



Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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 2

Refer to the exhibit.

```
<IMG SRC=j%41vascript:alert('attack')>
```

Which kind of attack method is depicted in this string?

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

Answer: A

NEW QUESTION 3

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 4

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

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

Answer: B

NEW QUESTION 5

What is the difference between deep packet inspection and stateful inspection?

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

Answer: D

NEW QUESTION 6

What is a difference between inline traffic interrogation and traffic mirroring?

- A. Inline inspection acts on the original traffic data flow
- B. Traffic mirroring passes live traffic to a tool for blocking
- C. Traffic mirroring inspects live traffic for analysis and mitigation
- D. Inline traffic copies packets for analysis and security

Answer: A

Explanation:

Inline traffic interrogation analyzes traffic in real time and has the ability to prevent certain traffic from being forwarded Traffic mirroring doesn't pass the live traffic instead it copies traffic from one or more source ports and sends the copied traffic to one or more destinations for analysis by a network analyzer or other monitoring device

NEW QUESTION 7

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 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 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 10

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

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

Answer: B

Explanation:

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

NEW QUESTION 10

A user received an email attachment named "Hr405-report2609-empl094.exe" but did not run it. Which category of the cyber kill chain should be assigned to this type of event?

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

Answer: D

NEW QUESTION 15

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 18

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 19

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 21

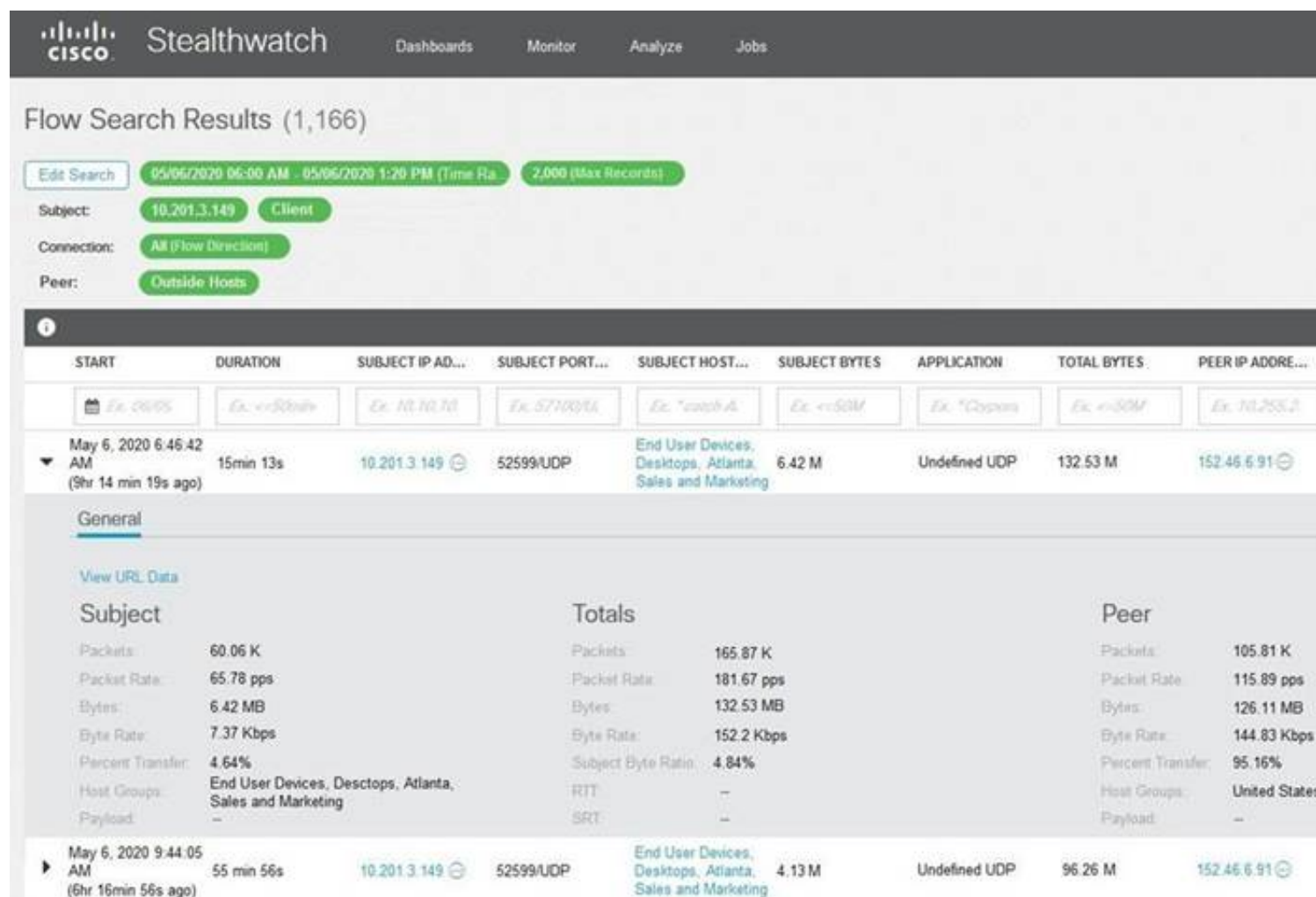
An engineer needs to configure network systems to detect command and control communications by decrypting ingress and egress perimeter traffic and allowing network security devices to detect malicious outbound communications. Which technology should be used to accomplish the task?

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

Answer: A

NEW QUESTION 25

Refer to the exhibit.



The screenshot shows the Cisco Stealthwatch interface. At the top, there's a navigation bar with 'Dashboards', 'Monitor', 'Analyze', and 'Jobs'. Below this, the 'Flow Search Results' section shows 1,166 results. The search filters are: Subject: 10.201.3.149 (Client), Connection: All (Flow Direction), Peer: Outside Hosts. The search criteria are: 05/06/2020 06:00 AM - 05/06/2020 1:20 PM (Time Ra), 2,000 (Max Records).

The results table has columns: START, DURATION, SUBJECT IP AD..., SUBJECT PORT..., SUBJECT HOST..., SUBJECT BYTES, APPLICATION, TOTAL BYTES, and PEER IP ADRE... The first result is for May 6, 2020 6:46:42 AM (9hr 14 min 19s ago), with a duration of 15min 13s. The subject IP is 10.201.3.149, subject port is 52599/UDP, subject host is End User Devices, Desktops, Atlanta, Sales and Marketing, subject bytes is 6.42 M, application is Undefined UDP, total bytes is 132.53 M, and peer IP address is 152.46.6.91.

Below the table, the 'General' tab is selected, showing 'View URL Data'. The 'Subject' section displays statistics: Packets: 60.06 K, Packet Rate: 65.78 pps, Bytes: 6.42 MB, Byte Rate: 7.37 Kbps, Percent Transfer: 4.64%, Host Groups: End User Devices, Desktops, Atlanta, Sales and Marketing, Payload: -. The 'Totals' section displays: Packets: 165.87 K, Packet Rate: 181.67 pps, Bytes: 132.53 MB, Byte Rate: 152.2 Kbps, Subject Byte Ratio: 4.84%, RTT: -, SRT: -. The 'Peer' section displays: Packets: 105.81 K, Packet Rate: 115.89 pps, Bytes: 126.11 MB, Byte Rate: 144.83 Kbps, Percent Transfer: 95.16%, Host Groups: United States, Payload: -.

What is the potential threat identified in this Stealthwatch dashboard?

- A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.
- B. Host 152.46.6.91 is being identified as a watchlist country for data transfer.
- C. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.
- D. Host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91.

Answer: D

NEW QUESTION 27

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 30

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 31

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 33

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 38

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 42

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 44

Refer to the exhibit.



Where is the executable file?

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

Answer: C

NEW QUESTION 49

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 51

Which event is user interaction?

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

Answer: D

NEW QUESTION 55

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 60

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 62

Which type of data consists of connection level, application-specific records generated from network traffic?

- A. transaction data
- B. location data
- C. statistical data
- D. alert data

Answer: A

NEW QUESTION 64

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 67

During which phase of the forensic process are tools and techniques used to extract information from the collected data?

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

Answer: D

NEW QUESTION 68

What is an example of social engineering attacks?

- A. receiving an unexpected email from an unknown person with an attachment from someone in the same company
- B. receiving an email from human resources requesting a visit to their secure website to update contact information
- C. sending a verbal request to an administrator who knows how to change an account password
- D. receiving an invitation to the department's weekly WebEx meeting

Answer: C

NEW QUESTION 69

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

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

Answer: C

NEW QUESTION 73

What describes the defense-in-depth principle?

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

Answer: B

NEW QUESTION 74

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 76

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 78

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 81

What are two categories of DDoS attacks? (Choose two.)

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

Answer: DE

NEW QUESTION 84

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 86

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 88

A security engineer notices confidential data being exfiltrated to a domain "Ranso4134-mware31-895" address that is attributed to a known advanced persistent threat group. The engineer discovers that the activity is part of a real attack and not a network misconfiguration. Which category does this event fall under as defined in the Cyber Kill Chain?

- A. reconnaissance
- B. delivery
- C. action on objectives
- D. weaponization

Answer: C

NEW QUESTION 89

According to the NIST SP 800-86, which two types of data are considered volatile? (Choose two.)

- A. swap files
- B. temporary files
- C. login sessions

- D. dump files
- E. free space

Answer: CE

NEW QUESTION 92

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 95

An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the link launched, it infected machines and the intruder was able to access the corporate network. Which testing method did the intruder use?

- A. social engineering
- B. eavesdropping
- C. piggybacking
- D. tailgating

Answer: A

NEW QUESTION 98

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 103

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 105

Refer to the exhibit.

Date	Flow Start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2020-01-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→ 192.168.0.1:20521	1	82	1

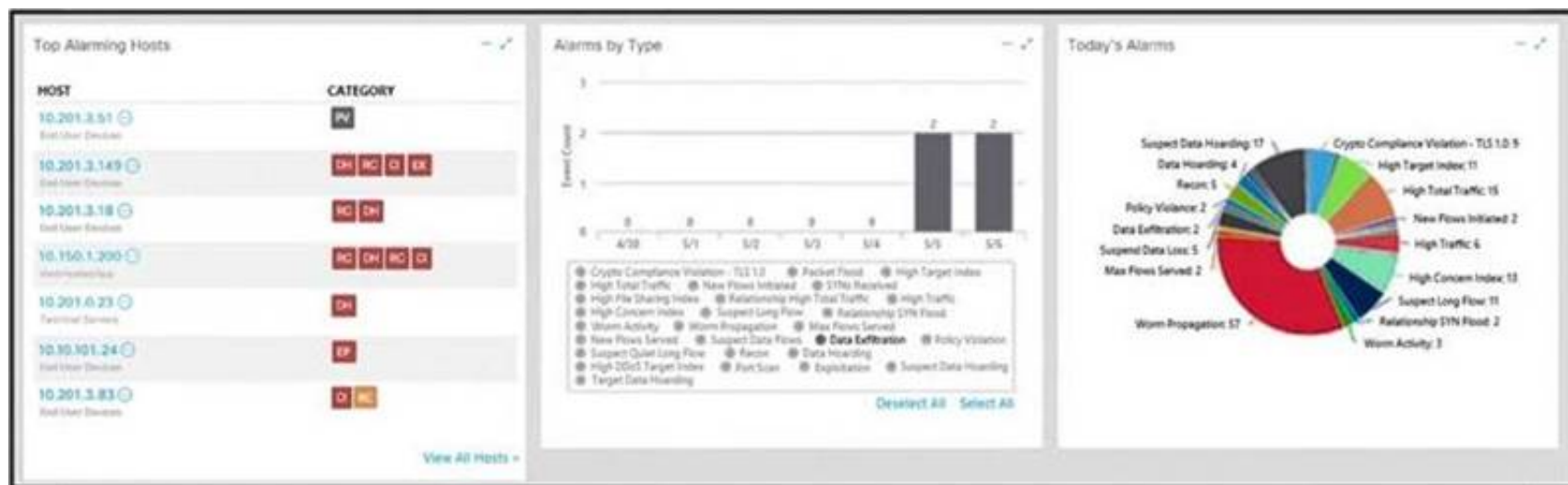
Which type of log is displayed?

- A. proxy
- B. NetFlow
- C. IDS
- D. sys

Answer: B

NEW QUESTION 108

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 113

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 115

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 117

What is obtained using NetFlow?

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

Answer: A

NEW QUESTION 120

What is the difference between a threat and a risk?

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

Answer: A

Explanation:

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

latent and not yet realized.

NEW QUESTION 125

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

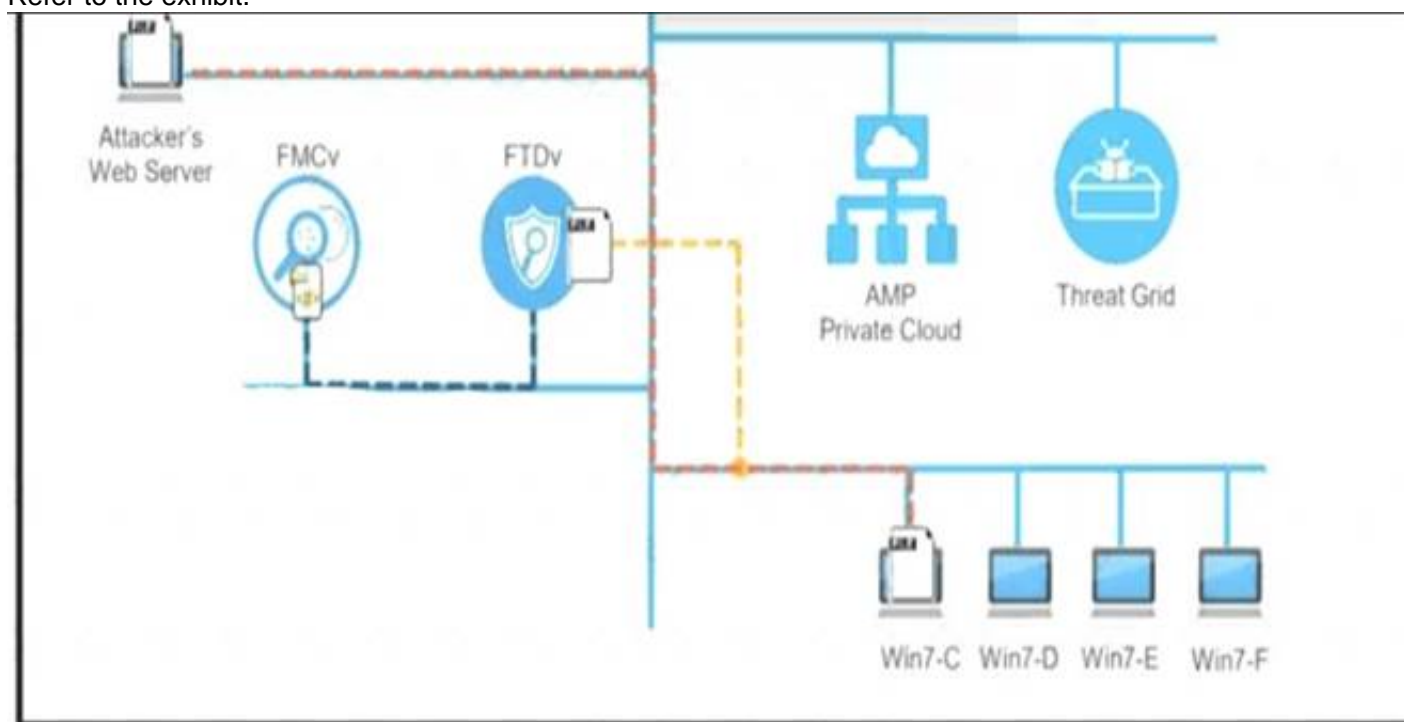
Session duration – the time between the establishment of a data flow and its termination Ports used – a list of TCP or UDP processes that are available to accept data

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 129

Refer to the exhibit.



A workstation downloads a malicious docx file from the Internet and a copy is sent to FTDv. The FTDv sends the file hash to FMC and the file event is recorded. What would have occurred with stronger data visibility?

- A. The traffic would have been monitored at any segment in the network.
- B. Malicious traffic would have been blocked on multiple devices
- C. An extra level of security would have been in place
- D. Detailed information about the data in real time would have been provided

Answer: B

NEW QUESTION 131

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 135

Refer to the exhibit.

Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2014-02-23 21:52:16	2014-02-23 21:52:34	18 seconds	1.0
File Details				
File name	win32.polip.a.exe			
File size	114720 bytes			
File type	PE32_executable (GUI) Intel: 80386, for MS Windows			
CRC32	8048E2EA			
MD5	09019069a77833c939286c864c8cae8			
SHA1	f891d31d3e4a5895a1729136322d8ec979b79ba			
SHA256	f4855d1b1017ab3a2e6b99016437f72c5f98579d69f08b6312cc24400f483172			
SHA512	9756e0af8981bc9796a3879fe02d0e102c5557ba99a09423bca4f1df083592cf497c123d2a6a05596b07432188aef42976e0bd9da742c0900275b6721db2595			
Ssdeep	6144:EuZU7Ye1LnfrB7pRL8I+5zLq1Z49XC0yWg0yCyuE/1rNDep1XXt+o6YUPL:EuZU7Yeand1d+SWG0yG7Ck/1r7EE			
PEID	None matched			
Yara	• shellcode (Matched shellcode byte patterns)			
VirusTotal	Permalink VirusTotal Scan Date: 2014-01-12 23:43:56 Detection Rate: 26/47 (collapse)			

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

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

Answer: C

NEW QUESTION 138

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 143

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 146

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 149

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 154

How does an attack surface differ from an attack vector?

- A. An attack vector recognizes the potential outcomes of an attack, and the attack surface is choosing a method of an attack.
- B. An attack surface identifies vulnerable parts for an attack, and an attack vector specifies which attacks are feasible to those parts.
- C. An attack surface mitigates external vulnerabilities, and an attack vector identifies mitigation techniques and possible workarounds.
- D. An attack vector matches components that can be exploited, and an attack surface classifies the potential path for exploitation

Answer: B

NEW QUESTION 157

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 158

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 163

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 168

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 173

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 178

A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?

- A. CD data copy prepared in Windows
- B. CD data copy prepared in Mac-based system
- C. CD data copy prepared in Linux system
- D. CD data copy prepared in Android-based system

Answer: A

NEW QUESTION 180

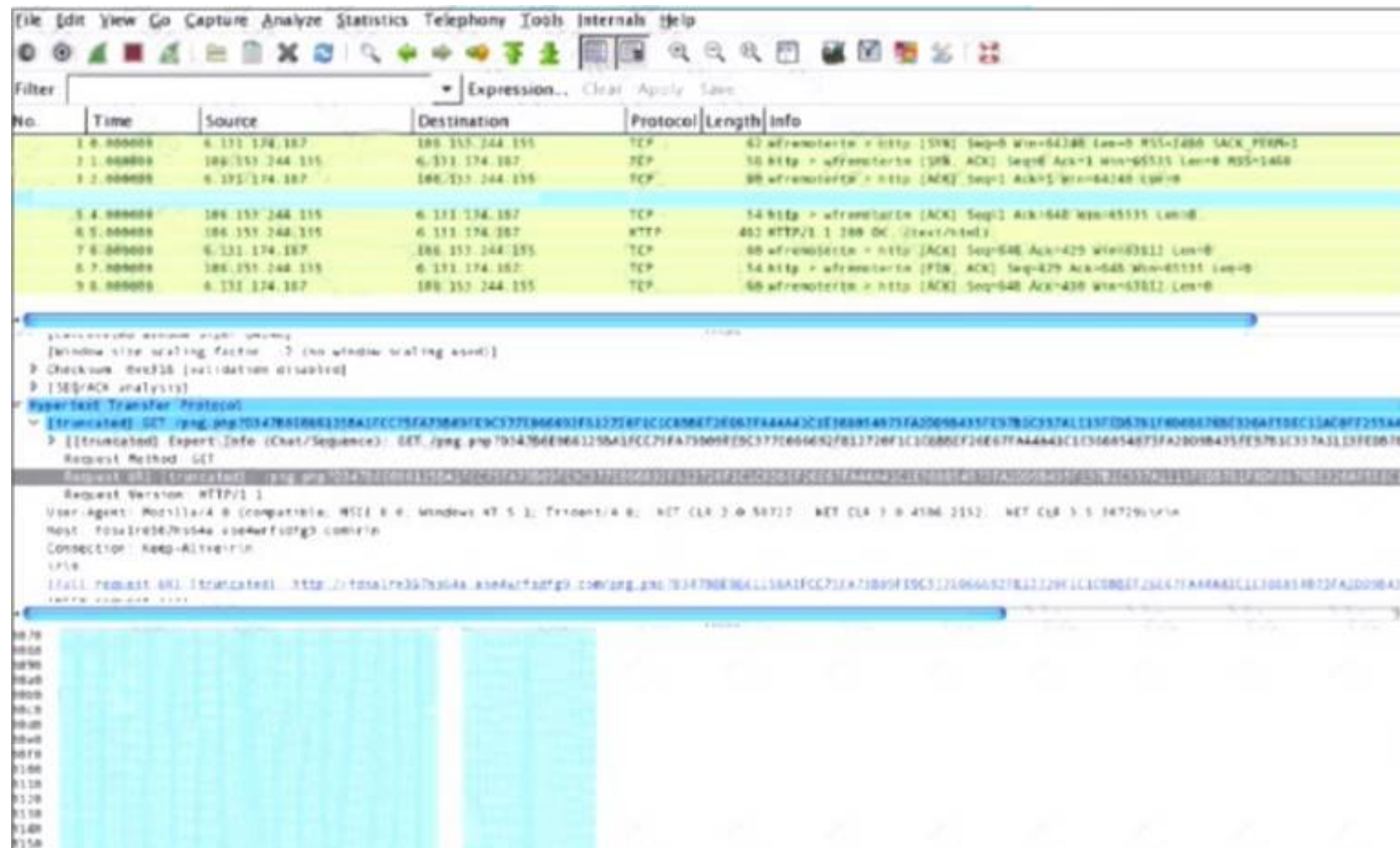
What is the relationship between a vulnerability and a threat?

- 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 184

Refer to the exhibit.



No.	Time	Source	Destination	Protocol	Length	Info
1.0.00000	0.131174.187	10.0.0.1	10.0.0.2	TCP	60	60 → 80 [RST] Seq=64388 Len=0 RST=1460 SACK_PERM=1
2.1.00000	0.131174.187	10.0.0.1	10.0.0.2	TCP	60	60 → 80 [RST] Seq=64388 Len=0 RST=1460 SACK_PERM=1
3.2.00000	0.131174.187	10.0.0.1	10.0.0.2	TCP	60	60 → 80 [RST] Seq=64388 Len=0 RST=1460 SACK_PERM=1
4.3.00000	0.131174.187	10.0.0.1	10.0.0.2	TCP	60	60 → 80 [RST] Seq=64388 Len=0 RST=1460 SACK_PERM=1
5.4.00000	0.131174.187	10.0.0.1	10.0.0.2	TCP	60	60 → 80 [RST] Seq=64388 Len=0 RST=1460 SACK_PERM=1
6.5.00000	0.131174.187	10.0.0.1	10.0.0.2	TCP	60	60 → 80 [RST] Seq=64388 Len=0 RST=1460 SACK_PERM=1
7.6.00000	0.131174.187	10.0.0.1	10.0.0.2	TCP	60	60 → 80 [RST] Seq=64388 Len=0 RST=1460 SACK_PERM=1
8.7.00000	0.131174.187	10.0.0.1	10.0.0.2	TCP	60	60 → 80 [RST] Seq=64388 Len=0 RST=1460 SACK_PERM=1
9.8.00000	0.131174.187	10.0.0.1	10.0.0.2	TCP	60	60 → 80 [RST] Seq=64388 Len=0 RST=1460 SACK_PERM=1

What is shown in this PCAP file?

- A. Timestamps are indicated with error.
- B. The protocol is TCP.
- C. The User-Agent is Mozilla/5.0.
- D. The HTTP GET is encoded.

Answer: D

NEW QUESTION 185

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 186

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 188

Which tool provides a full packet capture from network traffic?

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

Answer: D

NEW QUESTION 193

What is the impact of encryption?

- A. Confidentiality of the data is kept secure and permissions are validated
- B. Data is accessible and available to permitted individuals
- C. Data is unaltered and its integrity is preserved
- D. Data is secure and unreadable without decrypting it

Answer: A

NEW QUESTION 194

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 199

Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

- A. known-plaintext
- B. replay
- C. dictionary
- D. man-in-the-middle

Answer: D

NEW QUESTION 200

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

Answer: A

NEW QUESTION 202

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 206

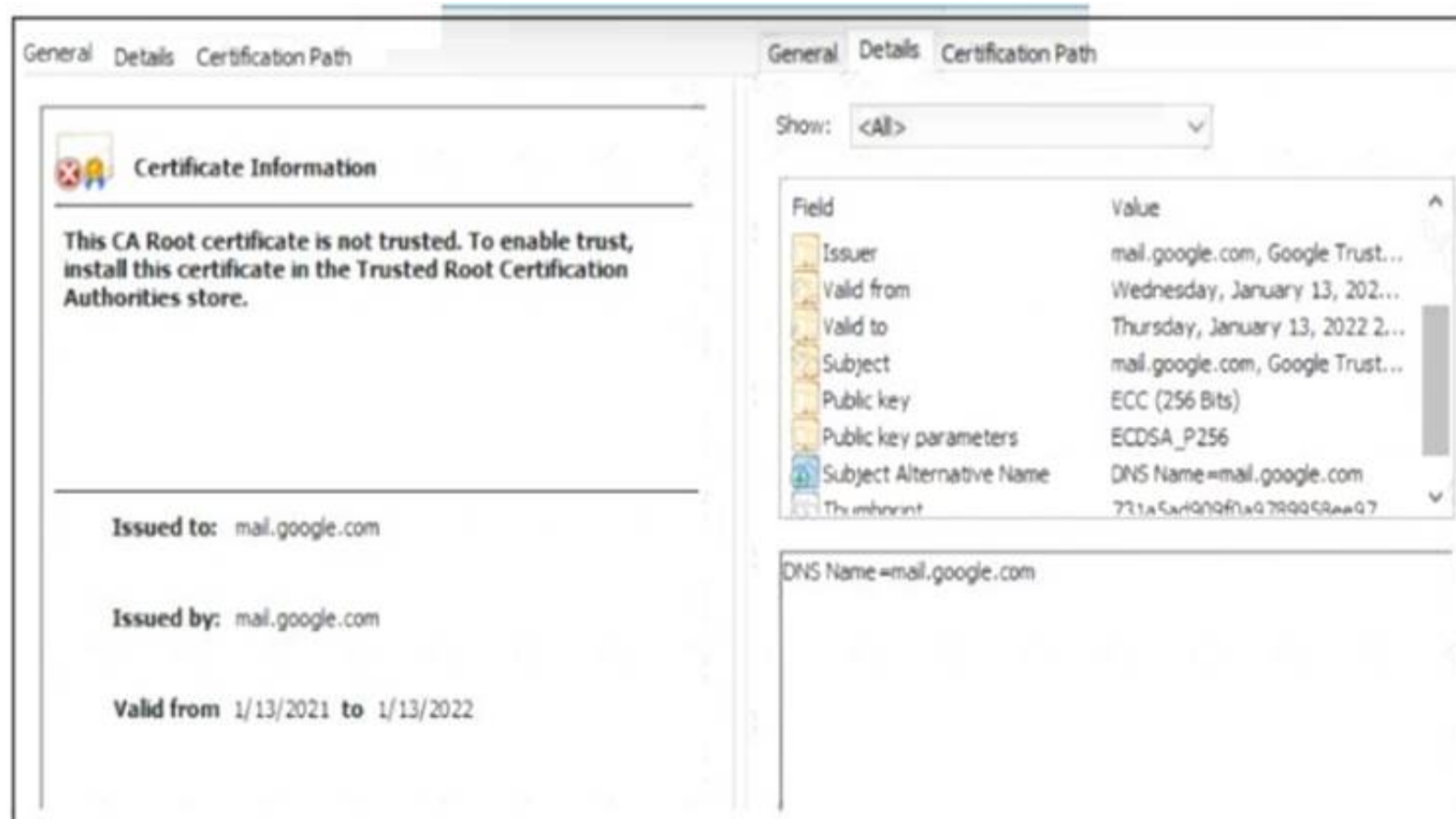
How is attacking a vulnerability categorized?

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

Answer: C

NEW QUESTION 211

Refer to the exhibit.



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

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

Answer: C

NEW QUESTION 216

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 218

What is a difference between signature-based and behavior-based detection?

- A. Signature-based identifies behaviors that may be linked to attacks, while behavior-based has a predefined set of rules to match before an alert.
- B. Behavior-based identifies behaviors that may be linked to attacks, while signature-based has a predefined set of rules to match before an alert.
- C. Behavior-based uses a known vulnerability database, while signature-based intelligently summarizes existing data.
- D. Signature-based uses a known vulnerability database, while behavior-based intelligently summarizes existing data.

Answer: B

Explanation:

Instead of searching for patterns linked to specific types of attacks, behavior-based IDS solutions monitor behaviors that may be linked to attacks, increasing the likelihood of identifying and mitigating a malicious action before the network is compromised.

<https://accedian.com/blog/what-is-the-difference-between-signature-based-and-behavior-based-ids/>

NEW QUESTION 220

Which security technology guarantees the integrity and authenticity of all messages transferred to and from a web application?

- A. Hypertext Transfer Protocol
- B. SSL Certificate
- C. Tunneling
- D. VPN

Answer: B

NEW QUESTION 221

.....

Relate Links

100% Pass Your 200-201 Exam with ExamBible Prep Materials

<https://www.exambible.com/200-201-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>