Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

NEW QUESTION 1
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 2
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 3
What is a collection of compromised machines that attackers use to carry out a DDoS attack?

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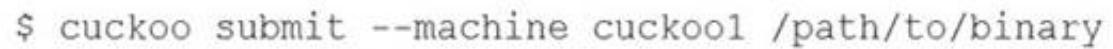D. command and control

Answer: B

NEW QUESTION 4
What makes HTTPS traffic difficult to monitor?

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

Answer: D

NEW QUESTION 5
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 6
What are two denial of service attacks? (Choose two.)

A. MITM
B. TCP connections
C. ping of death

D. UDP flooding
E. code red

Answer: CD

NEW QUESTION 7
Drag and drop the type of evidence from the left onto the description of that evidence on the right.

direct evidence		log that shows a command and control check-in from verified malware
corroborative evidence		firewall log showing successful communication and threat intelligence stating an IP is known to host malware
indirect evidence		NetFlow-based spike in DNS traffic

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

NEW QUESTION 8
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 9
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 10
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 10
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 12
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 13
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 16
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 17
Refer to the exhibit.

Where is the executable file?

A. info

B. tags
C. MIME
D. name

Answer: C

NEW QUESTION 18
Drag and drop the elements from the left into the correct order for incident handling on the right.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

preparation	containment, eradication, and recovery
containment, eradication, and recovery	preparation
post-incident analysis	detection and analysis
detection and analysis	post-incident analysis

NEW QUESTION 22
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 25

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 27

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 30

Which step in the incident response process researches an attacking host through logs in a SIEM?

A. detection and analysis
B. preparation
C. eradication
D. containment

Answer: A

Explanation:

Preparation --> Detection and Analysis --> Containment, Erradicaion and Recovery --> Post-Incident Activity Detection and Analysis --> Profile networks and systems, Understand normal behaviors, Create a log retention policy, Perform event correlation. Maintain and use a knowledge base of information.Use Internet search engines for research. Run packet sniffers to collect additional data. Filter the data. Seek assistance from others. Keep all host clocks synchronized. Know the different types of attacks and attack vectors. Develop processes and procedures to recognize the signs of an incident. Understand the sources of precursors and indicators. Create appropriate incident documentation capabilities and processes. Create processes to effectively prioritize security incidents. Create processes to effectively communicate incident information (internal and external communications).
Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

NEW QUESTION 33

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 38

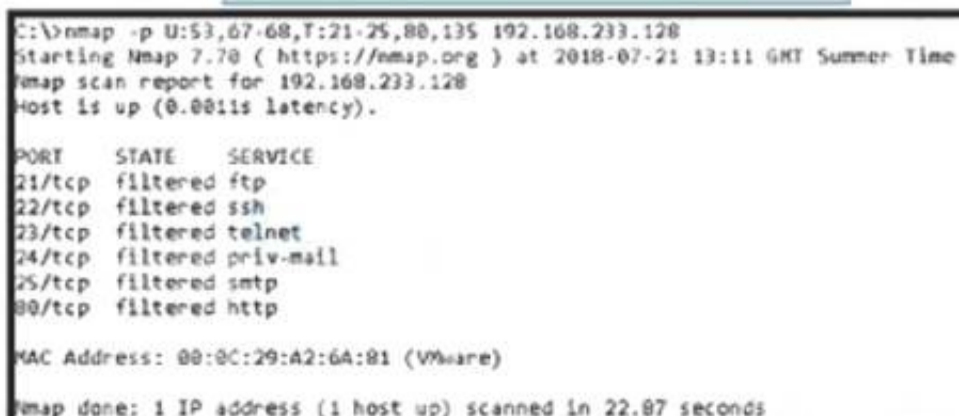Which evasion technique is a function of ransomware?

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

Answer: B

NEW QUESTION 39

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 40
Which technology prevents end-device to end-device IP traceability?

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

Answer: C

NEW QUESTION 41
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 44
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 47
Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?

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

Answer: D

NEW QUESTION 49
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 51
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 55
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 57
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 58
What ate two categories of DDoS attacks? (Choose two.)

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

Answer: DE

NEW QUESTION 63
An engineer received an alert affecting the degraded performance of a critical server. Analysis showed a heavy CPU and memory load. What is the next step the engineer should take to investigate this resource usage?

A. Run "ps -d" to decrease the priority state of high load processes to avoid resource exhaustion.
B. Run "ps -u" to find out who executed additional processes that caused a high load on a server.
C. Run "ps -ef" to understand which processes are taking a high amount of resources.
D. Run "ps -m" to capture the existing state of daemons and map required processes to find the gap.

Answer: C

NEW QUESTION 65
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 66
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 67
Refer to the exhibit.

```
GET /item.php?id=34' or sleep(10)
```

This request was sent to a web application server driven by a database. Which type of web server attack is represented?

A. parameter manipulation
B. heap memory corruption
C. command injection
D. blind SQL injection

Answer: D

NEW QUESTION 71
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 74
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 77
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
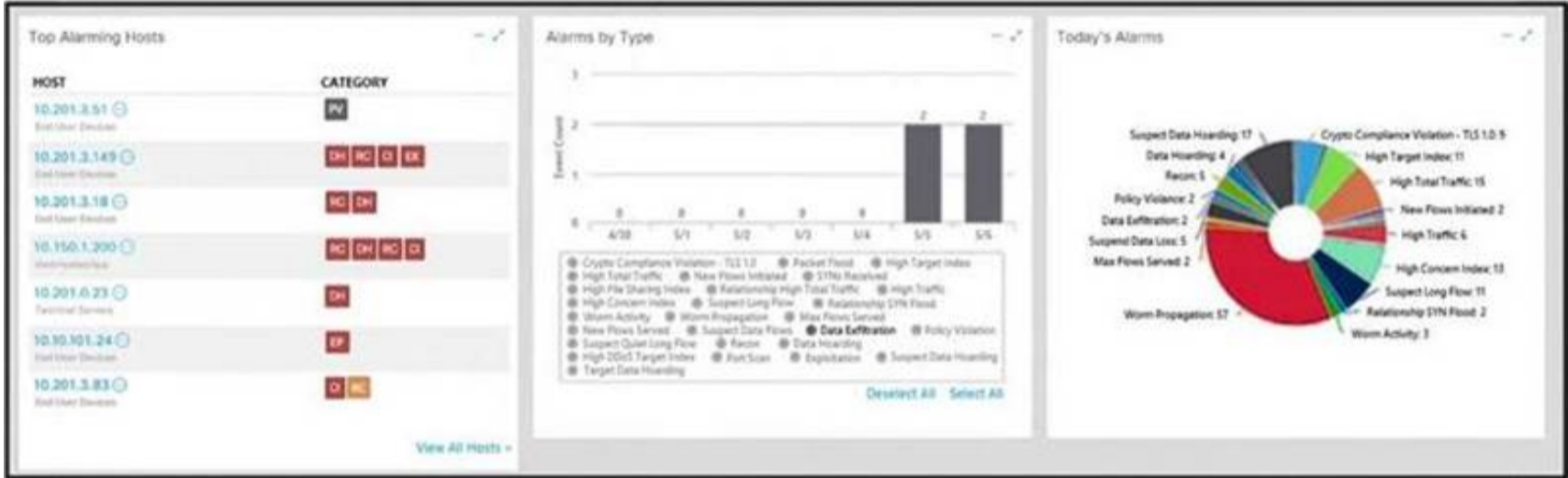
Answer: C

NEW QUESTION 79
Refer to the exhibit.

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

A. The file will appear legitimate by evading signature-based detection.
B. The file will not execute its behavior in a sandbox environment to avoid detection.
C. The file will insert itself into an application and execute when the application is run.
D. The file will monitor user activity and send the information to an outside source.

Answer: B

NEW QUESTION 82
Refer to the exhibit.

What is the potential threat identified in this Stealthwatch dashboard?

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

Answer: C

NEW QUESTION 84
What is obtained using NetFlow?

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

Answer: A

NEW QUESTION 85
Drag and drop the technology on the left onto the data type the technology provides on the right.

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 90
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 NSS=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 NSS=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 NSS=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 NSS=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 92
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 96
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 101
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 106
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 110
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 113
Which two pieces of information are collected from the IPv4 protocol header? (Choose two.)

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

Answer: CD

NEW QUESTION 117
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 122
Refer to the exhibit.

What is occurring?

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

Answer: D

NEW QUESTION 123
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.

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 125

What is the difference between the ACK flag and the RST flag?

A. The RST flag approves the connection, and the ACK flag terminates spontaneous connections.
B. The ACK flag confirms the received segment, and the RST flag terminates the connection.
C. The RST flag approves the connection, and the ACK flag indicates that a packet needs to be resent
D. The ACK flag marks the connection as reliable, and the RST flag indicates the failure within TCP Handshake

Answer: B

NEW QUESTION 128
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 133
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 136
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 141
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 146
Which vulnerability type is used to read, write, or erase information from a database?

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

Answer: D

NEW QUESTION 147
Refer to the exhibit.

No.	Time	Source	Destination	Protoc	Length	Info
6	16:40:35.636314	195.144.107.198	192.168.31.44	FTP	104	Response: 227 Entering Passive Mode (195,144,107,198,4,2).
7	16:40:35.637786	192.168.31.44	195.144.107.198	FTP	82	Request: RETR ResumableTransfer.png
8	16:40:35.638091	192.168.31.44	195.144.107.198	TCP	66	1084 → 1026 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	16:40:35.696788	195.144.107.198	192.168.31.44	FTP	96	Response: 150 Opening BINARY mode data connection.
10	16:40:35.698384	195.144.107.198	192.168.31.44	TCP	66	1026 → 1084 [SYN, ACK] Seq=0 Ack=1 Win=8192 MSS=1456 WS=256 SACK
11	16:40:35.698521	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=1 Win=132352 Len=0
12	16:40:35.698802	192.168.31.44	195.144.107.198	TCP	54	[TCP Window Update] 1084 → 1026 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
13	16:40:35.739249	192.168.31.44	195.144.107.198	TCP	54	1031 → 21 [ACK] Seq=43 Ack=113 Win=513 Len=0
14	16:40:35.759825	195.144.107.198	192.168.31.44	FTP...	2966	FTP Data: 2912 bytes (PASV) (RETR ResumableTransfer.png)
15	16:40:35.759925	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=2913 Win=4194304 Len=0
16	16:40:35.822152	195.144.107.198	192.168.31.44	FTP...	5878	FTP Data: 5824 bytes (PASV) (RETR ResumableTransfer.png)
17	16:40:35.822263	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=0
18	16:40:35.883496	195.144.107.198	192.168.31.44	FTP...	1510	FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)
19	16:40:35.883496	195.144.107.198	192.168.31.44	FTP...	1408	FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)
20	16:40:35.883559	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=11547 Win=4194304 Len=0
21	16:40:35.944841	195.144.107.198	192.168.31.44	FTP	78	Response: 226 Transfer complete.
22	16:40:35.944841	195.144.107.198	192.168.31.44	TCP	54	1026 → 1084 [FIN, ACK] Seq=11547 Ack=1 Win=66816 Len=0
23	16:40:35.944978	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=11548 Win=4194304 Len=0
24	16:40:35.945371	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [FIN, ACK] Seq=1 Ack=11548 Win=4194304 Len=0

```
Frame 21: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{E75C8230-BD9F-4B7C-B722-94BD6CF16174}, id 0
Ethernet II, Src: BeijingX_06:3f:00 (50:d2:f5:06:3f:00), Dst: IntelCor_7c:b2:fd (18:26:49:7c:b2:fd)
Internet Protocol Version 4, Src: 195.144.107.198, Dst: 192.168.31.44
Transmission Control Protocol, Src Port: 21, Dst Port: 1031, Seq: 113, Ack: 43, Len: 24
File Transfer Protocol (FTP)
[Current working directory: ]
```

Which frame numbers contain a file that is extractable via TCP stream within Wireshark?

A. 7,14, and 21
B. 7 and 21
C. 14,16,18, and 19
D. 7 to 21

Answer: B

NEW QUESTION 148
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 150
Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
14...	27.405297	192.168.1.83	192.168.1.80	HTTP	335	GET /news.php HTTP/1.1
14...	27.423516	192.168.1.80	192.168.1.83	HTTP	12...	HTTP/1.0 200 OK (text/html)
14...	27.843983	192.168.1.83	192.168.1.80	HTTP	516	POST /admin/get.php HTTP/1.1
14...	27.856474	192.168.1.80	192.168.1.83	HTTP	519	HTTP/1.0 200 OK (text/html)
14...	28.053803	192.168.1.83	192.168.1.80	HTTP	276	POST /news.php HTTP/1.1
15...	28.065561	192.168.1.80	192.168.1.83	HTTP	11...	HTTP/1.0 200 OK (text/html)
20...	33.245337	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
20...	33.253440	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
23...	38.265103	192.168.1.83	192.168.1.80	HTTP	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 151
What are two denial-of-service (DoS) attacks? (Choose two)

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

Answer: BC

NEW QUESTION 153
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 157
......

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