

# Cisco

## Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals



#### NEW QUESTION 1

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

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

**Answer: B**

#### NEW QUESTION 2

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

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

**Answer: D**

#### NEW QUESTION 3

Which regex matches only on all lowercase letters?

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

**Answer: A**

#### NEW QUESTION 4

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

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

**Answer: B**

#### NEW QUESTION 5

What makes HTTPS traffic difficult to monitor?

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

**Answer: D**

#### NEW QUESTION 6

How does certificate authority impact a security system?

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

**Answer: B**

#### NEW QUESTION 7

A network engineer discovers that a foreign government hacked one of the defense contractors in their home country and stole intellectual property. What is the threat agent in this situation?

- A. the intellectual property that was stolen
- B. the defense contractor who stored the intellectual property
- C. the method used to conduct the attack
- D. the foreign government that conducted the attack

**Answer: D**

#### NEW QUESTION 8

A system administrator is ensuring that specific registry information is accurate.  
Which type of configuration information does the HKEY\_LOCAL\_MACHINE hive contain?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 9

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 10

Refer to the exhibit.

#Time Format: Local														
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmp type icmpcode info path														
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63064	135	0	-	0	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.14	63065	49156	0	-	0	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63066	65386	0	-	0	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63067	389	0	-	0	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	UDP	10.40.4.182	10.40.1.14	62292	389	0	-	-	-	-	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63068	389	0	-	0	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63069	445	0	-	0	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	UDP	10.40.4.182	10.40.1.13	62293	389	0	-	-	-	-	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.13	63070	88	0	-	0	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63071	445	0	-	0	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63072	445	0	-	0	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.11	63073	445	0	-	0	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.13	63074	88	0	-	0	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.13	63075	88	0	-	0	0	0	-	SEND
2015-07-16	11:35:26	ALLOW	TCP	10.40.4.182	10.40.1.13	63076	88	0	-	0	0	0	-	SEND
2015-07-16	11:35:27	ALLOW	UDP	10.40.4.182	10.40.1.11	55053	53	0	-	-	-	-	-	SEND
2015-07-16	11:35:27	ALLOW	UDP	10.40.4.182	10.40.1.11	50845	53	0	-	-	-	-	-	SEND
2015-07-16	11:35:30	ALLOW	UDP	fe80::29ea:1a3c:24d6:fb49	ff02::1:3	57333	5355	0	-	-	-	-	-	RECEIVE
2015-07-16	11:35:30	ALLOW	UDP	10.40.4.252	224.0.0.252	59629	5355	0	-	-	-	-	-	RECEIVE
2015-07-16	11:35:30	ALLOW	UDP	fe80::4c2e:505d:b3a7:caaf	ff02::1:3	58846	5355	0	-	-	-	-	-	SEND
2015-07-16	11:35:30	ALLOW	UDP	10.40.4.182	224.0.0.252	58846	5355	0	-	-	-	-	-	SEND
2015-07-16	11:35:31	ALLOW	UDP	10.40.4.182	224.0.0.252	137	137	0	-	-	-	-	-	SEND
2015-07-16	11:35:31	ALLOW	UDP	fe80::4c2e:505d:b3a7:caaf	ff02::1:3	63504	5355	0	-	-	-	-	-	SEND
2015-07-16	11:35:31	ALLOW	UDP	10.40.4.182	224.0.0.252	63504	5355	0	-	-	-	-	-	SEND

An engineer received an event log file to review. Which technology generated the log?

- A. NetFlow
- B. proxy
- C. firewall
- D. IDS/IPS

**Answer:** C

#### 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 12

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 15

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 18

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 22

Which piece of information is needed for attribution in an investigation?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 26

Which action should be taken if the system is overwhelmed with alerts when false positives and false negatives are compared?

- A. Modify the settings of the intrusion detection system.
- B. Design criteria for reviewing alerts.
- C. Redefine signature rules.
- D. Adjust the alerts schedule.

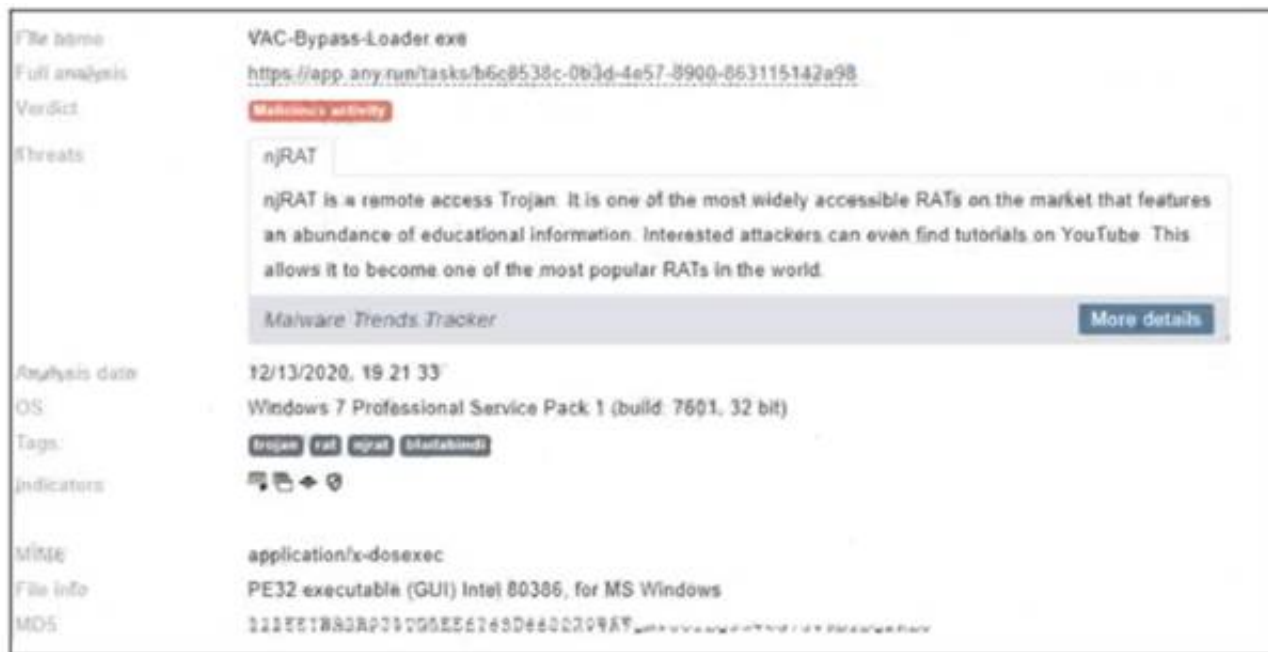
**Answer:** A

#### Explanation:

Traditional intrusion detection system (IDS) and intrusion prevention system (IPS) devices need to be tuned to avoid false positives and false negatives. Next-generation IPSs do not need the same level of tuning compared to traditional IPSs. Also, you can obtain much deeper reports and functionality, including advanced malware protection and retrospective analysis to see what happened after an attack took place. Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

#### NEW QUESTION 30

Refer to the exhibit.



Where is the executable file?

- A. info
- B. tags
- C. MIME
- D. name

**Answer: C**

#### NEW QUESTION 34

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

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

**Answer: C**

#### NEW QUESTION 39

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 40

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 45

Which information must an organization use to understand the threats currently targeting the organization?

- A. threat intelligence
- B. risk scores
- C. vendor suggestions
- D. vulnerability exposure

**Answer: A**

#### NEW QUESTION 47

A malicious file has been identified in a sandbox analysis tool.



File Details	
File name	770327a0-1000-4000-8000-000000000000
File size	414720 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows
CRC32	8048E2EA
MD5	090f966b81776bec18288cc84c8cae9
SHA1	f891d31d3e4a5f07a1f950156322d8ec979079ba
SHA256	f4855d1b18f7ab3a2e6b99036437f72c5f98579d09f00b6312cc24480f483177
SHA512	9756e8af8981bc9296a3879fe82d8e182c5557ba99a084238ca4f1dffd03592cf497c123d2aba05596b07432188aaef42976e8bd9da742c09902756e721db2595
Ssdeep	6144:EuZU7Ye1Lnfn87pR18I+S2Lq1Z49XU3g8p9yCY8E/1rM8epTXXt+o6Y8PL:EuZU7Yeand1d+SV6CugP7Ck/1r7EE
PEID	None matched
Yara	<ul style="list-style-type: none"> <li>• shellcode (Matched shellcode byte patterns)</li> </ul>
VirusTotal	Pending VirusTotal Scan Date: 2014-01-12 23:43:56 Detection Rate: 26/47 (calapase)

Which piece of information is needed to search for additional downloads of this file by other hosts?

- A. file header type
- B. file size
- C. file name
- D. file hash value

Answer: D

NEW QUESTION 49

What specific type of analysis is assigning values to the scenario to see expected outcomes?

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

Answer: A

NEW QUESTION 52

An engineer is investigating a case of the unauthorized usage of the “Tcpdump” tool. The analysis revealed that a malicious insider attempted to sniff traffic on a specific interface. What type of information did the malicious insider attempt to obtain?

- A. tagged protocols being used on the network
- B. all firewall alerts and resulting mitigations
- C. tagged ports being used on the network
- D. all information and data within the datagram

Answer: C

NEW QUESTION 54

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

Risk Assessment	network is compromised
Vulnerability	lack of an access list
Exploit	configuration review
Threat	leakage of confidential information

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Risk Assessment	Threat
Vulnerability	Vulnerability
Exploit	Risk Assessment
Threat	Exploit

#### NEW QUESTION 55

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 57

Which process is used when IPS events are removed to improve data integrity?

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

**Answer:** B

#### NEW QUESTION 61

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 66

Drag and drop the access control models from the left onto the correct descriptions on the right.

MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC

NEW QUESTION 67

What is the function of a command and control server?

- A. It enumerates open ports on a network device
- B. It drops secondary payload into malware
- C. It is used to regain control of the network after a compromise
- D. It sends instruction to a compromised system

Answer: D

NEW QUESTION 68

Refer to the exhibit.

Interface: 192.168.1.29 --- 0x11		
Internet Address	Physical Address	Type
192.168.1.10	d8-a7-56-d7-19-ea	dynamic
192.168.1.67	d8-a7-56-d7-19-ea	dynamic
192.168.1.1	01-00-5e-00-00-16	static

What is occurring in this network?

- A. ARP cache poisoning
- B. DNS cache poisoning
- C. MAC address table overflow
- D. MAC flooding attack

Answer: A

NEW QUESTION 69

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

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

Answer: C

NEW QUESTION 71

Which system monitors local system operation and local network access for violations of a security policy?

- A. host-based intrusion detection
- B. systems-based sandboxing
- C. host-based firewall
- D. antivirus



**Answer:** A

**Explanation:**

HIDS is capable of monitoring the internals of a computing system as well as the network packets on its network interfaces. Host-based firewall is a piece of software running on a single Host that can restrict incoming and outgoing Network activity for that host only.

**NEW QUESTION 76**

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 80**

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

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

**Answer:** C

**NEW QUESTION 82**

What is a difference between SOAR and SIEM?

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

**Answer:** A

**NEW QUESTION 86**

Refer to the exhibit.

Top 10 Src IP Addr ordered by flows:								
Date first seen	Duration	Src IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2019-11-30 06:45:50.990	1147.332	192.168.12.234	109183	202523	13.1 M	176	96116	68
2019-11-30 06:45:02.928	1192.834	10.10.151.203	62794	219715	25.9 M	184	182294	123
2019-11-30 06:59:24.563	330.110	192.168.28.173	27864	47943	2.2 M	145	55769	48

What information is depicted?

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

**Answer:** B

**NEW QUESTION 88**

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 file size is exceeded. Which action resolves the issue?

- A. Add space to the existing partition and lower the retention period.
- 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 90**

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 takes actions to violate data integrity and availability.	Exploitation
The targeted environment is taken advantage of triggering the threat actor's code.	Installation
Backdoor is placed on the victim system allowing the threat actor to maintain the persistence.	Command and Control
An outbound connection is established to an Internet-based controller server.	Actions and Objectives

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Exploitation - The targeted Environment is taken advantage of triggering the threat actor's code  
 Installation - Backdoor is placed on the victim system allowing the threat actor to maintain the persistence.  
 Command and Control - An outbound connection is established to an Internet-based controller server.  
 Actions and Objectives - The threat actor takes actions to violate data integrity and availability

**NEW QUESTION 92**

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 95**

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 97**

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/ntpgetag.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 100**

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?

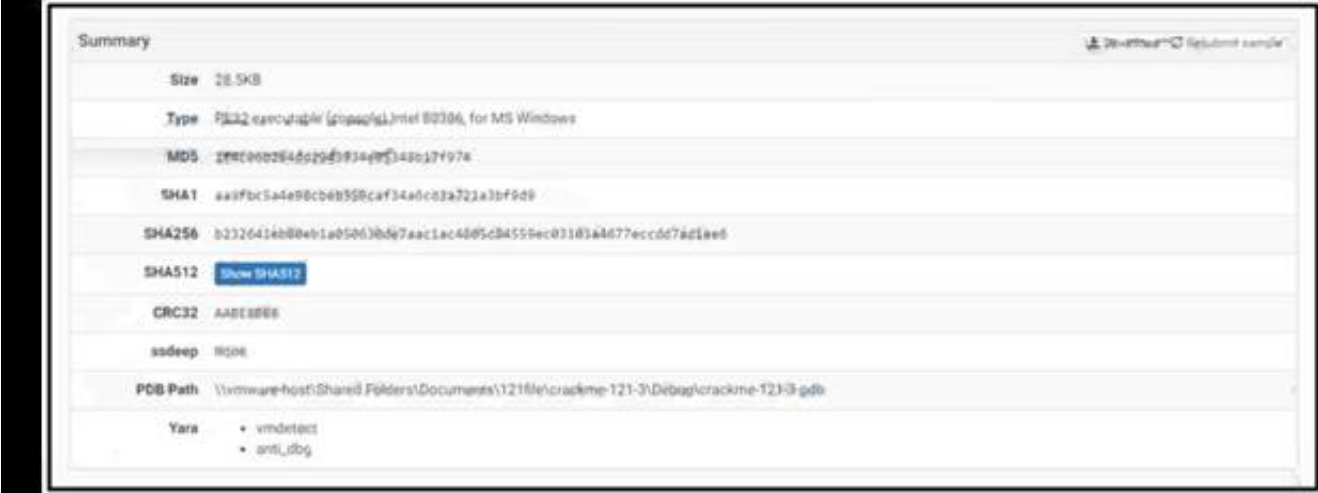
- A. Isolate the infected endpoint from the network.  
 B. Perform forensics analysis on the infected endpoint.  
 C. Collect public information on the malware behavior.

D. Prioritize incident handling based on the impact.

Answer: C

NEW QUESTION 101

Refer to the exhibit.



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

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

Answer: B

NEW QUESTION 105

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 106

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

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

Answer: B

Explanation:

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

NEW QUESTION 111

Which utility blocks a host portscan?

- A. HIDS
- B. sandboxing



- C. host-based firewall
- D. antimalware

Answer: C

NEW QUESTION 115

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 117

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 120

What describes the impact of false-positive alerts compared to false-negative alerts?

- A. A false negative is alerting for an XSS attac
- B. An engineer investigates the alert and discovers that an XSS attack happened A false positive is when an XSS attack happens and no alert is raised
- C. A false negative is a legitimate attack triggering a brute-force aler
- D. An engineer investigates the alert and finds out someone intended to break into the system A false positive is when no alert and no attack is occurring
- E. A false positive is an event alerting for a brute-force attack An engineer investigates the alert and discovers that a legitimate user entered the wrong credential several times A false negative is when a threat actor tries to brute-force attack a system and no alert is raised.
- F. A false positive is an event alerting for an SQL injection attack An engineer investigates the alert and discovers that an attack attempt was blocked by IPS A false negative is when the attack gets detected but succeeds and results in a breach.

Answer: C

NEW QUESTION 122

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 127

Refer to the exhibit.

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

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 131

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

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

**Answer:** C

#### NEW QUESTION 136

Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

- A. availability
- B. confidentiality
- C. scope
- D. integrity

**Answer:** D

#### NEW QUESTION 137

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

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

**Answer:** B

#### NEW QUESTION 140

An offline audit log contains the source IP address of a session suspected to have exploited a vulnerability resulting in system compromise. Which kind of evidence is this IP address?

- A. best evidence
- B. corroborative evidence
- C. indirect evidence
- D. forensic evidence

**Answer:** B

#### NEW QUESTION 142

What is the difference between an attack vector and attack surface?

- A. An attack surface identifies vulnerabilities that require user input or validation; and an attack vector identifies vulnerabilities that are independent of user actions.
- B. An attack vector identifies components that can be exploited, and an attack surface identifies the potential path an attack can take to penetrate the network.
- C. An attack surface recognizes which network parts are vulnerable to an attack; and an attack vector identifies which attacks are possible with these vulnerabilities.
- D. An attack vector identifies the potential outcomes of an attack; and an attack surface launches an attack using several methods against the identified vulnerabilities.



Answer: C

#### NEW QUESTION 144

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 145

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

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

Answer: B

#### NEW QUESTION 146

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 147**

What is a description of a social engineering attack?

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

**Answer:** D

**NEW QUESTION 151**

What is a purpose of a vulnerability management framework?

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

**Answer:** A

**NEW QUESTION 154**

How is attacking a vulnerability categorized?

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

**Answer:** C

**NEW QUESTION 155**

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 157**

What is indicated by an increase in IPv4 traffic carrying protocol 41 ?

- A. additional PPTP traffic due to Windows clients
- B. unauthorized peer-to-peer traffic
- C. deployment of a GRE network on top of an existing Layer 3 network
- D. attempts to tunnel IPv6 traffic through an IPv4 network

**Answer:** D

**NEW QUESTION 160**

Refer to the exhibit.

```
Mar 07 2020 16:16:48: %ASA-4-106023: Deny tcp src
outside:10.22.219.221/54602 dst outside:10.22.250.212/504
by access-group "outside" [0x0, 0x0]
```

Which technology generates this log?

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

**Answer:** D

**NEW QUESTION 164**

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 166**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### 200-201 Practice Exam Features:

- \* 200-201 Questions and Answers Updated Frequently
- \* 200-201 Practice Questions Verified by Expert Senior Certified Staff
- \* 200-201 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* 200-201 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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