



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

Which of these describes SOC metrics in relation to security incidents?

- A. time it takes to detect the incident
- B. time it takes to assess the risks of the incident
- C. probability of outage caused by the incident
- D. probability of compromise and impact caused by the incident

Answer: A

NEW QUESTION 3

When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification. Which information is available on the server certificate?

- A. server name, trusted subordinate CA, and private key
- B. trusted subordinate CA, public key, and cipher suites
- C. trusted CA name, cipher suites, and private key
- D. server name, trusted CA, and public key

Answer: D

NEW QUESTION 4

What is an advantage of symmetric over asymmetric encryption?

- A. A key is generated on demand according to data type.
- B. A one-time encryption key is generated for data transmission
- C. It is suited for transmitting large amounts of data.
- D. It is a faster encryption mechanism for sessions

Answer: D

NEW QUESTION 5

What makes HTTPS traffic difficult to monitor?

- A. SSL interception
- B. packet header size
- C. signature detection time
- D. encryption

Answer: D

NEW QUESTION 6

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

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

Answer: B

NEW QUESTION 7

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 8

Drag and drop the type of evidence from the left onto the description of that evidence on the right.

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 9

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

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 10

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 11

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. ^Parent File Clean\$
C. File: Clean (.*)
D. ^File: Clean\$

Answer: A

NEW QUESTION 15

What describes a buffer overflow attack?

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

Answer: C

NEW QUESTION 17

What is the difference between discretionary access control (DAC) and role-based access control (RBAC)?

- A. DAC requires explicit authorization for a given user on a given object, and RBAC requires specific conditions.
- B. RBAC access is granted when a user meets specific conditions, and in DAC, permissions are applied on user and group levels.
- C. RBAC is an extended version of DAC where you can add an extra level of authorization based on time.
- D. DAC administrators pass privileges to users and groups, and in RBAC, permissions are applied to specific groups

Answer: A

NEW QUESTION 22

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

An organization's security team has detected network spikes coming from the internal network. An investigation has concluded that the spike in traffic was from intensive network scanning. How should the analyst collect the traffic to isolate the suspicious host?

- A. by most active source IP
- B. by most used ports
- C. based on the protocols used
- D. based on the most used applications

Answer: A

NEW QUESTION 27

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

What is a benefit of using asymmetric cryptography?

- A. decrypts data with one key
- B. fast data transfer
- C. secure data transfer
- D. encrypts data with one key

Answer: C

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 30

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 35

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 36

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 blinkley
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.
27356	245.7772000	192.168.154.131	192.168.154.129	FTP	88	Response: 530 Login incorrect.

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

- A. dstport == FTP
- B. tcp.port==21
- C. tcpport = FTP
- D. dstport = 21

Answer: B

NEW QUESTION 37

Refer to the exhibit.

Security Intelligence Events (switch workflow)												
Security Intelligence with Application Details > Table View of Security Intelligence Events												
Search Constraints (Edit Search Serve Search)												
2018-03-02 07:20:20 - 2018-03-07 13:47:20												
Expanding Disabled Columns												
First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port/ICMP Type
2018-03-07 13:42:01		Sinkhole DNS Block		10.0.10.75		JERILABORDE (DCLOUD-SOC-LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
2018-03-07 13:42:01		Sinkhole DNS Block		10.0.0.100		AMPARO GIVENS (DCLOUD-SOC-LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
2018-03-07 13:42:01		Sinkhole DNS Block		10.112.10.158		VERNETTA DONNEL (DCLOUD-SOC-LDAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp

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

- A. First Packet
- B. Initiator User
- C. Ingress Security Zone
- D. Source Port
- E. Initiator IP

Answer: DE

NEW QUESTION 41

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

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

Answer: AE

Explanation:

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

NEW QUESTION 46

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 47

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 49

How does agentless monitoring differ from agent-based monitoring?

- A. Agentless can access the data via AP
- B. while agent-base uses a less efficient method and accesses log data through WMI.
- C. Agent-based monitoring is less intrusive in gathering log data, while agentless requires open ports to fetch the logs
- D. Agent-based monitoring has a lower initial cost for deployment, while agentless monitoring requires resource-intensive deployment.
- E. Agent-based has a possibility to locally filter and transmit only valuable data, while agentless has much higher network utilization

Answer: B

NEW QUESTION 54

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 56

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



NEW QUESTION 63

An engineer needs to fetch logs from a proxy server and generate actual events according to the data received. Which technology should the engineer use to accomplish this task?

- A. Firepower
- B. Email Security Appliance
- C. Web Security Appliance
- D. Stealthwatch

Answer: C

NEW QUESTION 65

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 69

What specific type of analysis is assigning values to the scenario to see expected outcomes?

- A. deterministic
- B. exploratory
- C. probabilistic
- D. descriptive

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 76

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. reconnaissance
- D. installation

Answer: B

NEW QUESTION 80

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 82

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

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

Answer: A

NEW QUESTION 84

Refer to the exhibit.

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

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

MAC Address: 08:0C:29:A2:6A:81 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 22.07 seconds
```

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

- A. Identified a firewall device preventing the port state from being returned.
- B. Identified open SMB ports on the server
- C. Gathered information on processes running on the server
- D. Gathered a list of Active Directory users

Answer: C

NEW QUESTION 87

What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

- A. least privilege
- B. need to know
- C. integrity validation
- D. due diligence

Answer: A

NEW QUESTION 91

Which process is used when IPS events are removed to improve data integrity?

- A. data availability
- B. data normalization
- C. data signature
- D. data protection

Answer: B

NEW QUESTION 92

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 96

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 101

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 104

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

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

Answer: C

NEW QUESTION 107

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

- A. destination IP address
- B. TCP ACK
- C. HTTP status code
- D. URI

Answer: D

NEW QUESTION 108

Refer to the exhibit.

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

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

What should be interpreted from this packet capture?

- A. 81.179.179.69 is sending a packet from port 80 to port 50272 of IP address 192.168.122.100 using UDP protocol.
- B. 192.168.122.100 is sending a packet from port 50272 to port 80 of IP address 81.179.179.69 using TCP protocol.
- C. 192.168.122.100 is sending a packet from port 80 to port 50272 of IP address 81.179.179.69 using UDP protocol.
- D. 81.179.179.69 is sending a packet from port 50272 to port 80 of IP address 192.168.122.100 using TCP UDP protocol.

Answer: B

NEW QUESTION 112

Drag and drop the access control models from the left onto the correct descriptions on the right.

MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC

NEW QUESTION 116

What is the function of a command and control server?

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

Answer: D

NEW QUESTION 119

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 123

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 128

Refer to the exhibit.

Interface: 192.168.1.29 --- 0x11		
Internet Address	Physical Address	Type
192.168.1.10	d8-a7-56-d7-19-ea	dynamic
192.168.1.67	d8-a7-56-d7-19-ea	dynamic
192.168.1.1	01-00-5e-00-00-16	static

What is occurring in this network?

- A. ARP cache poisoning

- B. DNS cache poisoning
- C. MAC address table overflow
- D. MAC flooding attack

Answer: A

NEW QUESTION 130

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

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

Answer: C

NEW QUESTION 135

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 136

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 137

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 142

How does an attacker observe network traffic exchanged between two users?

- A. port scanning
- B. man-in-the-middle
- C. command injection
- D. denial of service

Answer: B

NEW QUESTION 145

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 149

An engineer received an alert affecting the degraded performance of a critical server. Analysis showed a heavy CPU and memory load. What is the next step the engineer should take to investigate this resource usage?

- A. Run "ps -d" to decrease the priority state of high load processes to avoid resource exhaustion.
- B. Run "ps -u" to find out who executed additional processes that caused a high load on a server.
- C. Run "ps -ef" to understand which processes are taking a high amount of resources.
- D. Run "ps -m" to capture the existing state of daemons and map required processes to find the gap.

Answer: C

NEW QUESTION 151

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

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

Answer: D

NEW QUESTION 155

Refer to the exhibit.

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

What is occurring within the exhibit?

- A. regular GET requests
- B. XML External Entities attack
- C. insecure deserialization
- D. cross-site scripting attack

Answer: A

NEW QUESTION 157

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

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

Answer: C

NEW QUESTION 159

What is the difference between inline traffic interrogation (TAPS) and traffic mirroring (SPAN)?

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

Answer: D

NEW QUESTION 162

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 163

An employee reports that someone has logged into their system and made unapproved changes, files are out of order, and several documents have been placed in the recycle bin. The security specialist reviewed the system logs, found nothing suspicious, and was not able to determine what occurred. The software is up to

date; there are no alerts from antivirus and no failed login attempts. What is causing the lack of data visibility needed to detect the attack?

- A. The threat actor used a dictionary-based password attack to obtain credentials.
- B. The threat actor gained access to the system by known credentials.
- C. The threat actor used the teardrop technique to confuse and crash login services.
- D. The threat actor used an unknown vulnerability of the operating system that went undetected.

Answer: C

NEW QUESTION 166

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

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

Answer: CE

NEW QUESTION 170

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 174

An engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. Which command will accomplish this goal?

- A. `nmap --top-ports 192.168.1.0/24`
- B. `nmap -sP 192.168.1.0/24`
- C. `nmap -sL 192.168.1.0/24`
- D. `nmap -sV 192.168.1.0/24`

Answer: B

Explanation:

<https://explainshell.com/explain?cmd=nmap+-sP>

NEW QUESTION 177

What is the difference between vulnerability and risk?

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

Answer: C

NEW QUESTION 178

The SOC team has confirmed a potential indicator of compromise on an endpoint. The team has narrowed the executable file's type to a new trojan family. According to the NIST Computer Security Incident Handling Guide, what is the next step in handling this event?

- A. Isolate the infected endpoint from the network.
- B. Perform forensics analysis on the infected endpoint.
- C. Collect public information on the malware behavior.
- D. Prioritize incident handling based on the impact.

Answer: C

NEW QUESTION 180

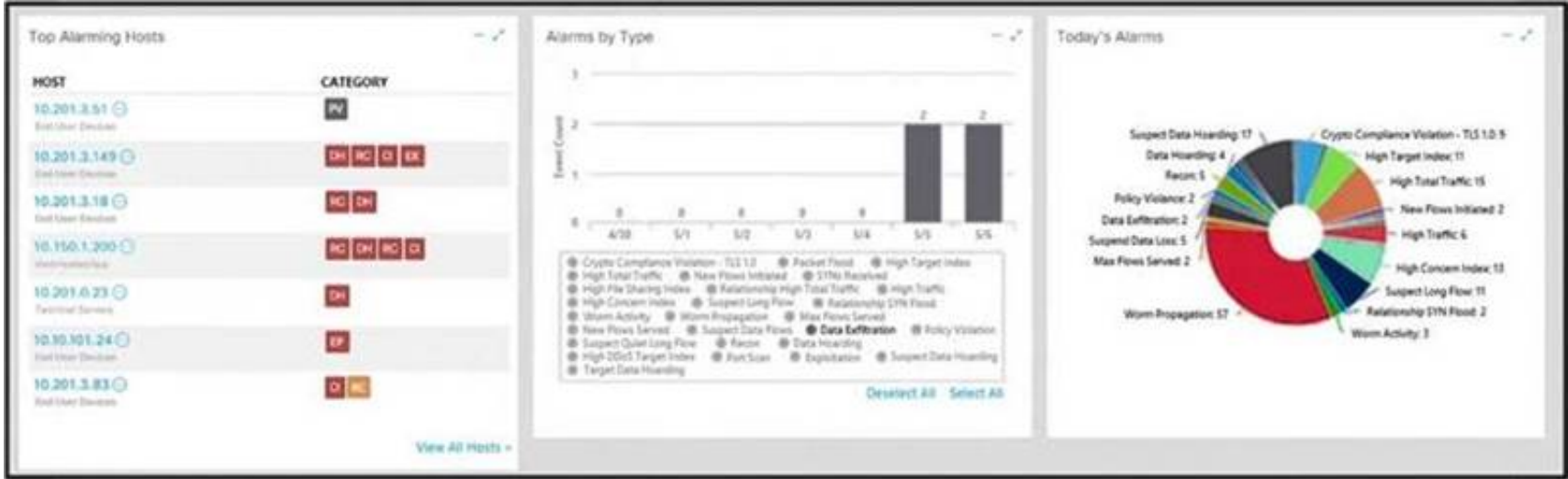
Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

- A. syslog messages
- B. full packet capture
- C. NetFlow
- D. firewall event logs

Answer: C

NEW QUESTION 182

Refer to the exhibit.



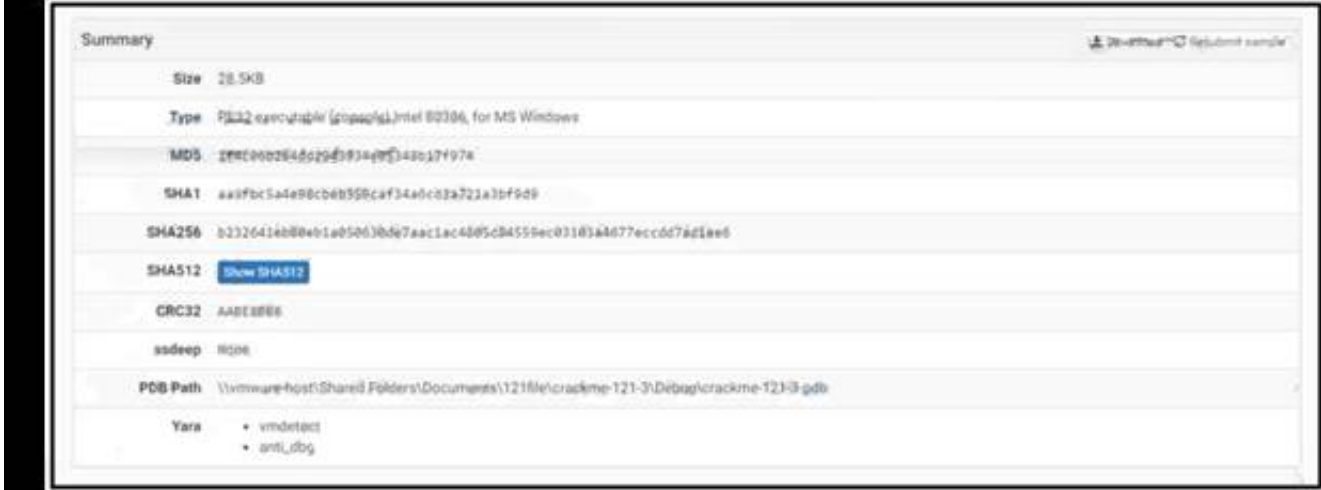
What is the potential threat identified in this Stealthwatch dashboard?

- A. A policy violation is active for host 10.10.101.24.
- B. A host on the network is sending a DDoS attack to another inside host.
- C. There are two active data exfiltration alerts.
- D. A policy violation is active for host 10.201.3.149.

Answer: C

NEW QUESTION 187

Refer to the exhibit.



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

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

Answer: B

NEW QUESTION 188

Refer to the exhibit.

Date	Flow Start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2020-01-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→ 192.168.0.1:20521	1	82	1

Which type of log is displayed?

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

Answer: B

NEW QUESTION 192

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 194

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 197

What should an engineer use to aid the trusted exchange of public keys between user tom0411976943 and dan1968754032?

- A. central key management server
- B. web of trust
- C. trusted certificate authorities
- D. registration authority data

Answer: C

NEW QUESTION 202

How does TOR alter data content during transit?

- A. It spoofs the destination and source information protecting both sides.
- B. It encrypts content and destination information over multiple layers.
- C. It redirects destination traffic through multiple sources avoiding traceability.
- D. It traverses source traffic through multiple destinations before reaching the receiver

Answer: B

NEW QUESTION 203

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

- A. principle of least privilege
- B. organizational separation
- C. separation of duties
- D. need to know principle

Answer: A

NEW QUESTION 208

An analyst discovers that a legitimate security alert has been dismissed. Which signature caused this impact on network traffic?

- A. true negative
- B. false negative
- C. false positive
- D. true positive

Answer: B

Explanation:

A false negative occurs when the security system (usually a WAF) fails to identify a threat. It produces a “negative” outcome (meaning that no threat has been observed), even though a threat exists.

NEW QUESTION 211

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

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 212

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
18	0.011918	10.0.2.15	192.124.249.9	TCP	78	50588→443 [FIN] Seq=1
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443→50588 [SYN, ACK]
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588→443 [ACK] Seq=1
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443→50586 [SYN, ACK]
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586→443 [ACK] Seq=1
23	0.023212	10.0.2.15	192.124.249.9	TCP	261	50588→443 [PSH, ACK]
24	0.023373	10.0.2.15	192.124.249.9	TCP	261	50586→443 [PSH, ACK]
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443→50588 [ACK] Seq=1
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443→50586 [ACK] Seq=1
27	0.037413	192.124.249.9	10.0.2.15	TCP	2792	443→50586 [PSH, ACK]
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586→443 [ACK] Seq=2

> Frame 24: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
 > Linux cooked capture
 > Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)
 > Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, A
 > Data [205 bytes]
 Data: 16030100c8010000c403030e06ead078d17676c13ab46ebf...
 [Length: 205]

0000	00 04 00 01 00 06 08 00	27 7a 3c 93 00 00 08 00 *z<.....
0010	45 00 00 f5 48 7b 40 00	40 06 2b f3 0a 00 02 0f	E...H{@. @.+.....
0020	c0 7c f9 09 c5 9a 01 bb	0e 1f dc b4 00 b4 aa 02
0030	50 18 72 10 c6 7c 00 00	16 03 01 00 c8 01 00 00	P.r..
0040	c4 03 03 0e 06 ea d0 78	d1 76 76 c1 3a b4 6e bfx .vv.:n..
0050	e6 b8 b8 b2 ba 08 d6 6d	0d 38 fb 91 45 de fc eem .8..E...
0060	8b 6e f8 00 00 1e c0 2b	c0 2f cc a9 cc a8 c0 2c	.n.....+ ./.....
0070	c0 30 c0 0a c0 09 c0 13	c0 14 00 33 00 39 00 2f	.0..... ...3.9./
0080	00 35 00 0a 01 00 00 7d	00 00 00 16 00 14 00 00	.5.....}
0090	11 77 77 77 2e 6c 69 6e	75 78 6d 69 6e 74 2e 63	.wwwlin uxmint.c
00a0	6f 6d 00 17 00 00 ff 01	00 01 00 00 0a 00 08 00	om.....
00b0	06 00 17 00 18 00 19 00	0b 00 02 01 00 00 23 00
00c0	00 33 74 00 00 00 10 00	17 00 15 02 68 32 08 73	.3t.....h2.s
00d0	70 64 79 2f 33 2e 31 08	68 74 74 70 2f 31 2e 31	pdv/3.1. http/1.1
00e0	00 05 00 05 01 00 00 00	00 00 0d 00 18 00 16 04
00f0	01 05 01 06 01 02 01 04	03 05 03 06 03 02 03 05
0100	02 04 02 02 02	

Which application protocol is in this PCAP file?

- A. SSH
- B. TCP
- C. TLS
- D. HTTP

Answer: D

NEW QUESTION 215

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

tcpdump	session data
web content filtering	full packet capture
traditional stateful firewall	transaction data
NetFlow	connection event

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

tcpdump	web content filtering
web content filtering	tcpdump
traditional stateful firewall	NetFlow
NetFlow	traditional stateful firewall

NEW QUESTION 218

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 219

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.2	10.128.0.2	TCP	54	3341 → 80 [SYN] Seq=0 Win=512 Len=0
2	0.003987	10.128.0.2	10.0.0.2	TCP	58	88 → 3222 [SYN, ACK] Seq=0 Ack=1 Win=29288 Len=0 MSS=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 MSS=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 MSS=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 MSS=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) on interface 0
 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 224

Refer to the exhibit.

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

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

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

Answer: D

NEW QUESTION 227

What is the difference between a threat and an exploit?

- A. A threat is a result of utilizing flow in a system, and an exploit is a result of gaining control over the system.

- B. A threat is a potential attack on an asset and an exploit takes advantage of the vulnerability of the asset
C. An exploit is an attack vector, and a threat is a potential path the attack must go through.
D. An exploit is an attack path, and a threat represents a potential vulnerability

Answer: B

NEW QUESTION 229

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 233

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

- A. colo?ur
B. col[08]+our
C. colou?r
D. col[09]+our

Answer: C

NEW QUESTION 238

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	090f9069a7780bca98286c3b4c0cae8			
SHA1	f891d31d3e4a5885a1738a136322d8ec979b79ba			
SHA256	f4855d1b10f7ab1a2e6b99016437f72c5f98579d69f08b6312cc24400f483177			
SHA512	9756e0a18981bc9296a3879fe02d0e182c5557ba99a004238ca4f1df083592cf497c123d2a6a0596607432188aef42976e0bd9da742c0900275b6721db2595			
Ssdeep	6144jEuZ0Y7e1LnfrB7pRL8I+5zLqJZ49XC0gNqGyCnuE/1r9Dep1YX1+oeYUPL:EuZ0Y7eand1d+SWG3ug97CK/1r7EE			
PEID	None matched			
Yara	* .shelcode (Matched shelcode 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 240

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 environment
C. an exploitable weakness in a system or its design
D. the individuals who perform an attack

Answer: C

Explanation:

An attack surface is the total sum of vulnerabilities that can be exploited to carry out a security attack. Attack surfaces can be physical or digital. The term attack surface is often confused with the term attack vector, but they are not the same thing. The surface is what is being attacked; the vector is the means by which an intruder gains access.

NEW QUESTION 244

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 249

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.

The threat actor engages in identification and selection of targets.	reconnaissance
An exploit is coupled with a remote access trojan.	weaponization
The weapon is transferred to the target environment.	delivery

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Weaponization: In this step, the intruder creates a malware weapon like a virus, worm or such in order to exploit the vulnerabilities of the target. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as the zero-day exploits) or it can focus on a combination of different vulnerabilities.

Reconnaissance: In this step, the attacker / intruder chooses their target. Then they conduct an in-depth research on this target to identify its vulnerabilities that can be exploited.

NEW QUESTION 253

What describes the impact of false-positive alerts compared to false-negative alerts?

- A. A false negative is alerting for an XSS attac
- B. An engineer investigates the alert and discovers that an XSS attack happened A false positive is when an XSS attack happens and no alert is raised
- C. A false negative is a legitimate attack triggering a brute-force aler
- D. An engineer investigates the alert and finds out someone intended to break into the system A false positive is when no alert and no attack is occurring
- E. A false positive is an event alerting for a brute-force attack An engineer investigates the alert and discovers that a legitimate user entered the wrong credential several times A false negative is when a threat actor tries to brute-force attack a system and no alert is raised.
- F. A false positive is an event alerting for an SQL injection attack An engineer investigates the alert and discovers that an attack attempt was blocked by IPS A false negative is when the attack gets detected but succeeds and results in a breach.

Answer: C

NEW QUESTION 257

How is NetFlow different from traffic mirroring?

- A. NetFlow collects metadata and traffic mirroring clones data.
- B. Traffic mirroring impacts switch performance and NetFlow does not.
- C. Traffic mirroring costs less to operate than NetFlow.
- D. NetFlow generates more data than traffic mirroring.

Answer: A

NEW QUESTION 258

Refer to the exhibit.

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

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

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

Answer: C

Explanation:

Indirect=circumstantial so there is no possibility to match A or B (only one answer is needed in this question). For 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 261

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 263

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: B

NEW QUESTION 265

Refer to the exhibit.

5585 43.600360	192.168.56.101	192.168.56.1	TCP	66 22 - 39978 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142352 TSecr=17155
5586 43.604379	192.168.56.101	192.168.56.1	SSHv2	148 Server: Encrypted packet (len=80)
5587 43.604402	192.168.56.1	192.168.56.101	SSHv2	162 Client: Encrypted packet (len=96)
5588 43.604497	192.168.56.101	192.168.56.1	TCP	86 22 - 39924 [ACK] Seq=1122 Ack=743 Win=30336 Len=0 TSval=3697142357 TSecr=17155
5589 43.611441	192.168.56.101	192.168.56.1	SSHv2	138 Server: Encrypted packet (len=64)
5590 43.611542	192.168.56.1	192.168.56.101	SSHv2	146 Client: Encrypted packet (len=80)
5591 43.611806	192.168.56.101	192.168.56.1	SSHv2	538 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=192)
5592 43.612193	192.168.56.1	192.168.56.101	SSHv2	82 Client: New Keys
5593 43.612287	192.168.56.101	192.168.56.1	TCP	66 22 - 39884 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142364 TSecr=17155
5594 43.612608	192.168.56.1	192.168.56.101	SSHv2	130 Client: Encrypted packet (len=64)
5595 43.612697	192.168.56.101	192.168.56.1	TCP	86 22 - 39884 [ACK] Seq=1594 Ack=823 Win=30336 Len=0 TSval=3697142365 TSecr=17155
5596 43.615355	192.168.56.101	192.168.56.1	SSHv2	187 Server: Protocol (SSH-2.0-OpenSSH_7.9p1 Debian 10+deb10u1)
5597 43.615375	192.168.56.1	192.168.56.101	TCP	66 39956 - 22 [ACK] Seq=23 Ack=42 Win=29312 Len=0 TSval=1715548358 TSecr=369714236
5598 43.615717	192.168.56.1	192.168.56.101	SSHv2	738 Client: Key Exchange Init
5599 43.616098	192.168.56.101	192.168.56.1	SSHv2	130 Server: Encrypted packet (len=64)
5600 43.619184	192.168.56.1	192.168.56.101	SSHv2	146 Client: Encrypted packet (len=80)
5601 43.624638	192.168.56.101	192.168.56.1	TCP	66 22 - 40018 [RST, ACK] Seq=1 Ack=23 Min=29856 Len=0 TSval=3697142377 TSecr=17155
5602 43.624751	192.168.56.101	192.168.56.1	TCP	66 22 - 40020 [RST, ACK] Seq=1 Ack=23 Min=29856 Len=0 TSval=3697142377 TSecr=17155
5603 43.624867	192.168.56.101	192.168.56.1	TCP	66 22 - 40022 [RST, ACK] Seq=1 Ack=23 Min=29856 Len=0 TSval=3697142377 TSecr=17155
5604 43.625018	192.168.56.101	192.168.56.1	TCP	66 22 - 40024 [RST, ACK] Seq=1 Ack=23 Min=29856 Len=0 TSval=3697142377 TSecr=17155
5605 43.625111	192.168.56.101	192.168.56.1	TCP	66 22 - 40026 [RST, ACK] Seq=1 Ack=23 Min=29856 Len=0 TSval=3697142377 TSecr=17155
5606 43.625723	192.168.56.101	192.168.56.1	TCP	66 22 - 40030 [RST, ACK] Seq=1 Ack=23 Min=29856 Len=0 TSval=3697142378 TSecr=17155
5607 43.625835	192.168.56.101	192.168.56.1	TCP	66 22 - 40032 [RST, ACK] Seq=1 Ack=23 Min=29856 Len=0 TSval=3697142378 TSecr=17155
5608 43.625985	192.168.56.101	192.168.56.1	TCP	66 22 - 40034 [RST, ACK] Seq=1 Ack=23 Min=29856 Len=0 TSval=3697142378 TSecr=17155
5609 43.626094	192.168.56.101	192.168.56.1	TCP	66 22 - 40038 [RST, ACK] Seq=1 Ack=23 Min=29856 Len=0 TSval=3697142378 TSecr=17155
5610 43.626193	192.168.56.101	192.168.56.1	TCP	66 22 - 40040 [RST, ACK] Seq=1 Ack=23 Min=29856 Len=0 TSval=3697142378 TSecr=17155
5611 43.626293	192.168.56.101	192.168.56.1	TCP	66 22 - 40042 [RST, ACK] Seq=1 Ack=23 Min=29856 Len=0 TSval=3697142378 TSecr=17155
5612 43.626788	192.168.56.101	192.168.56.1	SSHv2	538 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=192)
5613 43.627975	192.168.56.1	192.168.56.101	SSHv2	82 Client: New Keys
5614 43.627621	192.168.56.101	192.168.56.1	TCP	66 22 - 39978 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142380 TSecr=17155

An engineer is analyzing a PCAP file after a recent breach. An engineer identified that the attacker used an aggressive ARP scan to scan the hosts and found web and SSH servers. Further analysis showed several SSH Server Banner and Key Exchange Initiations. The engineer cannot see the exact data being transmitted over an encrypted channel and cannot identify how the attacker gained access. How did the attacker gain access?

- A. by using the buffer overflow in the URL catcher feature for SSH
- B. by using an SSH Tectia Server vulnerability to enable host-based authentication
- C. by using an SSH vulnerability to silently redirect connections to the local host
- D. by using brute force on the SSH service to gain access

Answer: C

NEW QUESTION 266

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 270

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 273

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 277

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

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

Answer: B

NEW QUESTION 282

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

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

Answer: B

NEW QUESTION 287

What is the difference between an attack vector and attack surface?

- A. An attack surface identifies vulnerabilities that require user input or validation; and an attack vector identifies vulnerabilities that are independent of user actions.
- B. An attack vector identifies components that can be exploited, and an attack surface identifies the potential path an attack can take to penetrate the network.
- C. An attack surface recognizes which network parts are vulnerable to an attack; and an attack vector identifies which attacks are possible with these vulnerabilities.
- D. An attack vector identifies the potential outcomes of an attack; and an attack surface launches an attack using several methods against the identified vulnerabilities.

Answer: C

NEW QUESTION 291

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 296

What is the difference between statistical detection and rule-based detection models?

- A. Rule-based detection involves the collection of data in relation to the behavior of legitimate users over a period of time
- B. Statistical detection defines legitimate data of users over a period of time and rule-based detection defines it on an IF/THEN basis
- C. Statistical detection involves the evaluation of an object on its intended actions before it executes that behavior
- D. Rule-based detection defines legitimate data of users over a period of time and statistical detection defines it on an IF/THEN basis

Answer: B

NEW QUESTION 300

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 305

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

- A. Tap mirrors existing traffic from specified ports, while SPAN presents more structured data for deeper analysis.
- B. SPAN passively splits traffic between a network device and the network without altering it, while Tap alters response times.
- C. SPAN improves the detection of media errors, while Tap provides direct access to traffic with lowered data visibility.
- D. Tap sends traffic from physical layers to the monitoring device, while SPAN provides a copy of network traffic from switch to destination

Answer: D

NEW QUESTION 310

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 315

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 318

How does statistical detection differ from rule-based detection?

- A. Statistical detection involves the evaluation of events, and rule-based detection requires an evaluated set of events to function.
- B. Statistical detection defines legitimate data over time, and rule-based detection works on a predefined set of rules
- C. Rule-based detection involves the evaluation of events, and statistical detection requires an evaluated set of events to function Rule-based detection defines
- D. legitimate data over a period of time, and statistical detection works on a predefined set of rules

Answer: B

NEW QUESTION 319

In a SOC environment, what is a vulnerability management metric?

- A. code signing enforcement
- B. full assets scan
- C. internet exposed devices
- D. single factor authentication

Answer: C

NEW QUESTION 324

Which type of data collection requires the largest amount of storage space?

- A. alert data
- B. transaction data
- C. session data
- D. full packet capture

Answer: D

NEW QUESTION 329

How does a certificate authority impact security?

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

Answer: D

Explanation:

A certificate authority is a computer or entity that creates and issues digital certificates. CA do not "authenticate" it validates. "D" is wrong because The digital certificate validate a user. CA --> DC --> user, server or whatever.

NEW QUESTION 331

While viewing packet capture data, an analyst sees that one IP is sending and receiving traffic for multiple devices by modifying the IP header. Which technology makes this behavior possible?

- A. encapsulation
- B. TOR
- C. tunneling
- D. NAT

Answer: D

Explanation:

Network address translation (NAT) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

NEW QUESTION 333

Which regular expression is needed to capture the IP address 192.168.20.232?

- A. ^(?:[0-9]{1,3}\.){3}[0-9]{1,3}
- B. ^(?:[0-9]{1,3}\.){1,4}
- C. ^(?:[0-9]{1,3}\.)'
- D. ^([0-9]-{3})

Answer: A

NEW QUESTION 336

How is attacking a vulnerability categorized?

- A. action on objectives
- B. delivery
- C. exploitation
- D. installation

Answer: C

NEW QUESTION 341

What is the impact of encryption?

- A. Confidentiality of the data is kept secure and permissions are validated
- B. Data is accessible and available to permitted individuals
- C. Data is unaltered and its integrity is preserved
- D. Data is secure and unreadable without decrypting it

Answer: A

NEW QUESTION 342

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: D

NEW QUESTION 346

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

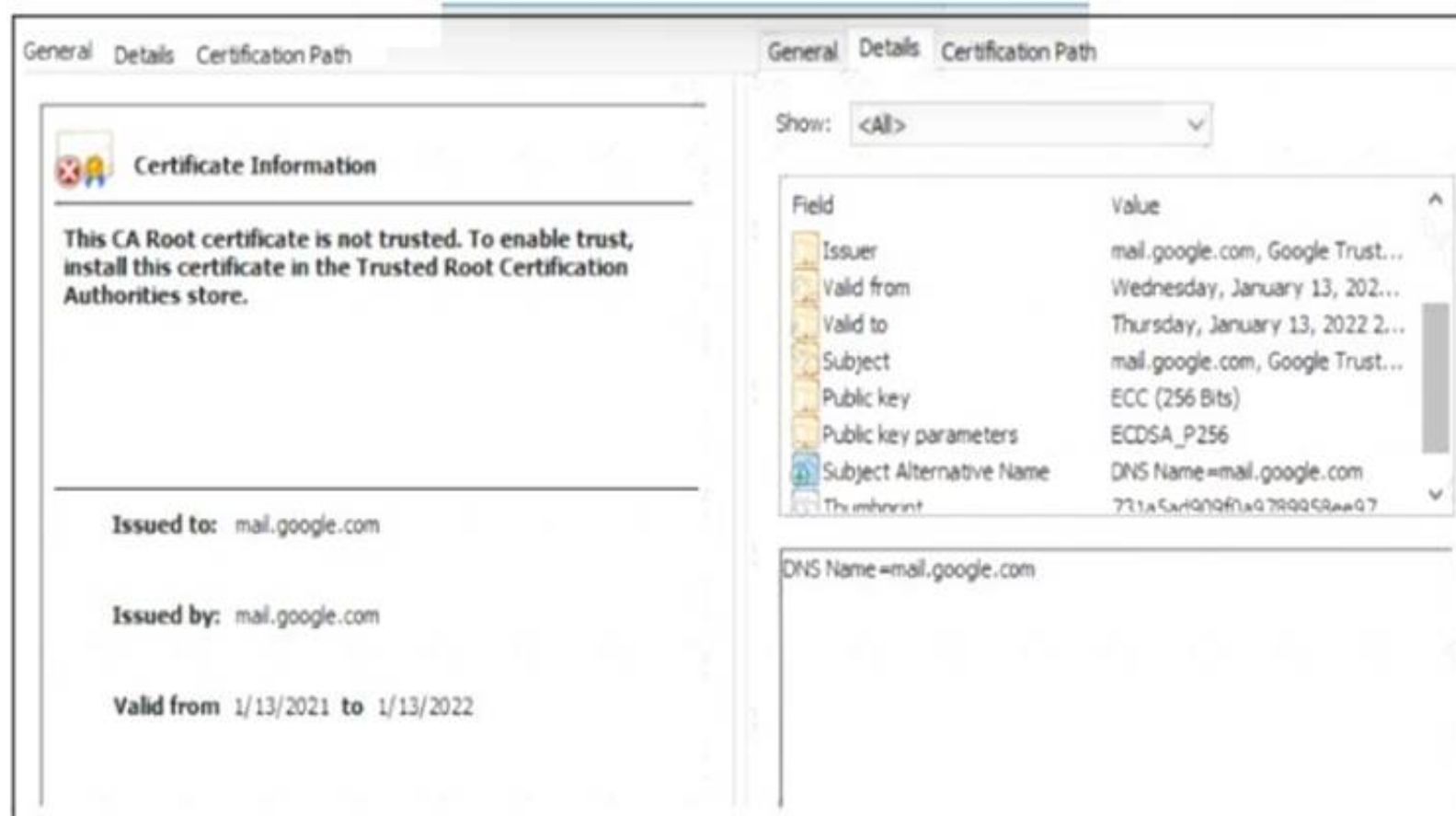
Answer: D

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 348

Refer to the exhibit.



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-in-the-middle attack

Answer: C

NEW QUESTION 349

Refer to the exhibit.

No.	Time	Source	Destination	Protoc	Length	Info
6	16:40:35.636314	195.144.107.198	192.168.31.44	FTP	104	Response: 227 Entering Passive Mode (195,144,107,198,4,2).
7	16:40:35.637786	192.168.31.44	195.144.107.198	FTP	82	Request: RETR ResumableTransfer.png
8	16:40:35.638091	192.168.31.44	195.144.107.198	TCP	66	1084 → 1026 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	16:40:35.696788	195.144.107.198	192.168.31.44	FTP	96	Response: 150 Opening BINARY mode data connection.
10	16:40:35.698384	195.144.107.198	192.168.31.44	TCP	66	1026 → 1084 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1456 WS=256 SACK
11	16:40:35.698521	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=1 Win=132352 Len=0
12	16:40:35.698802	192.168.31.44	195.144.107.198	TCP	54	[TCP Window Update] 1084 → 1026 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
13	16:40:35.739249	192.168.31.44	195.144.107.198	TCP	54	1031 → 21 [ACK] Seq=43 Ack=113 Win=513 Len=0
14	16:40:35.759825	195.144.107.198	192.168.31.44	FTP	2966	FTP Data: 2912 bytes (PASV) (RETR ResumableTransfer.png)
15	16:40:35.759925	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=2913 Win=4194304 Len=0
16	16:40:35.822152	195.144.107.198	192.168.31.44	FTP	5878	FTP Data: 5824 bytes (PASV) (RETR ResumableTransfer.png)
17	16:40:35.822263	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=0
18	16:40:35.883496	195.144.107.198	192.168.31.44	FTP	1510	FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)
19	16:40:35.883496	195.144.107.198	192.168.31.44	FTP	1408	FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)
20	16:40:35.883559	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=11547 Win=4194304 Len=0
21	16:40:35.944841	195.144.107.198	192.168.31.44	FTP	78	Response: 226 Transfer complete.
22	16:40:35.944841	195.144.107.198	192.168.31.44	TCP	54	1026 → 1084 [FIN, ACK] Seq=11547 Ack=1 Win=66816 Len=0
23	16:40:35.944978	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=11548 Win=4194304 Len=0
24	16:40:35.945371	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [FIN, ACK] Seq=1 Ack=11548 Win=4194304 Len=0

Which frame numbers contain a file that is extractable via TCP stream within Wireshark?

- A. 7,14, and 21
- B. 7 and 21
- C. 14,16,18, and 19
- D. 7 to 21

Answer: B

NEW QUESTION 354

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

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 357

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
14.	27.405297	192.168.1.83	192.168.1.80	HTTP	335	GET /news.php HTTP/1.1
14.	27.423516	192.168.1.80	192.168.1.83	HTTP	12	HTTP/1.0 200 OK (text/html)
14.	27.843983	192.168.1.83	192.168.1.80	HTTP	516	POST /admin/get.php HTTP/1.1
14.	27.856474	192.168.1.80	192.168.1.83	HTTP	519	HTTP/1.0 200 OK (text/html)
14.	28.053803	192.168.1.83	192.168.1.80	HTTP	276	POST /news.php HTTP/1.1
15.	28.065561	192.168.1.80	192.168.1.83	HTTP	11	HTTP/1.0 200 OK (text/html)
20.	33.245337	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
20.	33.253440	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
23.	38.265103	192.168.1.83	192.168.1.80	HTTP	250	GET /news.php HTTP/1.1
23.	38.271353	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
26.	43.291043	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
26.	43.298364	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
30.	48.311212	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
30.	48.322750	192.168.1.80	192.168.1.83	HTTP	340	HTTP/1.0 200 OK (text/html)
30.	48.439913	192.168.1.83	192.168.1.80	HTTP	148	POST /admin/get.php HTTP/1.1
30.	48.455743	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 404 NOT FOUND (text/html)
35.	53.482265	192.168.1.83	192.168.1.80	HTTP	255	GET /admin/get.php HTTP/1.1
35.	53.491062	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
40.	58.515011	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
40.	58.522942	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)

A network administrator is investigating suspicious network activity by analyzing captured traffic. An engineer notices abnormal behavior and discovers that the default user agent is present in the headers of requests and data being transmitted What is occurring?

- A. indicators of denial-of-service attack due to the frequency of requests
- B. garbage flood attack attacker is sending garbage binary data to open ports
- C. indicators of data exfiltration HTTP requests must be plain text
- D. cache bypassing attack: attacker is sending requests for noncacheable content

Answer: D

NEW QUESTION 361

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 364

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 369

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 371

Refer to the exhibit.

``

Which kind of attack method is depicted in this string?

- A. cross-site scripting
- B. man-in-the-middle
- C. SQL injection
- D. denial of service

Answer: A

NEW QUESTION 375

.....

Relate Links

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

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

Contact us

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

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