Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

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

NEW QUESTION 1
What is a difference between an inline and a tap mode traffic monitoring?

A. Inline monitors traffic without examining other devices, while a tap mode tags traffic and examines the data from monitoring devices.
B. Tap mode monitors traffic direction, while inline mode keeps packet data as it passes through the monitoring devices.
C. Tap mode monitors packets and their content with the highest speed, while the inline mode draws a packet path for analysis.
D. Inline mode monitors traffic path, examining any traffic at a wire speed, while a tap mode monitors traffic as it crosses the network.

Answer: D

NEW QUESTION 2
Which of these describes SOC metrics in relation to security incidents?

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

Answer: A

NEW QUESTION 3
Refer to the exhibit.

HKEY_LOCAL_MACHINE

Which component is identifiable in this exhibit?

A. Trusted Root Certificate store on the local machine
B. Windows PowerShell verb
C. Windows Registry hive
D. local service in the Windows Services Manager

Answer: C

Explanation:
https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives
https://ldapwiki.com/wiki/HKEY_LOCAL_MACHINE#:~:text=HKEY_LOCAL_MACHINE%20Windows%2

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
Which regex matches only on all lowercase letters?

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

Answer: A

NEW QUESTION 6
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 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
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 9
What is the difference between discretionary access control (DAC) and role-based access control (RBAC)?

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

Answer: A

NEW QUESTION 10
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
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 14
An organization's security team has detected network spikes coming from the internal network. An investigation has concluded that the spike in traffic was from intensive network scanning How should the analyst collect the traffic to isolate the suspicious host?

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

Answer: A

NEW QUESTION 17
When an event is investigated, which type of data provides the investigate capability to determine if data exfiltration has occurred?

A. full packet capture
B. NetFlow data
C. session data
D. firewall logs

Answer: A

NEW QUESTION 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 21
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 26
Which two elements are assets in the role of attribution in an investigation? (Choose two.)

A. context
B. session
C. laptop
D. firewall logs
E. threat actor

Answer: CD

Explanation:
The following are some factors that are used during attribution in an investigation: Assets, Threat actor, Indicators of Compromise (IoCs), Indicators of Attack (IoAs), Chain of custody Asset: This factor identifies which assets were compromised by a threat actor or hacker. An example of an asset can be an organization's domain controller (DC) that runs Active Directory Domain Services (AD DS). AD is a service that allows an administrator to manage user accounts, user groups, and policies across a Microsoft Windows environment. Keep in mind that an asset is anything that has value to an organization; it can be something physical, digital, or even people. Cisco Certified CyberOps Associate 200-201 Certification Guide

NEW QUESTION 30
A company is using several network applications that require high availability and responsiveness, such that milliseconds of latency on network traffic is not acceptable. An engineer needs to analyze the network and identify ways to improve traffic movement to minimize delays. Which information must the engineer obtain for this analysis?

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

Answer: C

NEW QUESTION 32
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 35
An investigator is examining a copy of an ISO file that is stored in CDFS format. What type of evidence is this file?

A. data from a CD copied using Mac-based system
B. data from a CD copied using Linux system
C. data from a DVD copied using Windows system
D. data from a CD copied using Windows

Answer: B

Explanation:
CDfs is a virtual file system for Unix-like operating systems; it provides access to data and audio tracks on Compact Discs. When the CDfs driver mounts a Compact Disc, it represents each track as a file. This is consistent with the Unix convention "everything is a file". Source: https://en.wikipedia.org/wiki/CDfs

NEW QUESTION 36
Refer to the exhibit.

Vo.	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 binkley
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	245.7772040	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 39
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 44
Refer to the exhibit.

Overview	Analysis	Policies Devices Objects									Health System Hel

Content Explorer   Connections > Security Intelligence Events   Intrusions ▾   Files ▾   Hosts ▾   Users ▾   Vulnerabilities ▾   Correlation ▾   Custom ▾   Search

Security Intelligence Events (switch workflow)   Bookmark This Page Report Designer Dashboard View Bookr
Security Intelligence with Application Details > Table View of Security Intelligence Events   II 2018-03-02 07:20:20 - 2018-03-07 13:47:20
Search Constraints (Edit Search Serve Search)   Expanding
                                                                                                                                Disabled Columns

Jump to... ▾

	▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port/ ICMP Type
⬇ ☐	2018-03-07 13:42:01		Sinkhole DNS Block		10.0.10.75		JERI LABORDE (DCLOUD-SOC.LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
⬇ ☐	2018-03-07 13:42:01		Sinkhole DNS Block		10.0.0.100		AMPARO GIVENS (DCLOUD-SOC.LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
⬇ ☐	2018-03-07 13:42:01		Sinkhole DNS Block		10.112.10.158		VERNETTA DONNEL (DCLOUD-SOC.LDAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp

|< < Page 1 of 1 > >| Displaying rows 1-3 of 3 rows

View   Delete
View All   Delete All

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

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

Answer: DE

NEW QUESTION 49
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 52
What are two differences in how tampered and untampered disk images affect a security incident? (Choose two.)

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

Answer: AE

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

NEW QUESTION 55
Refer to the exhibit.

Employee Name	Role
Employee 1	Chief Accountant
Employee 2	Head of Managed Cyber Security Services
Employee 3	System Administration
Employee 4	Security Operation Center Analyst
Employee 5	Head of Network & Security Infrastructure Services
Employee 6	Financial Manager
Employee 7	Technical Director

Which stakeholders must be involved when a company workstation is compromised?

A. Employee 1 Employee 2, Employee 3, Employee 4, Employee 5, Employee 7
B. Employee 1, Employee 2, Employee 4, Employee 5
C. Employee 4, Employee 6, Employee 7
D. Employee 2, Employee 3, Employee 4, Employee 5

Answer: D

NEW QUESTION 58
Which artifact is used to uniquely identify a detected file?

A. file timestamp
B. file extension
C. file size
D. file hash

Answer: D

NEW QUESTION 59
A company encountered a breach on its web servers using IIS 7 5 Dunng the investigation, an engineer discovered that an attacker read and altered the data on a secure communication using TLS 1 2 and intercepted sensitive information by downgrading a connection to export-grade cryptography. The engineer must mitigate similar incidents in the future and ensure that clients and servers always negotiate with the most secure protocol versions and cryptographic parameters. Which action does the engineer recommend?

A. Upgrade to TLS v1 3.
B. Install the latest IIS version.
C. Downgrade to TLS 1.1.
D. Deploy an intrusion detection system

Answer: B

NEW QUESTION 63
A user received a targeted spear-phishing email and identified it as suspicious before opening the content. To which category of the Cyber Kill Chain model does to this type of event belong?

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

Answer: B

NEW QUESTION 68
Which type of verification consists of using tools to compute the message digest of the original and copied data, then comparing the similarity of the digests?

A. evidence collection order
B. data integrity
C. data preservation
D. volatile data collection

Answer: B

NEW QUESTION 70
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 71
What is a benefit of agent-based protection when compared to agentless protection?

A. It lowers maintenance costs
B. It provides a centralized platform
C. It collects and detects all traffic locally
D. It manages numerous devices simultaneously

Answer: C

Explanation:
Host-based antivirus protection is also known as agent-based. Agent-based antivirus runs on every protected machine. Agentless antivirus protection performs scans on hosts from a centralized system. Agentless systems have become popular for virtualized environments in which multiple OS instances are running on a host simultaneously. Agent-based antivirus running in each virtualized system can be a serious drain on system resources. Agentless antivirus for virtual hosts involves the use of a special security virtual appliance that performs optimized scanning tasks on the virtual hosts. An example of this is VMware's vShield.

NEW QUESTION 73
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 74
According to the September 2020 threat intelligence feeds a new malware called Egregor was introduced and used in many attacks. Distnbution of Egregor is pnmanly 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 76
The security team has detected an ongoing spam campaign targeting the organization. The team's approach is to push back the cyber kill chain and mitigate ongoing incidents. At which phase of the cyber kill chain should the security team mitigate this type of attack?

A. actions
B. delivery
C. reconnaissance
D. installation

Answer: B

NEW QUESTION 81
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 84
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 88
What is rule-based detection when compared to statistical detection?

A. proof of a user's identity
B. proof of a user's action
C. likelihood of user's action
D. falsification of a user's identity

Answer: B

NEW QUESTION 93
Drag and drop the uses on the left onto the type of security system on the right.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 97
An engineer is working with the compliance teams to identify the data passing through the network. During analysis, the engineer informs the compliance team that external penmeter data flows contain records, writings, and artwork Internal segregated network flows contain the customer choices by gender, addresses, and product preferences by age. The engineer must identify protected data. Which two types of data must be identified'? (Choose two.)

A. SOX
B. PII
C. PHI
D. PCI
E. copyright

Answer: BC

NEW QUESTION 98
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 102
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 104
Which event is a vishing attack?

A. obtaining disposed documents from an organization
B. using a vulnerability scanner on a corporate network
C. setting up a rogue access point near a public hotspot
D. impersonating a tech support agent during a phone call

Answer: D

NEW QUESTION 105
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 106
Refer to the exhibit.

```
Capturing on 'eth0'

    1 0.000000000 ca:4f:4d:4b:38:5a ? Broadcast    ARP 42 Who has 192.168.88.149?
Tell 192.168.88.12

    2 0.000055428 82:69:61:3e:fa:99 ? ca:4f:4d:4b:38:5a ARP 42 192.168.88.149 is at
82:69:61:3e:fa:99

    3 0.000080556 192.168.88.12 ? 192.168.88.149 TCP 74 49098 ? 80 [SYN] Seq=0
Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=65609529 TSecr=0 WS=128
```

What must be interpreted from this packet capture?

A. IP address 192.168.88 12 is communicating with 192 168 88 149 with a source port 74 to destination port 49098 using TCP protocol
B. IP address 192.168.88.12 is communicating with 192 168 88 149 with a source port 49098 to destination port 80 using TCP protocol.
C. IP address 192.168.88.149 is communicating with 192.168 88.12 with a source port 80 to destination port 49098 using TCP protocol.
D. IP address 192.168.88.149 is communicating with 192.168.88.12 with a source port 49098 to destination port 80 using TCP protocol.

Answer: B

NEW QUESTION 110
At which layer is deep packet inspection investigated on a firewall?

A. internet
B. transport
C. application

D. data link

Answer: C

Explanation:
Deep packet inspection is a form of packet filtering usually carried out as a function of your firewall. It is applied at the Open Systems Interconnection's application layer. Deep packet inspection evaluates the contents of a packet that is going through a checkpoint.

NEW QUESTION 113
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 114
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 115
What is a difference between tampered and untampered disk images?

A. Tampered images have the same stored and computed hash.
B. Tampered images are used as evidence.
C. Untampered images are used for forensic investigations.
D. Untampered images are deliberately altered to preserve as evidence

Answer: D

NEW QUESTION 120
An engineer receives a security alert that traffic with a known TOR exit node has occurred on the network. What is the impact of this traffic?

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

Answer: D

NEW QUESTION 125
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 130
Syslog collecting software is installed on the server For the log containment, a disk with FAT type partition is used An engineer determined that log files are being corrupted when the 4 GB tile size is exceeded. Which action resolves the issue?

A. Add space to the existing partition and lower the retention penod.
B. Use FAT32 to exceed the limit of 4 GB.
C. Use the Ext4 partition because it can hold files up to 16 TB.
D. Use NTFS partition for log file containment

Answer: D

NEW QUESTION 133
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 135
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 140
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 141
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 145
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 147
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 150
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 152
Which attack method intercepts traffic on a switched network?

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

Answer: B

Explanation:
An ARP-based MITM attack is achieved when an attacker poisons the ARP cache of two devices with the MAC address of the attacker's network interface card (NIC). Once the ARP caches have been successfully poisoned, each victim device sends all its packets to the attacker when communicating to the other device and puts the attacker in the middle of the communications path between the two victim devices. It allows an attacker to easily monitor all communication between victim devices. The intent is to intercept and view the information being passed between the two victim devices and potentially introduce sessions and traffic between the two victim devices

NEW QUESTION 156
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 159
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 164
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 167
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 170
What is obtained using NetFlow?

A. session data
B. application logs
C. network downtime report
D. full packet capture

Answer: A

NEW QUESTION 175
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 177
Refer to the exhibit.

```
No.      Time      ▾  Source          Destination      Protocol  Length  Info
    18  0.011916     10.0.2.15       192.124.249.9    TCP          76  50588→443 [SIN] Seq=(
    19  0.022656     192.124.249.9   10.0.2.15        TCP          62  443→50588 [SYN, ACK]
    20  0.022702     10.0.2.15       192.124.249.9    TCP          56  50588→443 [ACK] Seq=]
    21  0.022988     192.124.249.9   10.0.2.15        TCP          62  443→50586 [SYN, ACK]
    22  0.022996     10.0.2.15       192.124.249.9    TCP          56  50586→443 [ACK] Seq=]
    23  0.023212     10.0.2.15       192.124.249.9    TCP         261  50588→443 [PSH, ACK]
    24  0.023373     10.0.2.15       192.124.249.9    TCP         261  50586→443 [PSH, ACK]
    25  0.023445     192.124.249.9   10.0.2.15        TCP          62  443→50588 [ACK] Seq=]
    26  0.023617     192.124.249.9   10.0.2.15        TCP          62  443→50586 [ACK] Seq=]
    27  0.037413     192.124.249.9   10.0.2.15        TCP        2792  443→50586 [PSH, ACK]
    28  0.037426     10.0.2.15       192.124.249.9    TCP          56  50586→443 [ACK] Seq=2
```

```
> Frame 24: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.2
> Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, A
v Data [205 bytes]
     Data: 16030100c8010000c403030e06ead078d17676c13ab46ebf...
     [Length: 205]
```

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

Which application protocol is in this PCAP file?

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

Answer: D

NEW QUESTION 181
Drag and drop the technology on the left onto the data type the technology provides on the right.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 182
Which two elements are used for profiling a network? (Choose two.)

A. session duration
B. total throughput
C. running processes
D. listening ports
E. OS fingerprint

Answer: AB

Explanation:
A network profile should include some important elements, such as the following:
Total throughput – the amount of data passing from a given source to a given destination in a given period of time
Session duration – the time between the establishment of a data flow and its termination Ports used – a list of TCP or UDP processes that are available to accept data
Critical asset address space – the IP addresses or the logical location of essential systems or data
Profiling data are data that system has gathered, these data helps for incident response and to detect incident Network profiling = throughput, sessions duration, port used, Critical Asset Address Space Host profiling = Listening ports, logged in accounts, running processes, running tasks,applications

NEW QUESTION 184
Refer to the exhibit.

```
No.  Time       Source      Destination  Protocol  Length Info
  1 0.000000   10.0.0.2    10.128.0.2   TCP       54 3341 - 66 [SYN] Seq=0 Win=512 Len=0
  2 0.003987   10.128.0.2  10.0.0.2     TCP       58 88 - 3222 [SYN, ACK] Seq=0 Ack=1 Win=29288 Len=0 MSS=1468
  3 0.005514   10.128.0.2  10.0.0.2     TCP       58 88 - 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  4 0.008429   10.0.0.2    10.128.0.2   TCP       54 3342 - 80 [SYN] Seq=0 Win=512 Len=0
  5 0.010233   10.128.0.2  10.0.0.2     TCP       58 88 - 3220 [SYN, ACK] Seq=0 Ack=1 Win=2988 Len=0 MSS=1468
  6 0.014072   10.128.0.2  10.0.0.2     TCP       58 80 - 3342 [SYN, ACK] Seq=0 Ack=1 Win=2900 Len=0 MSS=1460
  7 0.016830   10.0.0.2    10.128.0.2   TCP       54 3343 - 88 [SYN] Seq=0 Win=512 Len=0
  8 0.022220   10.128.0.2  10.0.0.2     TCP       58 89 - 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  9 0.023496   10.128.0.2  10.0.0.2     TCP       58 89 - 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 10 0.025243   10.0.0.2    10.128.0.2   TCP       54 3344 - 88 [SYN] Seq=0 Win=512 Len=0
 11 0.026672   10.128.0.2  10.0.0.2     TCP       58 89 - 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 12 0.028038   10.128.0.2  10.0.0.2     TCP       58 80 - 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
 13 0.030523   10.128.0.2  10.0.0.2     TCP       58 88 - 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)
Internet Protocol Version 4, Src: 18.0.0.2, Dst: 10.128.0.2
Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 3341
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0 (relative sequence number)
    [Next sequence number: 0 (relative sequence number)]
  Acknowledgement number: 1023350884
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x002 (SYN)
    Windows Size Value: 512
    [Calculated window size: 512]
    Checksum: 0x8d5a [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  [Timestamps]
```

What is occurring in this network traffic?

A. High rate of SYN packets being sent from a multiple source towards a single destination IP.
B. High rate of ACK packets being sent from a single source IP towards multiple destination IPs.
C. Flood of ACK packets coming from a single source IP to multiple destination IPs.
D. Flood of SYN packets coming from a single source IP to a single destination IP.

Answer: D

NEW QUESTION 188
What is the difference between a threat and an exploit?

A. A threat is a result of utilizing flow in a system, and an exploit is a result of gaining control over the system.
B. A threat is a potential attack on an asset and an exploit takes advantage of the vulnerability of the asset
C. An exploit is an attack vector, and a threat is a potential path the attack must go through.
D. An exploit is an attack path, and a threat represents a potential vulnerability

Answer: B

NEW QUESTION 192
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 195
Which regular expression matches "color" and "colour"?

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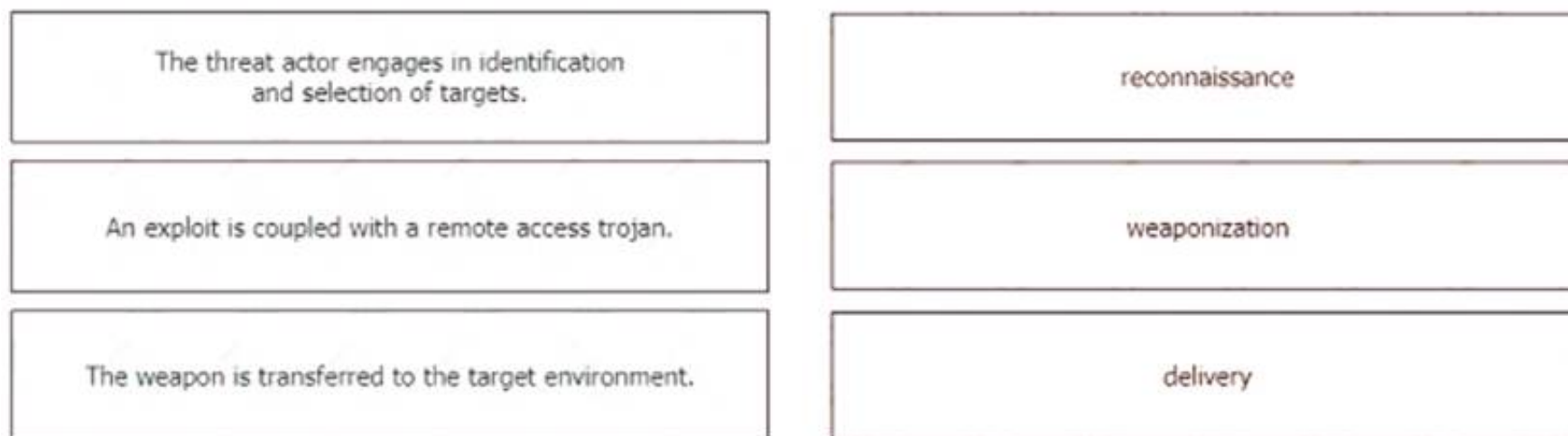C. colou?r
D. col[09]+our

Answer: C

NEW QUESTION 197
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 200
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 205
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 210
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 215
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 219
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 220
What is a difference between tampered and untampered disk images?

A. Tampered images have the same stored and computed hash.
B. Untampered images are deliberately altered to preserve as evidence.
C. Tampered images are used as evidence.
D. Untampered images are used for forensic investigations.

Answer: D

Explanation:
The disk image must be intact for forensics analysis. As a cybersecurity professional, you may be given the task of capturing an image of a disk in a forensic manner. Imagine a security incident has occurred on a system and you are required to perform some forensic investigation to determine who and what caused the attack. Additionally, you want to ensure the data that was captured is not tampered with or modified during the creation of a disk image process. Ref: Cisco Certified CyberOps Associate 200-201 Certification Guide

NEW QUESTION 223
What does an attacker use to determine which network ports are listening on a potential target device?

A. man-in-the-middle
B. port scanning
C. SQL injection
D. ping sweep

Answer: B

NEW QUESTION 227
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 231
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 232
What is the difference between deep packet inspection and stateful inspection?

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

Answer: D

NEW QUESTION 235
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 236
Which technology should be used to implement a solution that makes routing decisions based on HTTP header, uniform resource identifier, and SSL session ID attributes?

A. AWS
B. IIS
C. Load balancer
D. Proxy server

Answer: C

Explanation:
Load Balancing: HTTP(S) load balancing is one of the oldest forms of load balancing. This form of load balancing relies on layer 7, which means it operates in the application layer. This allows routing decisions based on attributes like HTTP header, uniform resource identifier, SSL session ID, and HTML form data.
Load balancing applies to layers 4-7 in the seven-layer Open System Interconnection (OSI) model. Its capabilities are: L4. Directing traffic based on network data and transport layer protocols, e.g., IP address and TCP port. L7. Adds content switching to load balancing, allowing routing decisions depending on characteristics such as HTTP header, uniform resource identifier, SSL session ID, and HTML form data. GSLB. Global Server Load Balancing expands L4 and L7 capabilities to servers in different sites

NEW QUESTION 241
An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group.
What is the initial event called in the NIST SP800-61?

A. online assault
B. precursor
C. trigger
D. instigator

Answer: B

Explanation:
A precursor is a sign that a cyber-attack is about to occur on a system or network. An indicator is the actual alerts that are generated as an attack is happening. Therefore, as a security professional, it's important to know where you can find both precursor and indicator sources of information.
The following are common sources of precursor and indicator information:
≫ Security Information and Event Management (SIEM)
≫ Anti-virus and anti-spam software
≫ File integrity checking applications/software
≫ Logs from various sources (operating systems, devices, and applications)
≫ People who report a security incident https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NEW QUESTION 243
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 248
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 252
What is a difference between data obtained from Tap and SPAN ports?

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

Answer: D

NEW QUESTION 255
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 258
Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)

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

Answer: AB

NEW QUESTION 259
How does statistical detection differ from rule-based detection?

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

Answer: B

NEW QUESTION 264
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 269
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 272
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 275
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 278
Drag and drop the event term from the left onto the description on the right.

true negative	malicious traffic is identified and an alert is generated
false negative	benign traffic incorrectly generates an alert
true positive	benign traffic does not generate an alert
false positive	malicious traffic does not generate an alert

A. Mastered
B. Not Mastered

Answer: A

Explanation:

true negative		false negative
false negative		true positive
true positive		true negative
false positive		false positive
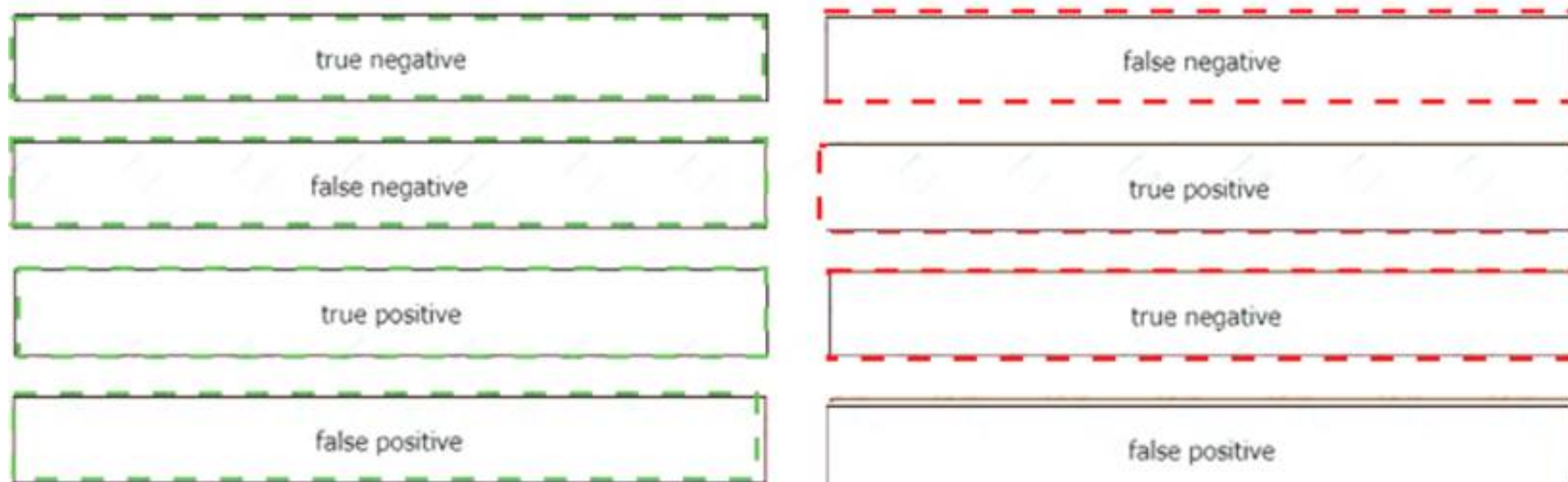
NEW QUESTION 281
How is attacking a vulnerability categorized?

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

Answer: C

NEW QUESTION 284
A user received a malicious attachment but did not run it. Which category classifies the intrusion?

A. weaponization
B. reconnaissance
C. installation
D. delivery

Answer: D

NEW QUESTION 285
A threat actor penetrated an organization's network. Using the 5-tuple approach, which data points should the analyst use to isolate the compromised host in a grouped set of logs?

A. event name, log source, time, source IP, and host name
B. protocol, source IP, source port, destination IP, and destination port
C. event name, log source, time, source IP, and username
D. protocol, log source, source IP, destination IP, and host name

Answer: B

NEW QUESTION 289
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 294
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 298
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 302
Refer to the exhibit.

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 305
An engineer received a flood of phishing emails from HR with the source address HRjacobm@companycom. What is the threat actor in this scenario?

A. phishing email
B. sender
C. HR
D. receiver

Answer: B

NEW QUESTION 310
Refer to the exhibit.

Which technology generates this log?

A. NetFlow
B. IDS
C. web proxy
D. firewall

Answer: D

NEW QUESTION 312
An employee received an email from a colleague's address asking for the password for the domain controller. The employee noticed a missing letter within the sender's address. What does this incident describe?

A. brute-force attack
B. insider attack
C. shoulder surfing
D. social engineering

Answer: B

NEW QUESTION 317
Refer to the exhibit.

```
# nmap -sV 172.18.104.139

Starting Nmap 7.01 ( https://nmap.org ) at 2020-03-07 11:36 EST
Nmap scan report for 172.18.104.139
Host is up (0.000018s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
25/tcp   open  smtp     Postfix smtpd
110/tcp  open  pop3     Dovecot pop3d
143/tcp  open  imap     Dovecot imapd
Service Info: Host:   172.18.108.139; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

What does the output indicate about the server with the IP address 172.18.104.139?

A. open ports of a web server
B. open port of an FTP server
C. open ports of an email server
D. running processes of the server

Answer: C

NEW QUESTION 321
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 323
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

200-201 Practice Exam Features:

* 200-201 Questions and Answers Updated Frequently

* 200-201 Practice Questions Verified by Expert Senior Certified Staff

* 200-201 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

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