

## Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

<https://www.2passeasy.com/dumps/200-201/>



### NEW QUESTION 1

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

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

**Answer:** D

### NEW QUESTION 2

A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver. Which event category is described?

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

**Answer:** D

### NEW QUESTION 3

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 4

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 5

Refer to the exhibit.

#Time Format: Local													
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmp type icmpcode info path													
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63064	135	0	-	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.14	63065	49156	0	-	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63066	65386	0	-	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63067	389	0	-	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	UDP	10.40.4.182	10.40.1.14	62292	389	0	-	-	-	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63068	389	0	-	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63069	445	0	-	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	UDP	10.40.4.182	10.40.1.13	62293	389	0	-	-	-	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.13	63070	88	0	-	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63071	445	0	-	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63072	445	0	-	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63073	445	0	-	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.13	63074	88	0	-	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.13	63075	88	0	-	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.13	63076	88	0	-	0	0	-	SEND
2015-07-16	11:35:27	ALLOW	UDP	10.40.4.182	10.40.1.11	55053	53	0	-	-	-	-	SEND
2015-07-16	11:35:27	ALLOW	UDP	10.40.4.182	10.40.1.11	50845	53	0	-	-	-	-	SEND
2015-07-16	11:35:30	ALLOW	UDP	fe80::29ea:1a3c:24d6:fb49	ff02::1:3	57333	5355	0	-	-	-	-	RECEIVE
2015-07-16	11:35:30	ALLOW	UDP	10.40.4.252	224.0.0.252	59629	5355	0	-	-	-	-	RECEIVE
2015-07-16	11:35:30	ALLOW	UDP	fe80::4c2e:505d:b3a7:caaf	ff02::1:3	58846	5355	0	-	-	-	-	SEND
2015-07-16	11:35:30	ALLOW	UDP	10.40.4.182	224.0.0.252	58846	5355	0	-	-	-	-	SEND
2015-07-16	11:35:31	ALLOW	UDP	10.40.4.182	224.0.0.252	137	137	0	-	-	-	-	SEND
2015-07-16	11:35:31	ALLOW	UDP	fe80::4c2e:505d:b3a7:caaf	ff02::1:3	63504	5355	0	-	-	-	-	SEND
2015-07-16	11:35:31	ALLOW	UDP	10.40.4.182	224.0.0.252	63504	5355	0	-	-	-	-	SEND

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

- A. NetFlow

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

**Answer:** C

#### NEW QUESTION 6

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 7

Why is HTTPS traffic difficult to screen?

- A. HTTPS is used internally and screening traffic (or external parties is hard due to isolation.
- B. The communication is encrypted and the data in transit is secured.
- C. Digital certificates secure the session, and the data is sent at random intervals.
- D. Traffic is tunneled to a specific destination and is inaccessible to others except for the receiver.

**Answer:** B

#### NEW QUESTION 8

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

- A. Tapping interrogation replicates signals to a separate port for analyzing traffic
- B. Tapping interrogations detect and block malicious traffic
- C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies
- D. Inline interrogation detects malicious traffic but does not block the traffic

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 9

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 10

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 10**

Refer to the exhibit.

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		JERI LABORDE (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 12**

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

- A. True positives affect security as no alarm is raised when an attack has taken place, while false positives are alerts raised appropriately to detect and further mitigate them.
- B. True-positive alerts are blocked by mistake as potential attacks, while False-positives are actual attacks Identified as harmless.
- C. False-positive alerts are detected by confusion as potential attacks, while true positives are attack attempts identified appropriately.
- D. False positives alerts are manually ignored signatures to avoid warnings that are already acknowledged, while true positives are warnings that are not yet acknowledged.

**Answer:** C

**NEW QUESTION 17**

A company encountered a breach on its web servers using IIS 7.5. During 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 18**

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

- A. weaponization
- B. delivery
- C. exploitation
- D. reconnaissance

**Answer:** B

#### NEW QUESTION 23

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 28

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 31

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 32

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 37

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 38

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 43

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 45

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 50

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 51

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

ensures protection of individual devices	Endpoint
detects intrusion attempts	
monitors host for suspicious activity	
monitors incoming traffic and connections	Network

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

ensures protection of individual devices	Endpoint
	ensures protection of individual devices
detects intrusion attempts	
	monitors incoming traffic and connections
monitors host for suspicious activity	
monitors incoming traffic and connections	Network
	detects intrusion attempts
	monitors host for suspicious activity

#### NEW QUESTION 53

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 57

Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?

- A. decision making
- B. rapid response
- C. data mining
- D. due diligence

**Answer:** D

#### NEW QUESTION 58

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

- A. legal
- B. compliance
- C. regulated
- D. contractual

**Answer:** C

#### NEW QUESTION 59

What is personally identifiable information that must be safeguarded from unauthorized access?

- A. date of birth
- B. driver's license number
- C. gender
- D. zip code

**Answer:** B

#### Explanation:

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

The following are a few examples:

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

#### NEW QUESTION 60

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 65

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 67

Which HTTP header field is used in forensics to identify the type of browser used?

- A. referrer
- B. host
- C. user-agent
- D. accept-language

**Answer: C**

#### Explanation:

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:12.0) Gecko/20100101 Firefox/12.0 In computing, a user agent is any software, acting on behalf of a user, which "retrieves, renders and facilitates end-user interaction with Web content".[1] A user agent is therefore a special kind of software agent.

[https://en.wikipedia.org/wiki/User\\_agent#User\\_agent\\_identification](https://en.wikipedia.org/wiki/User_agent#User_agent_identification)

A user agent is a computer program representing a person, for example, a browser in a Web context. [https://developer.mozilla.org/en-US/docs/Glossary/User\\_agent](https://developer.mozilla.org/en-US/docs/Glossary/User_agent)

#### NEW QUESTION 69

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 72

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 77

Refer to the exhibit.

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

What is occurring?

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

**Answer: A**

#### NEW QUESTION 79

According to the NIST SP 800-86. which two types of data are considered volatile? (Choose two.)

- A. swap files
- B. temporary files
- C. login sessions
- D. dump files
- E. free space

**Answer: CE**



#### NEW QUESTION 84

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 takes actions to violate data integrity and availability.	Exploitation
The targeted environment is taken advantage of triggering the threat actor's code.	Installation
Backdoor is placed on the victim system allowing the threat actor to maintain the persistence.	Command and Control
An outbound connection is established to an Internet-based controller server.	Actions and Objectives

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Exploitation - The targeted Environment is taken advantage of triggering the threat actor's code  
 Installation - Backdoor is placed on the victim system allowing the threat actor to maintain the persistence.  
 Command and Control - An outbound connection is established to an Internet-based controller server.  
 Actions and Objectives - The threat actor takes actions to violate data integrity and availability

#### NEW QUESTION 85

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 90

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](https://docs.legato.io/16_10/basicIPC.html)

#### NEW QUESTION 95

An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the link launched, it infected machines and the intruder was able to access the corporate network. Which testing method did the intruder use?

- A. social engineering
- B. eavesdropping
- C. piggybacking
- D. tailgating

**Answer:** A

#### NEW QUESTION 96

Which attack method intercepts traffic on a switched network?

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

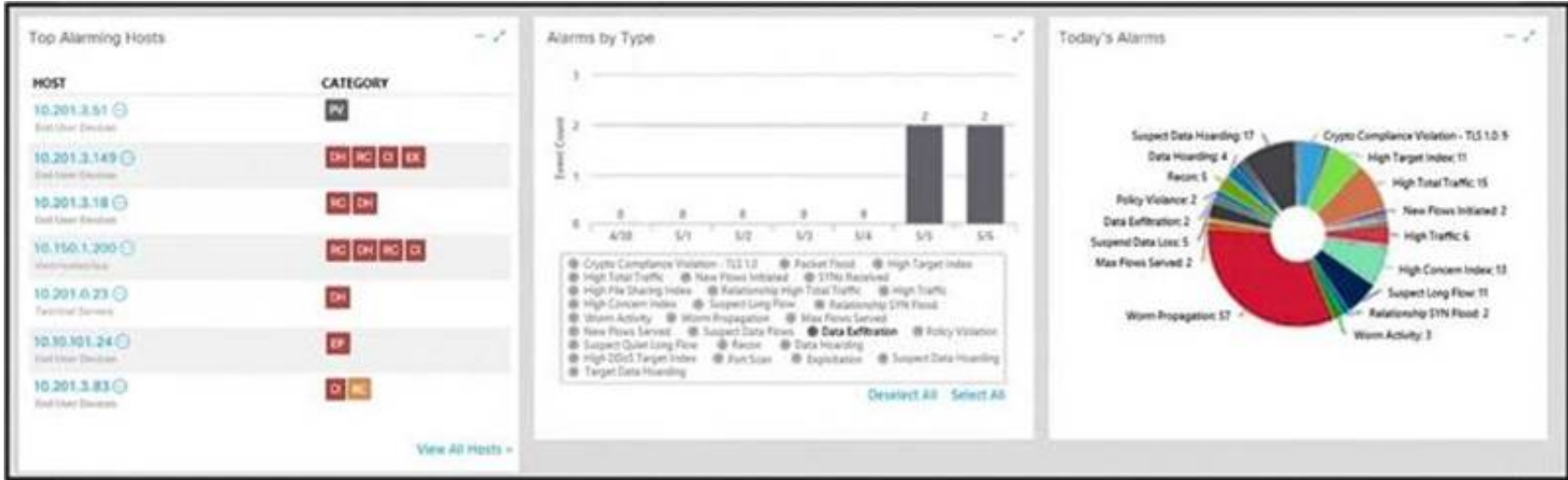
**Answer:** B

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 101

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 106

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 107

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 112

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 113

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 114

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 118

Which utility blocks a host portscan?

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

Answer: C

#### NEW QUESTION 122

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 126

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)
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 129

What are the two characteristics of the full packet captures? (Choose two.)

- A. Identifying network loops and collision domains.  
B. Troubleshooting the cause of security and performance issues.  
C. Reassembling fragmented traffic from raw data.  
D. Detecting common hardware faults and identify faulty assets.  
E. Providing a historical record of a network transaction.

Answer: CE

#### NEW QUESTION 130

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	09019069a77844a7829f29f2b64c0ce08			
SHA1	f891d31d3e4a5885d17b0136322d8ec979b79ba			
SHA256	f4855d1b1017ab1a2e6b99016437f72c5f98579d69f08b6312cc24400f483177			
SHA512	9756e0af8981bc9796a3879fe02d0e182c5557ba99a094236ca4f1df083592cf497c123d2a6a05996b07432188aef42976e0bd9da742c0900275b6721db2595			
Ssdeep	6144jEuZ0Y7e1LnfrB7pR18I+5zLqI249XCjgKqGyCyuE/1rMDep1XXt+o6YUPL:EuZ0Y7eand1d+SWGClgPCK/1r7EE			
PEID	None matched			
Yara	• shellcode (Matched shellcode byte patterns)			
VirusTotal	<a href="#">Permalink</a> 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 132

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 136

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 137

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

- A. management and reporting
- B. traffic filtering
- C. adaptive AVC
- D. metrics collection and exporting
- E. application recognition

Answer: AE

#### NEW QUESTION 139

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 140

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

- A. True positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.
- B. True positive alerts are blocked by mistake as potential attacks affecting application availability.
- C. False positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.
- D. False positive alerts are blocked by mistake as potential attacks affecting application availability.

Answer: C

#### NEW QUESTION 145

Refer to the exhibit.

5545 43.600368	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
5546 43.604379	192.168.56.101	192.168.56.1	SSHv2	148 Server: Encrypted packet (len=80)
5587 43.604462	192.168.56.1	192.168.56.101	SSHv2	148 Client: Encrypted packet (len=80)
5588 43.604497	192.168.56.101	192.168.56.1	TCP	66 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 43.611547	192.168.56.1	192.168.56.101	SSHv2	146 Client: Encrypted packet (len=80)
5591 43.611886	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 43.612668	192.168.56.1	192.168.56.101	SSHv2	138 Client: Encrypted packet (len=64)
5595 43.612697	192.168.56.101	192.168.56.1	TCP	66 22 - 39884 [ACK] Seq=1594 Ack=759 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 43.619098	192.168.56.101	192.168.56.1	SSHv2	138 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 Win=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 Win=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 Win=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 Win=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 Win=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 Win=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 Win=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 Win=29856 Len=0 TSval=3697142378 TSecr=17155
5609 43.626094	192.168.56.101	192.168.56.1	TCP	66 22 - 40036 [RST, ACK] Seq=1 Ack=23 Win=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 Win=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 Win=29856 Len=0 TSval=3697142378 TSecr=17155
5612 43.626738	192.168.56.101	192.168.56.1	SSHv2	538 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=192)
5613 43.627075	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 147

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 151

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 152

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 153

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 158

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 159

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

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

**Answer:** AB

#### NEW QUESTION 160

Refer to the exhibit.



What is shown in this PCAP file?

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

**Answer: D**

## NEW QUESTION 161

## 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 163**

Which tool provides a full packet capture from network traffic?

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

**Answer: D**

## NEW QUESTION 164

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

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

**Answer: D**

## NEW QUESTION 165

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 167

Refer to the exhibit.

SPRT	Show TCP summary in protocol tree:	<input checked="" type="checkbox"/>
SRVLOC	Validate the TCP checksum if possible:	<input type="checkbox"/>
SSCOP	Allow subdissector to reassemble TCP streams:	<input checked="" type="checkbox"/>
SSH	Analyze TCP sequence numbers:	<input checked="" type="checkbox"/>
SSL	Relative sequence numbers:	<input checked="" type="checkbox"/>
STANAG 5066	Scaling factor to use when not available from capture:	Not known
StarTeam	Track number of bytes in flight:	<input checked="" type="checkbox"/>
STP	Calculate conversation timestamps:	<input type="checkbox"/>
SUA	Try heuristic sub-dissectors first:	<input type="checkbox"/>
SYNCHROPHASOR	Ignore TCP Timestamps in summary:	<input type="checkbox"/>
T.38	Do not call subdissectors for error packets:	<input type="checkbox"/>
TACACS+	TCP Experimental Options with a Magic Number:	<input checked="" type="checkbox"/>
TALI		
TCAP		
TCP		
TCPENCAP		
TDMoE		

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 170

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 172

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

- A. IoA is the evidence that a security breach has occurred, and IoC allows organizations to act before the vulnerability can be exploited.
- B. IoA refers to the individual responsible for the security breach, and IoC refers to the resulting loss.
- C. IoC is the evidence that a security breach has occurred, and IoA allows organizations to act before the vulnerability can be exploited.
- D. IoC refers to the individual responsible for the security breach, and IoA refers to the resulting loss.

Answer: C

#### NEW QUESTION 177

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 178

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 183

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 185

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 200-201 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 200-201 Product From:

<https://www.2passeasy.com/dumps/200-201/>

## Money Back Guarantee

### 200-201 Practice Exam Features:

- \* 200-201 Questions and Answers Updated Frequently
- \* 200-201 Practice Questions Verified by Expert Senior Certified Staff
- \* 200-201 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 200-201 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year