

# Cisco

## Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals



#### NEW QUESTION 1

Refer to the exhibit.

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

Which kind of attack method is depicted in this string?

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

**Answer: A**

#### 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

An engineer must compare NIST vs ISO frameworks The engineer deeded to compare as readable documentation and also to watch a comparison video review. Using Windows 10 OS. the engineer started a browser and searched for a NIST document and then opened a new tab in the same browser and searched for an ISO document for comparison

The engineer tried to watch the video, but there 'was an audio problem with OS so the engineer had to troubleshoot it At first the engineer started CMD and looked fee a driver path then locked for a corresponding registry in the registry editor The engineer enabled "Audiosrv" in task manager and put it on auto start and the problem was solved Which two components of the OS did the engineer touch? (Choose two)

- A. permissions
- B. PowerShell logs
- C. service
- D. MBR
- E. process and thread

**Answer: AC**

#### NEW QUESTION 4

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

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

**Answer: D**

#### NEW QUESTION 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

Refer to the exhibit.

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

Which event is occurring?

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

**Answer: B**

**Explanation:**

<https://cuckoo.readthedocs.io/en/latest/usage/submit/>

#### NEW QUESTION 7

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 8

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 9

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

- A. Deep packet inspection gives insights up to Layer 7, and stateful inspection gives insights only up to Layer 4.
- B. Deep packet inspection is more secure due to its complex signatures, and stateful inspection requires less human intervention.
- C. Stateful inspection is more secure due to its complex signatures, and deep packet inspection requires less human intervention.
- D. Stateful inspection verifies data at the transport layer and deep packet inspection verifies data at the application layer

**Answer:** B

#### NEW QUESTION 10

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 10

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

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

**Answer:** D

#### NEW QUESTION 12

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.

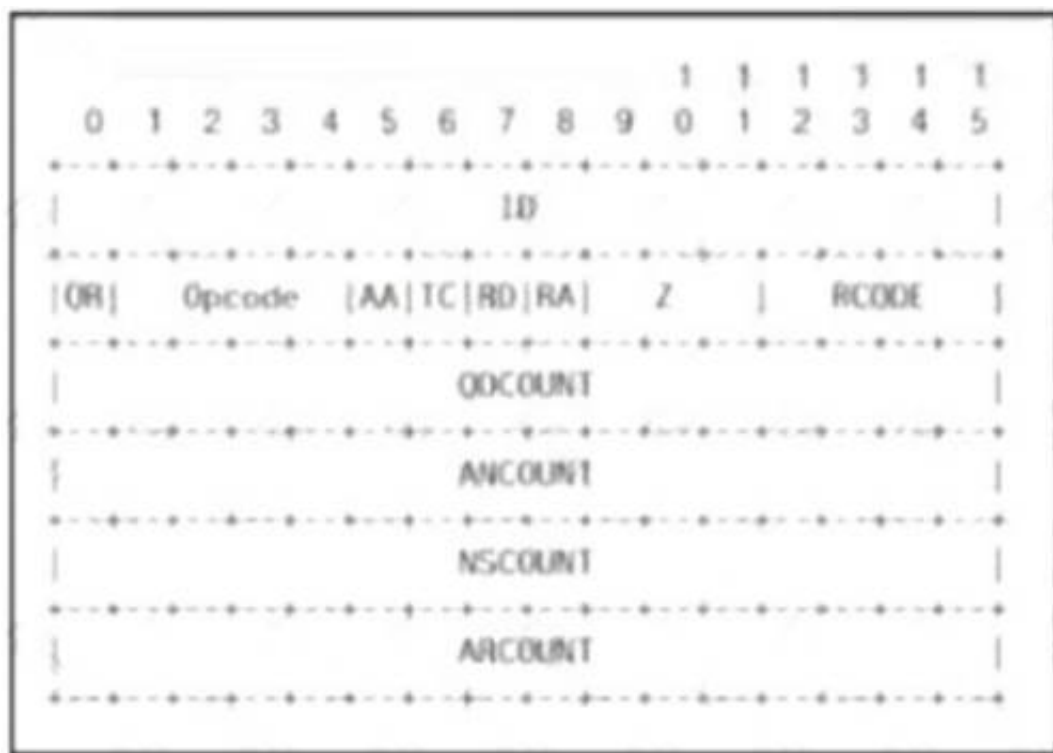
An analyst was given a PCAP file, which is associated with a recent intrusion event in the company FTP server Which display filters should the analyst use to filter the FTP traffic?

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

**Answer: B**

#### NEW QUESTION 17

Refer to the exhibit.



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

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

**Answer: B**

#### NEW QUESTION 21

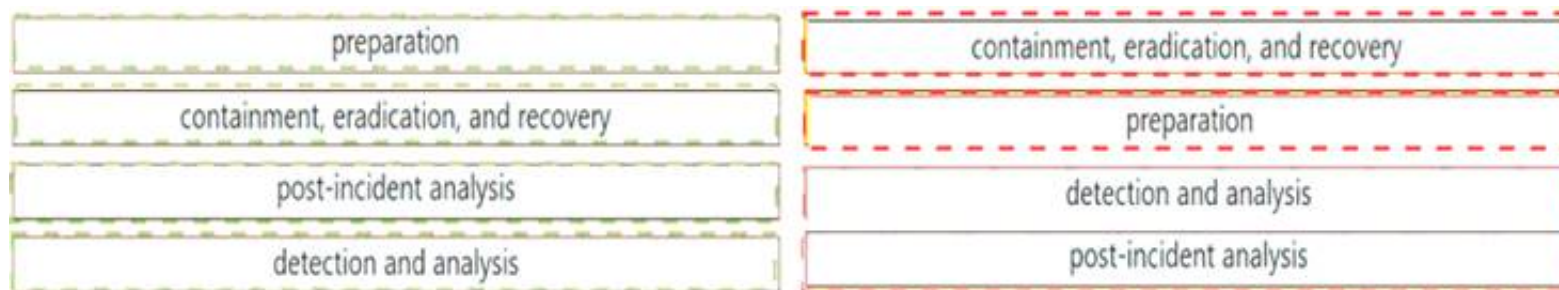
Drag and drop the elements from the left into the correct order for incident handling on the right.

preparation	create communication guidelines for effective incident handling
containment, eradication, and recovery	gather indicators of compromise and restore the system
post-incident analysis	document information to mitigate similar occurrences
detection and analysis	collect data from systems for further investigation

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



#### NEW QUESTION 23

Which two components reduce the attack surface on an endpoint? (Choose two.)

- A. secure boot
- B. load balancing
- C. increased audit log levels
- D. restricting USB ports
- E. full packet captures at the endpoint

**Answer:** AD

#### NEW QUESTION 25

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 28

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

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

**Answer:** B

#### NEW QUESTION 30

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 35

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 40

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 41



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: 00:0C:29:A2:6A:81 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 22.87 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 45

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

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

**Answer: C**

#### NEW QUESTION 48

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 52

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

- A. statistical data
- B. session data
- C. connectivity data
- D. alert data

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 57

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 59

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 62

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 67

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 69

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 73

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 74

What is threat hunting?

- A. Managing a vulnerability assessment report to mitigate potential threats.
- B. Focusing on proactively detecting possible signs of intrusion and compromise.
- C. Pursuing competitors and adversaries to infiltrate their system to acquire intelligence data.
- D. Attempting to deliberately disrupt servers by altering their availability

**Answer: B**

#### NEW QUESTION 75

An engineer is analyzing a recent breach where confidential documents were altered and stolen by the receptionist Further analysis shows that the threat actor connected an external USB device to bypass security restrictions and steal data The engineer could not find an external USB device Which piece of information must an engineer use for attribution in an investigation?

- A. list of security restrictions and privileges boundaries bypassed
- B. external USB device
- C. receptionist and the actions performed
- D. stolen data and its criticality assessment

**Answer: C**

#### NEW QUESTION 77

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 82

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 85

A security engineer deploys an enterprise-wide host/endpoint technology for all of the company's corporate PCs. Management requests the engineer to block a selected set of applications on all PCs. Which technology should be used to accomplish this task?

- A. application whitelisting/blacklisting
- B. network NGFW
- C. host-based IDS
- D. antivirus/antispyware software

**Answer: A**

#### NEW QUESTION 87

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 89

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 90

Which attack is the network vulnerable to when a stream cipher like RC4 is used twice with the same key?

- A. forgery attack
- B. plaintext-only attack
- C. ciphertext-only attack
- D. meet-in-the-middle attack

**Answer:** C

#### NEW QUESTION 94

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 97

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 99

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 100

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 101

Refer to the exhibit.



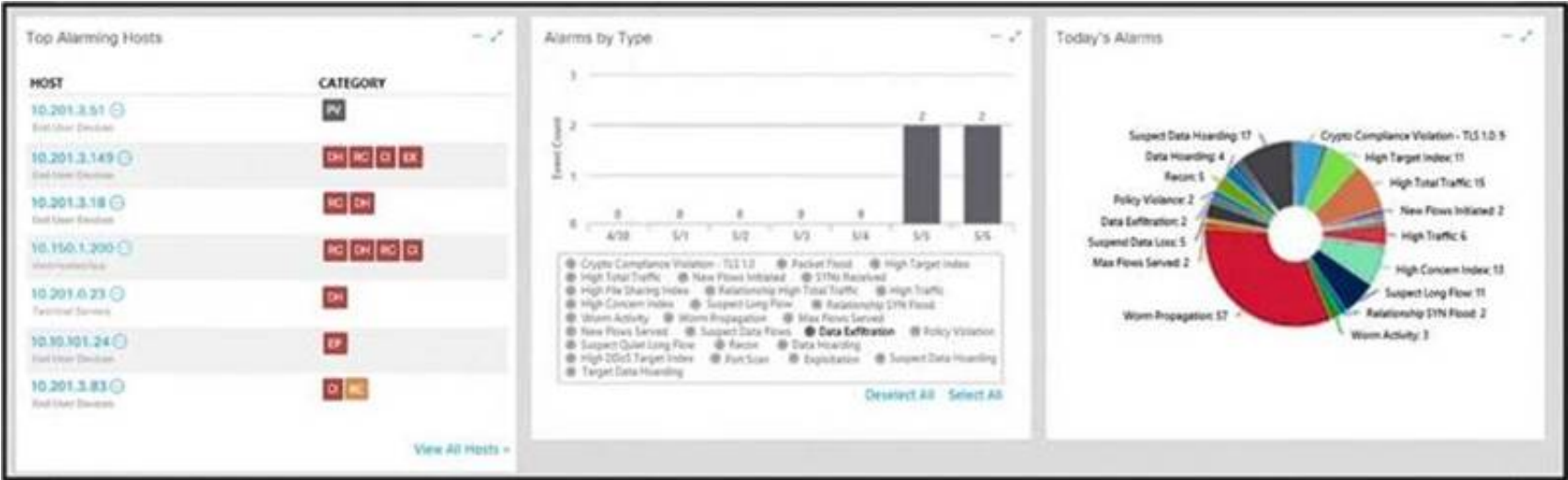
An engineer is reviewing a Cuckoo report of a file. What must the engineer interpret from the report?

- 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 105

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 108

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 110

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

threat	anything that can exploit a weakness that was not mitigated
risk	a gap in security or software that can be utilized by threats
vulnerability	possibility for loss and damage of an asset or information
exploit	taking advantage of a software flaw to compromise a resource

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Table Description automatically generated

NEW QUESTION 111

What is obtained using NetFlow?

- A. session data
- B. application logs

- C. network downtime report
- D. full packet capture

**Answer:** A

#### NEW QUESTION 115

Which utility blocks a host portscan?

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

**Answer:** C

#### NEW QUESTION 116

Refer to the exhibit.

```
443/tcp closed https
'nap done: 1. IP address (1 host up) scanned in 0.19 seconds
Ps C:\Program Files (x86)\Nmap> nmap --top-ports 10 172.31.45.240
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 22:05 Coordinated Universal Time
'nap scan report for ip-172-31-45-240.us-west-2.compute.internal (172.31.45.240)
Host is up (0.00s latency).

PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    closed http
110/tcp   closed pop3
139/tcp   open  netbios-ssn
443/tcp   closed https
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

'map done: 1 IP address (1 host up) scanned in 0.19 seconds PS
C:\Program Files (x86)\Nmap>
```

What does this output indicate?

- A. HTTPS ports are open on the server.
- B. SMB ports are closed on the server.
- C. FTP ports are open on the server.
- D. Email ports are closed on the server.

**Answer:** D

#### NEW QUESTION 117

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 120

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 125

Refer to the exhibit.

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

Which type of log is displayed?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 129

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 133

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 134

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

Which security principle requires more than one person is required to perform a critical task?

- A. least privilege
- B. need to know
- C. separation of duties
- D. due diligence

**Answer:** C

#### NEW QUESTION 142

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

- A. UDP port to which the traffic is destined
- B. TCP port from which the traffic was sourced
- C. source IP address of the packet
- D. destination IP address of the packet
- E. UDP port from which the traffic is sourced



Answer: CD

#### NEW QUESTION 144

Refer to the exhibit.

5585 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
5586 43.604379	192.168.56.101	192.168.56.1	SSHv2	146 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	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	130 Server: Encrypted packet (len=64)
5590 43.611542	192.168.56.1	192.168.56.101	SSHv2	146 Client: Encrypted packet (len=80)
5591 43.611886	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 43.612608	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	66 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=19312 Len=0 TSval=1715540358 TSecr=369714236
5598 43.615717	192.168.56.1	192.168.56.101	SSHv2	738 Client: Key Exchange Init
5599 43.616096	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 - 48818 [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 - 48820 [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 - 48822 [RST, ACK] Seq=1 Ack=23 Win=29856 Len=0 TSval=3697142377 TSecr=17155
5604 43.625010	192.168.56.101	192.168.56.1	TCP	66 22 - 48824 [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 - 48826 [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 - 48830 [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 - 48832 [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 - 48834 [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 - 48838 [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 - 48840 [RST, ACK] Seq=1 Ack=23 Win=29856 Len=0 TSval=3697142378 TSecr=17155
5611 43.626283	192.168.56.101	192.168.56.1	TCP	66 22 - 48842 [RST, ACK] Seq=1 Ack=23 Win=29856 Len=0 TSval=3697142378 TSecr=17155
5612 43.626718	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=3697142388 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 146

Refer to the exhibit.



What is the potential threat identified in this Stealthwatch dashboard?

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

Answer: C

#### Explanation:

"EX" = exfiltration. And there are three.

Also the "suspect long flow" and "suspect data heading" suggest, for example, DNS exfiltration.

[https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management\\_console/smc\\_users\\_guide/SW\\_6\\_page\\_177](https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6_page_177).

#### NEW QUESTION 150

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 154

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 155

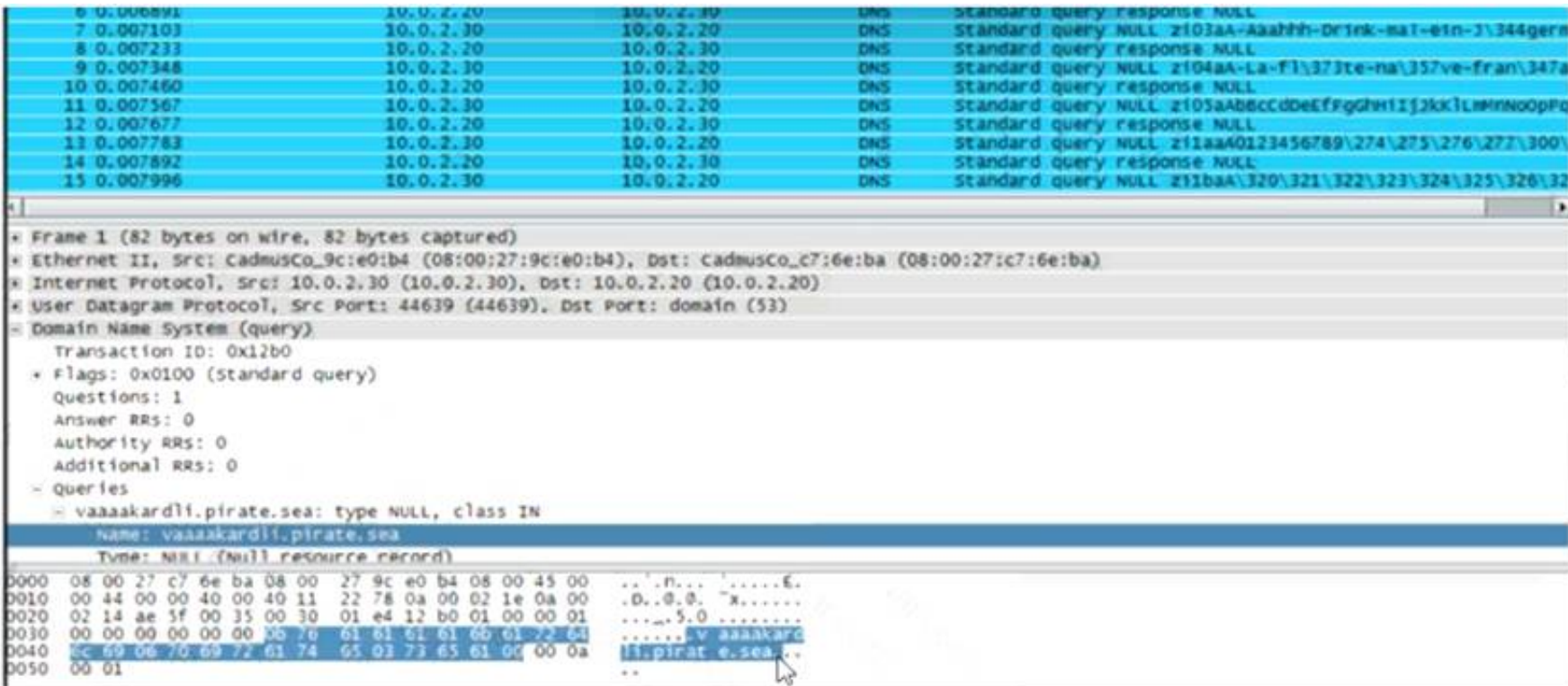
Which filter allows an engineer to filter traffic in Wireshark to further analyze the PCAP file by only showing the traffic for LAN 10.11.x.x, between workstations and servers without the Internet?

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

**Answer: B**

#### NEW QUESTION 156

Refer to the exhibit.



What is occurring?

- A. ARP flood
- B. DNS amplification
- C. ARP poisoning
- D. DNS tunneling

**Answer: D**

#### NEW QUESTION 160

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

```
File      Actions      Edit      View      Help

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

Which obfuscation technique is the attacker using?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 163**

What is a description of a social engineering attack?

- A. fake offer for free music download to trick the user into providing sensitive data
- B. package deliberately sent to the wrong receiver to advertise a new product
- C. mistakenly received valuable order destined for another person and hidden on purpose
- D. email offering last-minute deals on various vacations around the world with a due date and a counter

**Answer:** D

**NEW QUESTION 168**

Which action prevents buffer overflow attacks?

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

**Answer:** C

**NEW QUESTION 170**

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 171**

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 173

Which tool provides a full packet capture from network traffic?

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

**Answer:** D

#### NEW QUESTION 176

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 180

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 182

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 187

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 192

What is a purpose of a vulnerability management framework?

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

**Answer:** A



#### NEW QUESTION 197

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 200

Which attack represents the evasion technique of resource exhaustion?

- A. SQL injection
- B. man-in-the-middle
- C. bluesnarfing
- D. denial-of-service

**Answer: D**

#### NEW QUESTION 204

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 208

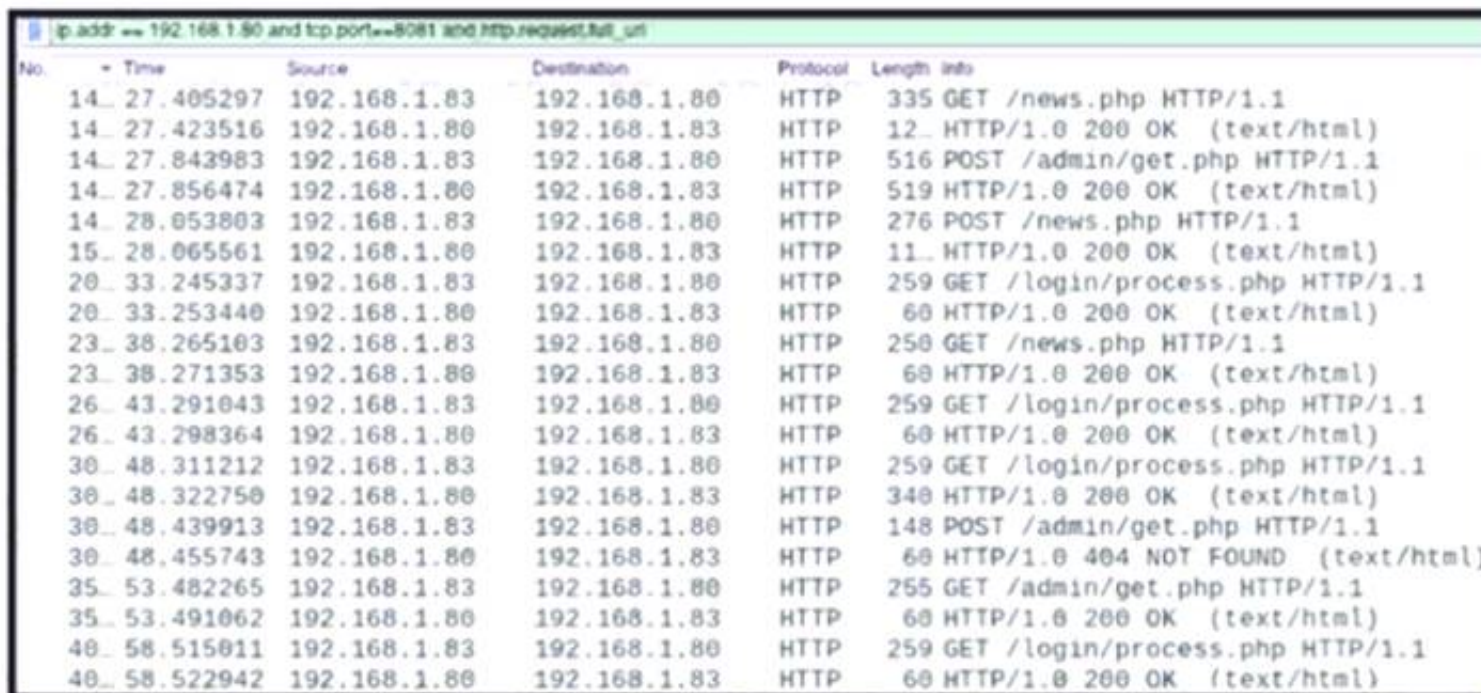
Which security technology guarantees the integrity and authenticity of all messages transferred to and from a web application?

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

**Answer: B**

#### NEW QUESTION 213

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 214**

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

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

**Answer:** BC

**NEW QUESTION 216**

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 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 First Try
- \* 200-201 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 200-201 Practice Test Here](#)**