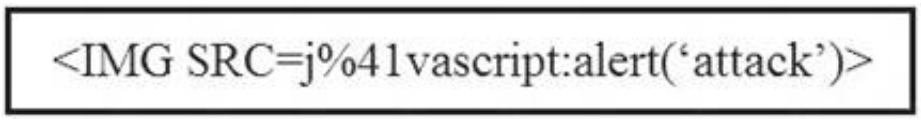
Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

NEW QUESTION 1
Refer to the exhibit.



Which kind of attack method is depicted in this string?

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

Answer: A

NEW QUESTION 2
What is a difference between SIEM and SOAR?

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

Answer: B

NEW QUESTION 3
What causes events on a Windows system to show Event Code 4625 in the log messages?

A. The system detected an XSS attack
B. Someone is trying a brute force attack on the network
C. Another device is gaining root access to the system
D. A privileged user successfully logged into the system

Answer: B

NEW QUESTION 4
When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification.
Which information is available on the server certificate?

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

Answer: D

NEW QUESTION 5
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

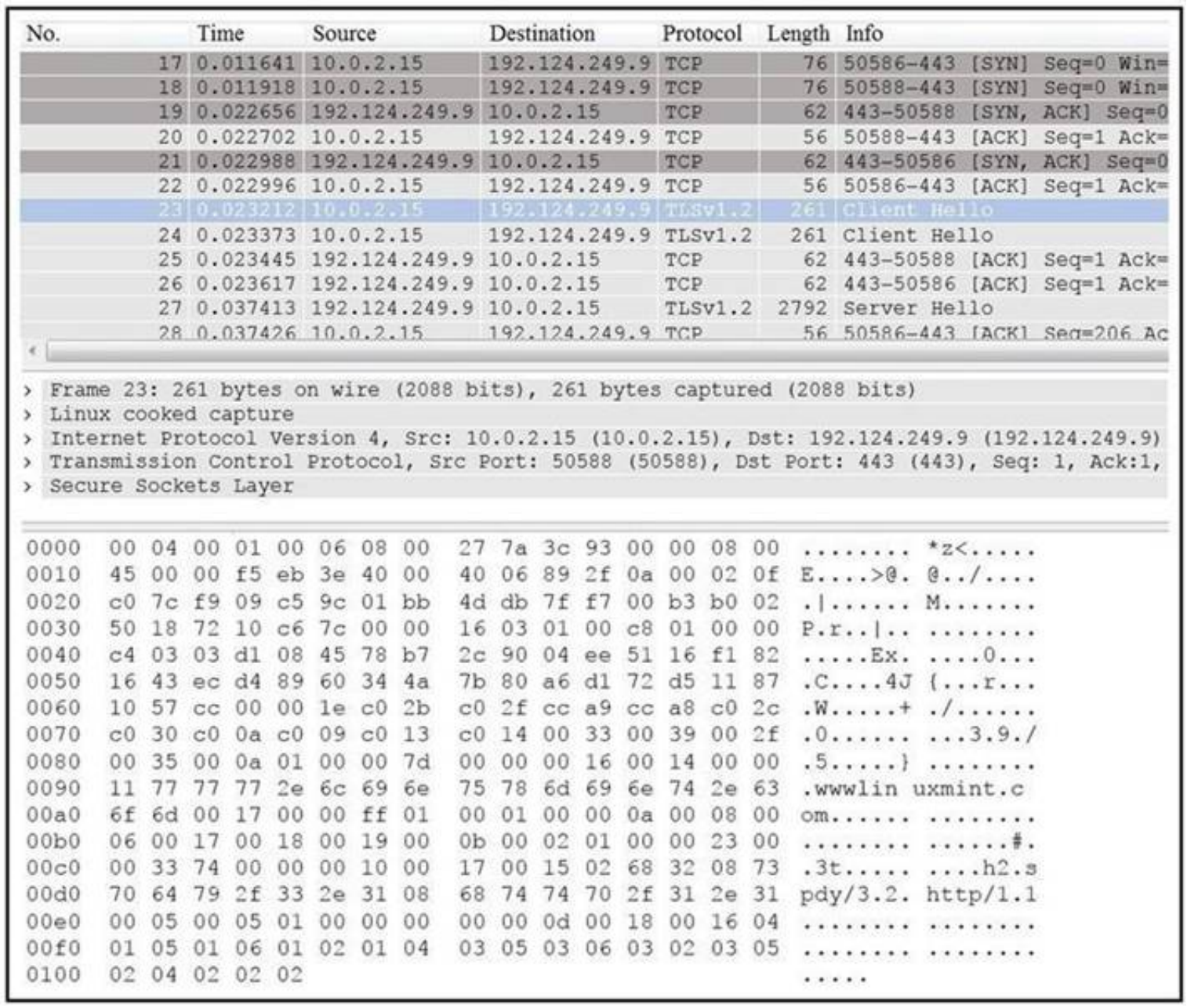
Explanation:
* 3.3.3 Identifying the Attacking Hosts During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts. Although this information can be important, incident handlers should generally stay focused on containment, eradication, and recovery.
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 6
What is a collection of compromised machines that attackers use to carry out a DDoS attack?

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

Answer: B

NEW QUESTION 7
Refer to the exhibit.



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

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

0000  00 04 00 01 00 06 08 00  27 7a 3c 93 00 00 08 00  ........ *z<.....
0010  45 00 00 f5 eb 3e 40 00  40 06 89 2f 0a 00 02 0f  E....>@. @../....
0020  c0 7c f9 09 c5 9c 01 bb  4d db 7f f7 00 b3 b0 02  .|...... M.......
0030  50 18 72 10 c6 7c 00 00  16 03 01 00 c8 01 00 00  P.r..|.. ........
0040  c4 03 03 d1 08 45 78 b7  2c 90 04 ee 51 16 f1 82  .....Ex. ....0...
0050  16 43 ec d4 89 60 34 4a  7b 80 a6 d1 72 d5 11 87  .C....4J {...r...
0060  10 57 cc 00 00 1e c0 2b  c0 2f cc a9 cc a8 c0 2c  .W.....+ ./......
0070  c0 30 c0 0a c0 09 c0 13  c0 14 00 33 00 39 00 2f  .0...... ...3.9./
0080  00 35 00 0a 01 00 00 7d  00 00 00 16 00 14 00 00  .5.....} ........
0090  11 77 77 77 2e 6c 69 6e  75 78 6d 69 6e 74 2e 63  .wwwlin uxmint.c
00a0  6f 6d 00 17 00 00 ff 01  00 01 00 00 0a 00 08 00  om...... ........
00b0  06 00 17 00 18 00 19 00  0b 00 02 01 00 00 23 00  ........ ......#.
00c0  00 33 74 00 00 00 10 00  17 00 15 02 68 32 08 73  .3t..... ....h2.s
00d0  70 64 79 2f 33 2e 31 08  68 74 74 70 2f 31 2e 31  pdy/3.2. http/1.1
00e0  00 05 00 05 01 00 00 00  00 00 0d 00 18 00 16 04  ........ ........
00f0  01 05 01 06 01 02 01 04  03 05 03 06 03 02 03 05  ........ ........
0100  02 04 02 02 02                                    .....
```

Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 8
What makes HTTPS traffic difficult to monitor?

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

Answer: D

NEW QUESTION 9
An engineer needs to configure network systems to detect command and control communications by decrypting ingress and egress perimeter traffic and allowing network security devices to detect malicious outbound communications. Which technology should be used to accomplish the task?

A. digital certificates
B. static IP addresses
C. signatures
D. cipher suite

Answer: A

NEW QUESTION 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
What is a benefit of using asymmetric cryptography?

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

Answer: C

NEW QUESTION 11
A company is using several network applications that require high availability and responsiveness, such that milliseconds of latency on network traffic is not acceptable. An engineer needs to analyze the network and identify ways to improve traffic movement to minimize delays. Which information must the engineer obtain for this analysis?

A. total throughput on the interface of the router and NetFlow records
B. output of routing protocol authentication failures and ports used
C. running processes on the applications and their total network usage
D. deep packet captures of each application flow and duration

Answer: C

NEW QUESTION 12
A security engineer has a video of a suspect entering a data center that was captured on the same day that files in the same data center were transferred to a competitor.
Which type of evidence is this?

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

Answer: C

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

NEW QUESTION 14
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 19
What is the difference between mandatory access control (MAC) and discretionary access control (DAC)?

A. MAC is controlled by the discretion of the owner and DAC is controlled by an administrator
B. MAC is the strictest of all levels of control and DAC is object-based access
C. DAC is controlled by the operating system and MAC is controlled by an administrator
D. DAC is the strictest of all levels of control and MAC is object-based access

Answer: B

NEW QUESTION 21
Which list identifies the information that the client sends to the server in the negotiation phase of the TLS handshake?

A. ClientStart, ClientKeyExchange, cipher-suites it supports, and suggested compression methods
B. ClientStart, TLS versions it supports, cipher-suites it supports, and suggested compression methods
C. ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression methods
D. ClientHello, ClientKeyExchange, cipher-suites it supports, and suggested compression methods

Answer: C

NEW QUESTION 22
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

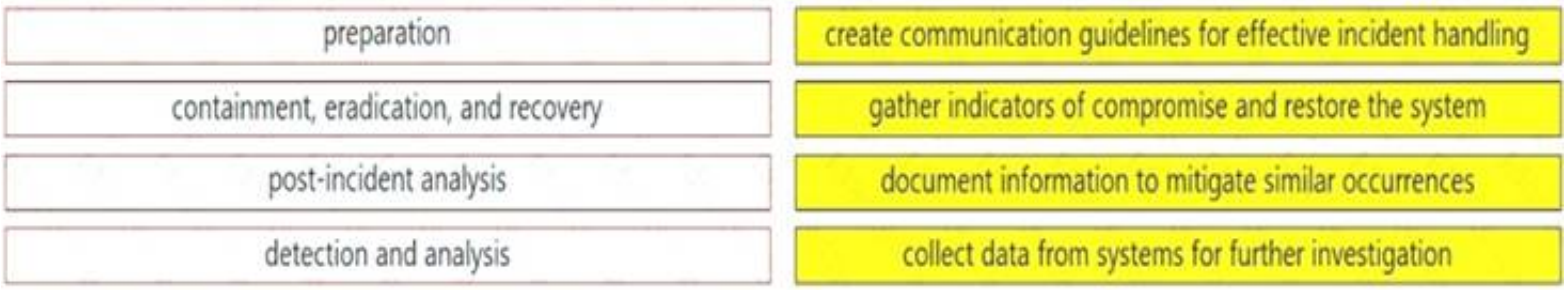
Answer: B

NEW QUESTION 26
Which event is user interaction?

A. gaining root access
B. executing remote code
C. reading and writing file permission
D. opening a malicious file

Answer: D

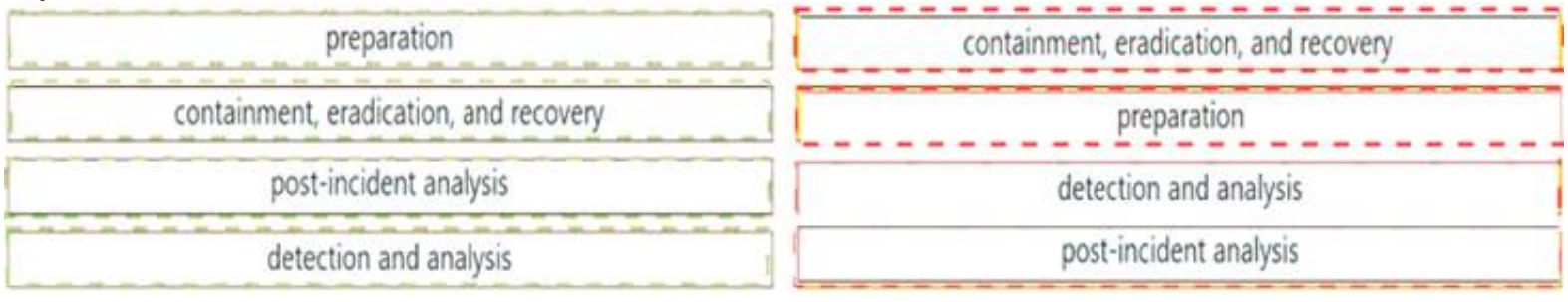
NEW QUESTION 28
Drag and drop the elements from the left into the correct order for incident handling on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 29
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 30
What specific type of analysis is assigning values to the scenario to see expected outcomes?

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

Answer: A

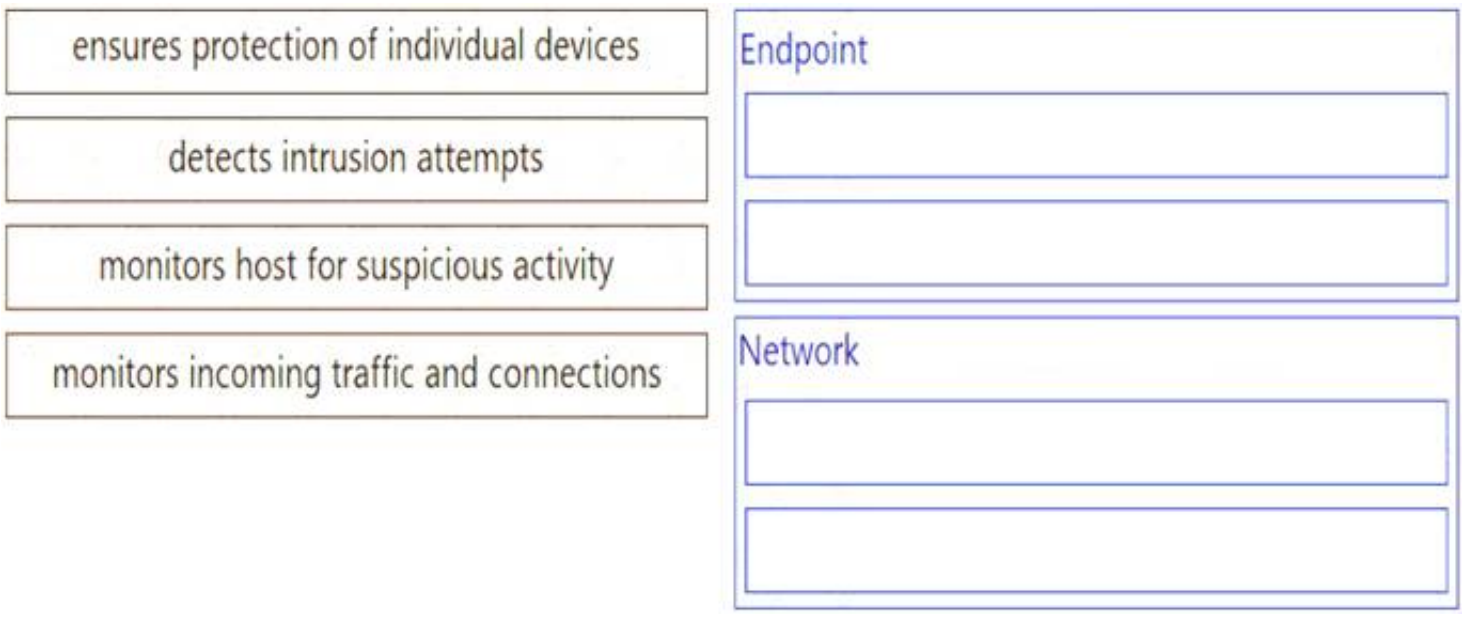
NEW QUESTION 34
What does cyber attribution identify in an investigation?

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

Answer: D

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

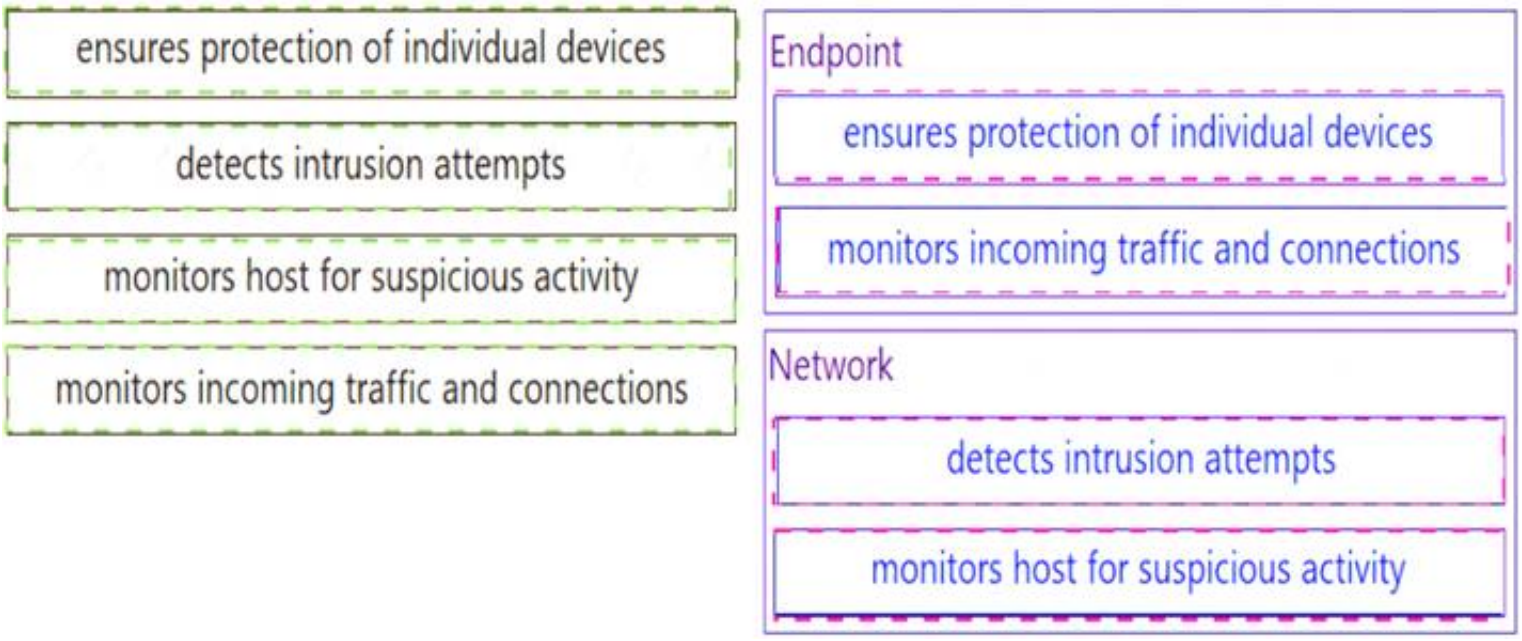
NEW QUESTION 37
Drag and drop the uses on the left onto the type of security system on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 38
Which type of access control depends on the job function of the user?

A. discretionary access control
B. nondiscretionary access control
C. role-based access control
D. rule-based access control

Answer: C

NEW QUESTION 43
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 46
What ate two categories of DDoS attacks? (Choose two.)

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

Answer: DE

NEW QUESTION 47

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

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

Answer: B

NEW QUESTION 48
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 53
Which are two denial-of-service attacks? (Choose two.)

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

Answer: BE

NEW QUESTION 54
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 58
What is a difference between SOAR and SIEM?

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

Answer: A

NEW QUESTION 60
Refer to the exhibit.

Top 10 Src IP Addr ordered by flows:

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

What information is depicted?

A. IIS data
B. NetFlow data
C. network discovery event
D. IPS event data

Answer: B

NEW QUESTION 62
Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

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

Answer: C

NEW QUESTION 64
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

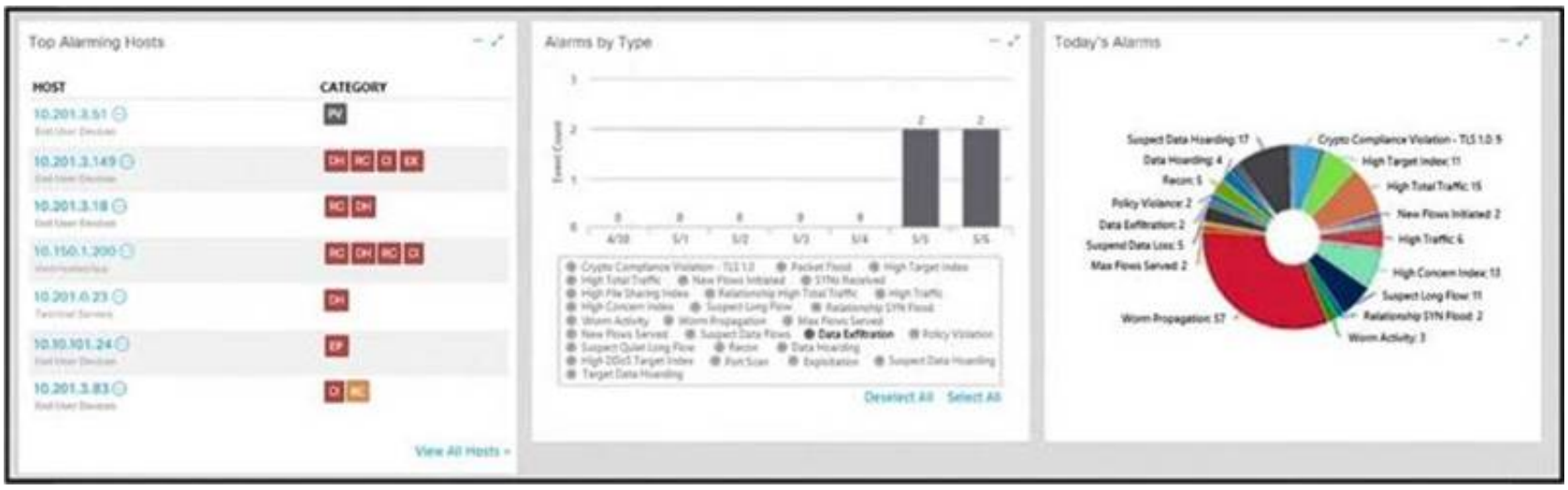
Answer: C

NEW QUESTION 65
Which security technology allows only a set of pre-approved applications to run on a system?

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

Answer: C

NEW QUESTION 69
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 74
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 75
An analyst discovers that a legitimate security alert has been dismissed. Which signature caused this impact on network traffic?

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

Answer: B

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

NEW QUESTION 79
An analyst is exploring the functionality of different operating systems.
What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?

A. queries Linux devices that have Microsoft Services for Linux installed
B. deploys Windows Operating Systems in an automated fashion

C. is an efficient tool for working with Active Directory
D. has a Common Information Model, which describes installed hardware and software

Answer: D

NEW QUESTION 84
Refer to the exhibit.

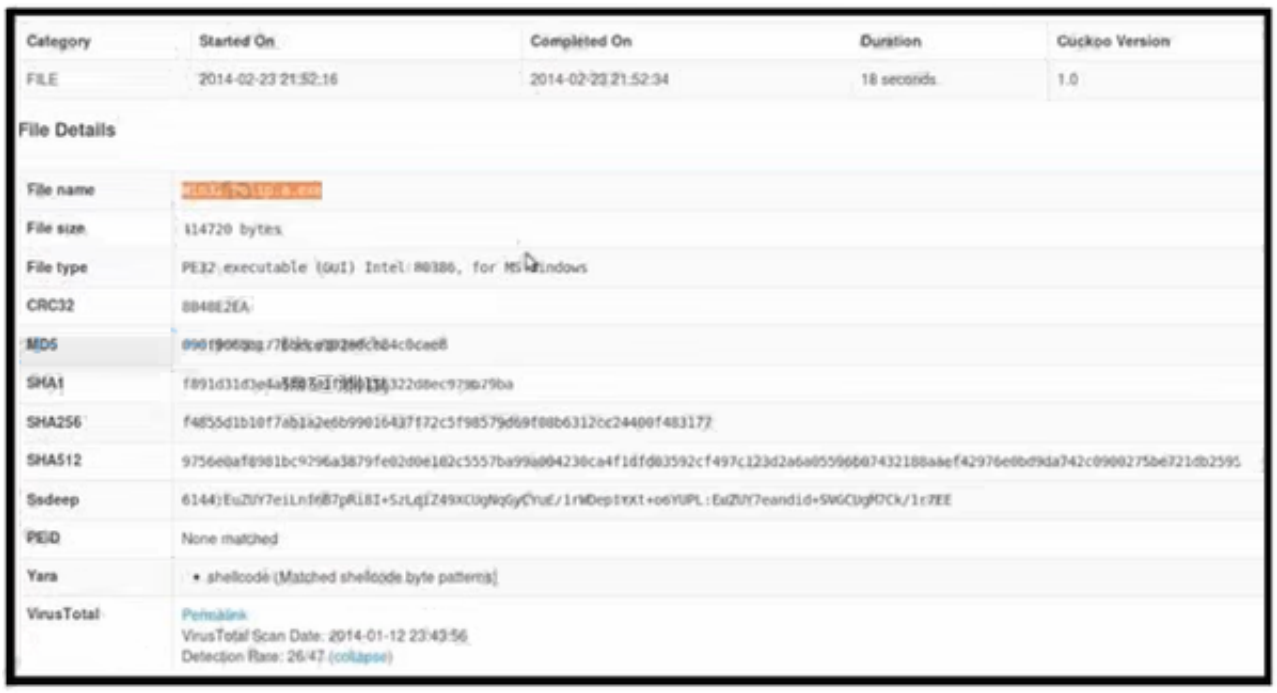
```
443/tcp closed https

'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 88
Refer to the exhibit.



An employee received an email from an unknown sender with an attachment and reported it as a phishing attempt. An engineer uploaded the file to Cuckoo for further analysis. What should an engineer interpret from the provided Cuckoo report?

A. 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 92
During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?

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

Answer: C

NEW QUESTION 94
Refer to the exhibit.

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

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

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

Answer: C

Explanation:
Indirect=circumstantail so there is no posibility to match A or B (only one answer is needed in this question). For suer it's not a BEST evidence - this FW data inform only of DROPPED traffic. If smth happend inside network, presented evidence could be used to support other evidences or make our narreation stronger but alone it's mean nothing.

NEW QUESTION 95
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.

NEW QUESTION 100
A security incident occurred with the potential of impacting business services. Who performs the attack?

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

Answer: B

NEW QUESTION 105
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 108
An engineer is addressing a connectivity issue between two servers where the remote server is unable to establish a successful session. Initial checks show that

the remote server is not receiving an SYN-ACK while establishing a session by sending the first SYN. What is causing this issue?

A. incorrect TCP handshake
B. incorrect UDP handshake
C. incorrect OSI configuration
D. incorrect snaplen configuration

Answer: A

NEW QUESTION 109
What is the relationship between a vulnerability and a threat?

A. A threat exploits a vulnerability
B. A vulnerability is a calculation of the potential loss caused by a threat
C. A vulnerability exploits a threat
D. A threat is a calculation of the potential loss caused by a vulnerability

Answer: A

NEW QUESTION 111
Which tool provides a full packet capture from network traffic?

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

Answer: D

NEW QUESTION 116
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 121
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

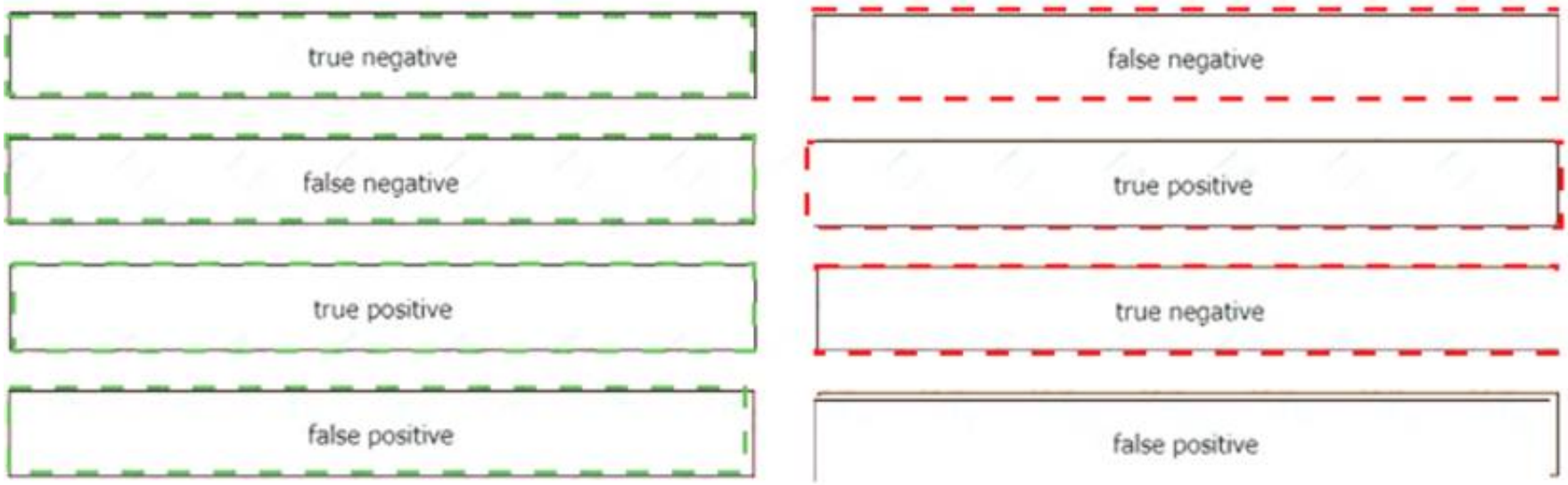
Explanation:
A certificate authority is a computer or entity that creates and issues digital certificates. CA do not "authenticate" it validates. "D" is wrong because The digital certificate validate a user. CA --> DC --> user, server or whatever.

NEW QUESTION 122
Drag and drop the event term from the left onto the description on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 127
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 132
An organization is cooperating with several third-party companies. Data exchange is on an unsecured channel using port 80 Internal employees use the FTP service to upload and download sensitive data An engineer must ensure confidentiality while preserving the integrity of the communication. Which technology must the engineer implement in this scenario'?

A. X 509 certificates
B. RADIUS server
C. CA server
D. web application firewall

Answer: A

NEW QUESTION 137
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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 FirstTry

* 200-201 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year