Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

NEW QUESTION 1
Which tool gives the ability to see session data in real time?

A. tcpdstat
B. trafdump
C. tcptrace
D. trafshow

Answer: C

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

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

Answer: D

NEW QUESTION 3
Which regex matches only on all lowercase letters?

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

Answer: A

NEW QUESTION 4
An analyst received a ticket regarding a degraded processing capability for one of the HR department's servers. On the same day, an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?

A. Recovery
B. Detection
C. Eradication
D. Analysis

Answer: B

NEW QUESTION 5
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 6
Which incidence response step includes identifying all hosts affected by an attack?

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

Answer: D

Explanation:
* 3.3.3 Identifying the Attacking Hosts During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts. Although this information can be important, incident handlers should generally stay focused on containment, eradication, and recovery.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
The response phase, or containment, of incident response, is the point at which the incident response team begins interacting with affected systems and attempts to keep further damage from occurring as a result of the incident.

NEW QUESTION 7
What is an advantage of symmetric over asymmetric encryption?

A. A key is generated on demand according to data type.
B. A one-time encryption key is generated for data transmission

C. It is suited for transmitting large amounts of data.
D. It is a faster encryption mechanism for sessions

Answer: D

NEW QUESTION 8
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 9
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. ....O...
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 10
How does certificate authority impact a security system?

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

Answer: B

NEW QUESTION 10
A system administrator is ensuring that specific registry information is accurate.
Which type of configuration information does the HKEY_LOCAL_MACHINE hive contain?

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

Answer: B

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

NEW QUESTION 11
An analyst is using the SIEM platform and must extract a custom property from a Cisco device and capture the phrase, "File: Clean." Which regex must the analyst import?

A. File: Clean
B. ^Parent File Clean$
C. File: Clean (.*)

D. ^File: Clean$

Answer: A

NEW QUESTION 14
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 16
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 20
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 24
An automotive company provides new types of engines and special brakes for rally sports cars. The company has a database of inventions and patents for their engines and technical information Customers can access the database through the company's website after they register and identify themselves. Which type of protected data is accessed by customers?

A. IP data
B. PII data
C. PSI data
D. PHI data

Answer: B

NEW QUESTION 27
Which evasion technique is indicated when an intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources?

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

Answer: A

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

NEW QUESTION 29
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 31
Which piece of information is needed for attribution in an investigation?

A. proxy logs showing the source RFC 1918 IP addresses
B. RDP allowed from the Internet
C. known threat actor behavior
D. 802.1x RADIUS authentication pass arid fail logs

Answer: C

Explanation:
Actually this is the most important thing: know who, what, how, why, etc.. attack the network.

NEW QUESTION 32
An engineer discovered a breach, identified the threat's entry point, and removed access. The engineer was able to identify the host, the IP address of the threat actor, and the application the threat actor targeted. What is the next step the engineer should take according to the NIST SP 800-61 Incident handling guide?

A. Recover from the threat.
B. Analyze the threat.
C. Identify lessons learned from the threat.
D. Reduce the probability of similar threats.

Answer: A

Explanation:
Per: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NEW QUESTION 33
What is the difference between inline traffic interrogation and traffic mirroring?

A. Inline interrogation is less complex as traffic mirroring applies additional tags to data.
B. Traffic mirroring copies the traffic rather than forwarding it directly to the analysis tools
C. Inline replicates the traffic to preserve integrity rather than modifying packets before sending them to other analysis tools.
D. Traffic mirroring results in faster traffic analysis and inline is considerably slower due to latency.

Answer: A

NEW QUESTION 37
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 41
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 46
Which list identifies the information that the client sends to the server in the negotiation phase of the TLS handshake?

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

Answer: C

NEW QUESTION 50
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 55
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 57
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 62
Drag and drop the data source from the left onto the data type on the right.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Wireshark	NetFlow
NetFlow	IPS
server log	Wireshark
IPS	server log

NEW QUESTION 67
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 70
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 71
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
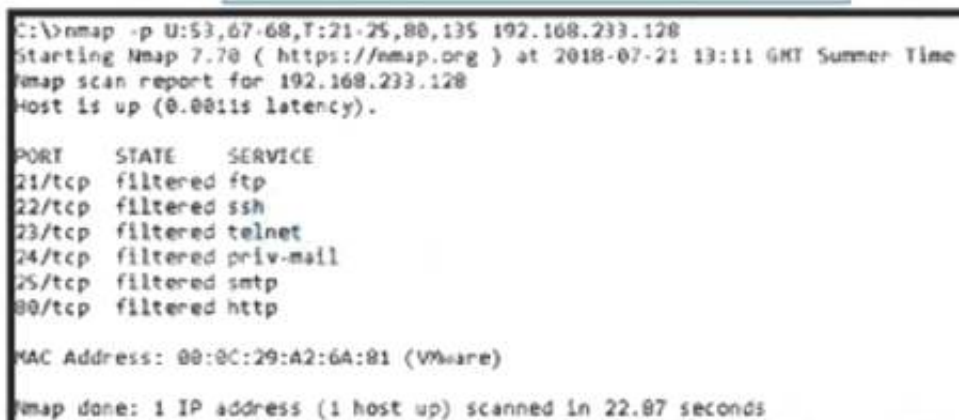
NEW QUESTION 73
Which evasion technique is a function of ransomware?

A. extended sleep calls
B. encryption
C. resource exhaustion
D. encoding

Answer: B

NEW QUESTION 76
Refer to the exhibit.

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

A. Identified a firewall device preventing the pert 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 77
Which process is used when IPS events are removed to improve data integrity?

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

Answer: B

NEW QUESTION 78
What describes the defense-m-depth principle?

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

Answer: B

NEW QUESTION 81
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 86
Refer to the exhibit.

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


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

What should be interpreted from this packet capture?

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

Answer: B

NEW QUESTION 87
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 92
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 96
A security analyst notices a sudden surge of incoming traffic and detects unknown packets from unknown senders After further investigation, the analyst learns that customers claim that they cannot access company servers According to NIST SP800-61, in which phase of the incident response process is the analyst?

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

Answer: B

NEW QUESTION 98
Which metric should be used when evaluating the effectiveness and scope of a Security Operations Center?

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

Answer: C

NEW QUESTION 100
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 103
Which NIST IR category stakeholder is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies?

A. CSIRT
B. PSIRT
C. public affairs
D. management

Answer: D

NEW QUESTION 105
What ate two categories of DDoS attacks? (Choose two.)

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

Answer: DE

NEW QUESTION 109
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 112
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 114
Refer to the exhibit.

```
192.168.10.10 – – [01/Dec/2020:11:12:22 -0200]  "GET /icons/powered_by_rh.png HTT
P/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-U
S; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 – – [01/Dec/2020:11:13:15 -0200] "GET /favicon.ico HTTP/1.1" 404 2
88 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812
Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 – – [01/Dec/2020:11:14:22 -0200] "GET /%27%27;!-%22%3CXSS%3E=&{()
} HTTP/1.1" 404 310 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12)
Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
```

What is occurring within the exhibit?

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

Answer: A

NEW QUESTION 116
Refer to the exhibit.

```
192.168.10.10 – – [01/Dec/2020:11:12:22 -0200]  "GET /icons/powered_by_rh.png HTT
P/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-U
S; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 – – [01/Dec/2020:11:13:15 -0200] "GET /favicon.ico HTTP/1.1" 404 2
88 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812
Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 – – [01/Dec/2020:11:14:22 -0200] "GET /%27%27;!-%22%3CXSS%3E=&{()
} HTTP/1.1" 404 310 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12)
Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
```

What is occurring?

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

Answer: A

NEW QUESTION 121
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 122
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 127
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 131
Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=2987 Ack=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/i/ntpagetag.gif?js=1&ts=147629607552.286&tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=6871 Ack=14979 Win=62480 Len=0

Which packet contains a file that is extractable within Wireshark?

A. 2317
B. 1986
C. 2318
D. 2542

Answer: D

NEW QUESTION 135
What is a sandbox interprocess communication service?

A. A collection of rules within the sandbox that prevent the communication between sandboxes.
B. A collection of network services that are activated on an interface, allowing for inter-port communication.
C. A collection of interfaces that allow for coordination of activities among processes.
D. A collection of host services that allow for communication between sandboxes.

Answer: C

Explanation:
Inter-process communication (IPC) allows communication between different processes. A process is one or more threads running inside its own, isolated address space. https://docs.legato.io/16_10/basicIPC.html

NEW QUESTION 137
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 141
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 146
The SOC team has confirmed a potential indicator of compromise on an endpoint. The team has narrowed the executable file's type to a new trojan family. According to the NIST Computer Security Incident Handling Guide, what is the next step in handling this event?

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

Answer: C

NEW QUESTION 148
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 149
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 154
Refer to the exhibit.

```
10.44.101.23 - - [20/Nov/2017:14:18:06 -0500] "GET / HTTP/1.1"
200 1254 "-" "Mozilla/5.0(X11; Ubuntu; Linux x86_64; rv:54.0)
Gecko/20100101 Firefox/54.0"
```

What does the message indicate?

A. an access attempt was made from the Mosaic web browser
B. a successful access attempt was made to retrieve the password file
C. a successful access attempt was made to retrieve the root of the website
D. a denied access attempt was made to retrieve the password file

Answer: C

NEW QUESTION 156
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 158
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 159
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 164
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 165
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 166
What is the difference between a threat and a risk?

A. Threat represents a potential danger that could take advantage of a weakness in a system
B. Risk represents the known and identified loss or danger in the system
C. Risk represents the nonintentional interaction with uncertainty in the system
D. Threat represents a state of being exposed to an attack or a compromise, either physically or logically.

Answer: A

Explanation:
A threat is any potential danger to an asset. If a vulnerability exists but has not yet been exploited—or, more importantly, it is not yet publicly known—the threat is latent and not yet realized.

NEW QUESTION 171
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 172
Refer to the exhibit.

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 177
When trying to evade IDS/IPS devices, which mechanism allows the user to make the data incomprehensible without a specific key, certificate, or password?

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

Answer: C

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

NEW QUESTION 180
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	8B48E2EA
MD5	090f90a1a78b4cbcae8...
SHA1	f891d31d3e4a5f0ba1f13322d8ec973b79ba
SHA256	f4f55d1b10f7ab1a2e6b99016437f72c5f98579d69f88b6312cc24400f483172
SHA512	9756e0af8981bc9296a3879fe82d0e182c5557ba99a04230ca4f16fd83592cf497c123d2a6a05596b07432188aaef42976e0bd9da742c0900275b6721db2595
Ssdeep	6144:EuZUY7eiLnfnB7pRi8I+SzLqjZ49XCUgNqGyCYuE/1rWDep1YXt+o6YUPL:EuZUY7eandid+SWGCUgM7Ck/1r7EE
PEID	None matched
Yara	• shellcode (Matched shellcode byte patterns)
VirusTotal	Permalink VirusTotal Scan Date: 2014-01-12 23:43:56 Detection Rate: 26/47 (collapse)

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

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

Answer: C

NEW QUESTION 184
What is an attack surface as compared to a vulnerability?

A. any potential danger to an asset
B. the sum of all paths for data into and out of the environment
C. an exploitable weakness in a system or its design
D. the individuals who perform an attack

Answer: C

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

NEW QUESTION 188
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 190
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 195
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 200
Refer to the exhibit.

File name	CVE-2009-4324 PDF 2009-11-30 note200911.pdf
File size	400918 bytes
File type	PDF document, version 1.6
CRC32	11638A9B
MD5	61baabd6fc12e01ff73ceacc07c84f9a
SHA1	0805d0ae62f5358b9a3f4c1868d552fc3561b17
SHA256	27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
SHA512	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
Ssdeep	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/QR/875+:prahGV6B
PEID	None matched
Yara	• embedded_pe (Contains an embedded PE32 file) • embedded_win_api (A non-Windows executable contains win32 API) • vmdetect (Possibly employs anti-virtualization techniques)
VirusTotal	Permalink VirusTotal Scan Date: 2013-12-27 06:51:52 Detection Rate: 32/46 (collapse)

An engineer is analyzing this Cuckoo Sandbox report for a PDF file that has been downloaded from an email. What is the state of this file?

A. The file has an embedded executable and was matched by PEiD threat signatures for further analysis.
B. The file has an embedded non-Windows executable but no suspicious features are identified.
C. The file has an embedded Windows 32 executable and the Yara field lists suspicious features for further analysis.
D. The file was matched by PEiD threat signatures but no suspicious features are identified since the signature list is up to date.

Answer: C

NEW QUESTION 204
What are the two differences between stateful and deep packet inspection? (Choose two)

A. Stateful inspection is capable of TCP state tracking, and deep packet filtering checks only TCP source and destination ports
B. Deep packet inspection is capable of malware blocking, and stateful inspection is not
C. Deep packet inspection operates on Layer 3 and 4. and stateful inspection operates on Layer 3 of the OSI model
D. Deep packet inspection is capable of TCP state monitoring only, and stateful inspection can inspect TCP and UDP.
E. Stateful inspection is capable of packet data inspections, and deep packet inspection is not

Answer: AB

NEW QUESTION 206
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 208
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 209
Refer to the exhibit.

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 211
Which type of evidence supports a theory or an assumption that results from initial evidence?

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

Answer: D

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

NEW QUESTION 216
Refer to the exhibit.

```
root@:~# cat access-logs/access_130603.txt | grep '192.168.1.91' | cut -d "\"" -f 2 |
uniq -c
    1 GET /portal.php?mode=addevent&date=2018-05-01 HTTP/1.1
    1 GET /blog/?attachment_id=2910 HTTP/1.1
    1 GET /blog/?attachment_id=2998&feed=rss2 HTTP/1.1
    1 GET /blog/?attachment_id=3156 HTTP/1.1
```

What is depicted in the exhibit?

A. Windows Event logs
B. Apache logs
C. IIS logs
D. UNIX-based syslog

Answer: B

NEW QUESTION 220
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 225
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 227
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 232
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 233
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 234
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 236
A SOC analyst is investigating an incident that involves a Linux system that is identifying specific sessions. Which identifier tracks an active program?

A. application identification number
B. active process identification number
C. runtime identification number
D. process identification number

Answer: D

NEW QUESTION 237
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 241
Which regular expression is needed to capture the IP address 192.168.20.232?

A. ^ (?:[0-9]{1,3}\.){3}[0-9]{1,3}
B. ^ (?:[0-9]f1,3}\.){1,4}
C. ^ (?:[0-9]{1,3}\.)'
D. ^ ([0-9]-{3})

Answer: A

NEW QUESTION 243
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 246
How is attacking a vulnerability categorized?

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

Answer: C

NEW QUESTION 248
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?
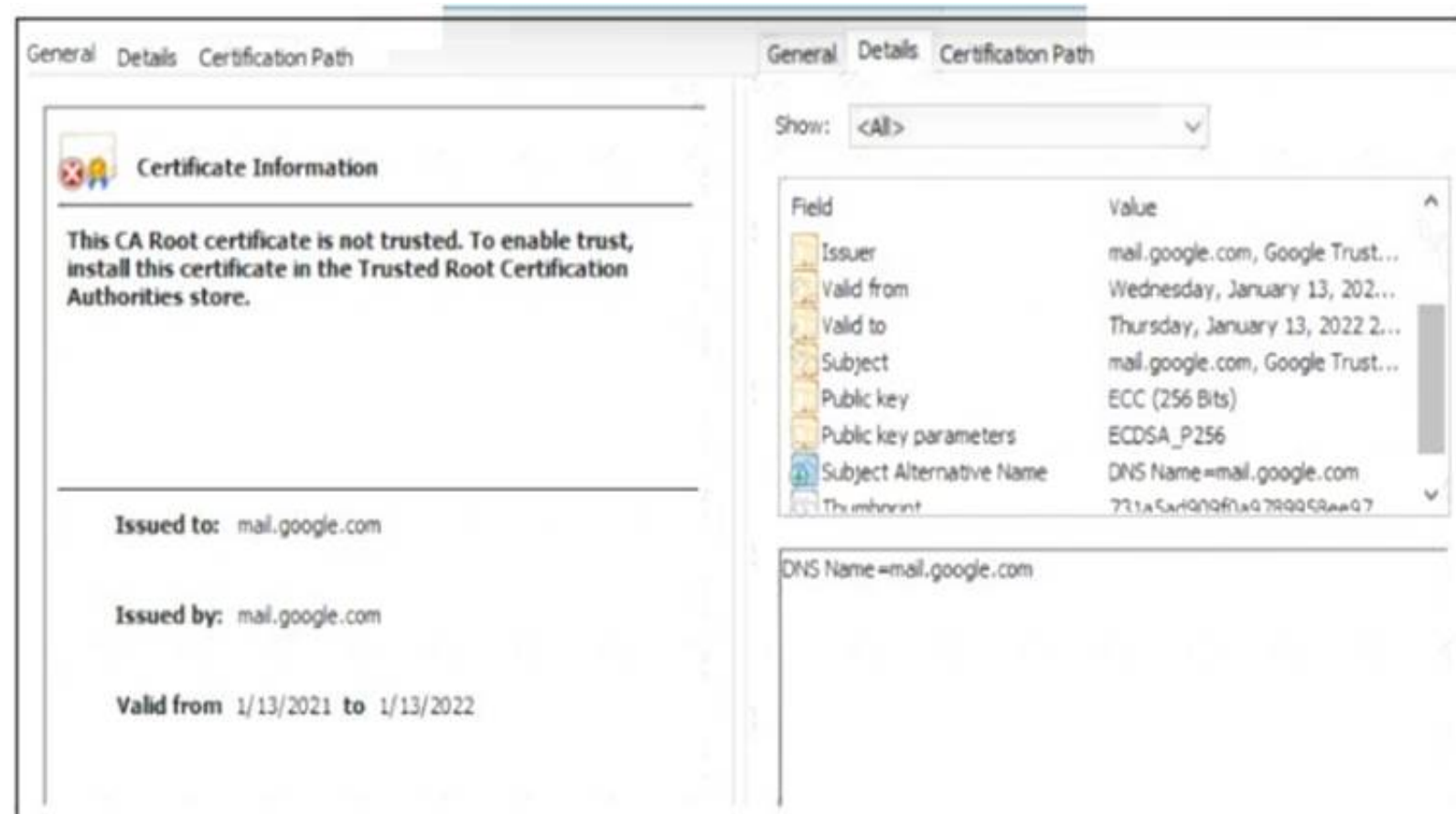
A. Biba
B. Object-capability
C. Take-Grant
D. Zero Trust

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 250
Refer to the exhibit.

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

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

Answer: C

NEW QUESTION 255
Refer to the exhibit.


```
ip.addr == 192.168.1.80 and tcp.port==8081 and http.request.full_uri

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      258 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 258
What is the difference between the rule-based detection when compared to behavioral detection?

A. Rule-Based detection is searching for patterns linked to specific types of attacks, while behavioral is identifying per signature.
B. Rule-Based systems have established patterns that do not change with new data, while behavioral changes.
C. Behavioral systems are predefined patterns from hundreds of users, while Rule-Based only flags potentially abnormal patterns using signatures.
D. Behavioral systems find sequences that match a particular attack signature, while Rule-Based identifies potential attacks.

Answer: D

NEW QUESTION 262
......

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

100% Actual & Verified — Instant Download, Please Click
Order The 200-201 Practice Test Here