLY)

NEW QUESTION: 72

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

Answer:



NEW QUESTION: 73

Which system monitors local system operation and local network access for violations of a security policy?

A. systems-based sandboxing

B. host-based intrusion detection

C. antivirus

D. host-based firewall

Answer: D (LEAVE A REPLY)

NEW QUESTION: 74

Refer to the exhibit. An employee received an email from an unknown sender with an attachment and reported it as a phishing attempt. An engineer uploaded the file to Cuckoo for further analysis. What should an engineer interpret from the provided Cuckoo report?
A. The file is clean and does not represent a risk.
B. Win32.polip.a.exe is an executable file and should be flagged as malicious.
C. Cuckoo cleaned the malicious file and prepared it for usage.
D. MD5 of the file was not identified as malicious.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 75
An analyst received an alert on their desktop computer showing that an attack was successful on the host.
After investigating, the analyst discovered that no mitigation action occurred during the attack.
What is the reason for this discrepancy?
A. The computer has a HIPS installed on it.
B. The computer has a NIPS installed on it.
C. The computer has a HIDS installed on it.
D. The computer has a NIDS installed on it.
Answer: (SHOW ANSWER)
Section: Host-Based Analysis

NEW QUESTION: 76
When an event is investigated, which type of data provides the investigate capability to determine if data exfiltration has occurred?
A. firewall logs
B. NetFlow data
C. session data
D. full packet capture
Answer: D (LEAVE A REPLY)

NEW QUESTION: 77

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. X 509 certificates

C. CA server

D. RADIUS server

Answer: B (LEAVE A REPLY)

NEW QUESTION: 78

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)

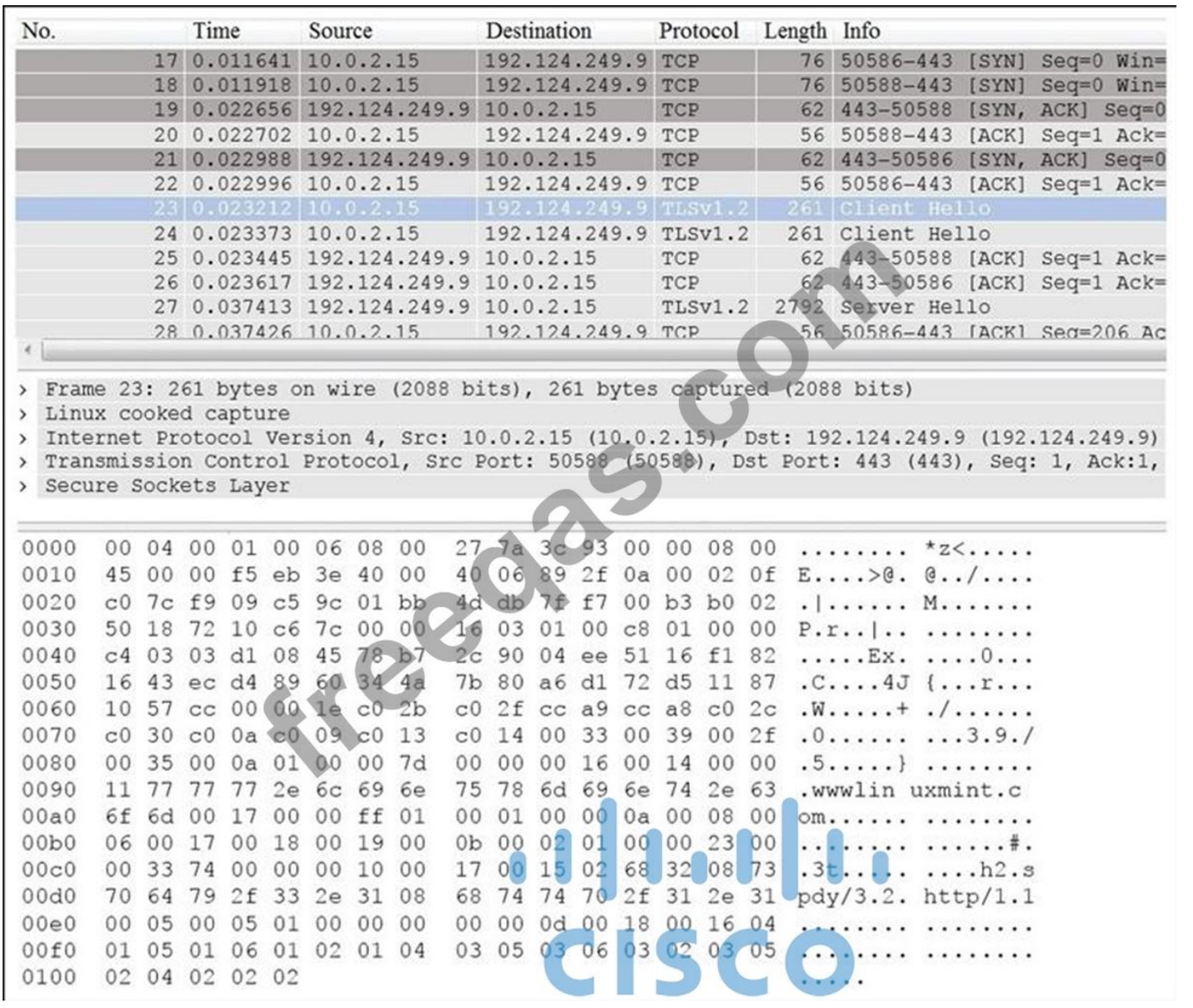
Explanation

Instead of searching for patterns linked to specific types of attacks, behavior-based IDS solutions monitor behaviors that may be linked to attacks, increasing the likelihood of identifying and mitigating a malicious action before the network is compromised.

https://accedian.com/blog/what-is-the-difference-between-signature-based-and-behavior-based-ids/

NEW QUESTION: 79

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

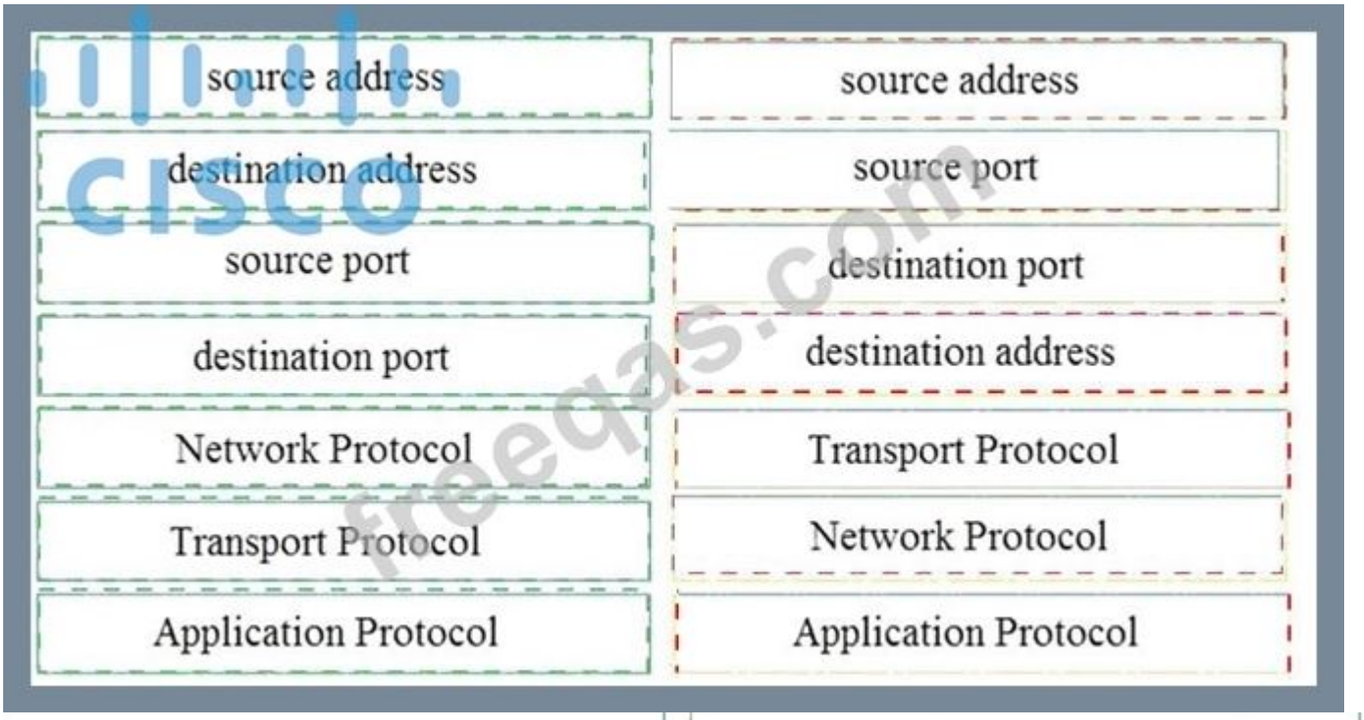
```
> Frame 23: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)
> Transmission Control Protocol, Src Port: 50588 (50588), Dst Port: 443 (443), Seq: 1, Ack:1,
> Secure Sockets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



source address
destination address
source port
destination port
Network Protocol
Transport Protocol
Application Protocol
source address
source port
destination port
destination address
Transport Protocol
Network Protocol
Application Protocol

NEW QUESTION: 80

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. Social Engineering

B. Piggybacking

C. Password Revelation Strategy

D. Phishing attack

Answer: (SHOW ANSWER)

NEW QUESTION: 81
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?
A. integrity
B. confidentiality
C. availability
D. scope
Answer: A (LEAVE A REPLY)

NEW QUESTION: 82
What is the difference between inline traffic interrogation and traffic mirroring?
A. Inline interrogation is less complex as traffic mirroring applies additional tags to data.
B. Inline replicates the traffic to preserve integrity rather than modifying packets before sending them to other analysis tools.
C. Traffic mirroring results in faster traffic analysis and inline is considerably slower due to latency.
D. Traffic mirroring copies the traffic rather than forwarding it directly to the analysis tools
Answer: A (LEAVE A REPLY)

NEW QUESTION: 83
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: (SHOW ANSWER)
Section: Network Intrusion Analysis
Explanation/Reference:

NEW QUESTION: 84
Refer to the exhibit.

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

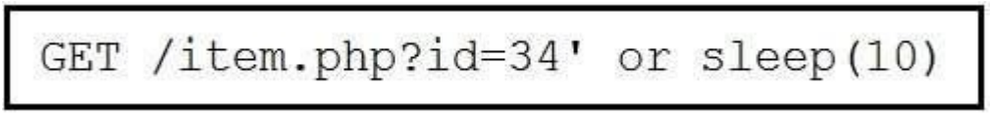
Which stakeholders must be involved when a company workstation is compromised?

A. Employee 2, Employee 3, Employee 4, Employee 5
B. Employee 1, Employee 2, Employee 4, Employee 5
C. Employee 4, Employee 6, Employee 7
D. Employee 1 Employee 2, Employee 3, Employee 4, Employee 5, Employee 7
Answer: A (LEAVE A REPLY)

NEW QUESTION: 85
Refer to the exhibit.

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

NEW QUESTION: 86



Refer to the exhibit. This request was sent to a web application server driven by a database.
Which type of web server attack is represented?
A. parameter manipulation
B. heap memory corruption
C. command injection
D. blind SQL injection
Answer: D (LEAVE A REPLY)
Section: Host-Based Analysis

NEW QUESTION: 87
A SOC analyst is investigating an incident that involves a Linux system that is identifying specific sessions.
Which identifier tracks an active program?
A. application identification number
B. active process identification number
C. runtime identification number
D. process identification number
Answer: D (LEAVE A REPLY)

Section: Host-Based Analysis

NEW QUESTION: 88
What is personally identifiable information that must be safeguarded from unauthorized access?
A. date of birth
B. driver's license number
C. gender
D. zip code
Answer: B (LEAVE A REPLY)
Section: Security Policies and Procedures

NEW QUESTION: 89
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 OSI configuration
B. incorrect snaplen configuration
C. incorrect UDP handshake
D. incorrect TCP handshake
Answer: D (LEAVE A REPLY)

NEW QUESTION: 90
How does TOR alter data content during transit?
A. It spoofs the destination and source information protecting both sides.
B. It redirects destination traffic through multiple sources avoiding traceability.
C. It traverses source traffic through multiple destinations before reaching the receiver
D. It encrypts content and destination information over multiple layers.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 91
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 port of an FTP server
B. running processes of the server
C. open ports of an email server
D. open ports of a web server
Answer: C (LEAVE A REPLY)

NEW QUESTION: 92
What is the difference between discretionary access control (DAC) and role-based access control (RBAC)?
A. DAC administrators pass privileges to users and groups, and in RBAC, permissions are applied to specific groups
B. DAC requires explicit authorization for a given user on a given object, and RBAC requires specific conditions.
C. RBAC access is granted when a user meets specific conditions, and in DAC, permissions are applied on user and group levels.
D. RBAC is an extended version of DAC where you can add an extra level of authorization based on time.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
Which type of data collection requires the largest amount of storage space?
A. alert data
B. transaction data
C. session data
D. full packet capture
Answer: D (LEAVE A REPLY)
Section: Network Intrusion Analysis

NEW QUESTION: 94
Which process is used when IPS events are removed to improve data integrity?
A. data availability

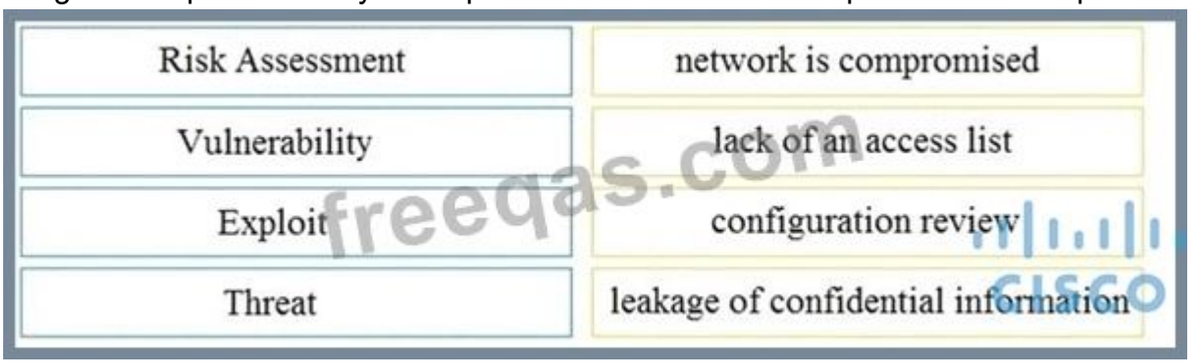
B. data normalization
C. data signature
D. data protection
Answer: B (LEAVE A REPLY)
Section: Security Concepts

NEW QUESTION: 95

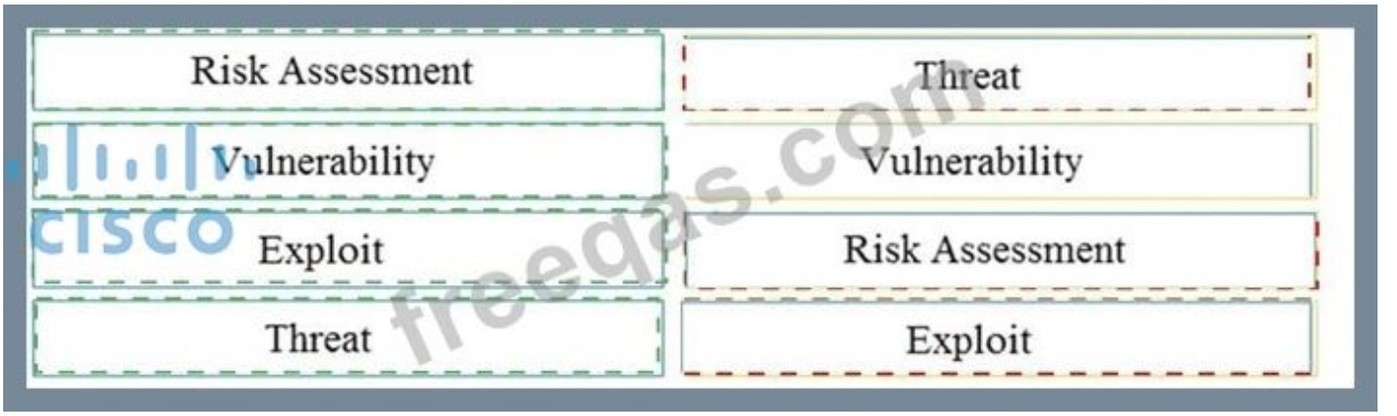
<IMG SRC=j%41vascript:alert('attack')>

Refer to the exhibit. Which kind of attack method is depicted in this string?
A. denial of service
B. SQL injection
C. man-in-the-middle
D. cross-site scripting
Answer: D (LEAVE A REPLY)

NEW QUESTION: 96
Drag and drop the security concept on the left onto the example of that concept on the right.



Answer:



NEW QUESTION: 97
What are two social engineering techniques? (Choose two.)
A. DDoS attack
B. man-in-the-middle
C. privilege escalation
D. pharming
E. phishing
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 98
Which evasion technique is a function of ransomware?
A. resource exhaustion
B. encryption
C. extended sleep calls
D. encoding
Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
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)
https://techdifferences.com/difference-between-steganography-and-cryptography.html#:~:text=The%20steganography%20and%20cryptography%20are,the%20structure%20of%20the%20message.

NEW QUESTION: 100
What ate two categories of DDoS attacks? (Choose two.)

A. direct
B. reflected
C. scanning
D. phishing
E. split brain
Answer: (SHOW ANSWER)

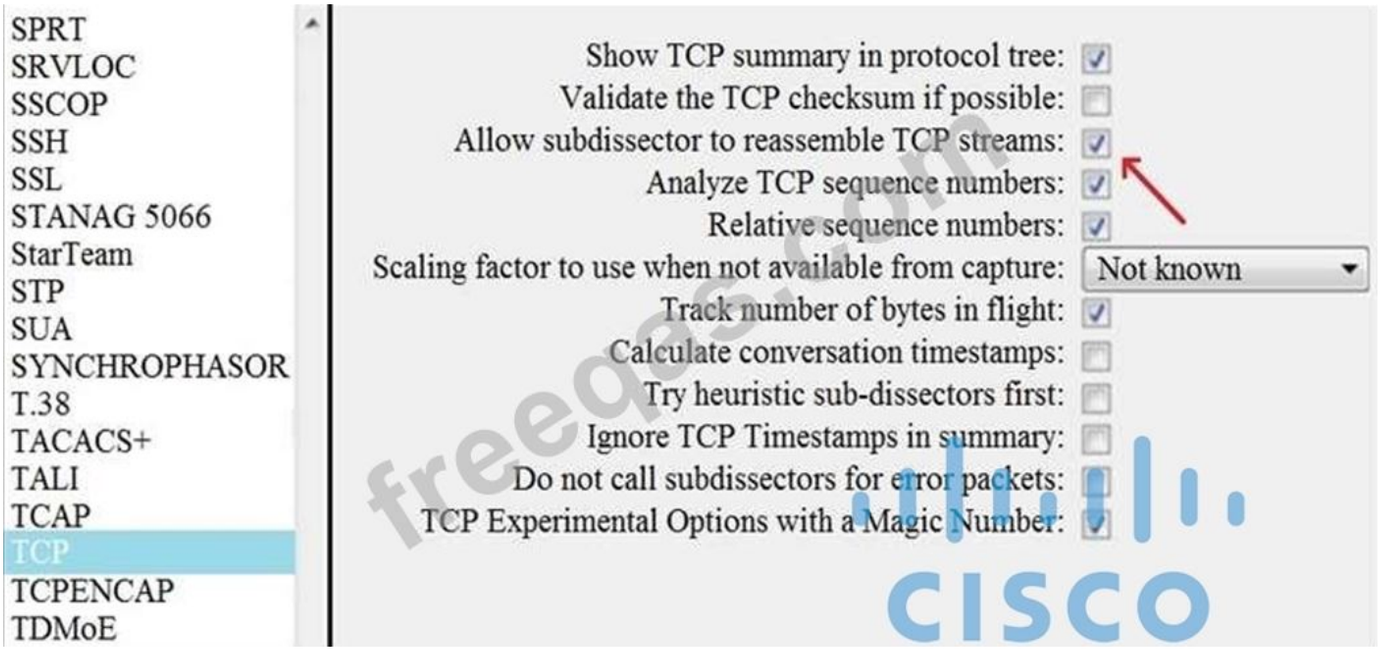
NEW QUESTION: 101
During which phase of the forensic process are tools and techniques used to extract information from the collected data?
A. examination
B. collection
C. investigation
D. reporting
Answer: (SHOW ANSWER)

NEW QUESTION: 102
What does cyber attribution identity in an investigation?
A. cause of an attack
B. vulnerabilities exploited
C. threat actors of an attack
D. exploit of an attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 103
Refer to the exhibit.

Which component is identifiable in this exhibit?
A. Trusted Root Certificate store on the local machine
B. Windows PowerShell verb
C. Windows Registry hive
D. local service in the Windows Services Manager
Answer: C (LEAVE A REPLY)
Explanation
https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives
https://ldapwiki.com/wiki/HKEY_LOCAL_MACHINE#:~:text=HKEY_LOCAL_MACHINE%20Windows%20

NEW QUESTION: 104



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: (SHOW ANSWER)

Section: Network Intrusion Analysis

NEW QUESTION: 105

Which security monitoring data type requires the largest storage space?

A. session data

B. transaction data

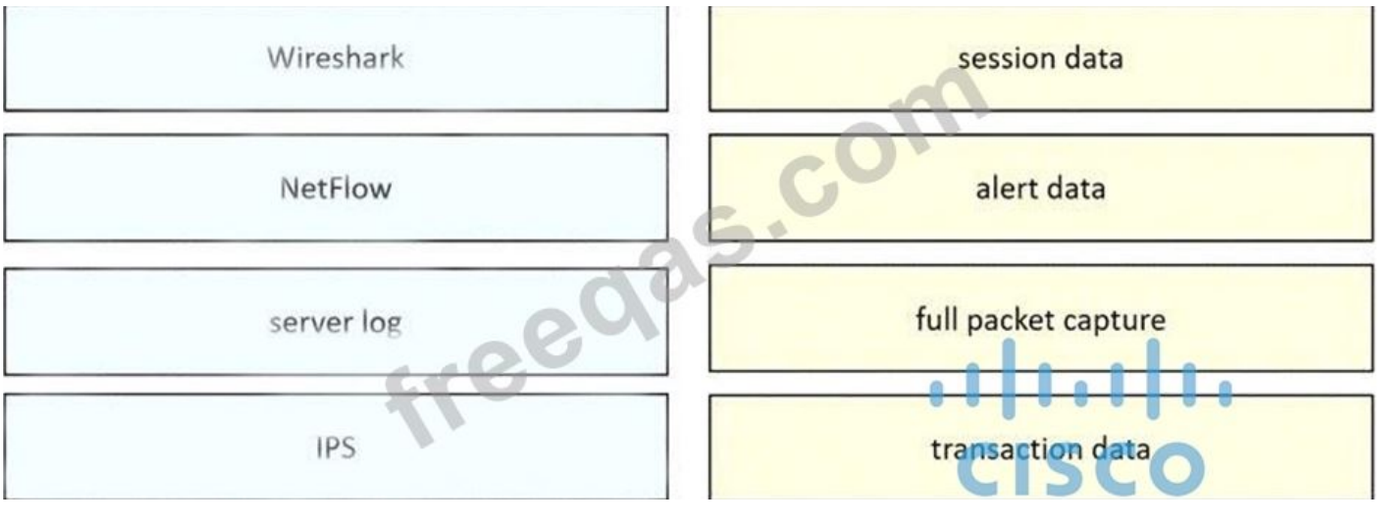
C. statistical data

D. full packet capture

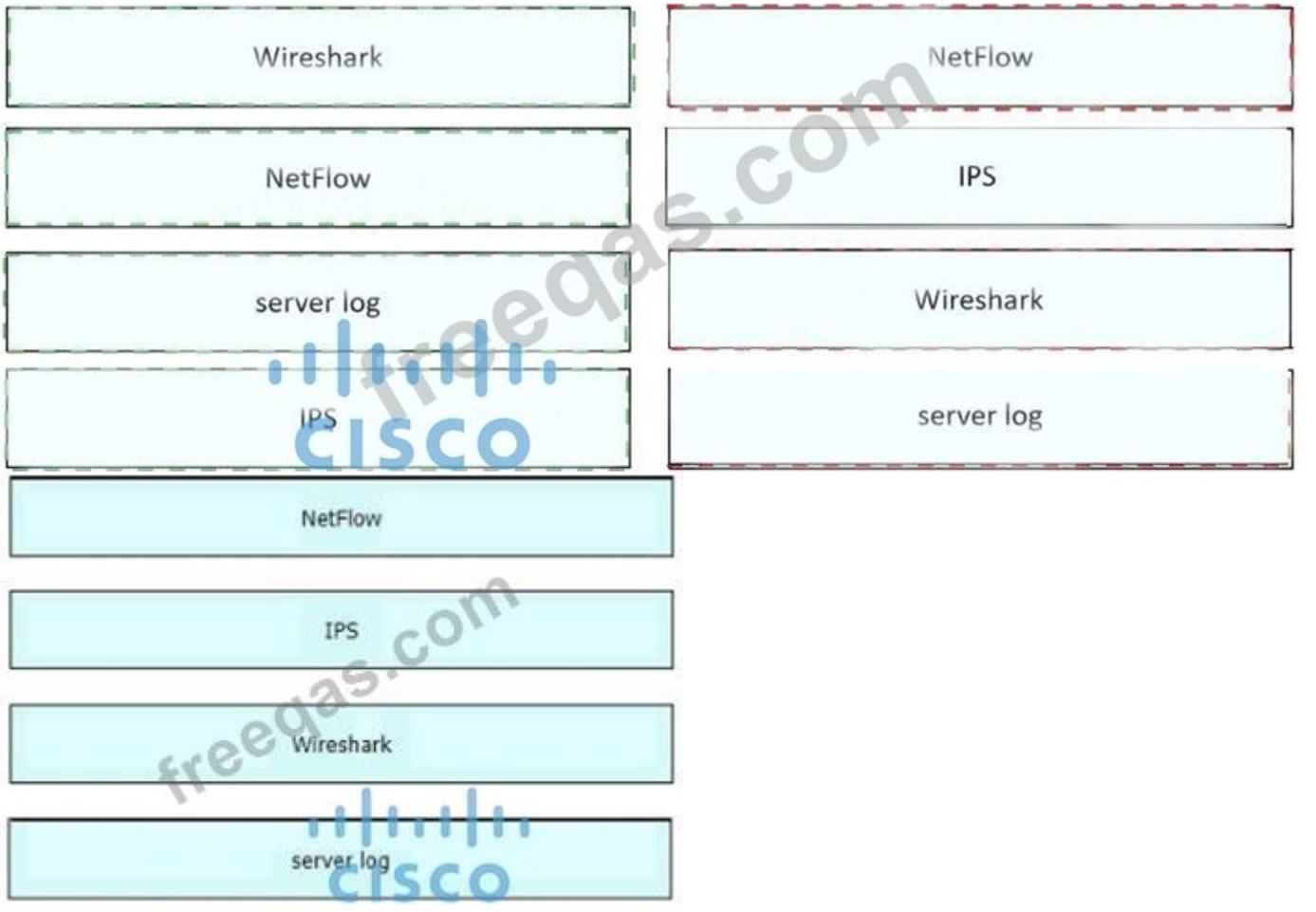
Answer: (SHOW ANSWER)

NEW QUESTION: 106

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

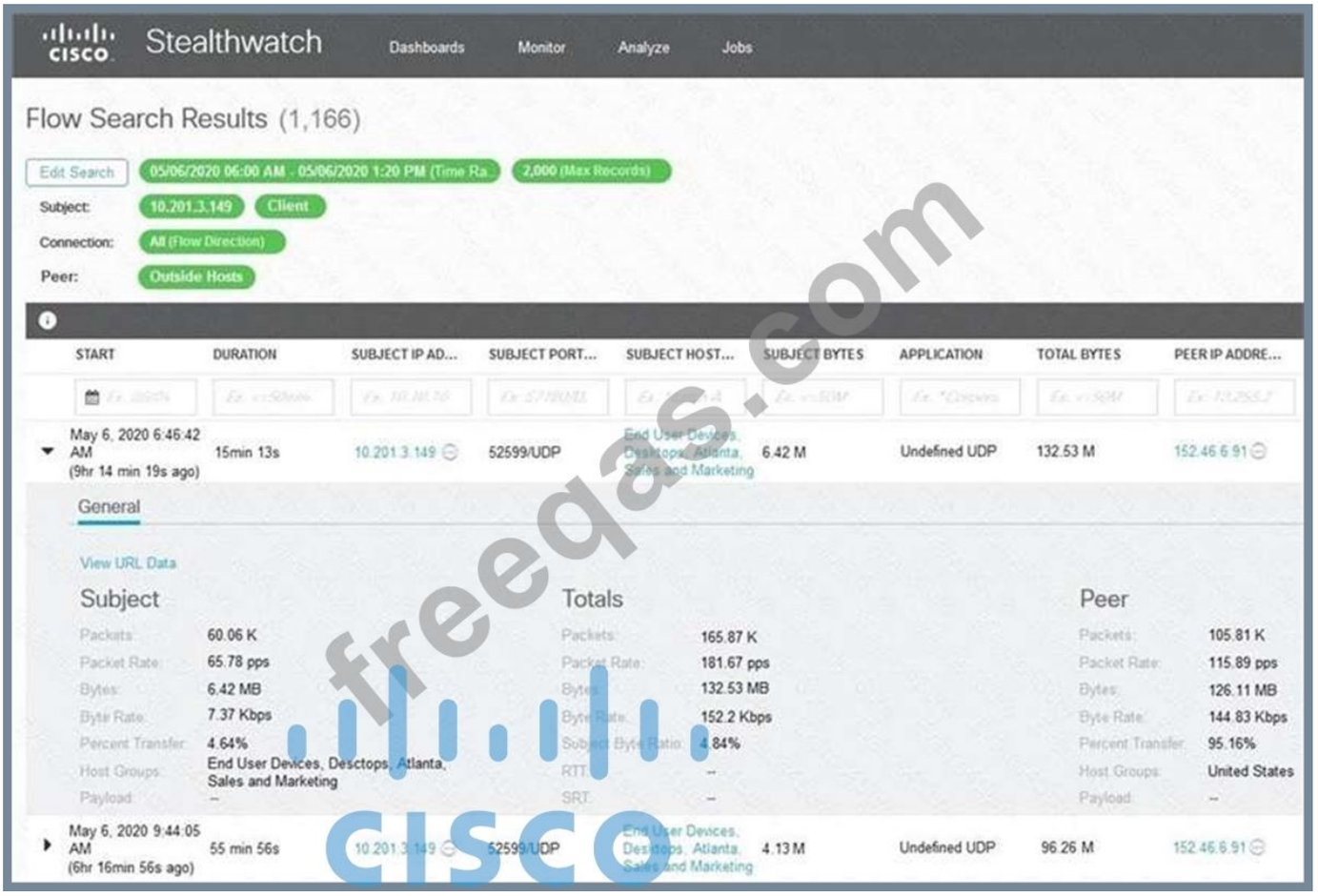


Answer:



NEW QUESTION: 107

Refer to the exhibit.



What is the potential threat identified in this Stealthwatch dashboard?

A. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.

B. Host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91.

C. Host 152.46.6.91 is being identified as a watchlist country for data transfer.

D. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 108

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

A. command and control

B. VLAN

C. subnet

D. botnet

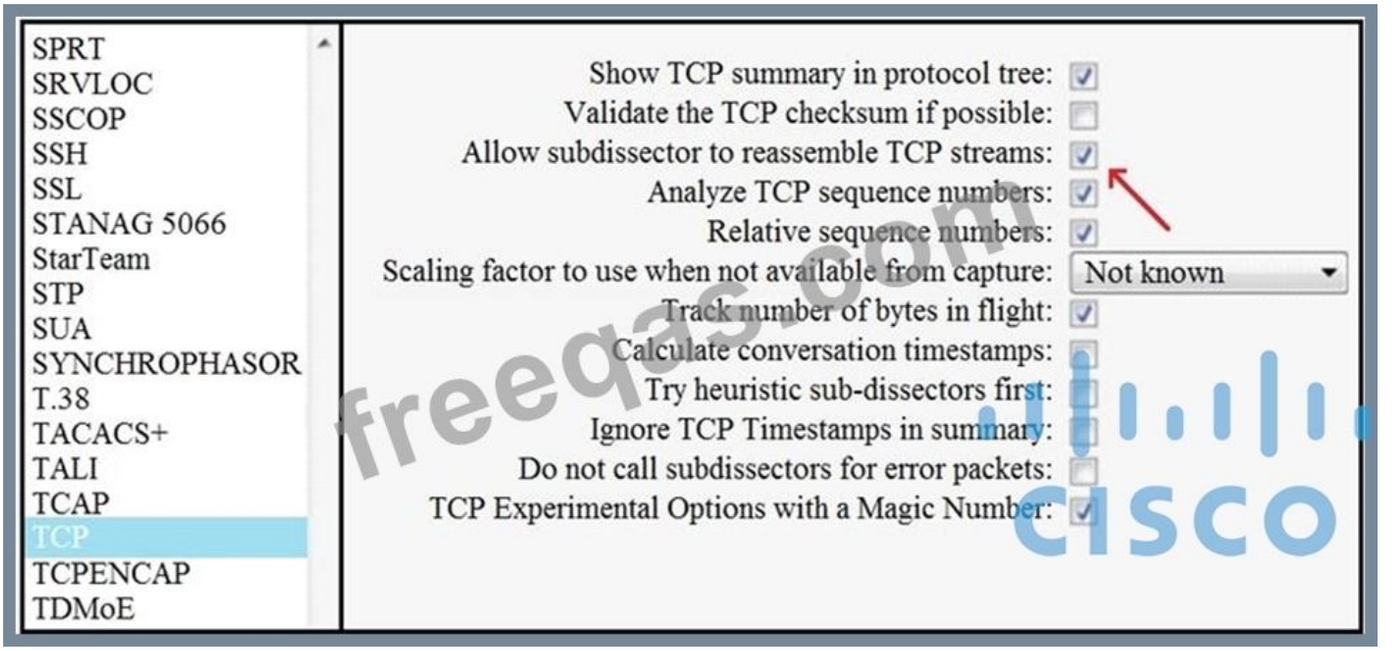
Answer: D (LEAVE A REPLY)

NEW QUESTION: 109
What is an incident response plan?
A. an organizational approach to events that could lead to asset loss or disruption of operations
B. an organizational approach to security management to ensure a service lifecycle and continuous improvements
C. an organizational approach to disaster recovery and timely restoration ot operational services
D. an organizational approach to system backup and data archiving aligned to regulations
Answer: C (LEAVE A REPLY)

NEW QUESTION: 110
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. vulnerability scoring
D. vulnerability management
E. risk assessment
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 111
What is a sandbox interprocess communication service?
A. A collection of rules within the sandbox that prevent the communication between sandboxes.
B. A collection of network services that are activated on an interface, allowing for inter-port communication.
C. A collection of interfaces that allow for coordination of activities among processes.
D. A collection of host services that allow for communication between sandboxes.
Answer: C (LEAVE A REPLY)
Explanation
Inter-process communication (IPC) allows communication between different processes. A process is one or more threads running inside its own, isolated address space.
https://docs.legato.io/16_10/basicIPC.html

NEW QUESTION: 112
Refer to the exhibit.



What is the expected result when the "Allow subdissector to reassemble TCP streams" feature is enabled?

A. extract a file from a packet capture

B. disable TCP streams

C. unfragment TCP

D. insert TCP subdissectors

Answer: C (LEAVE A REPLY)

NEW QUESTION: 113

What does cyber attribution identify in an investigation?

A. threat actors of an attack

B. exploit of an attack

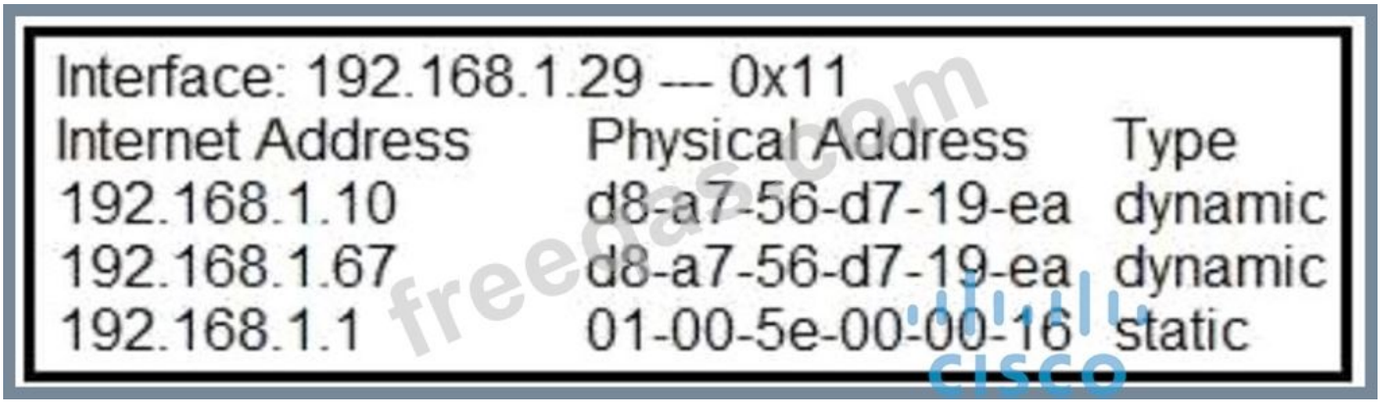
C. cause of an attack

D. vulnerabilities exploited

Answer: A (LEAVE A REPLY)

NEW QUESTION: 114

Refer to the exhibit.



What is occurring in this network?

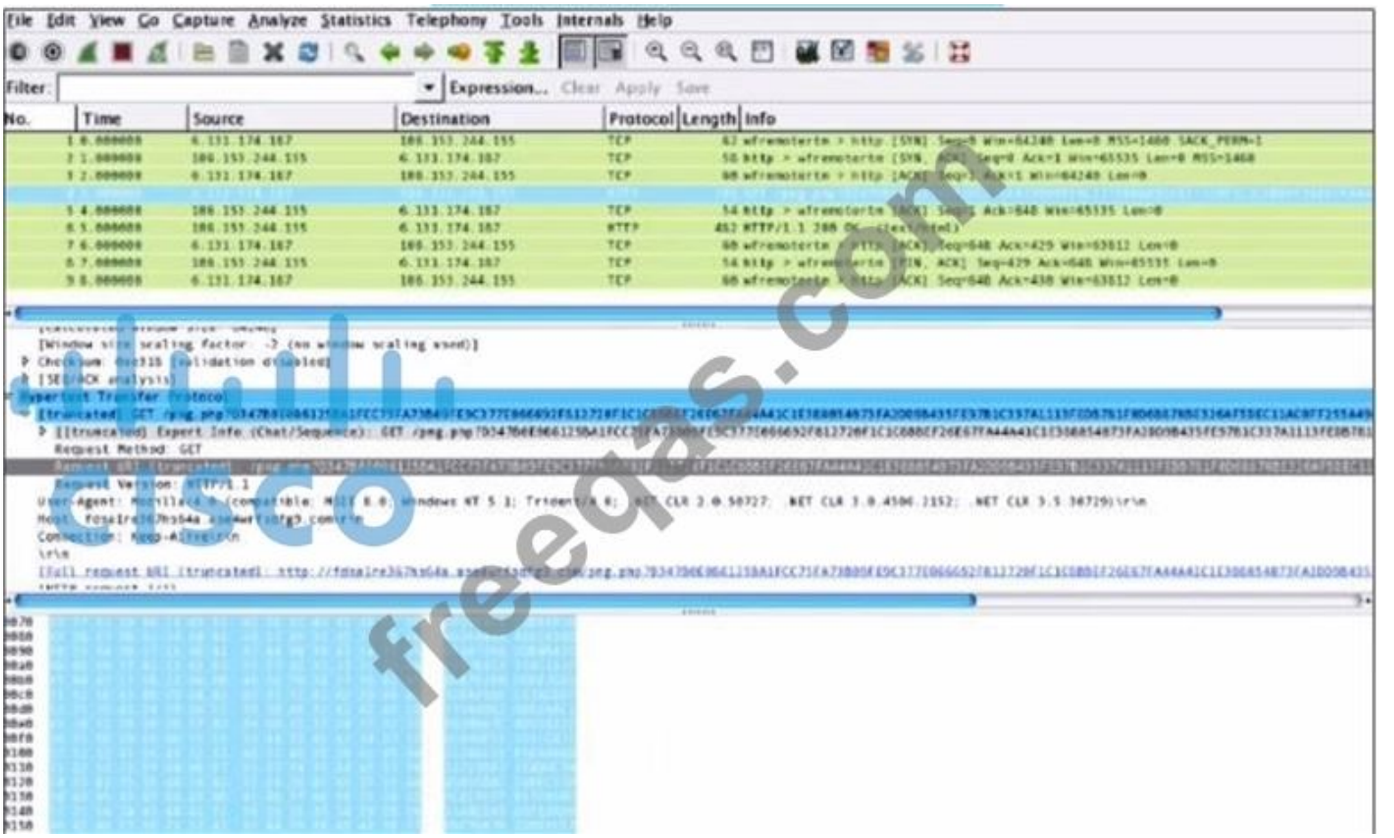
A. MAC address table overflow
B. ARP cache poisoning
C. DNS cache poisoning
D. MAC flooding attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 115
Which event is a vishing attack?
A. setting up a rogue access point near a public hotspot
B. obtaining disposed documents from an organization
C. impersonating a tech support agent during a phone call
D. using a vulnerability scanner on a corporate network
Answer: C (LEAVE A REPLY)

NEW QUESTION: 116
Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?
A. man-in-the-middle
B. known-plaintext
C. dictionary
D. replay
Answer: A (LEAVE A REPLY)

NEW QUESTION: 117
What does an attacker use to determine which network ports are listening on a potential target device?
A. man-in-the-middle
B. port scanning
C. SQL injection
D. ping sweep
Answer: (SHOW ANSWER)
Section: Security Concepts

NEW QUESTION: 118
Refer to the exhibit.



What is shown in this PCAP file?

A. Timestamps are indicated with error.

B. The HTTP GET is encoded.

C. The protocol is TCP.

D. The User-Agent is Mozilla/5.0.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 119

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

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

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

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

D. 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.

Answer: (SHOW ANSWER)

NEW QUESTION: 120

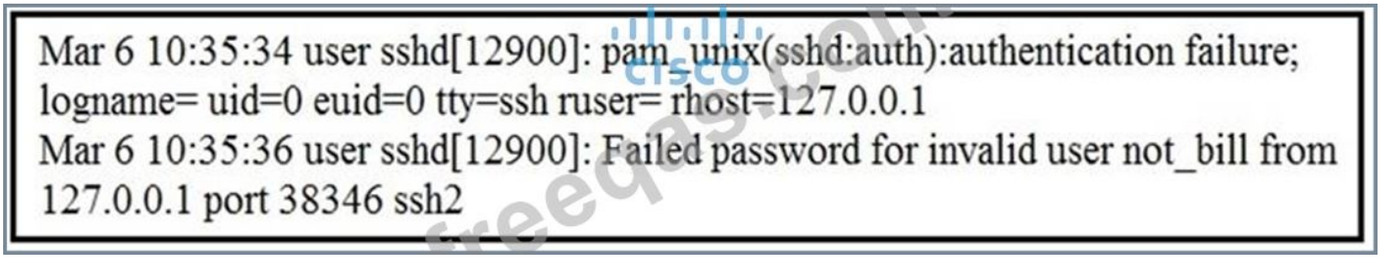
How is attacking a vulnerability categorized?

A. exploitation

B. action on objectives

C. installation
D. delivery
Answer: (SHOW ANSWER)

NEW QUESTION: 121
Refer to the exhibit.



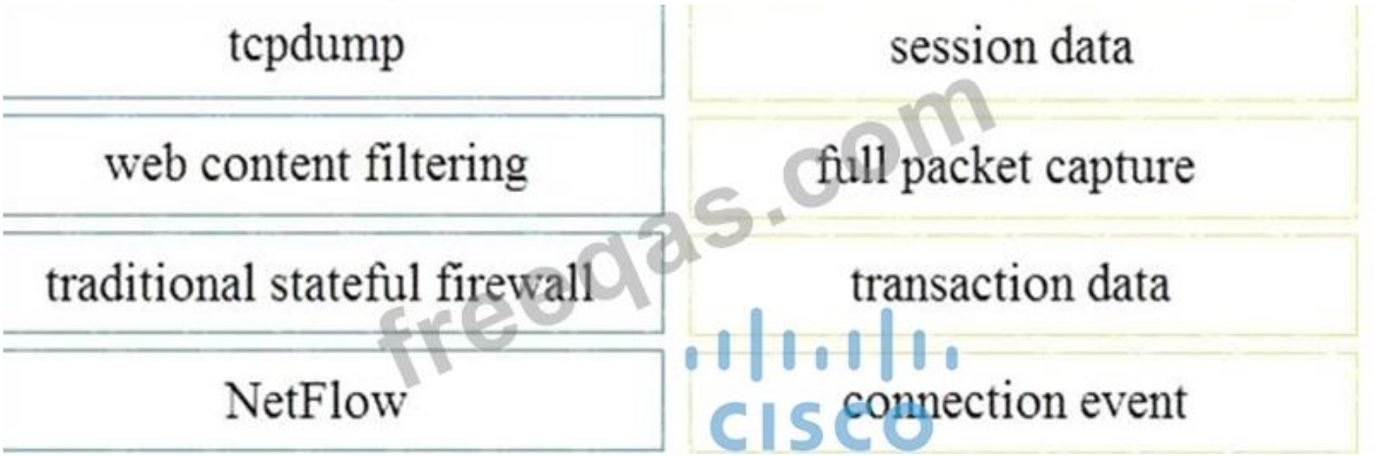
In which Linux log file is this output found?
A. /var/log/auth.log
B. /var/log/authorization.log
C. var/log/var.log
D. /var/log/dmesg
Answer: A (LEAVE A REPLY)

NEW QUESTION: 122
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)
Section: Security Monitoring

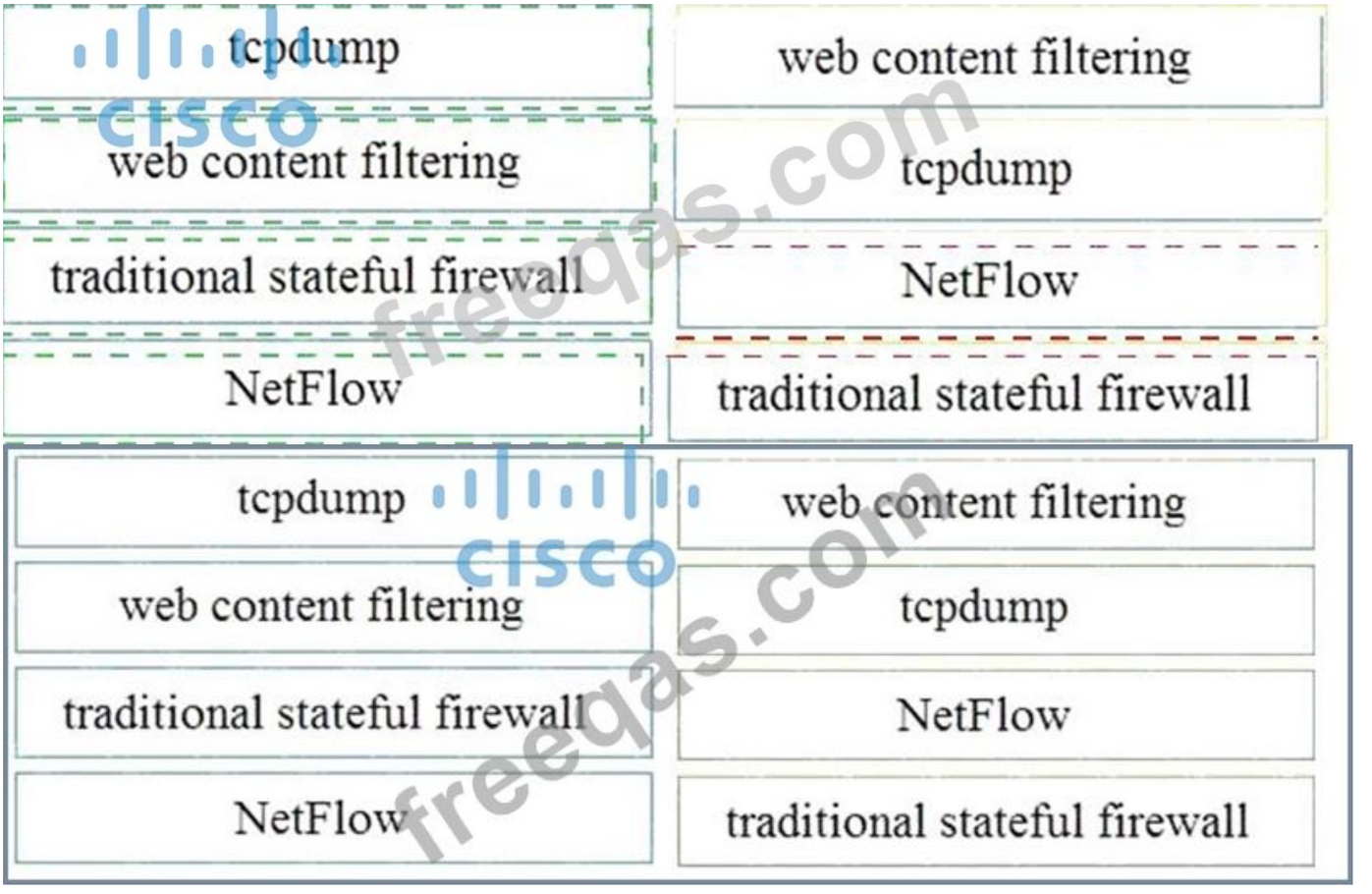
NEW QUESTION: 123
Which security principle requires more than one person is required to perform a critical task?
A. need to know

B. least privilege
C. due diligence
D. separation of duties
Answer: D (LEAVE A REPLY)

NEW QUESTION: 124
Drag and drop the technology on the left onto the data type the technology provides on the right.



Answer:



NEW QUESTION: 125
Refer to the exhibit.

```
lov 30 17:48:44 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
lov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
lov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
lov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
lov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
lov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
lov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
lov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
lov 30 17:48:49 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
lov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
lov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
lov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
lov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
lov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
lov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
lov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
lov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
lov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
lov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
lov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
lov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
lov 30 17:48:59 ip-172-31-27-153 sshd[23013]: Invalid user password from 218.26.11.11
```

A security analyst is investigating unusual activity from an unknown IP address Which type of evidence is this file1?

A. indirect evidence

B. direct evidence

C. best evidence

D. corroborative evidence

Answer: (SHOW ANSWER)

NEW QUESTION: 126

What does an attacker use to determine which network ports are listening on a potential target device?

A. man-in-the-middle

B. port scanning

C. SQL injection

D. ping sweep

Answer: (SHOW ANSWER)

Explanation/Reference:

NEW QUESTION: 127

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. 1986

B. 2318

C. 2542

D. 2317

Answer: C (LEAVE A REPLY)

NEW QUESTION: 128

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	80	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. tcpport = FTP

B. dstport == FTP

C. dstport = 21

D. tcp.port==21

Answer: A (LEAVE A REPLY)

NEW QUESTION: 129

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

A. Deep packet inspection gives insights up to Layer 7, and stateful inspection gives insights only up to Layer 4.

B. Deep packet inspection is more secure due to its complex signatures, and stateful inspection requires less human intervention.

C. Stateful inspection verifies data at the transport layer and deep packet inspection verifies data at the application layer

D. Stateful inspection is more secure due to its complex signatures, and deep packet inspection requires less human intervention.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 130

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: 131
What describes the concept of data consistently and readily being accessible for legitimate users?
A. accessibility
B. availability
C. integrity
D. confidentiality
Answer: B (LEAVE A REPLY)

NEW QUESTION: 132
What is the difference between the rule-based detection when compared to behavioral detection?
A. Behavioral systems are predefined patterns from hundreds of users, while Rule-Based only flags potentially abnormal patterns using signatures.
B. Rule-Based systems have established patterns that do not change with new data, while behavioral changes.
C. Rule-Based detection is searching for patterns linked to specific types of attacks, while behavioral is identifying per signature.
D. Behavioral systems find sequences that match a particular attack signature, while Rule-Based identifies potential attacks.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 133
Refer to the exhibit.


Top 10 Src IP Addr ordered by flows:

Date first seen	Duration	Src IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2019-11-30 06:45:50.990	1147.332	192.168.12.234	109183	202523	13.1 M	176	96116	68
2019-11-30 06:45:02.928	1192.834	10.10.151.203	62794	219715	25.9 M	184	182294	123
2019-11-30 06:59:24.563	330.110	192.168.28.173	27864	47943	2.2 M	145	55769	48

What information is depicted?
A. NetFlow data
B. IPS event data
C. IIS data
D. network discovery event
Answer: (SHOW ANSWER)

NEW QUESTION: 134
Which access control model does SELinux use?
A. RBAC

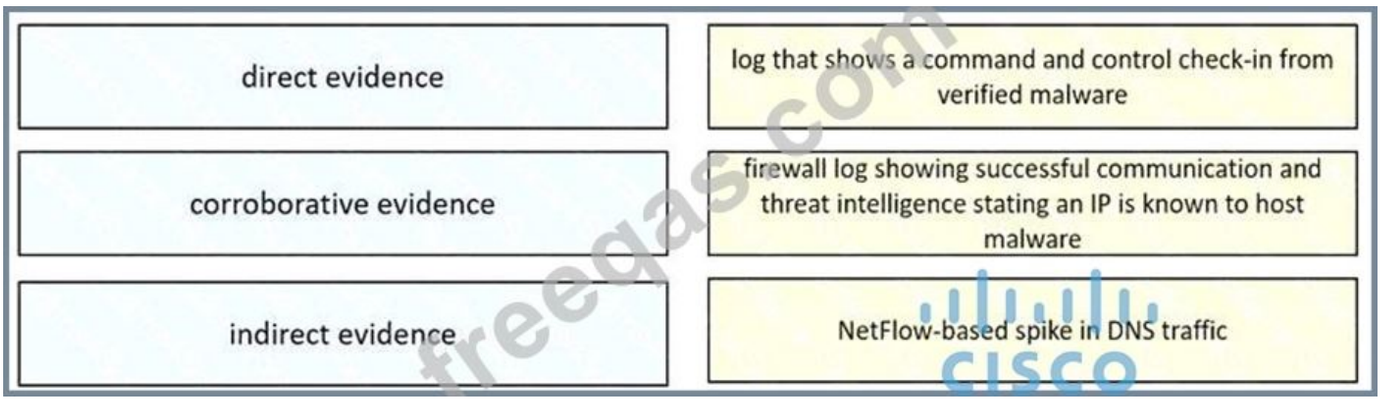
B. MAC
C. DAC
D. ABAC
Answer: (SHOW ANSWER)

NEW QUESTION: 135
What is the virtual address space for a Windows process?
A. set of virtual memory addresses that can be used
B. system-level memory protection feature built into the operating system
C. set of pages that reside in the physical memory
D. physical location of an object in memory
Answer: (SHOW ANSWER)

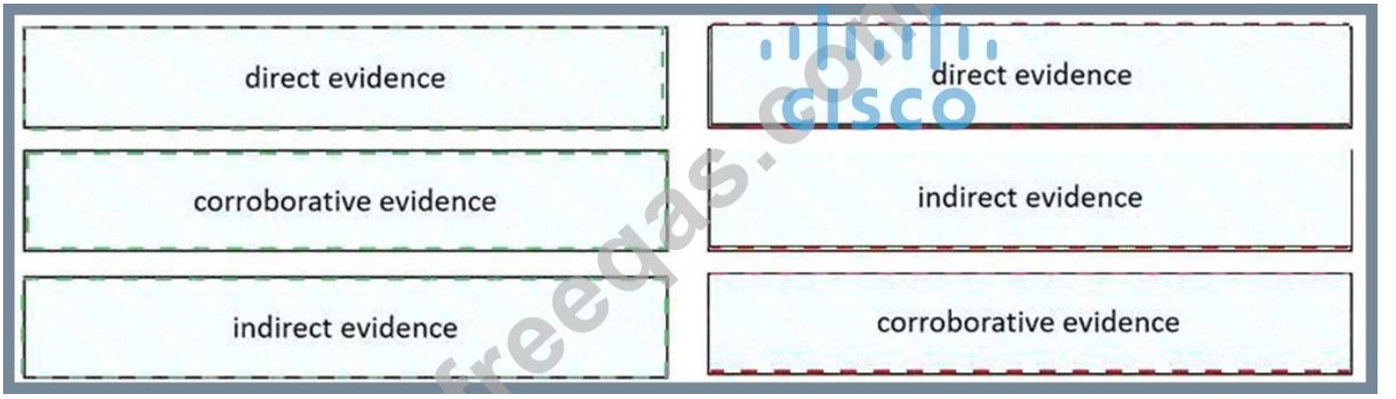
NEW QUESTION: 136
What is the principle of defense-in-depth?
A. Access control models are involved.
B. Several distinct protective layers are involved.
C. Authentication, authorization, and accounting mechanisms are used.
D. Agentless and agent-based protection for security are used.
Answer: (SHOW ANSWER)

NEW QUESTION: 137
What is the difference between mandatory access control (MAC) and discretionary access control (DAC)?
A. DAC is controlled by the operating system and MAC is controlled by an administrator
B. MAC is controlled by the discretion of the owner and DAC is controlled by an administrator
C. DAC is the strictest of all levels of control and MAC is object-based access
D. MAC is the strictest of all levels of control and DAC is object-based access
Answer: D (LEAVE A REPLY)

NEW QUESTION: 138
Drag and drop the type of evidence from the left onto the description of that evidence on the right.

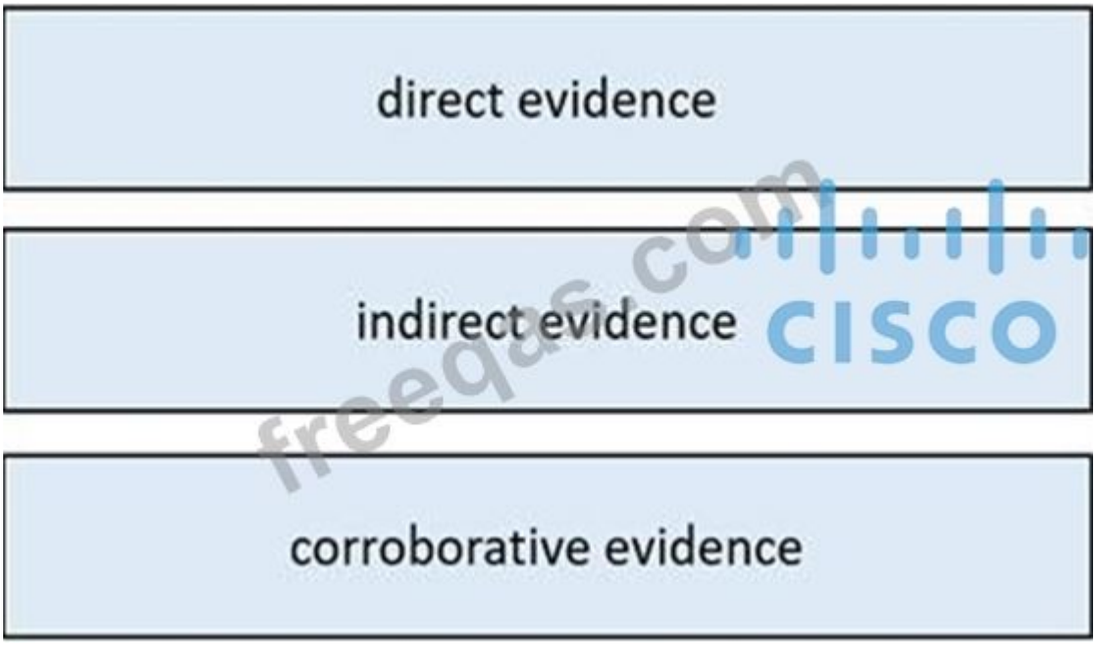


Answer:



Explanation

Graphical user interface, application Description automatically generated



NEW QUESTION: 139

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

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

D. Use NTFS partition for log file containment
Answer: (SHOW ANSWER)

NEW QUESTION: 140
What is the function of a command and control server?
A. It is used to regain control of the network after a compromise
B. It drops secondary payload into malware
C. It sends instruction to a compromised system
D. It enumerates open ports on a network device
Answer: (SHOW ANSWER)

NEW QUESTION: 141
What is the practice of giving an employee access to only the resources needed to accomplish their job?
A. need to know principle
B. separation of duties
C. organizational separation
D. principle of least privilege
Answer: D (LEAVE A REPLY)

NEW QUESTION: 142
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 DVD copied using Windows system
C. data from a CD copied using Linux system
D. data from a CD copied using Windows
Answer: C (LEAVE A REPLY)

NEW QUESTION: 143
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: 144
Which two compliance frameworks require that data be encrypted when it is transmitted over a public network?

(Choose two.)
A. COBIT
B. PCI
C. SOX
D. HIPAA
E. GLBA
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 145
What is an example of social engineering attacks?
A. receiving an email from human resources requesting a visit to their secure website to update contact information
B. sending a verbal request to an administrator who knows how to change an account password
C. receiving an invitation to the department's weekly WebEx meeting
D. receiving an unexpected email from an unknown person with an attachment from someone in the same company
Answer: (SHOW ANSWER)

NEW QUESTION: 146
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. output of routing protocol authentication failures and ports used
B. total throughput on the interface of the router and NetFlow records
C. deep packet captures of each application flow and duration
D. running processes on the applications and their total network usage
Answer: D (LEAVE A REPLY)

NEW QUESTION: 147
Which metric is used to capture the level of access needed to launch a successful attack?
A. user interaction
B. privileges required
C. attack vector
D. attack complexity
Answer: B (LEAVE A REPLY)

NEW QUESTION: 148
The security team has detected an ongoing spam campaign targeting the organization. The team's approach is to push back the cyber kill chain and mitigate ongoing incidents. At which phase of the cyber kill chain should the security team mitigate this type of attack?

A. actions
B. delivery
C. installation
D. reconnaissance
Answer: (SHOW ANSWER)

NEW QUESTION: 149

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	*

Refer to the exhibit. Which type of log is displayed?
A. IDS
B. proxy
C. NetFlow
D. sys
Answer: D (LEAVE A REPLY)
Section: Security Monitoring
Explanation

NEW QUESTION: 150
What is the difference between statistical detection and rule-based detection models?
A. Statistical detection involves the evaluation of an object on its intended actions before it executes that behavior
B. Rule-based detection defines legitimate data of users over a period of time and statistical detection defines it on an IF/THEN basis
C. Rule-based detection involves the collection of data in relation to the behavior of legitimate users over a period of time
D. Statistical detection defines legitimate data of users over a period of time and rule-based detection defines it on an IF/THEN basis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 151
Which two components reduce the attack surface on an endpoint? (Choose two.)
A. restricting USB ports
B. load balancing
C. secure boot
D. full packet captures at the endpoint
E. increased audit log levels
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 152
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.

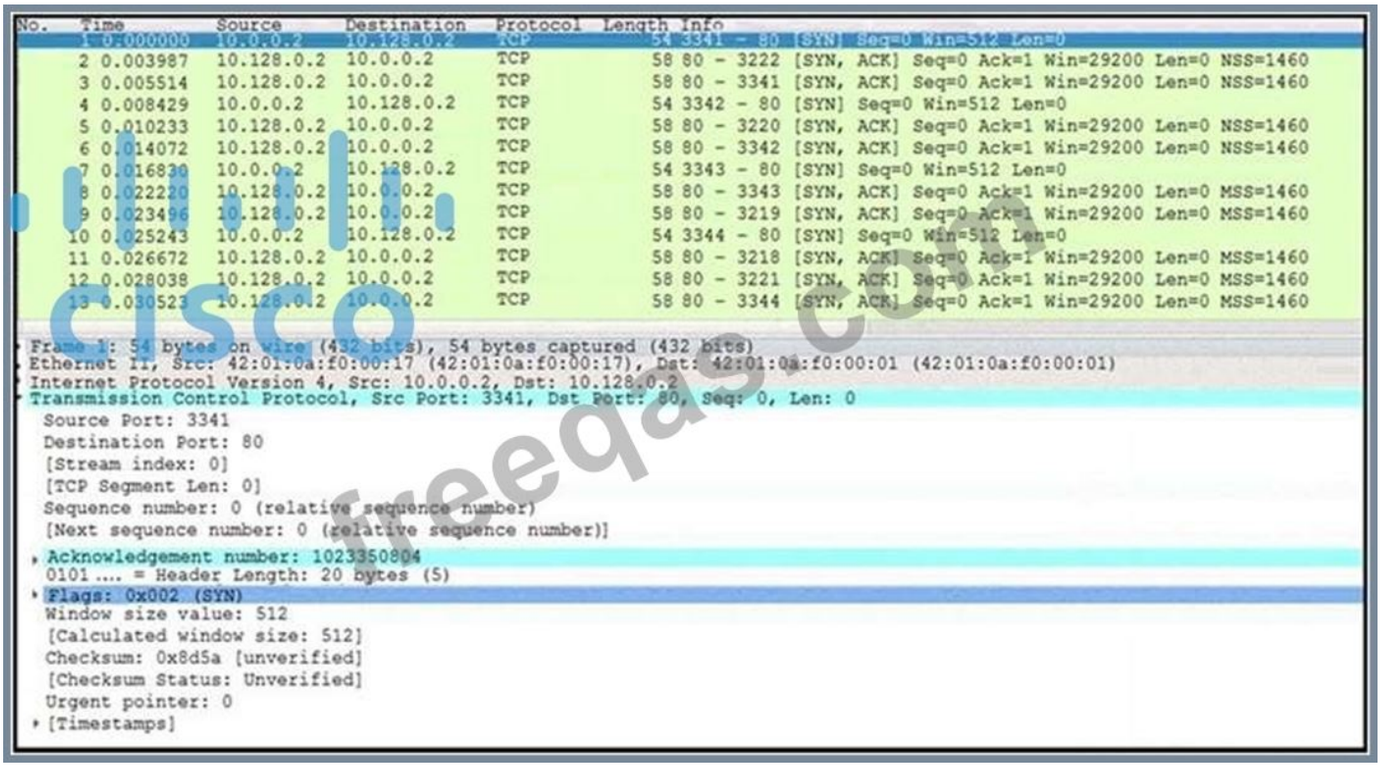
NEW QUESTION: 153
What is the difference between vulnerability and risk?
A. A risk is a potential threat that an exploit applies to, and a vulnerability represents the threat itself
B. A vulnerability represents a flaw in a security that can be exploited, and the risk is the potential damage it might cause.
C. A vulnerability is a sum of possible malicious entry points, and a risk represents the possibility of the unauthorized entry itself.
D. A risk is potential threat that adversaries use to infiltrate the network, and a vulnerability is an exploit
Answer: (SHOW ANSWER)

NEW QUESTION: 154
A security incident occurred with the potential of impacting business services. Who performs the attack?
A. threat actor
B. malware author
C. bug bounty hunter
D. direct competitor

Answer: A (LEAVE A REPLY)

NEW QUESTION: 155

Refer to the exhibit.



What is occurring in this network traffic?

A. Flood of ACK packets coming from a single source IP to multiple destination IPs.

B. Flood of SYN packets coming from a single source IP to a single destination IP.

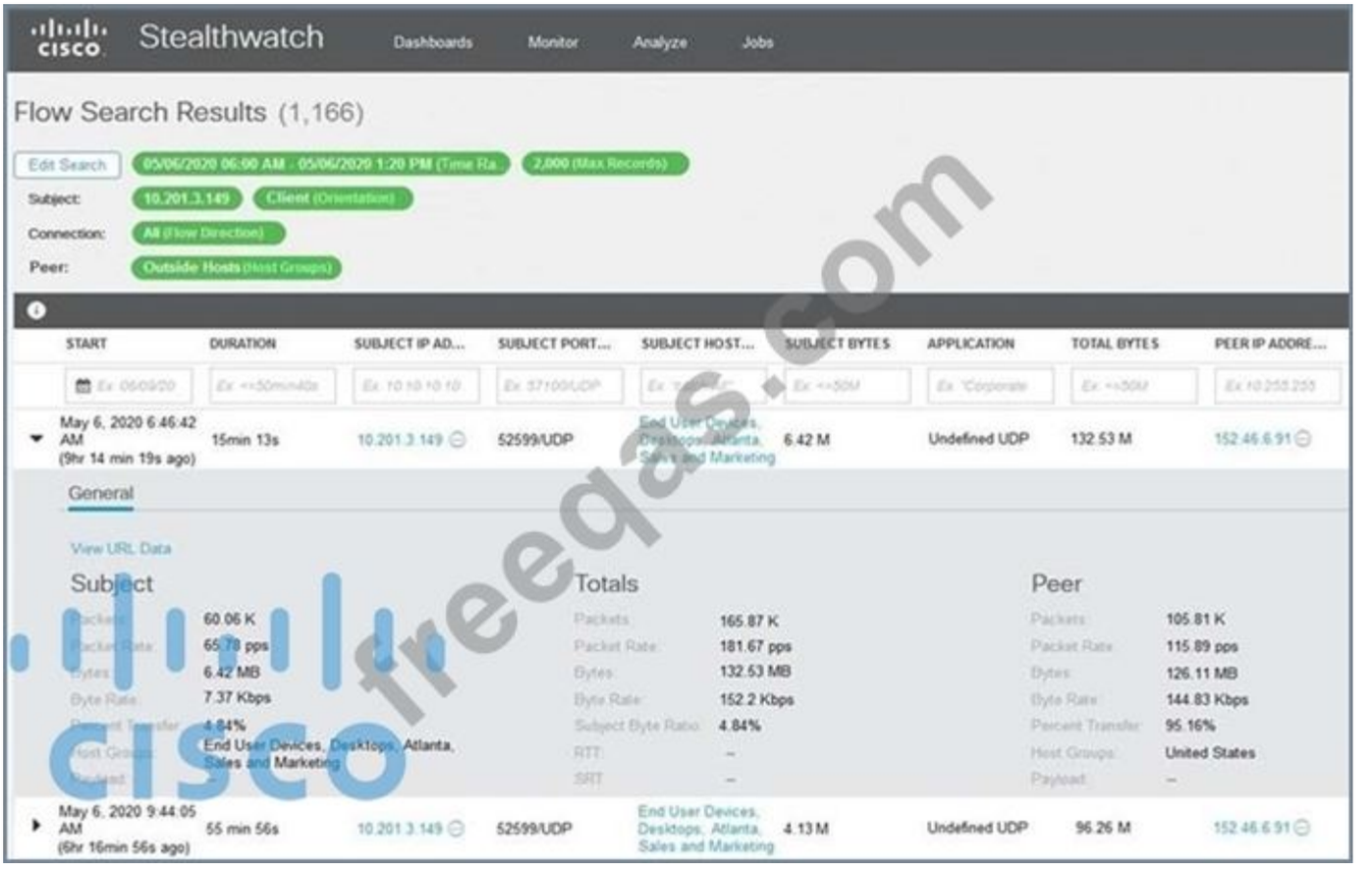
C. High rate of ACK packets being sent from a single source IP towards multiple destination IPs.

D. High rate of SYN packets being sent from a multiple source towards a single destination IP.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 156

Refer to the exhibit.



What is the potential threat identified in this Stealthwatch dashboard?

A. Host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91.

B. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.

C. Host 152.46.6.91 is being identified as a watchlist country for data transfer.

D. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 157

What is a difference between an inline and a tap mode traffic monitoring?

A. Inline mode monitors traffic path, examining any traffic at a wire speed, while a tap mode monitors traffic as it crosses the network.

B. Tap mode monitors packets and their content with the highest speed, while the inline mode draws a packet path for analysis.

C. Inline monitors traffic without examining other devices, while a tap mode tags traffic and examines the data from monitoring devices.

D. Tap mode monitors traffic direction, while inline mode keeps packet data as it passes through the monitoring devices.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 158

What is an attack surface as compared to a vulnerability?

A. any potential danger to an asset
B. the sum of all paths for data into and out of the application
C. an exploitable weakness in a system or its design
D. the individuals who perform an attack
Answer: B (LEAVE A REPLY)
Section: Security Monitoring

NEW QUESTION: 159
Which NIST IR category stakeholder is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies?
A. CSIRT
B. PSIRT
C. public affairs
D. management
Answer: D (LEAVE A REPLY)
Section: Security Policies and Procedures

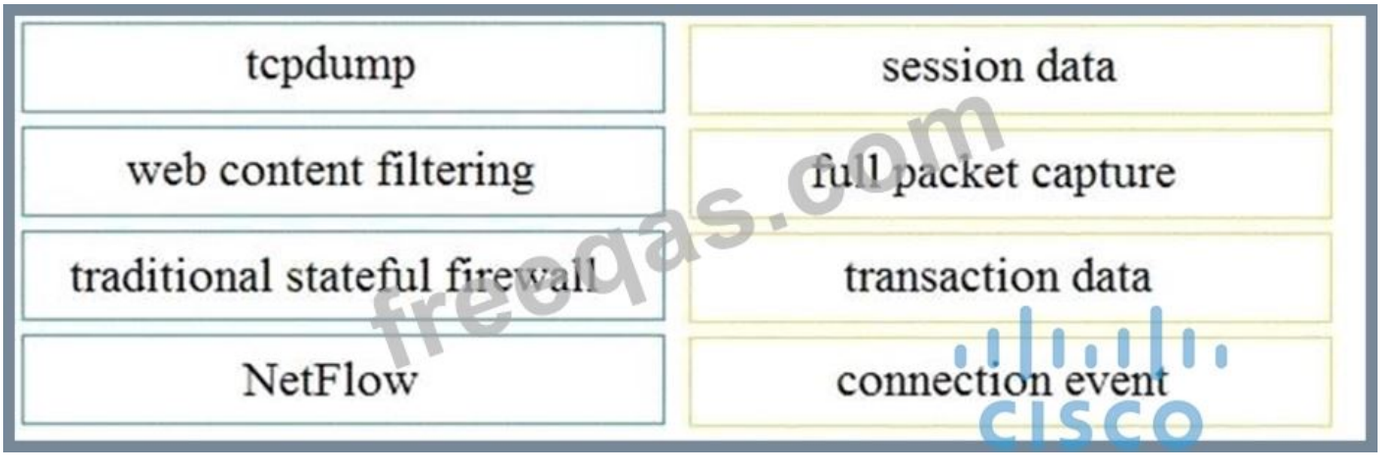
NEW QUESTION: 160
Which security principle is violated by running all processes as root or administrator?
A. principle of least privilege
B. role-based access control
C. separation of duties
D. trusted computing base
Answer: A (LEAVE A REPLY)
Section: Security Concepts

NEW QUESTION: 161

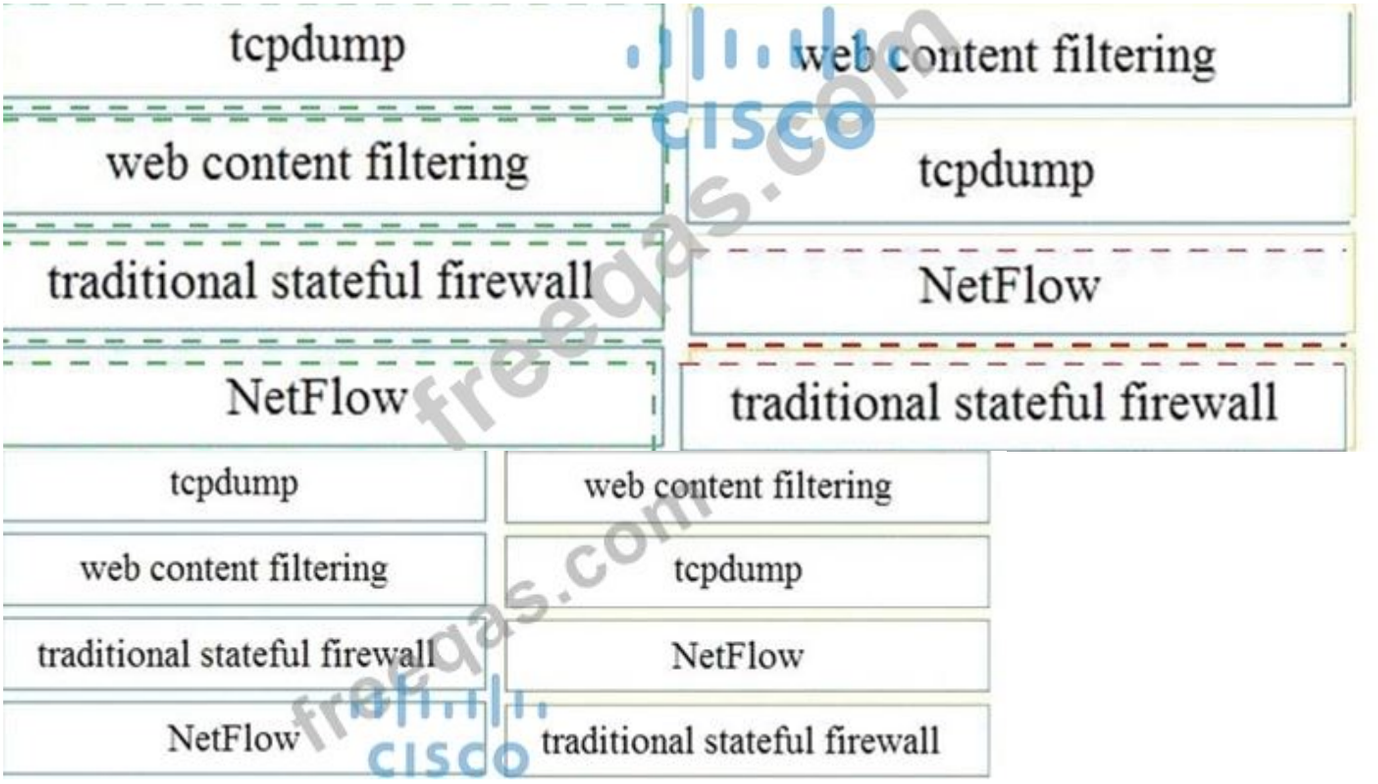
```
10.44.101.23 - - [20/Nov/2017:14:18:06 -0500] "GET / HTTP/1.1"
200 1254 "-" "Mozilla/5.0(X11; Ubuntu; Linux x86_64; rv:54.0)
Gecko/20100101 Firefox/54.0"
```

Refer to the exhibit. What does the message indicate?
A. an access attempt was made from the Mosaic web browser
B. a successful access attempt was made to retrieve the password file
C. a successful access attempt was made to retrieve the root of the website
D. a denied access attempt was made to retrieve the password file
Answer: C (LEAVE A REPLY)
Section: Host-Based Analysis

NEW QUESTION: 162
Drag and drop the technology on the left onto the data type the technology provides on the right.

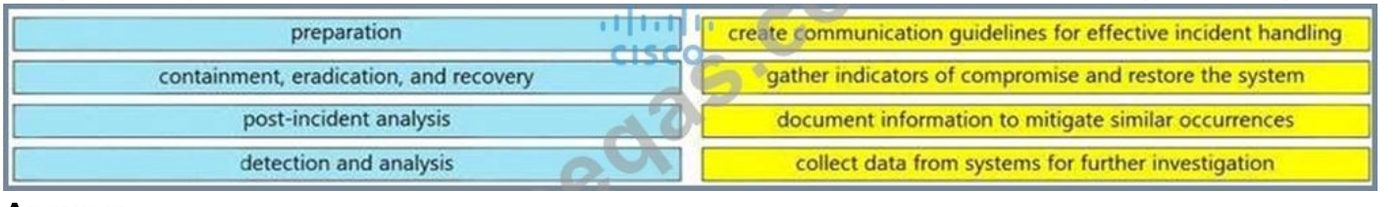


Answer:



NEW QUESTION: 163

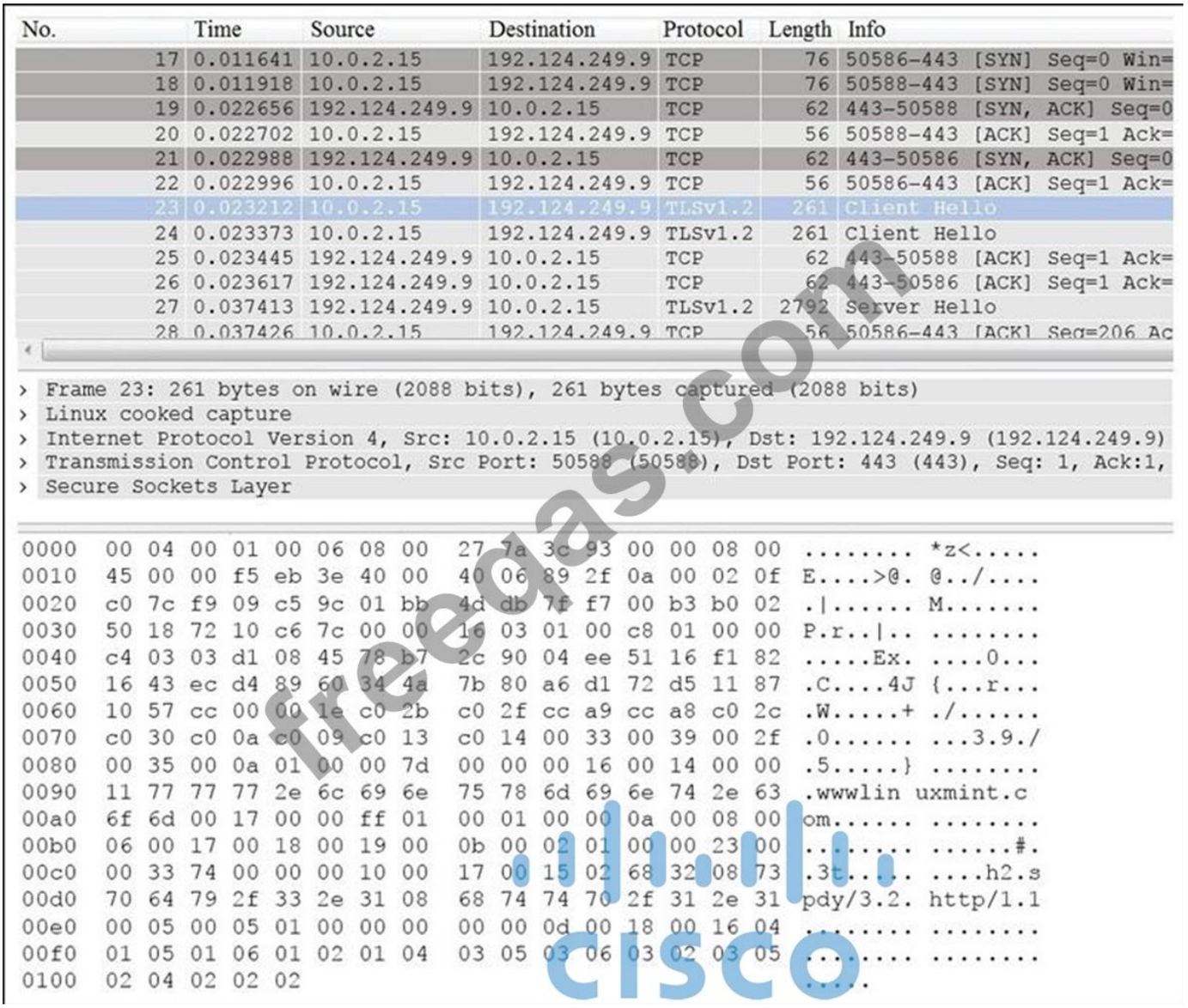
Drag and drop the elements from the left into the correct order for incident handling on the right.



Answer:

NEW QUESTION: 164

Refer to the exhibit.



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:

source address	source address
destination address	source port
source port	destination port
destination port	destination address
Network Protocol	Transport Protocol
Transport Protocol	Network Protocol
Application Protocol	Application Protocol