Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

About Exambible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1
What is a difference between 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

NEW QUESTION 2
What is the difference between the ACK flag and the RST flag in the NetFlow log session?

A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the datafor the payload is complete
B. The ACK flag confirms the beginning of the TCP connection, and the RST flag responds when the data for the payload is complete
C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection
D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

Answer: D

NEW QUESTION 3
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. permissions
B. PowerShell logs
C. service
D. MBR
E. process and thread

Answer: AC

NEW QUESTION 4
Which regex matches only on all lowercase letters?

A. [az]+
B. [^az]+
C. az+
D. a*z+

Answer: A

NEW QUESTION 5
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

Explanation:
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 6
Which incidence response step includes identifying all hosts affected by an attack?

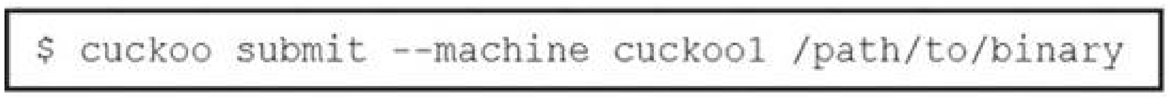
A. detection and analysis
B. post-incident activity
C. preparation
D. containment, eradication, and recovery

Answer: D

Explanation:
* 3.3.3 Identifying the Attacking Hosts During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts. Although this information can be important, incident handlers should generally stay focused on containment, eradication, and recovery.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

The response phase, or containment, of incident response, is the point at which the incident response team begins interacting with affected systems and attempts to keep further damage from occurring as a result of the incident.

NEW QUESTION 7
Refer to the exhibit.



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

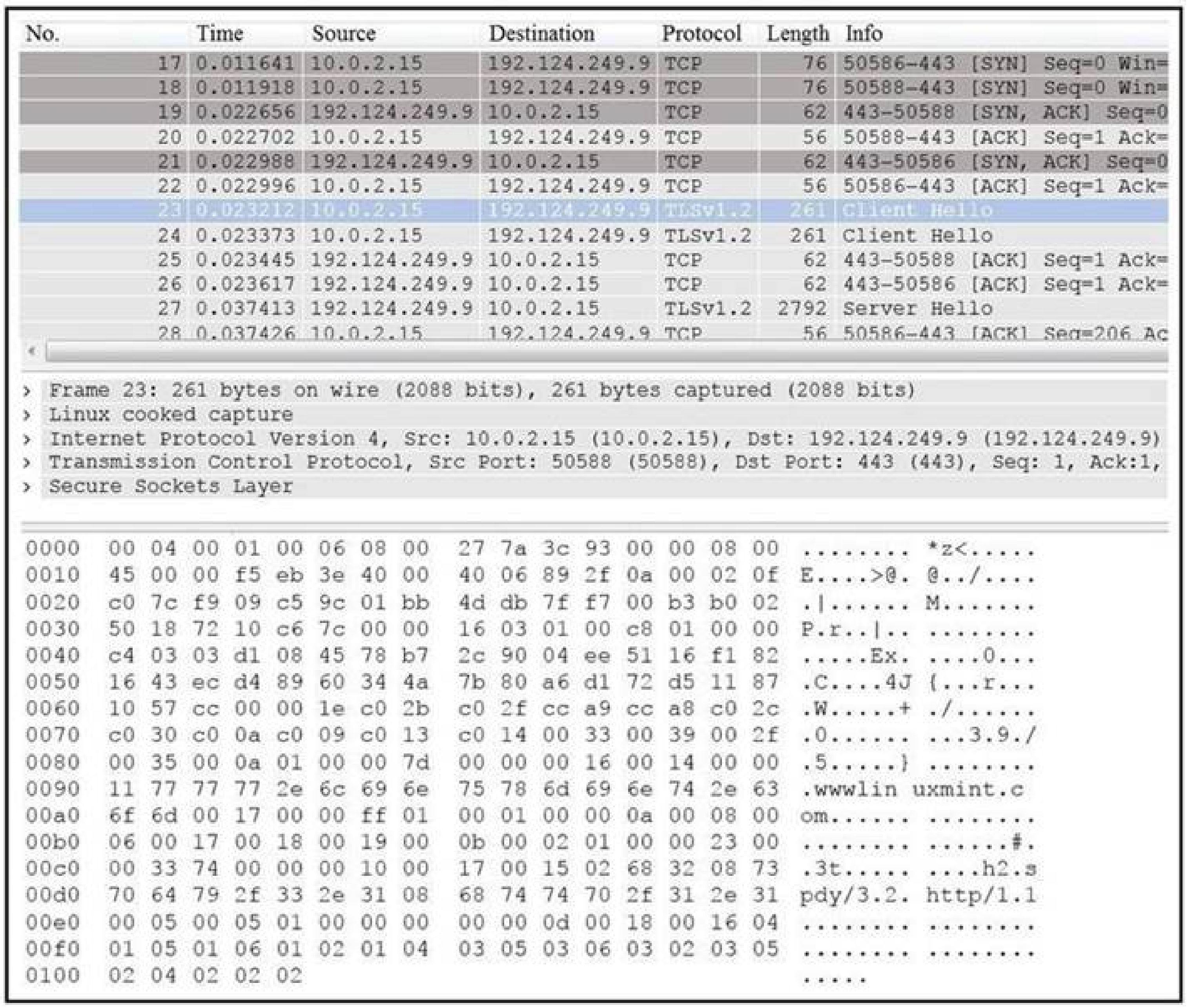
Which event is occurring?

A. A binary named "submit" is running on VM cuckoo1.
B. A binary is being submitted to run on VM cuckoo1
C. A binary on VM cuckoo1 is being submitted for evaluation
D. A URL is being evaluated to see if it has a malicious binary

Answer: B

Explanation:
https://cuckoo.readthedocs.io/en/latest/usage/submit/

NEW QUESTION 8
Refer to the exhibit.

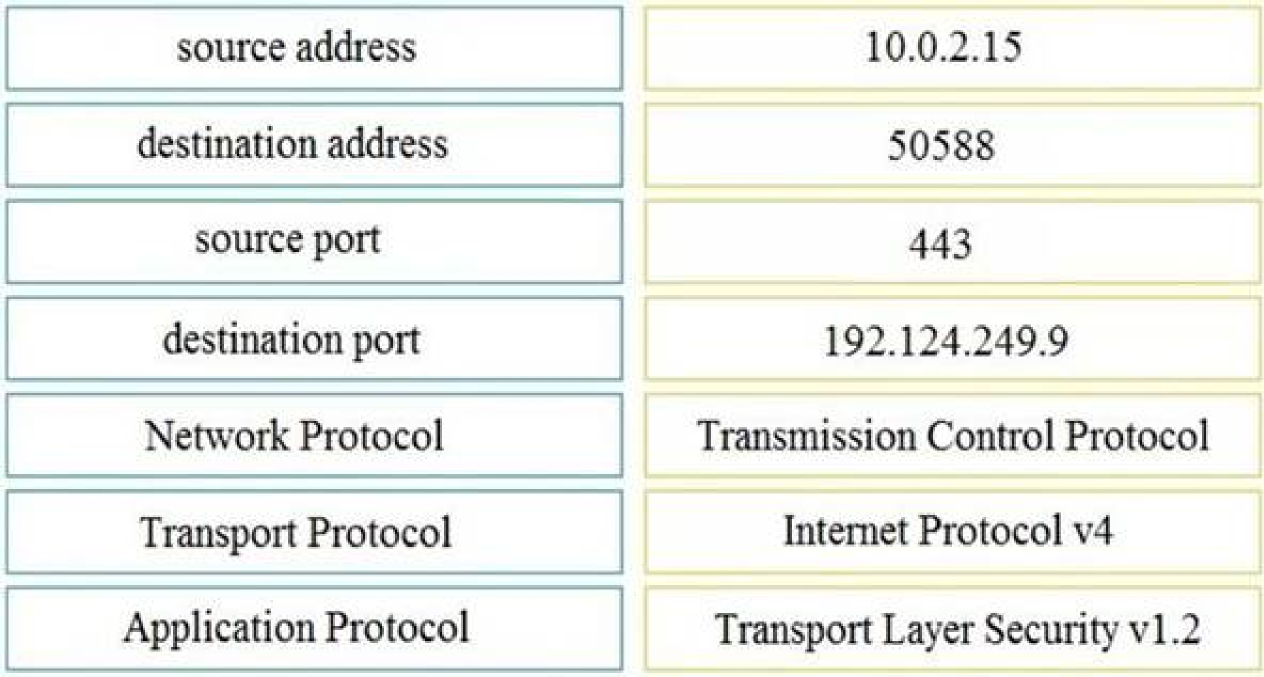


```
No.    Time      Source          Destination     Protocol  Length Info
    17 0.011641  10.0.2.15       192.124.249.9   TCP          76  50586-443 [SYN] Seq=0 Win=
    18 0.011918  10.0.2.15       192.124.249.9   TCP          76  50588-443 [SYN] Seq=0 Win=
    19 0.022656  192.124.249.9   10.0.2.15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

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

0000  00 04 00 01 00 06 08 00  27 7a 3c 93 00 00 08 00   ........ *z<.....
0010  45 00 00 f5 eb 3e 40 00  40 06 89 2f 0a 00 02 0f   E....>@. @../....
0020  c0 7c f9 09 c5 9c 01 bb  4d db 7f f7 00 b3 b0 02   .|...... M.......
0030  50 18 72 10 c6 7c 00 00  16 03 01 00 c8 01 00 00   P.r..|.. ........
0040  c4 03 03 d1 08 45 78 b7  2c 90 04 ee 51 16 f1 82   .....Ex. ....Q...
0050  16 43 ec d4 89 60 34 4a  7b 80 a6 d1 72 d5 11 87   .C....4J {...r...
0060  10 57 cc 00 00 1e c0 2b  c0 2f cc a9 cc a8 c0 2c   .W.....+ ./.....,
0070  c0 30 c0 0a c0 09 c0 13  c0 14 00 33 00 39 00 2f   .0...... ...3.9./
0080  00 35 00 0a 01 00 00 7d  00 00 00 16 00 14 00 00   .5.....} ........
0090  11 77 77 77 2e 6c 69 6e  75 78 6d 69 6e 74 2e 63   .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.

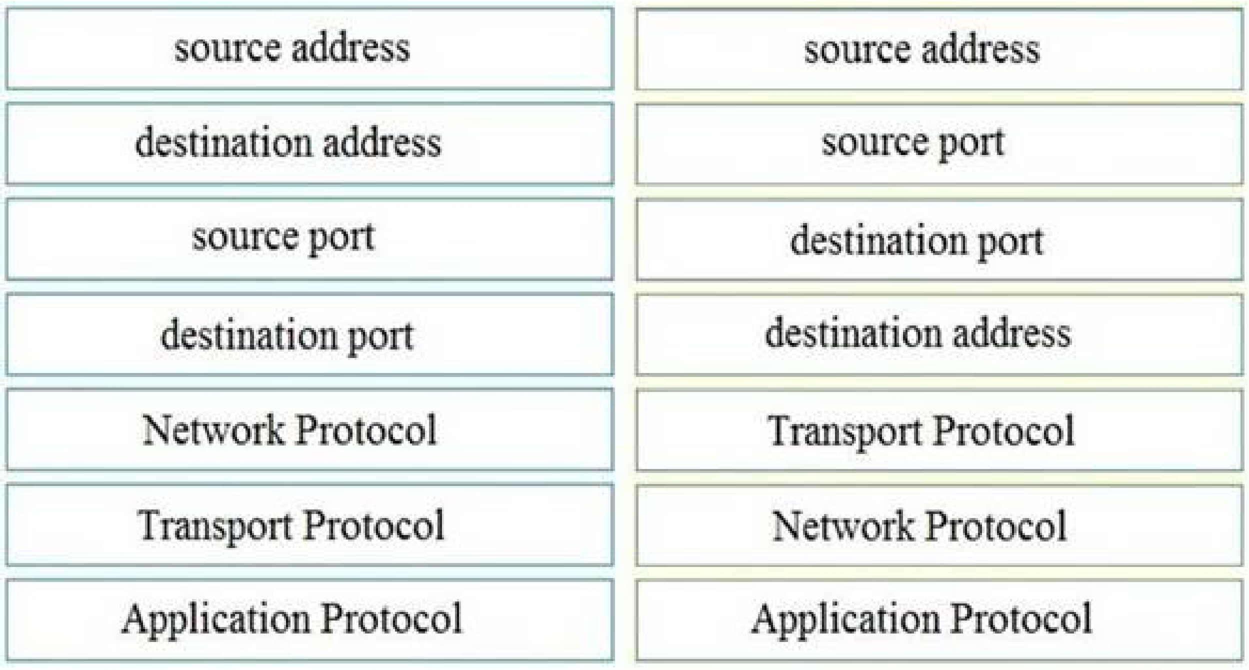


source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

NEW QUESTION 9
How does certificate authority impact a security system?

A. It authenticates client identity when requesting SSL certificate
B. It validates domain identity of a SSL certificate
C. It authenticates domain identity when requesting SSL certificate
D. It validates client identity when communicating with the server

Answer: B

NEW QUESTION 10
A network engineer discovers that a foreign government hacked one of the defense contractors in their home country and stole intellectual property. What is the threat agent in this situation?

A. the intellectual property that was stolen
B. the defense contractor who stored the intellectual property
C. the method used to conduct the attack
D. the foreign government that conducted the attack

Answer: D

NEW QUESTION 10
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

NEW QUESTION 14
What are two denial of service attacks? (Choose two.)

A. MITM
B. TCP connections
C. ping of death
D. UDP flooding
E. code red

Answer: CD

NEW QUESTION 18
A system administrator is ensuring that specific registry information is accurate.
Which type of configuration information does the HKEY_LOCAL_MACHINE hive contain?

A. file extension associations
B. hardware, software, and security settings for the system
C. currently logged in users, including folders and control panel settings

D. all users on the system, including visual settings

Answer: B

Explanation:
https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users

NEW QUESTION 20
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. digital certificates
B. static IP addresses
C. signatures
D. cipher suite

Answer: A

NEW QUESTION 25
When an event is investigated, which type of data provides the investigate capability to determine if data exfiltration has occurred?

A. full packet capture
B. NetFlow data
C. session data
D. firewall logs

Answer: A

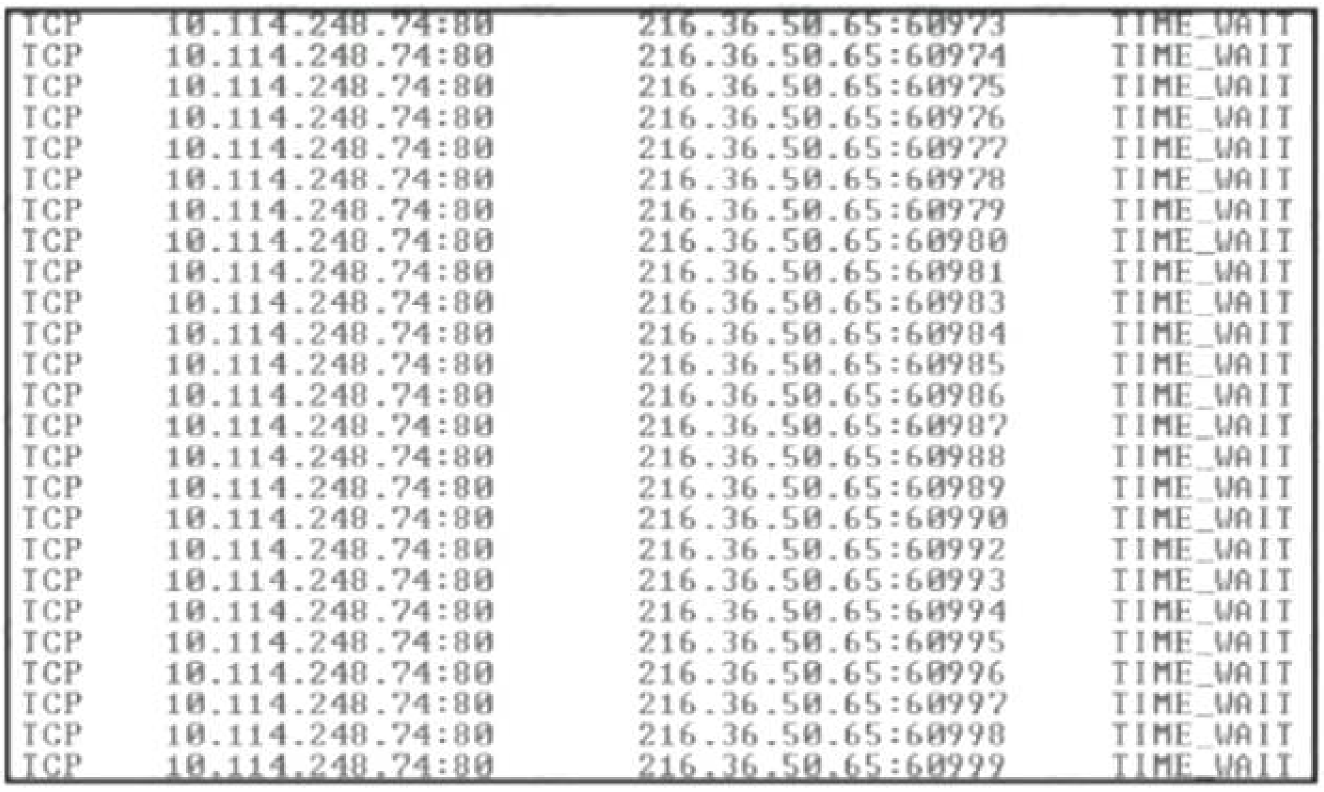
NEW QUESTION 28
Which evasion technique is indicated when an intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources?

A. resource exhaustion
B. tunneling
C. traffic fragmentation
D. timing attack

Answer: A

Explanation:
Resource exhaustion is a type of denial-of-service attack; however, it can also be used to evade detection by security defenses. A simple definition of resource exhaustion is “consuming the resources necessary to
perform an action.” Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

NEW QUESTION 29
Refer to the exhibit.



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

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

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

Answer: C

NEW QUESTION 32

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: CD

Explanation:
The following are some factors that are used during attribution in an investigation: Assets, Threat actor, Indicators of Compromise (IoCs), Indicators of Attack (IoAs), Chain of custody Asset: This factor identifies which assets were compromised by a threat actor or hacker. An example of an asset can be an organization's domain controller (DC) that runs Active Directory Domain Services (AD DS). AD is a service that allows an administrator to manage user accounts, user groups, and policies across a Microsoft Windows environment. Keep in mind that an asset is anything that has value to an organization; it can be something physical, digital, or even people. Cisco Certified CyberOps Associate 200-201 Certification Guide

NEW QUESTION 33
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: C

NEW QUESTION 34
A security engineer has a video of a suspect entering a data center that was captured on the same day that files in the same data center were transferred to a competitor.
Which type of evidence is this?

A. best evidence
B. prima facie evidence
C. indirect evidence
D. physical evidence

Answer: C

Explanation:
There are three general types of evidence:
--> Best evidence: can be presented in court in the original form (for example, an exact copy of a hard disk drive).
--> Corroborating evidence: tends to support a theory or an assumption deduced by some initial evidence. This corroborating evidence confirms the proposition.
--> Indirect or circumstantial evidence: extrapolation to a conclusion of fact (such as fingerprints, DNA evidence, and so on).

NEW QUESTION 39
Which action should be taken if the system is overwhelmed with alerts when false positives and false negatives are compared?

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

Answer: A

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

NEW QUESTION 40
An investigator is examining a copy of an ISO file that is stored in CDFS format. What type of evidence is this file?

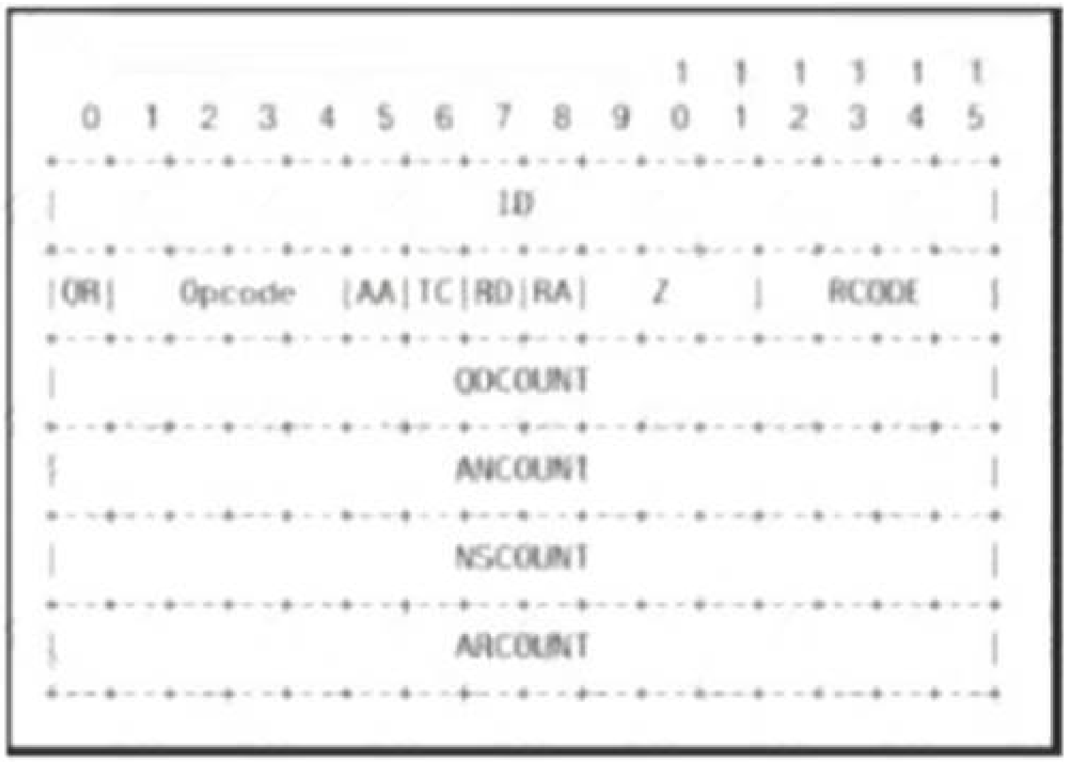
A. data from a CD copied using Mac-based system
B. data from a CD copied using Linux system
C. data from a DVD copied using Windows system
D. data from a CD copied using Windows

Answer: B

Explanation:
CDfs is a virtual file system for Unix-like operating systems; it provides access to data and audio tracks on Compact Discs. When the CDfs driver mounts a Compact Disc, it represents each track as a file. This is consistent with the Unix convention "everything is a file". Source: https://en.wikipedia.org/wiki/CDfs

NEW QUESTION 45

Refer to the exhibit.



```
                                1  1  1  1  1  1
  0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                      ID                       |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|QR|   Opcode  |AA|TC|RD|RA|   Z    |   RCODE   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    QDCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ANCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    NSCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ARCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Which field contains DNS header information if the payload is a query or a response?

A. Z
B. ID
C. TC
D. QR

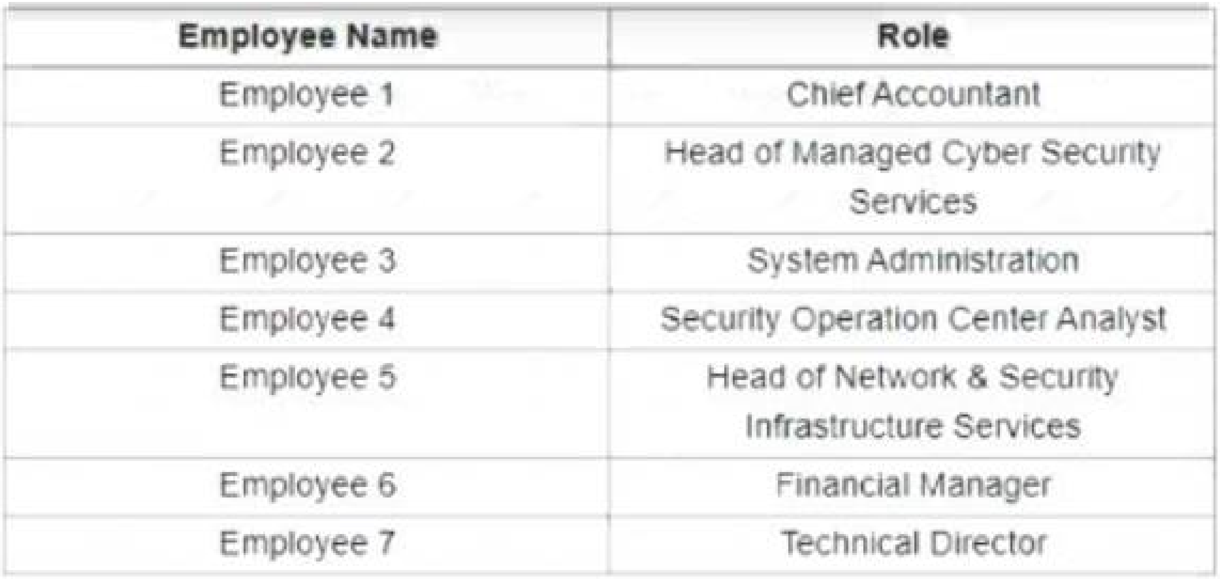
Answer: B

NEW QUESTION 48
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

NEW QUESTION 50
Refer to the exhibit.



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

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

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

Answer: D

NEW QUESTION 55
Which artifact is used to uniquely identify a detected file?

A. file timestamp
B. file extension
C. file size
D. file hash

Answer: D

NEW QUESTION 57
A company encountered a breach on its web servers using IIS 7 5 Dunng the investigation, an engineer discovered that an attacker read and altered the data on a secure communication using TLS 1 2 and intercepted sensitive information by downgrading a connection to export-grade cryptography. The engineer must mitigate similar incidents in the future and ensure that clients and servers always negotiate with the most secure protocol versions and cryptographic parameters. Which action does the engineer recommend?

A. Upgrade to TLS v1 3.
B. Install the latest IIS version.
C. Downgrade to TLS 1.1.
D. Deploy an intrusion detection system

Answer: B

NEW QUESTION 60
Which type of verification consists of using tools to compute the message digest of the original and copied data, then comparing the similarity of the digests?

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

Answer: B

NEW QUESTION 65
Which information must an organization use to understand the threats currently targeting the organization?

A. threat intelligence
B. risk scores
C. vendor suggestions
D. vulnerability exposure

Answer: A

NEW QUESTION 70
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

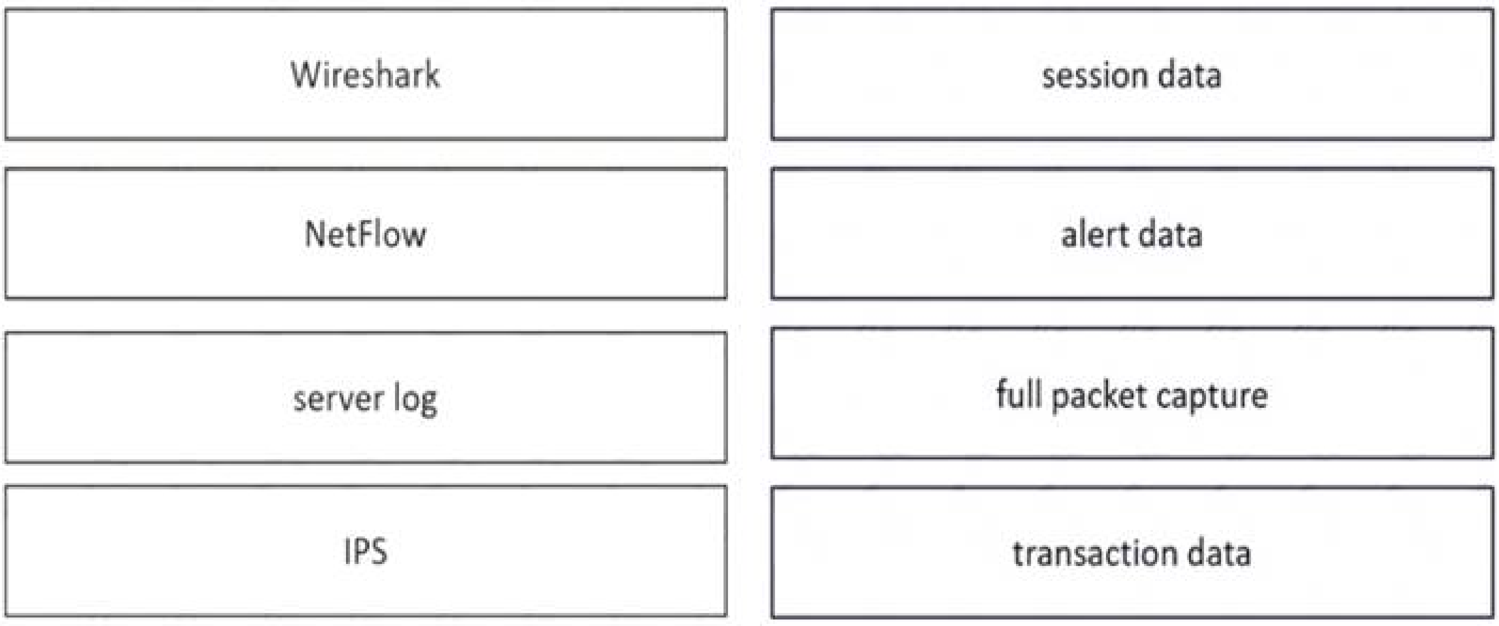
NEW QUESTION 74
What is a benefit of agent-based protection when compared to agentless protection?

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

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

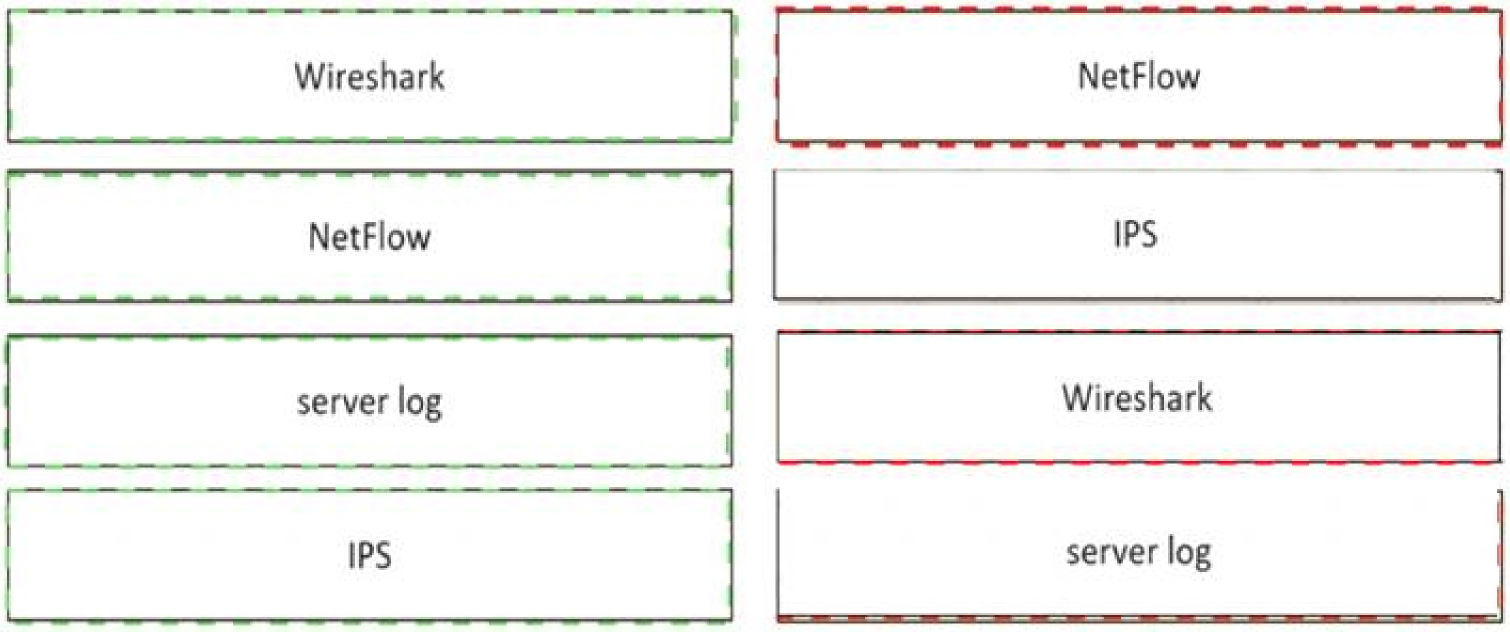


Wireshark	session data
NetFlow	alert data
server log	full packet capture
IPS	transaction data

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Wireshark	NetFlow
NetFlow	IPS
server log	Wireshark
IPS	server log

NEW QUESTION 81
According to the September 2020 threat intelligence feeds a new malware called Egregor was introduced and used in many attacks. Distnbution of Egregor is pnmanly through a Cobalt Strike that has been installed on victim's workstations using RDP exploits Malware exfiltrates the victim's data to a command and control server. The data is used to force victims pay or lose it by publicly releasing it. Which type of attack is described?

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

Answer: B

NEW QUESTION 82
During which phase of the forensic process are tools and techniques used to extract information from the collected data?

A. investigation
B. examination
C. reporting
D. collection

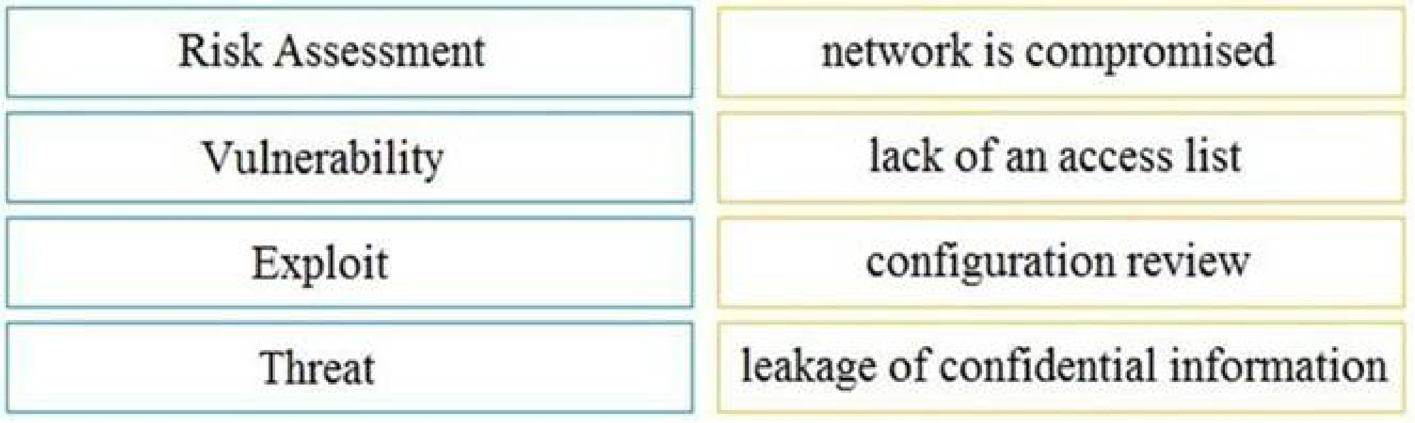
Answer: D

NEW QUESTION 84
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. tagged protocols being used on the network
B. all firewall alerts and resulting mitigations
C. tagged ports being used on the network
D. all information and data within the datagram

Answer: C

NEW QUESTION 87
Drag and drop the security concept on the left onto the example of that concept on the right.

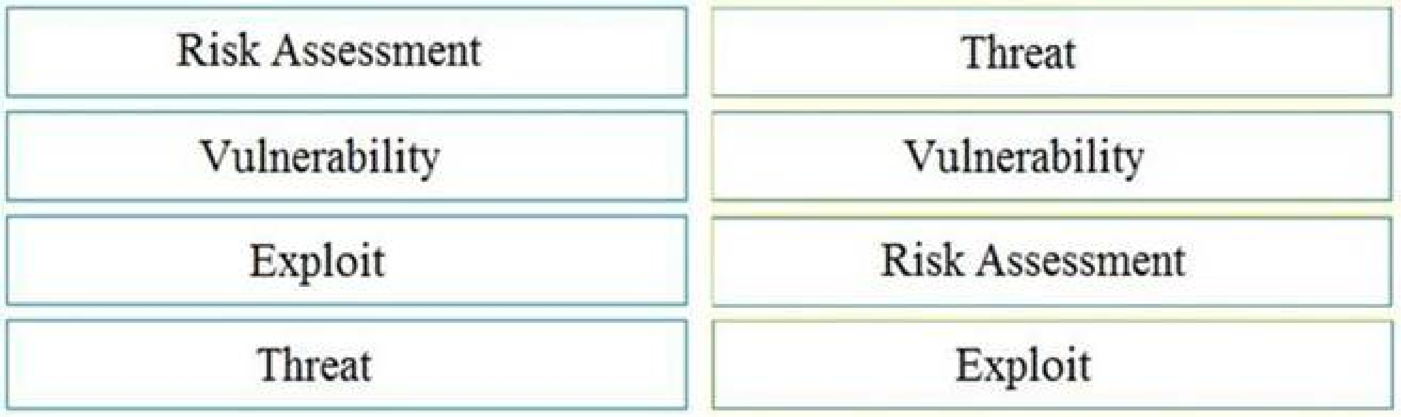


Risk Assessment	network is compromised
Vulnerability	lack of an access list
Exploit	configuration review
Threat	leakage of confidential information

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Risk Assessment	Threat
Vulnerability	Vulnerability
Exploit	Risk Assessment
Threat	Exploit

NEW QUESTION 92
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

Explanation:
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 96
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, identity, and authorization
B. confidentiality, integrity, and authorization
C. confidentiality, identity, and availability
D. confidentiality, integrity, and availability

Answer: D

NEW QUESTION 100
What is an example of social engineering attacks?

A. receiving an unexpected email from an unknown person with an attachment from someone in the same company
B. receiving an email from human resources requesting a visit to their secure website to update contact information
C. sending a verbal request to an administrator who knows how to change an account password
D. receiving an invitation to the department’s weekly WebEx meeting

Answer: C

NEW QUESTION 103
What does cyber attribution identify in an investigation?

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

Answer: D

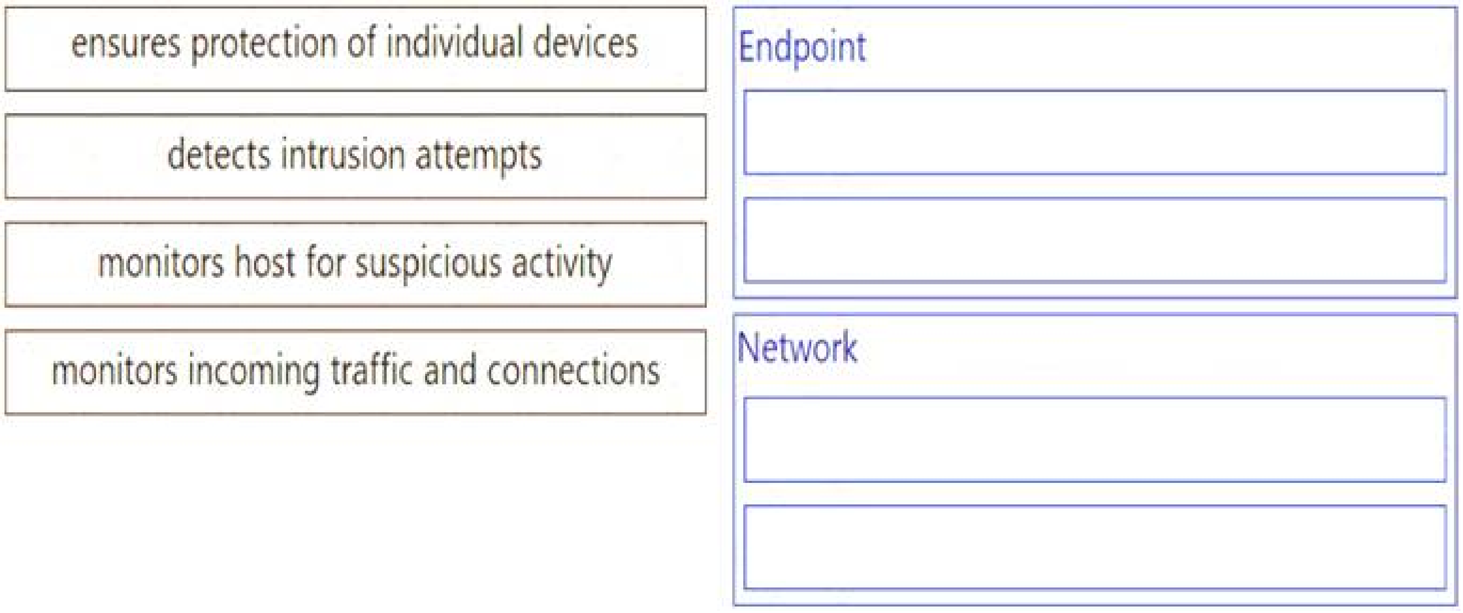
Explanation:
https://www.techtarget.com/searchsecurity/definition/cyber-attribution

NEW QUESTION 105
What is rule-based detection when compared to statistical detection?

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

Answer: B

NEW QUESTION 110
Drag and drop the uses on the left onto the type of security system on the right.



ensures protection of individual devices

detects intrusion attempts

monitors host for suspicious activity

monitors incoming traffic and connections

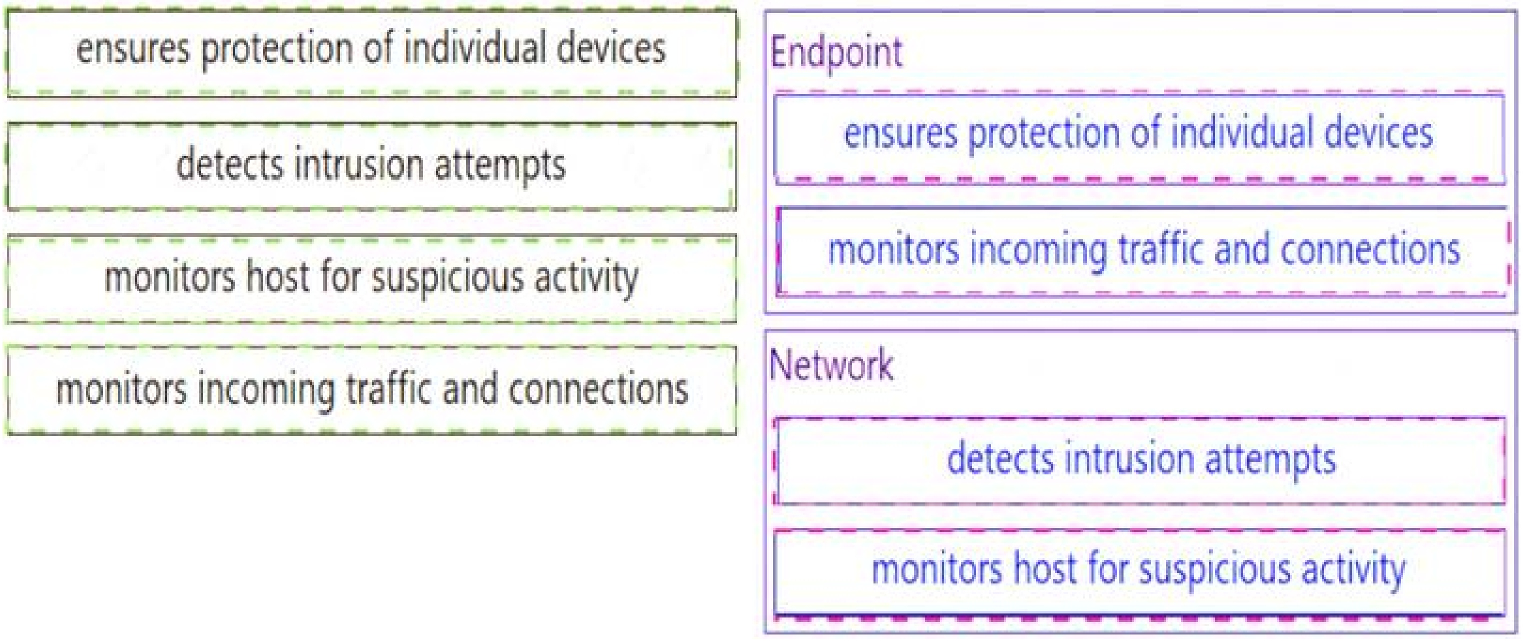
Endpoint

Network

A. Mastered
B. Not Mastered

Answer: A

Explanation:



ensures protection of individual devices

detects intrusion attempts

monitors host for suspicious activity

monitors incoming traffic and connections

Endpoint

ensures protection of individual devices

monitors incoming traffic and connections

Network

detects intrusion attempts

monitors host for suspicious activity

NEW QUESTION 111
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: BE

NEW QUESTION 114
What describes the defense-m-depth principle?

A. defining precise guidelines for new workstation installations
B. categorizing critical assets within the organization
C. isolating guest Wi-Fi from the focal network
D. implementing alerts for unexpected asset malfunctions

Answer: B

NEW QUESTION 119
Which technology prevents end-device to end-device IP traceability?

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

Answer: C

NEW QUESTION 124
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: BC

NEW QUESTION 129
Which event is a vishing attack?

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

Answer: D

NEW QUESTION 130
An analyst is investigating an incident in a SOC environment. Which method is used to identify a session from a group of logs?

A. sequence numbers
B. IP identifier
C. 5-tuple
D. timestamps

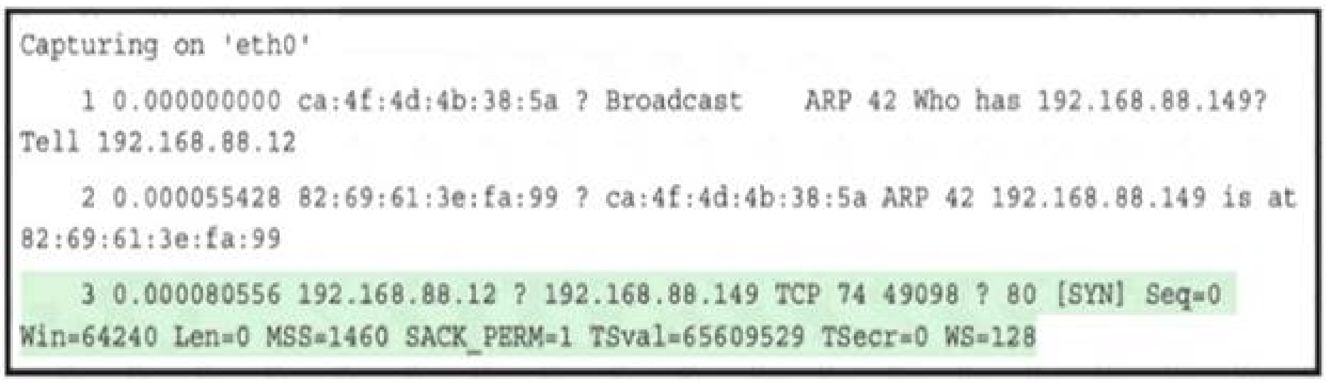
Answer: C

NEW QUESTION 134
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

NEW QUESTION 136
Refer to the exhibit.



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

What must be interpreted from this packet capture?

A. IP address 192.168.88 12 is communicating with 192 168 88 149 with a source port 74 to destination port 49098 using TCP protocol
B. IP address 192.168.88.12 is communicating with 192 168 88 149 with a source port 49098 to destination port 80 using TCP protocol.
C. IP address 192.168.88.149 is communicating with 192.168 88.12 with a source port 80 to destination port 49098 using TCP protocol.
D. IP address 192.168.88.149 is communicating with 192.168.88.12 with a source port 49098 to destination port 80 using TCP protocol.

Answer: B

NEW QUESTION 141
Which system monitors local system operation and local network access for violations of a security policy?

A. host-based intrusion detection
B. systems-based sandboxing
C. host-based firewall
D. antivirus

Answer: A

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

NEW QUESTION 144
Which two elements of the incident response process are stated in NIST SP 800-61 r2? (Choose two.)

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

Answer: AB

NEW QUESTION 148
What ate two categories of DDoS attacks? (Choose two.)

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

Answer: DE

NEW QUESTION 151
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

NEW QUESTION 156
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

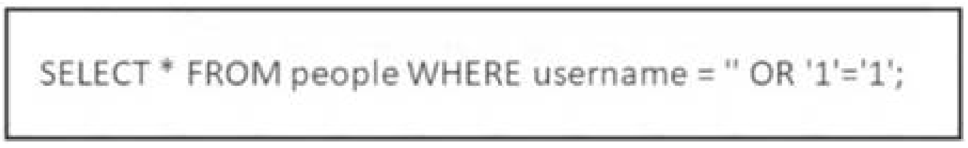
Answer: D

NEW QUESTION 158
What is a difference between SOAR and SIEM?

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

Answer: A

NEW QUESTION 160
Refer to the exhibit.



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

Which type of attack is being executed?

A. SQL injection
B. cross-site scripting
C. cross-site request forgery
D. command injection

Answer: A

NEW QUESTION 162
What is the principle of defense-in-depth?

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

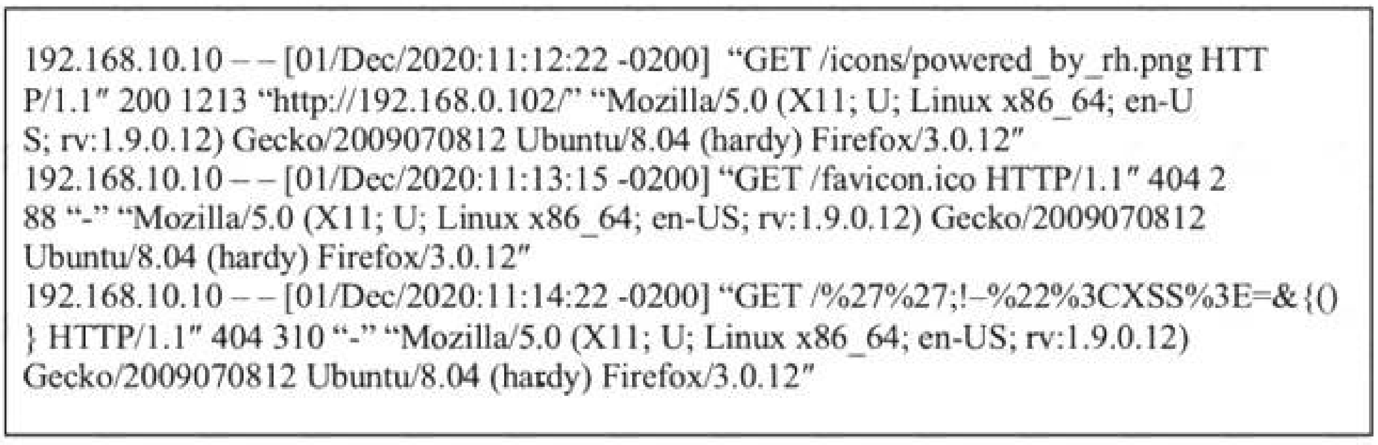
Answer: B

NEW QUESTION 165
Which are two denial-of-service attacks? (Choose two.)

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

Answer: BE

NEW QUESTION 166
Refer to the exhibit.



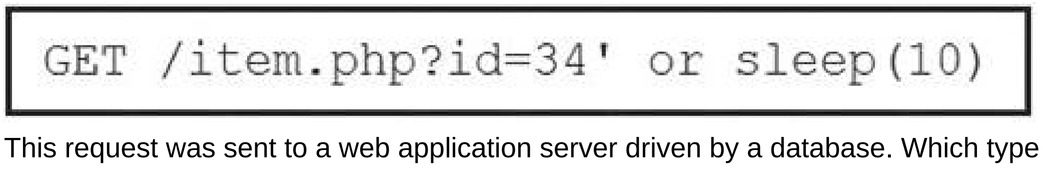
```
192.168.10.10 – – [01/Dec/2020:11:12:22 -0200]  "GET /icons/powered_by_rh.png HTT
P/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-U
S; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 – – [01/Dec/2020:11:13:15 -0200] "GET /favicon.ico 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. regular GET requests
B. XML External Entities attack
C. insecure deserialization
D. cross-site scripting attack

Answer: A

NEW QUESTION 170
Refer to the exhibit.



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

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

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

Answer: D

NEW QUESTION 171
Why is encryption challenging to security monitoring?

A. Encryption analysis is used by attackers to monitor VPN tunnels.
B. Encryption is used by threat actors as a method of evasion and obfuscation.
C. Encryption introduces additional processing requirements by the CPU.
D. Encryption introduces larger packet sizes to analyze and store.

Answer: B

NEW QUESTION 175
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

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 178
Which attack method intercepts traffic on a switched network?

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

Answer: B

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

NEW QUESTION 183
Which technology on a host is used to isolate a running application from other applications?

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

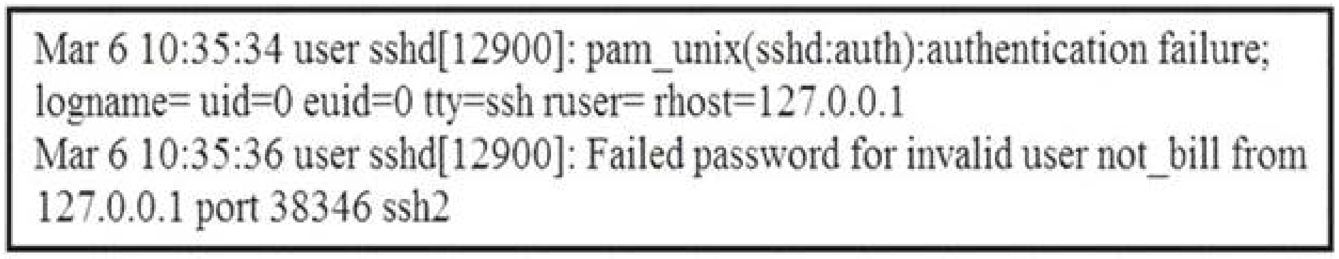
Answer: A

NEW QUESTION 188
Which security technology allows only a set of pre-approved applications to run on a system?

A. application-level blacklisting
B. host-based IPS
C. application-level whitelisting
D. antivirus

Answer: C

NEW QUESTION 189
Refer to the exhibit.



```
Mar 6 10:35:34 user sshd[12900]: pam_unix(sshd:auth):authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Mar 6 10:35:36 user sshd[12900]: Failed password for invalid user not_bill from
127.0.0.1 port 38346 ssh2
```

In which Linux log file is this output found?

A. /var/log/authorization.log
B. /var/log/dmesg
C. var/log/var.log
D. /var/log/auth.log

Answer: D

NEW QUESTION 193
Which utility blocks a host portscan?

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

Answer: C

NEW QUESTION 196
An analyst is exploring the functionality of different operating systems.
What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?

A. queries Linux devices that have Microsoft Services for Linux installed
B. deploys Windows Operating Systems in an automated fashion
C. is an efficient tool for working with Active Directory
D. has a Common Information Model, which describes installed hardware and software

Answer: D

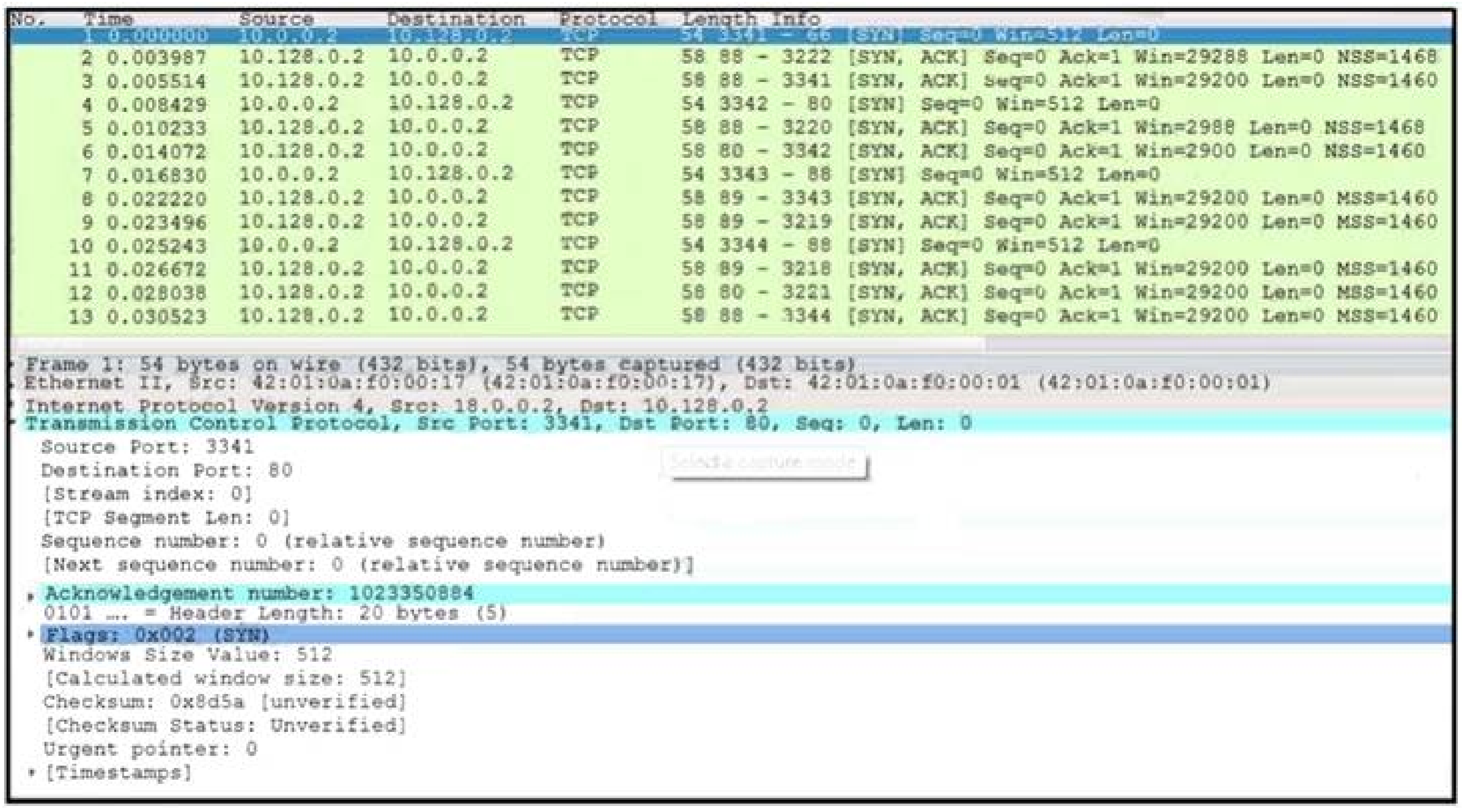
NEW QUESTION 200
Which two elements are used for profiling a network? (Choose two.)

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

Answer: AB

Explanation:
A network profile should include some important elements, such as the following:
Total throughput – the amount of data passing from a given source to a given destination in a given period of time
Session duration – the time between the establishment of a data flow and its termination Ports used – a list of TCP or UDP processes that are available to accept data
Critical asset address space – the IP addresses or the logical location of essential systems or data
Profiling data are data that system has gathered, these data helps for incident response and to detect incident Network profiling = throughput, sessions duration, port used, Critical Asset Address Space Host profiling = Listening ports, logged in accounts, running processes, running tasks,applications

NEW QUESTION 201
Refer to the exhibit.



```
No.  Time      Source      Destination  Protocol  Length Info
   1 0.000000  10.0.0.2    10.128.0.2   TCP       54 3341 - 66 [SYN] Seq=0 Win=512 Len=0
   2 0.003987  10.128.0.2  10.0.0.2     TCP       58 88 - 3222 [SYN, ACK] Seq=0 Ack=1 Win=29288 Len=0 NSS=1468
   3 0.005514  10.128.0.2  10.0.0.2     TCP       58 88 - 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
   4 0.008429  10.0.0.2    10.128.0.2   TCP       54 3342 - 80 [SYN] Seq=0 Win=512 Len=0
   5 0.010233  10.128.0.2  10.0.0.2     TCP       58 88 - 3220 [SYN, ACK] Seq=0 Ack=1 Win=2988 Len=0 NSS=1468
   6 0.014072  10.128.0.2  10.0.0.2     TCP       58 80 - 3342 [SYN, ACK] Seq=0 Ack=1 Win=2900 Len=0 NSS=1460
   7 0.016830  10.0.0.2    10.128.0.2   TCP       54 3343 - 88 [SYN] Seq=0 Win=512 Len=0
   8 0.022220  10.128.0.2  10.0.0.2     TCP       58 89 - 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
   9 0.023496  10.128.0.2  10.0.0.2     TCP       58 89 - 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  10 0.025243  10.0.0.2    10.128.0.2   TCP       54 3344 - 88 [SYN] Seq=0 Win=512 Len=0
  11 0.026672  10.128.0.2  10.0.0.2     TCP       58 89 - 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  12 0.028038  10.128.0.2  10.0.0.2     TCP       58 80 - 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  13 0.030523  10.128.0.2  10.0.0.2     TCP       58 88 - 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)
Internet Protocol Version 4, Src: 18.0.0.2, Dst: 10.128.0.2
Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 3341
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  [Next sequence number: 0 (relative sequence number)]
  Acknowledgement number: 1023350884
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x002 (SYN)
  Windows Size Value: 512
  [Calculated window size: 512]
  Checksum: 0x8d5a [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  [Timestamps]
```

What is occurring in this network traffic?

A. High rate of SYN packets being sent from a multiple source towards a single destination IP.
B. High rate of ACK packets being sent from a single source IP towards multiple destination IPs.
C. Flood of ACK packets coming from a single source IP to multiple destination IPs.
D. Flood of SYN packets coming from a single source IP to a single destination IP.

Answer: D

NEW QUESTION 203
How does an SSL certificate impact security between the client and the server?

A. by enabling an authenticated channel between the client and the server
B. by creating an integrated channel between the client and the server
C. by enabling an authorized channel between the client and the server
D. by creating an encrypted channel between the client and the server

Answer: D

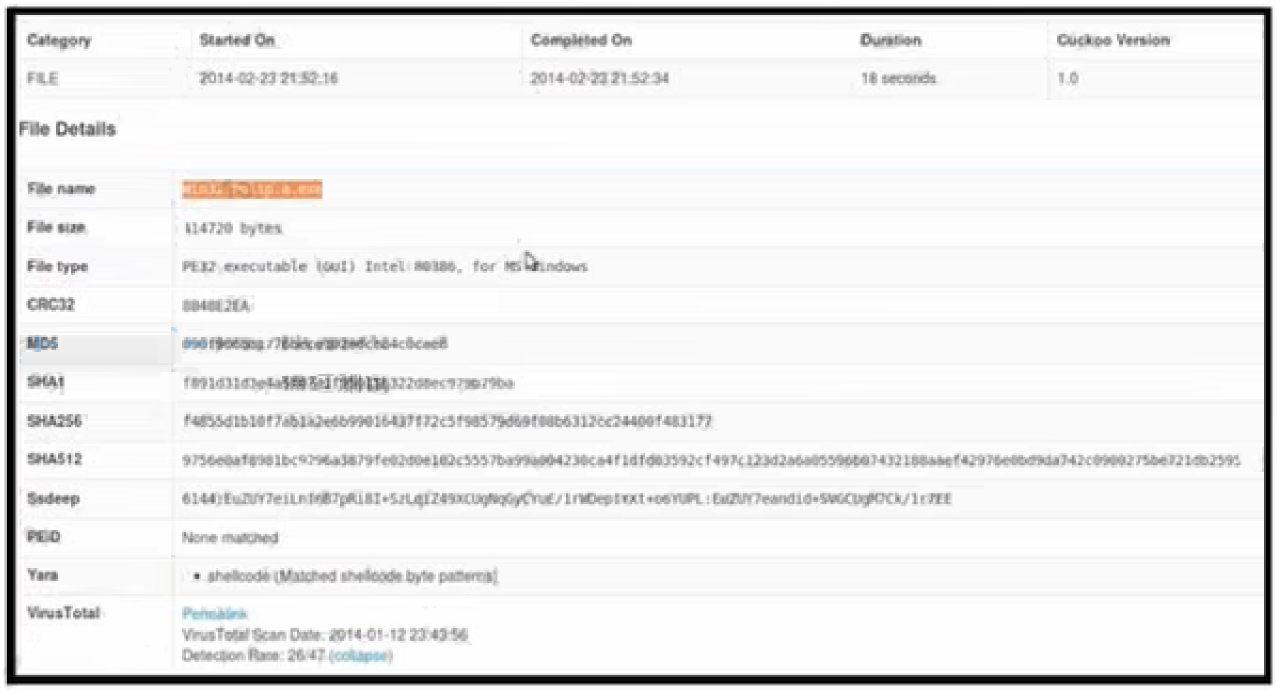
NEW QUESTION 205
When trying to evade IDS/IPS devices, which mechanism allows the user to make the data incomprehensible without a specific key, certificate, or password?

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

Answer: C

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

NEW QUESTION 207
Refer to the exhibit.



Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2014-02-23 21:52:16	2014-02-23 21:52:34	18 seconds	1.0

File Details

File name	win32.polip.a.exe
File size	114720 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows
CRC32	8848E2EA
MD5	[illegible]c84c0ca08
SHA1	f891d31d3e4a[illegible]322d8ec979b79ba
SHA256	f4855d1b10f7ab1a2e6b9901643f72c5f98579d69f08b6312cc24400f483177
SHA512	9756e0af8981bc9296a3879fe02d0e182c5557ba99a004230ca4f1dfd03592cf497c123d2a6a05596b07432188aaef42976e0bd9da742c0900275be721db2595
Ssdeep	6144:EuZUY7eiLnf6B7pRi8I+SzLqIZ49XCUgNqGyCYuE/1rWDep1YXt+o6YUPL:EuZUY7eandid+SWGCUgM7Ck/1r7EE
PEiD	None matched
Yara	• shellcode (Matched shellcode byte patterns)
VirusTotal	Permalink VirusTotal Scan Date: 2014-01-12 23:43:56 Detection Rate: 26/47 (collapse)

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. Win32.polip.a.exe is an executable file and should be flagged as malicious.
B. The file is clean and does not represent a risk.
C. Cuckoo cleaned the malicious file and prepared it for usage.
D. MD5 of the file was not identified as malicious.

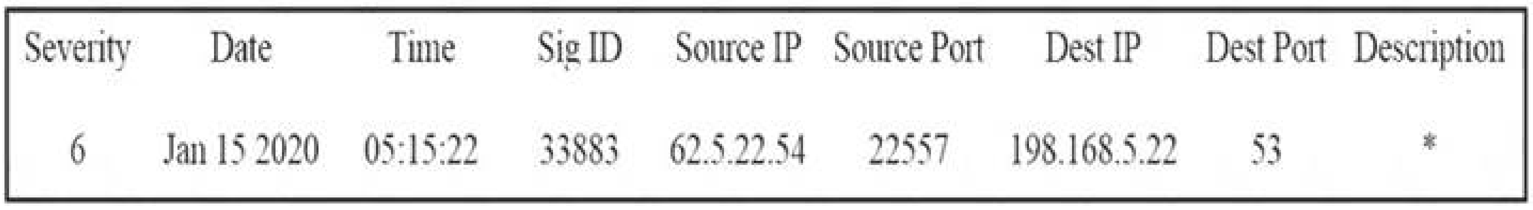
Answer: C

NEW QUESTION 210
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

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

Answer: A

NEW QUESTION 213
Refer to the exhibit.



Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2020	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	*

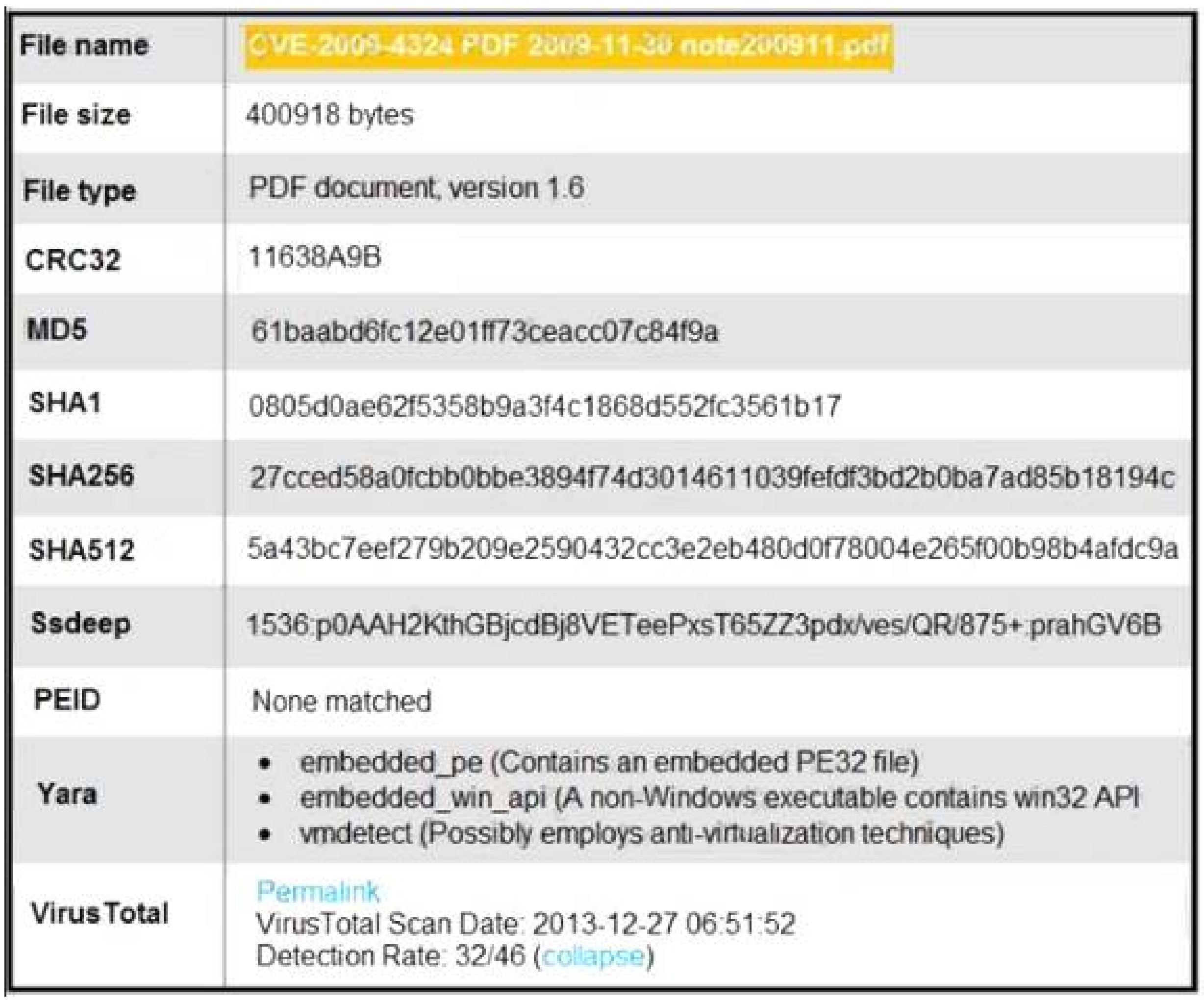
Which type of log is displayed?

A. IDS
B. proxy
C. NetFlow
D. sys

Answer: A

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

NEW QUESTION 216
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	0805d0ae62f5358b9a3f4c1868d552fc3561b17
SHA256	27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
SHA512	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
Ssdeep	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/QR/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 executable and was matched by PEiD threat signatures for further analysis.
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 was matched by PEiD threat signatures but no suspicious features are identified since the signature list is up to date.

Answer: C

NEW QUESTION 217
What is the virtual address space for a Windows process?

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

Answer: D

NEW QUESTION 220
What is a difference between tampered and untampered disk images?

A. Tampered images have the same stored and computed hash.
B. Untampered images are deliberately altered to preserve as evidence.
C. Tampered images are used as evidence.
D. Untampered images are used for forensic investigations.

Answer: D

Explanation:
The disk image must be intact for forensics analysis. As a cybersecurity professional, you may be given the task of capturing an image of a disk in a forensic manner. Imagine a security incident has occurred on a system and you are required to perform some forensic investigation to determine who and what caused the attack. Additionally, you want to ensure the data that was captured is not tampered with or modified during the creation of a disk image process. Ref: Cisco Certified CyberOps Associate 200-201 Certification Guide

NEW QUESTION 225
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: CD

NEW QUESTION 228
At a company party a guest asks questions about the company's user account format and password complexity. How is this type of conversation classified?

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

Answer: D

NEW QUESTION 231
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

Explanation:
Corroborating evidence (or corroboration) is evidence that tends to support a theory or an assumption deduced by some initial evidence. This corroborating evidence confirms the proposition. Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

NEW QUESTION 234
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

NEW QUESTION 235
What is the difference between deep packet inspection and stateful inspection?

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

Answer: D

NEW QUESTION 238
Which security monitoring data type requires the largest storage space?

A. transaction data
B. statistical data
C. session data
D. full packet capture

Answer: D

NEW QUESTION 243
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

Explanation:
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 244
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

Explanation:
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 245
Which filter allows an engineer to filter traffic in Wireshark to further analyze the PCAP file by only showing the traffic for LAN 10.11.x.x, between workstations and servers without the Internet?

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

Answer: B

NEW QUESTION 249
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

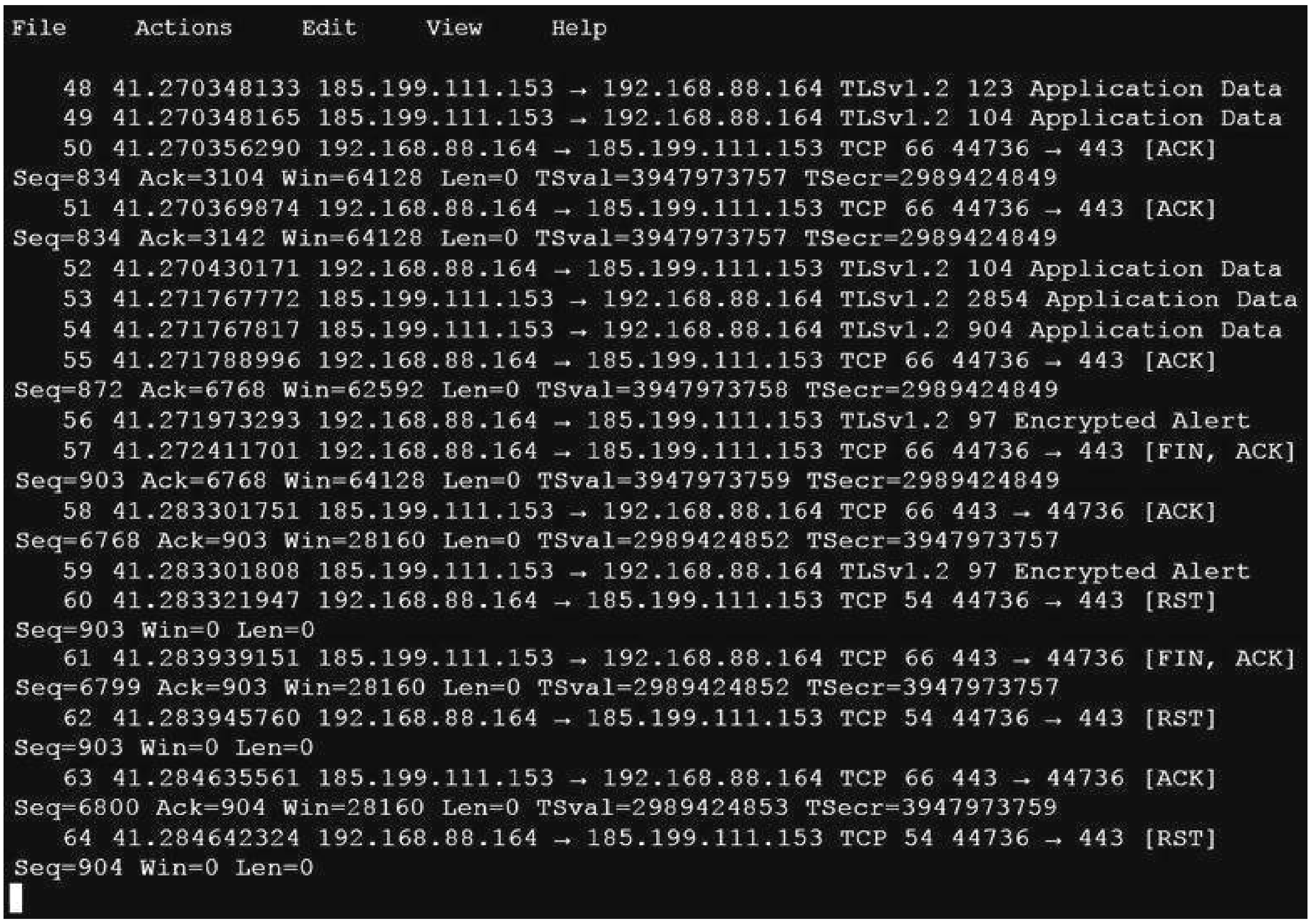
Answer: A

NEW QUESTION 252
What is an incident response plan?

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

Answer: C

NEW QUESTION 257
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.



```
    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
```

Which obfuscation technique is the attacker using?

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

Answer: B

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

NEW QUESTION 261
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

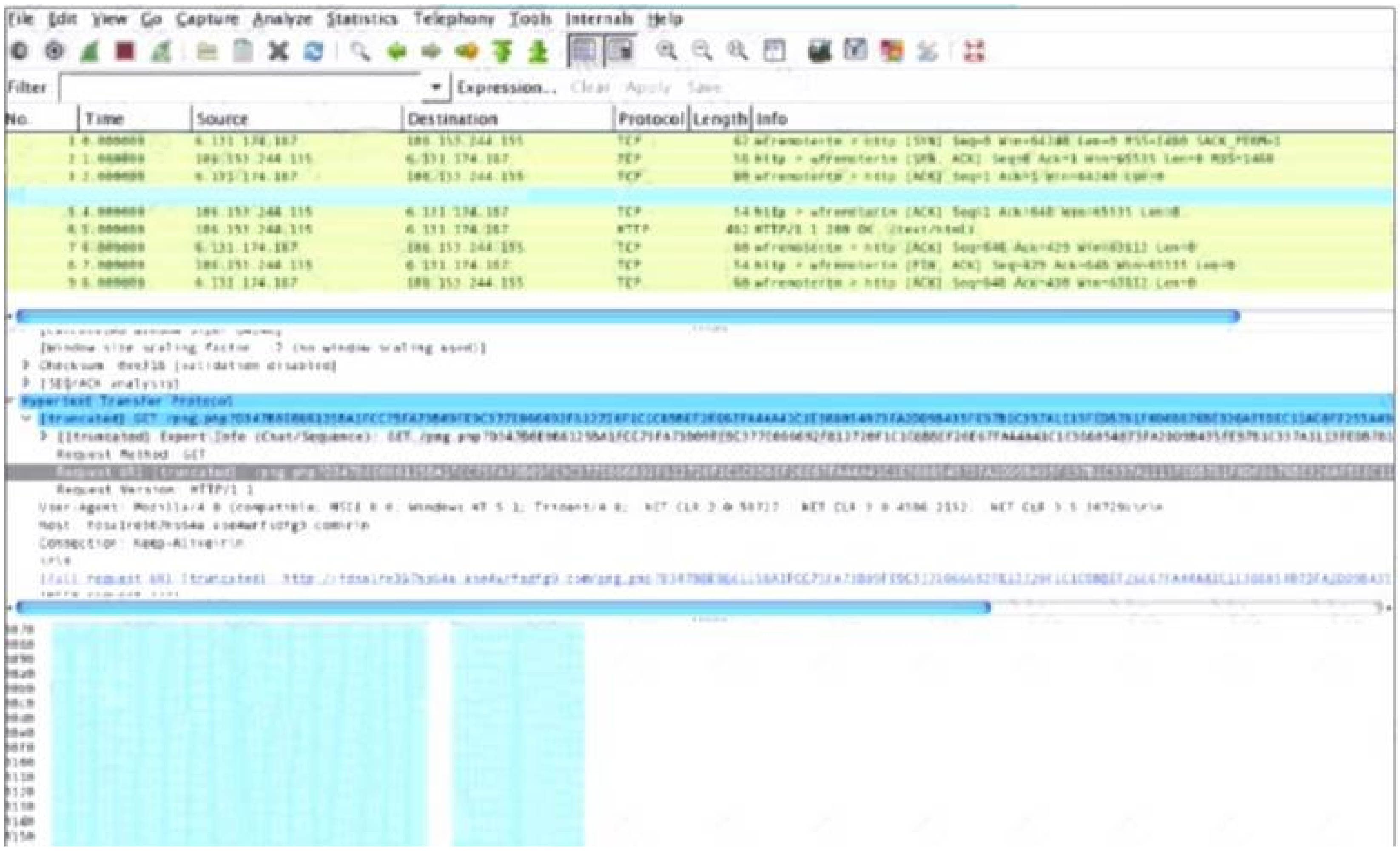
Answer: A

NEW QUESTION 266
A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?

A. CD data copy prepared in Windows
B. CD data copy prepared in Mac-based system
C. CD data copy prepared in Linux system
D. CD data copy prepared in Android-based system

Answer: A

NEW QUESTION 270
Refer to the exhibit.


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter
Expression... Clear Apply Save

```
No.  Time        Source            Destination       Protocol Length Info
1 0.000000   6.131.174.187     186.153.244.155   TCP   62 afremoterte > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
2 1.000000   186.153.244.155   6.131.174.187     TCP   58 http > afremoterte [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3 2.000000   6.131.174.187     186.153.244.155   TCP   60 afremoterte > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
5 4.000000   186.153.244.155   6.131.174.187     TCP   54 http > afremoterte [ACK] Seq=1 Ack=648 Win=65535 Len=0
6 5.000000   186.153.244.155   6.131.174.187     HTTP  482 HTTP/1.1 200 OK (text/html)
7 6.000000   6.131.174.187     186.153.244.155   TCP   60 afremoterte > http [ACK] Seq=648 Ack=429 Win=63512 Len=0
8 7.000000   186.153.244.155   6.131.174.187     TCP   54 http > afremoterte [FIN, ACK] Seq=429 Ack=648 Win=65535 Len=0
9 8.000000   6.131.174.187     186.153.244.155   TCP   60 afremoterte > http [ACK] Seq=648 Ack=430 Win=63512 Len=0

   [Window size scaling factor: -2 (no window scaling used)]
 ▶ Checksum: 0xe f16 [validation disabled]
 ▶ [SEQ/ACK analysis]
▼ Hypertext Transfer Protocol
  ▼ [truncated] GET /png.png?D347B0... HTTP/1.1\r\n
    ▶ [[truncated] Expert Info (Chat/Sequence): GET /png.png?D347B6E0661258A1FCC7... 
      Request Method: GET
      Request URI [truncated]: /png.png?D347B...
      Request Version: HTTP/1.1
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)\r\n
    Host: fdsalre367hs64a.ase4wrfsdfg3.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI [truncated]: http://fdsalre367hs64a.ase4wrfsdfg3.com/png.png?D347B0...]
```

What is shown in this PCAP file?

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

Answer: D

NEW QUESTION 274
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

NEW QUESTION 277
Which action prevents buffer overflow attacks?

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

Answer: C

NEW QUESTION 281
Which tool provides a full packet capture from network traffic?

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

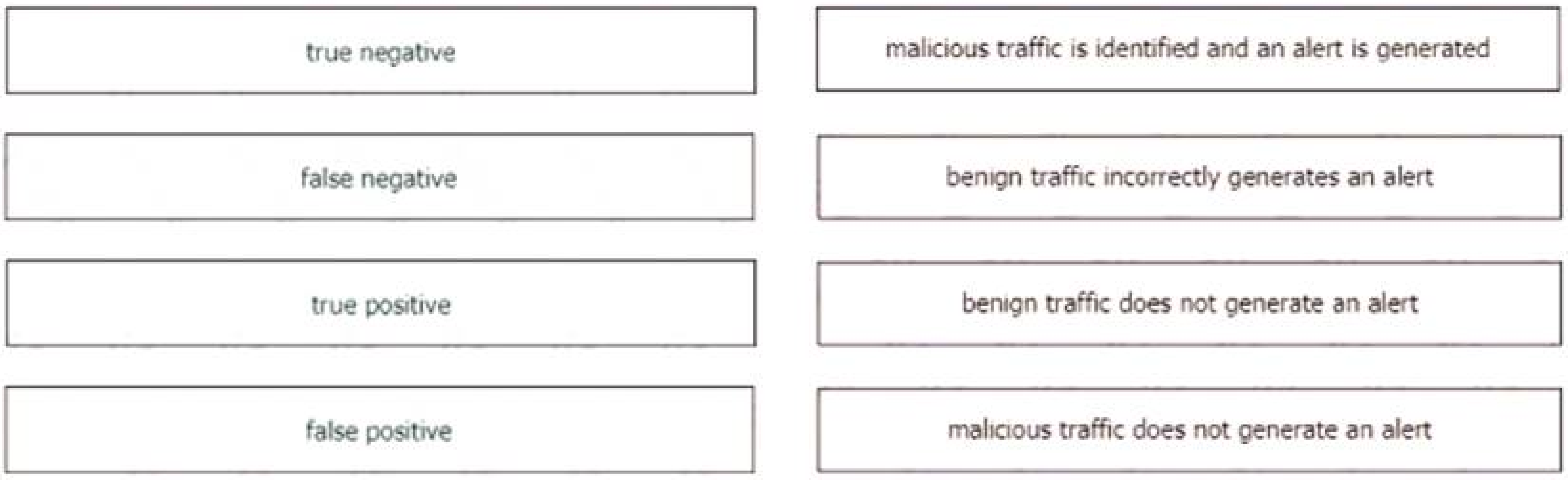
Answer: D

NEW QUESTION 282
What is a purpose of a vulnerability management framework?

A. identifies, removes, and mitigates system vulnerabilities
B. detects and removes vulnerabilities in source code
C. conducts vulnerability scans on the network
D. manages a list of reported vulnerabilities

Answer: A

NEW QUESTION 283
Drag and drop the event term from the left onto the description on the right.

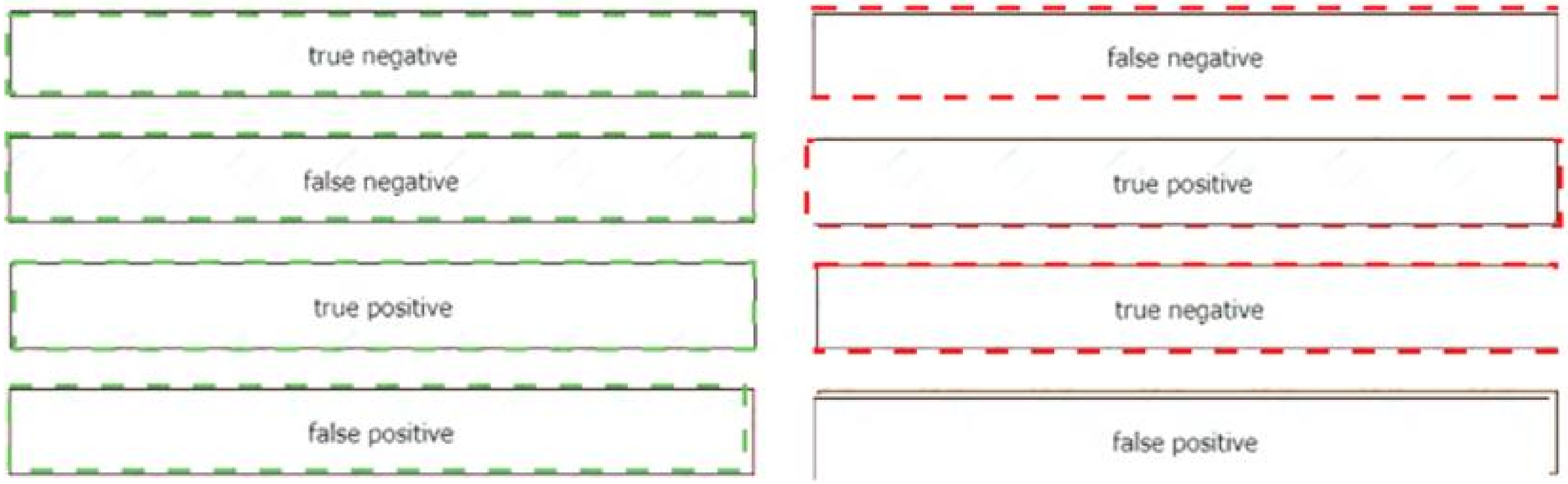


true negative	malicious traffic is identified and an alert is generated
false negative	benign traffic incorrectly generates an alert
true positive	benign traffic does not generate an alert
false positive	malicious traffic does not generate an alert

A. Mastered
B. Not Mastered

Answer: A

Explanation:



true negative	false negative
false negative	true positive
true positive	true negative
false positive	false positive

NEW QUESTION 287
A threat actor penetrated an organization's network. Using the 5-tuple approach, which data points should the analyst use to isolate the compromised host in a grouped set of logs?

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

Answer: B

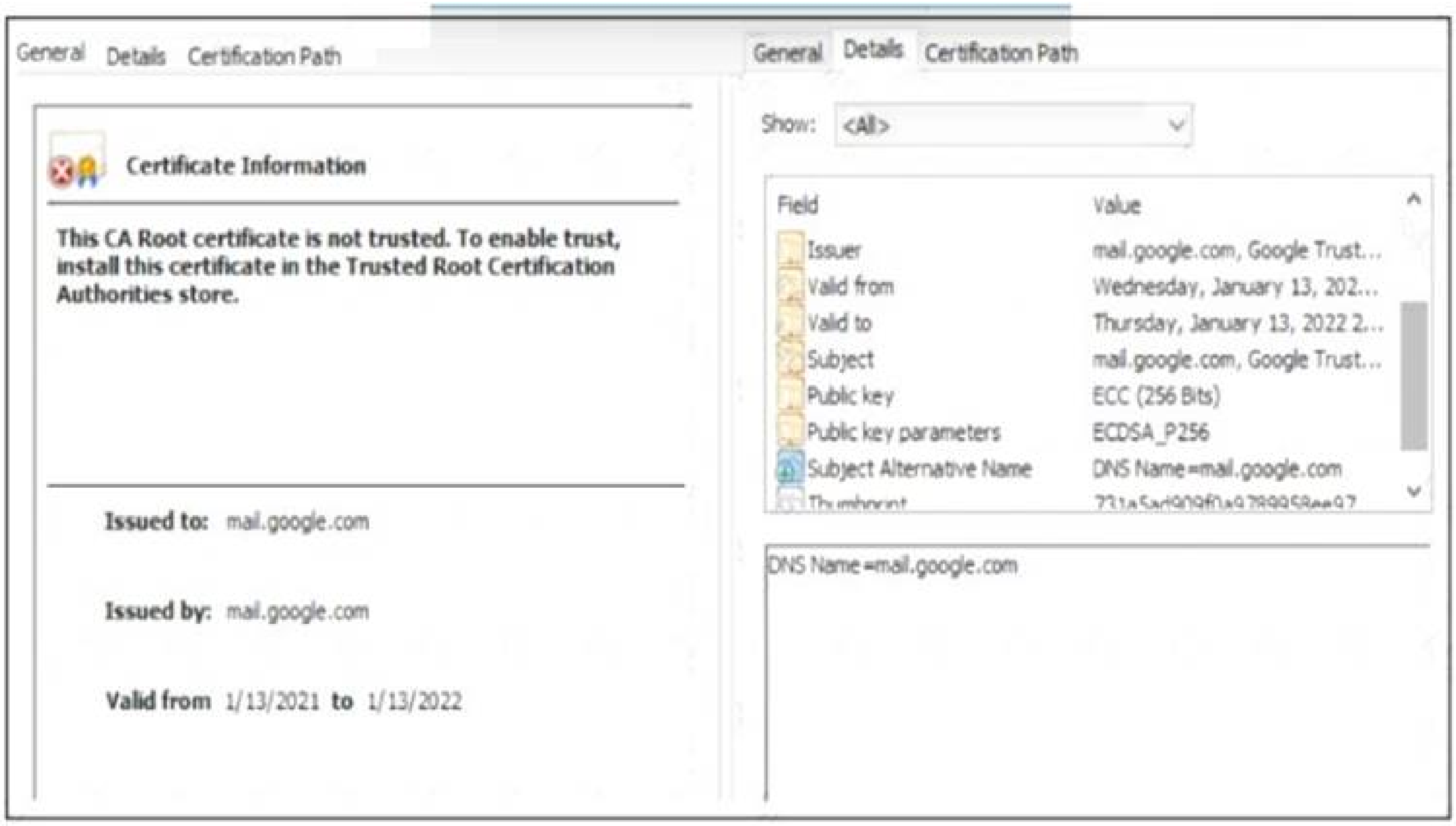
NEW QUESTION 288
Which security model assumes an attacker within and outside of the network and enforces strict verification
before connecting to any system or resource within the organization?

A. Biba
B. Object-capability
C. Take-Grant
D. Zero Trust

Answer: D

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 292
Refer to the exhibit.



General Details Certification Path

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: mail.google.com

Issued by: mail.google.com

Valid from 1/13/2021 to 1/13/2022

General Details Certification Path

Show: <All>

Field	Value
Issuer	mail.google.com, Google Trust...
Valid from	Wednesday, January 13, 202...
Valid to	Thursday, January 13, 2022 2...
Subject	mail.google.com, Google Trust...
Public key	ECC (256 Bits)
Public key parameters	ECDSA_P256
Subject Alternative Name	DNS Name=mail.google.com
Thumbprint	731a5ad909f0a9789958ee97

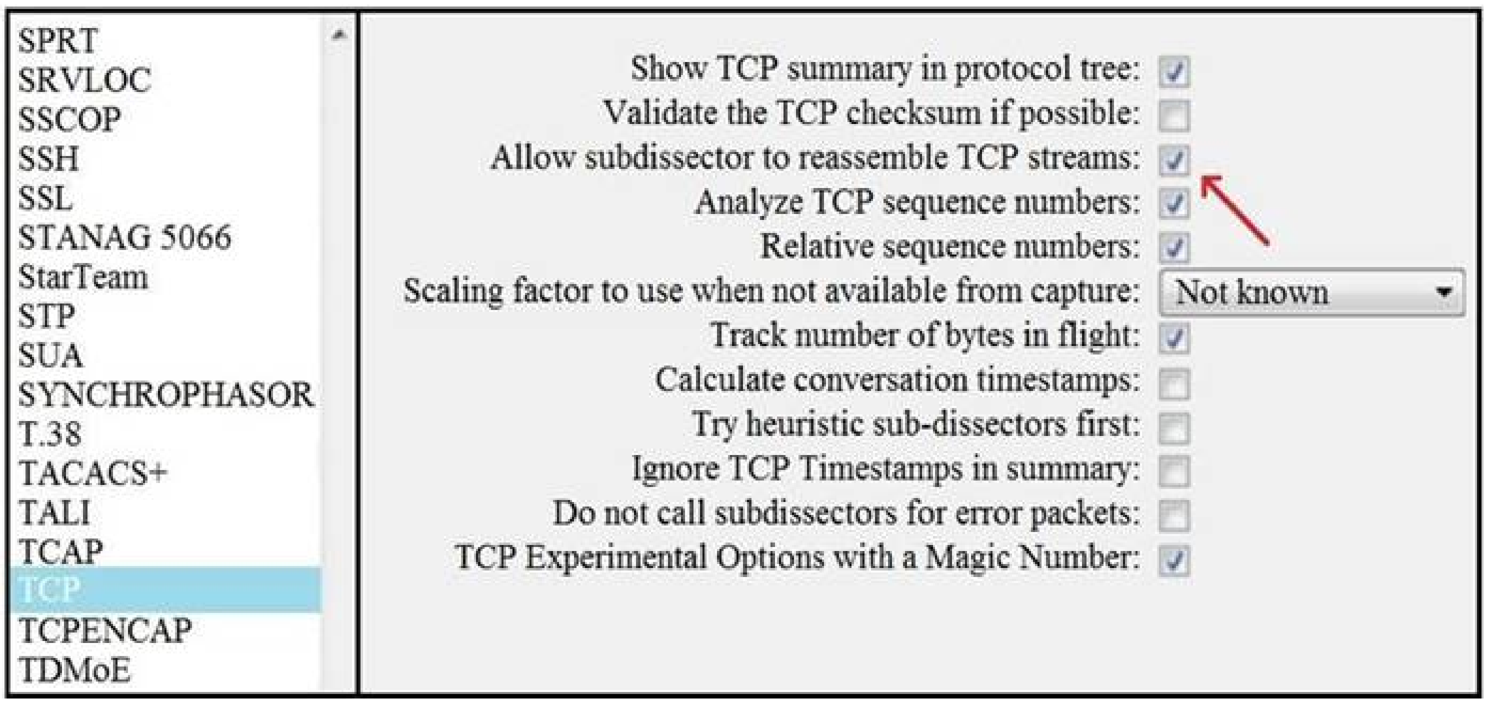
DNS Name=mail.google.com

A company employee is connecting to mail google.com from an endpoint device. The website is loaded but with an error. What is occurring?

A. DNS hijacking attack
B. Endpoint local time is invalid.
C. Certificate is not in trusted roots.
D. man-m-the-middle attack

Answer: C

NEW QUESTION 295
Refer to the exhibit.



SPRT
SRVLOC
SSCOP
SSH
SSL
STANAG 5066
StarTeam
STP
SUA
SYNCHROPHASOR
T.38
TACACS+
TALI
TCAP
TCP
TCPENCAP
TDMoE

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

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

A. insert TCP subdissectors
B. extract a file from a packet capture
C. disable TCP streams
D. unfragment TCP

Answer: D

NEW QUESTION 299
Which security technology guarantees the integrity and authenticity of all messages transferred to and from a web application?

A. Hypertext Transfer Protocol
B. SSL Certificate
C. Tunneling
D. VPN

Answer: B

NEW QUESTION 300
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. phishing email
B. sender
C. HR
D. receiver

Answer: B

NEW QUESTION 304
A developer is working on a project using a Linux tool that enables writing processes to obtain these required results:

- If the process is unsuccessful, a negative value is returned.
- If the process is successful, 0 value is returned to the child process, and the process ID is sent to the parent process.

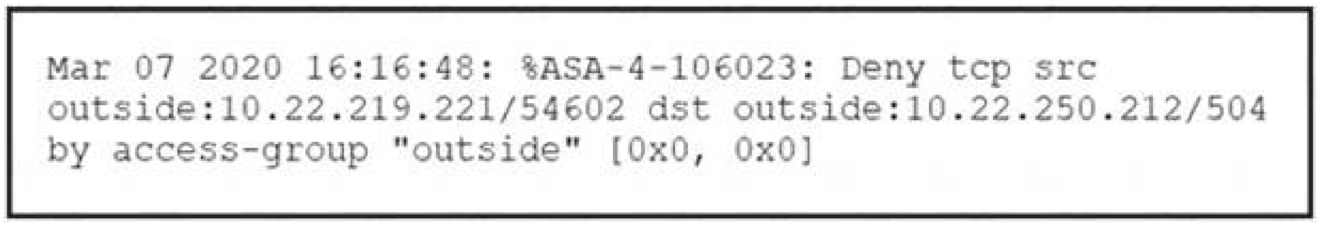
Which component results from this operation?

A. parent directory name of a file pathname
B. process spawn scheduled
C. macros for managing CPU sets
D. new process created by parent process

Answer: D

Explanation:
There are two tasks with specially distinguished process IDs: swapper or sched has process ID 0 and is responsible for paging, and is actually part of the kernel rather than a normal user-mode process. Process ID 1 is usually the init process primarily responsible for starting and shutting down the system. Originally, process ID 1 was not specifically reserved for init by any technical measures: it simply had this ID as a natural consequence of being the first process invoked by the kernel. More recent Unix systems typically have additional kernel components visible as 'processes', in which case PID 1 is actively reserved for the init process to maintain consistency with older systems

NEW QUESTION 305
Refer to the exhibit.



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

Which technology generates this log?

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

Answer: D

NEW QUESTION 308
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: B

NEW QUESTION 313
What are two denial-of-service (DoS) attacks? (Choose two)

A. port scan
B. SYN flood
C. man-in-the-middle
D. phishing
E. teardrop

Answer: BC

NEW QUESTION 315
What is a difference between SIEM and SOAR?

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

Answer: B

NEW QUESTION 316
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

NEW QUESTION 320
......

Relate Links

Contact us