

## 200-201 Dumps

# Understanding Cisco Cybersecurity Operations Fundamentals

<https://www.certleader.com/200-201-dumps.html>



**NEW QUESTION 1**

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

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

**Answer:** A

**NEW QUESTION 2**

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

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

**Answer:** C

**NEW QUESTION 3**

When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification. Which information is available on the server certificate?

- A. server name, trusted subordinate CA, and private key
- B. trusted subordinate CA, public key, and cipher suites
- C. trusted CA name, cipher suites, and private key
- D. server name, trusted CA, and public key

**Answer:** D

**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 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 6**

Which incident response step includes identifying all hosts affected by an attack?

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

**Answer:** D

**Explanation:**

\* 3.3.3 Identifying the Attacking Hosts During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts. Although this information can be important, incident handlers should generally stay focused on containment, eradication, and recovery.

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

The response phase, or containment, of incident response, is the point at which the incident response team begins interacting with affected systems and attempts to keep further damage from occurring as a result of the incident.

**NEW QUESTION 7**

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
17	0.011641	10.0.2.15	192.124.249.9	TCP	76	50586-443 [SYN] Seq=0 Win=
18	0.011918	10.0.2.15	192.124.249.9	TCP	76	50588-443 [SYN] Seq=0 Win=
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443-50588 [SYN, ACK] Seq=0
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588-443 [ACK] Seq=1 Ack=
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443-50586 [SYN, ACK] Seq=0
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=1 Ack=
23	0.023212	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
24	0.023373	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443-50588 [ACK] Seq=1 Ack=
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443-50586 [ACK] Seq=1 Ack=
27	0.037413	192.124.249.9	10.0.2.15	TLSv1.2	2792	Server Hello
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=206 Ac

> Frame 23: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)  
> Linux cooked capture  
> Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)  
> Transmission Control Protocol, Src Port: 50588 (50588), Dst Port: 443 (443), Seq: 1, Ack:1,  
> Secure Sockets Layer

```

0000 00 04 00 01 00 06 08 00 27 7a 3c 93 00 00 08 00 ..... *z<.....
0010 45 00 00 f5 eb 3e 40 00 40 06 89 2f 0a 00 02 0f E....>@. @../....
0020 c0 7c f9 09 c5 9c 01 bb 4d db 7f f7 00 b3 b0 02 .|..... M.....
0030 50 18 72 10 c6 7c 00 00 16 03 01 00 c8 01 00 00 P.r..|.. .....
0040 c4 03 03 d1 08 45 78 b7 2c 90 04 ee 51 16 f1 82 .....Ex. ....0...
0050 16 43 ec d4 89 60 34 4a 7b 80 a6 d1 72 d5 11 87 .C....4J {...r...
0060 10 57 cc 00 00 1e c0 2b c0 2f cc a9 cc a8 c0 2c .W.....+ ./.....
0070 c0 30 c0 0a c0 09 c0 13 c0 14 00 33 00 39 00 2f .0..... ...3.9./
0080 00 35 00 0a 01 00 00 7d 00 00 00 16 00 14 00 00 .5.....} .....
0090 11 77 77 77 2e 6c 69 6e 75 78 6d 69 6e 74 2e 63 .wwwlin uxmint.c
00a0 6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 08 00 om..... .....
00b0 06 00 17 00 18 00 19 00 0b 00 02 01 00 00 23 00 ..... .....#
00c0 00 33 74 00 00 00 10 00 17 00 15 02 68 32 08 73 .3t..... ...h2.s
00d0 70 64 79 2f 33 2e 31 08 68 74 74 70 2f 31 2e 31 pdy/3.2. http/1.1
00e0 00 05 00 05 01 00 00 00 00 00 0d 00 18 00 16 04 ..... .....
00f0 01 05 01 06 01 02 01 04 03 05 03 06 03 02 03 05 ..... .....
0100 02 04 02 02 02 .....
    
```

Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

source address	source address
destination address	source port
source port	destination port
destination port	destination address
Network Protocol	Transport Protocol
Transport Protocol	Network Protocol
Application Protocol	Application Protocol

**NEW QUESTION 8**

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 9**

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 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**

Refer to the exhibit.

**Flow Search Results (1,166)**

Subject: 10.201.3.149 Client  
Connection: All (Flow Direction)  
Peer: Outside Hosts

START	DURATION	SUBJECT IP AD...	SUBJECT PORT...	SUBJECT HOST...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADRE...
May 6, 2020 6:46:42 AM (9hr 14min 19s ago)	15min 13s	10.201.3.149	52599/UDP	End User Devices, Desktops, Atlanta, Sales and Marketing	6.42 M	Undefined UDP	132.53 M	152.46.6.91

**General**

View URL Data

Subject	Totals	Peer
Packets: 60.06 K	Packets: 165.87 K	Packets: 105.81 K
Packet Rate: 65.78 pps	Packet Rate: 181.67 pps	Packet Rate: 115.89 pps
Bytes: 6.42 MB	Bytes: 132.53 MB	Bytes: 126.11 MB
Byte Rate: 7.37 Kbps	Byte Rate: 152.2 Kbps	Byte Rate: 144.83 Kbps
Percent Transfer: 4.64%	Subject Byte Ratio: 4.84%	Percent Transfer: 95.16%
Host Groups: End User Devices, Desktops, Atlanta, Sales and Marketing	RTT: --	Host Groups: United States
Payload: --	SRT: --	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 14**

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 16**

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 18**

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

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

**Answer: C**

**NEW QUESTION 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 23**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 27**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 31**

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 35**

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 40**

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 this type of event belong?

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

**Answer:** B

**NEW QUESTION 42**

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



**NEW QUESTION 57**

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 60**

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 62**

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 67**

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 69**

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 71**

Which category relates to improper use or disclosure of PII data?

- A. legal
- B. compliance
- C. regulated
- D. contractual

**Answer: C**

**NEW QUESTION 76**

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 79**

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 84**

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

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

**Answer:** D

**NEW QUESTION 86**

Which HTTP header field is used in forensics to identify the type of browser used?

- A. referrer
- B. host
- C. user-agent
- D. accept-language

**Answer:** C

**Explanation:**

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:12.0) Gecko/20100101 Firefox/12.0 In computing, a user agent is any software, acting on behalf of a user, which "retrieves, renders and facilitates end-user interaction with Web content".[1] A user agent is therefore a special kind of software agent.

[https://en.wikipedia.org/wiki/User\\_agent#User\\_agent\\_identification](https://en.wikipedia.org/wiki/User_agent#User_agent_identification)

A user agent is a computer program representing a person, for example, a browser in a Web context. [https://developer.mozilla.org/en-US/docs/Glossary/User\\_agent](https://developer.mozilla.org/en-US/docs/Glossary/User_agent)

**NEW QUESTION 88**

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 89**

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 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 96**

Which attack is the network vulnerable to when a stream cipher like RC4 is used twice with the same key?

- A. forgery attack
- B. plaintext-only attack
- C. ciphertext-only attack
- D. meet-in-the-middle attack

**Answer: C**

**NEW QUESTION 97**

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 102**

Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

- A. syslog messages
- B. full packet capture
- C. NetFlow
- D. firewall event logs

**Answer: C**

**NEW QUESTION 105**

Which attack method intercepts traffic on a switched network?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 108**

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 113**

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 115**

Which technology on a host is used to isolate a running application from other applications?

- A. sandbox
- B. application allow list
- C. application block list
- D. host-based firewall

Answer: A

**NEW QUESTION 116**

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 119**

What should an engineer use to aid the trusted exchange of public keys between user tom0411976943 and dan1968754032?

- A. central key management server
- B. web of trust
- C. trusted certificate authorities
- D. registration authority data

Answer: C

**NEW QUESTION 121**

How does TOR alter data content during transit?

- A. It spoofs the destination and source information protecting both sides.
- B. It encrypts content and destination information over multiple layers.
- C. It redirects destination traffic through multiple sources avoiding traceability.
- D. It traverses source traffic through multiple destinations before reaching the receiver

Answer: B

**NEW QUESTION 123**

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 128**

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 131**

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
18	0.011710	10.0.2.15	192.124.249.9	TCP	70	50586-443 [FIN] Seq=1
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443-50588 [SYN, ACK]
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588-443 [ACK] Seq=1
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443-50586 [SYN, ACK]
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=1
23	0.023212	10.0.2.15	192.124.249.9	TCP	261	50588-443 [PSH, ACK]
24	0.023373	10.0.2.15	192.124.249.9	TCP	261	50586-443 [PSH, ACK]
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443-50588 [ACK] Seq=1
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443-50586 [ACK] Seq=1
27	0.037413	192.124.249.9	10.0.2.15	TCP	2792	443-50586 [PSH, ACK]
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=2

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

```

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

Which application protocol is in this PCAP file?

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

**Answer: D**

**NEW QUESTION 136**

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 140**

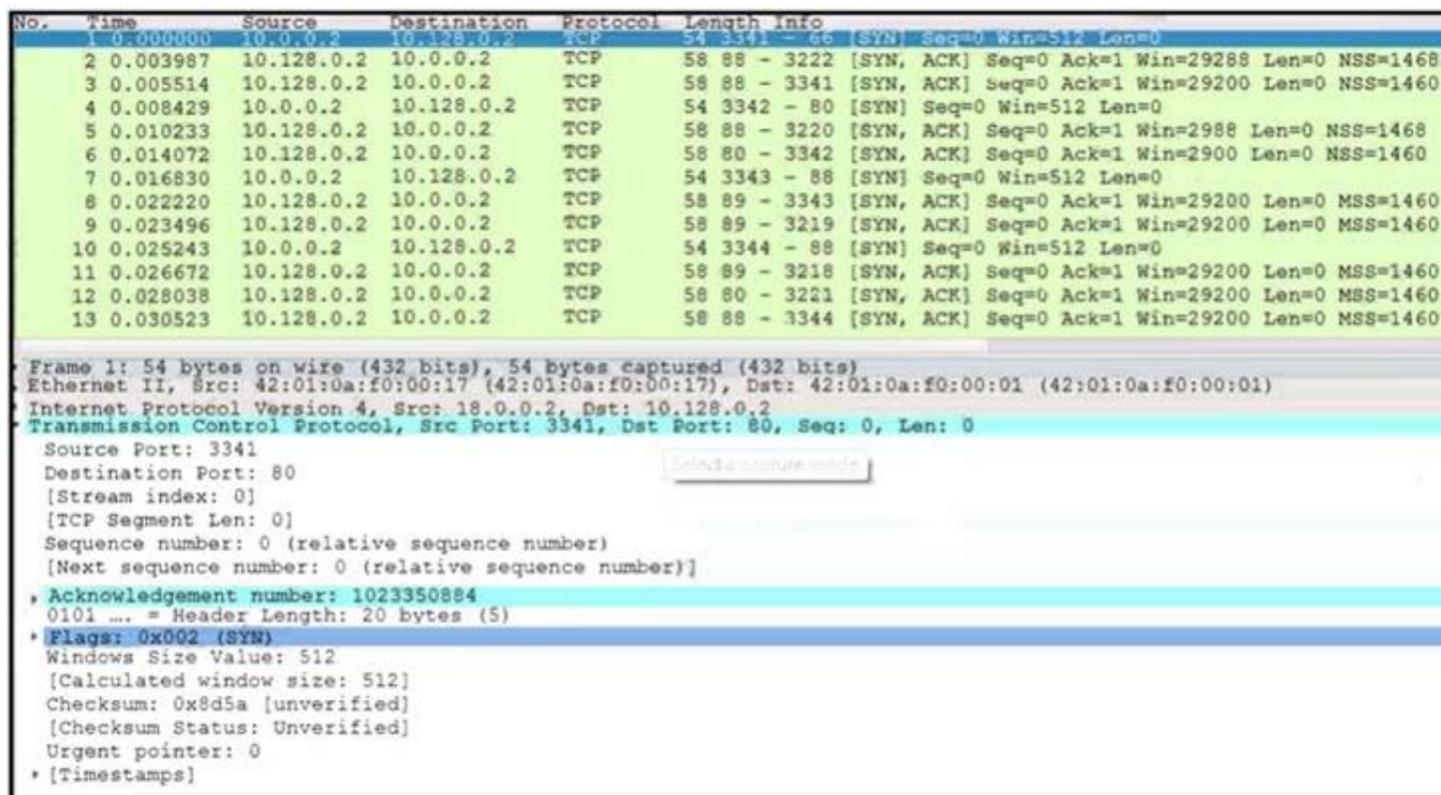
An analyst is exploring the functionality of different operating systems. What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?

- A. queries Linux devices that have Microsoft Services for Linux installed
- B. deploys Windows Operating Systems in an automated fashion
- C. is an efficient tool for working with Active Directory
- D. has a Common Information Model, which describes installed hardware and software

Answer: D

**NEW QUESTION 144**

Refer to the exhibit.



What is occurring in this network traffic?

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

Answer: D

**NEW QUESTION 149**

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: i686, for MS Windows
CRC32	8848E2EA
MD5	090f9009a77804e9296c764c0ce08
SHA1	f891d31d3e4a5885d170113632208ec979b79ba
SHA256	f4855d1b1077b132e6b99016437f72c5f98579d69f08b6312cc24400f483172
SHA512	9756e0af8981bc9796a3879fe0200e162c5557ba99a094236ca4f1df083592cf497c123d2a6a0596607432188aaef42976e0bd9da742c0960275b6721db2595
Ssdeep	6144:EuZ0Y7e1Lnfr87pR18I+5rLqjZ49XC0y0y0y0y0/1r0Dep1XX1+o6Y0PL:EuZ0Y7eand16+SWG0y0Y0ck/1r7EE
PEID	None matched
Yara	<ul style="list-style-type: none"> <li>• shellcode (Matched shellcode byte patterns)</li> </ul>
VirusTotal	<a href="#">Permalink</a> VirusTotal Scan Date: 2014-01-12 23:43:56 Detection Rate: 26/47 (collapser)

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 151**

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

- A. A false negative is alerting for an XSS attack
- 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 alert
- 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 152**

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 user 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 narration stronger but alone it's mean nothing.

**NEW QUESTION 153**

What is the impact of false positive alerts on business compared to true positive?

- A. True positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.
- B. True positive alerts are blocked by mistake as potential attacks affecting application availability.
- C. False positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.
- D. False positive alerts are blocked by mistake as potential attacks affecting application availability.

**Answer: C**

**NEW QUESTION 156**

At a company party a guest asks questions about the company's user account format and password complexity. How is this type of conversation classified?

- A. Phishing attack
- B. Password Revelation Strategy

- C. Piggybacking
- D. Social Engineering

**Answer:** D

**NEW QUESTION 157**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 162**

Refer to the exhibit.

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

What is depicted in the exhibit?

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

**Answer:** B

**NEW QUESTION 163**

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 166**

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 169**

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 174**

What is the difference between statistical detection and rule-based detection models?

- A. Rule-based detection involves the collection of data in relation to the behavior of legitimate users over a period of time

- B. Statistical detection defines legitimate data of users over a period of time and rule-based detection defines it on an IF/THEN basis
- C. Statistical detection involves the evaluation of an object on its intended actions before it executes that behavior
- D. Rule-based detection defines legitimate data of users over a period of time and statistical detection defines it on an IF/THEN basis

**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 179**

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

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

**Answer:** AB

**NEW QUESTION 182**

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 187**

In a SOC environment, what is a vulnerability management metric?

- A. code signing enforcement
- B. full assets scan
- C. internet exposed devices
- D. single factor authentication

**Answer:** C

**NEW QUESTION 188**

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 189**

How does a certificate authority impact security?

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

**Answer:** D

**Explanation:**

A certificate authority is a computer or entity that creates and issues digital certificates. CA do not "authenticate" it validates. "D" is wrong because The digital certificate validate a user. CA --> DC --> user, server or whatever.

**NEW QUESTION 193**

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 198**

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 199**

Which security model assumes an attacker within and outside of the network and enforces strict verification before connecting to any system or resource within the organization?

- A. Biba
- B. Object-capability
- C. Take-Grant
- D. Zero Trust

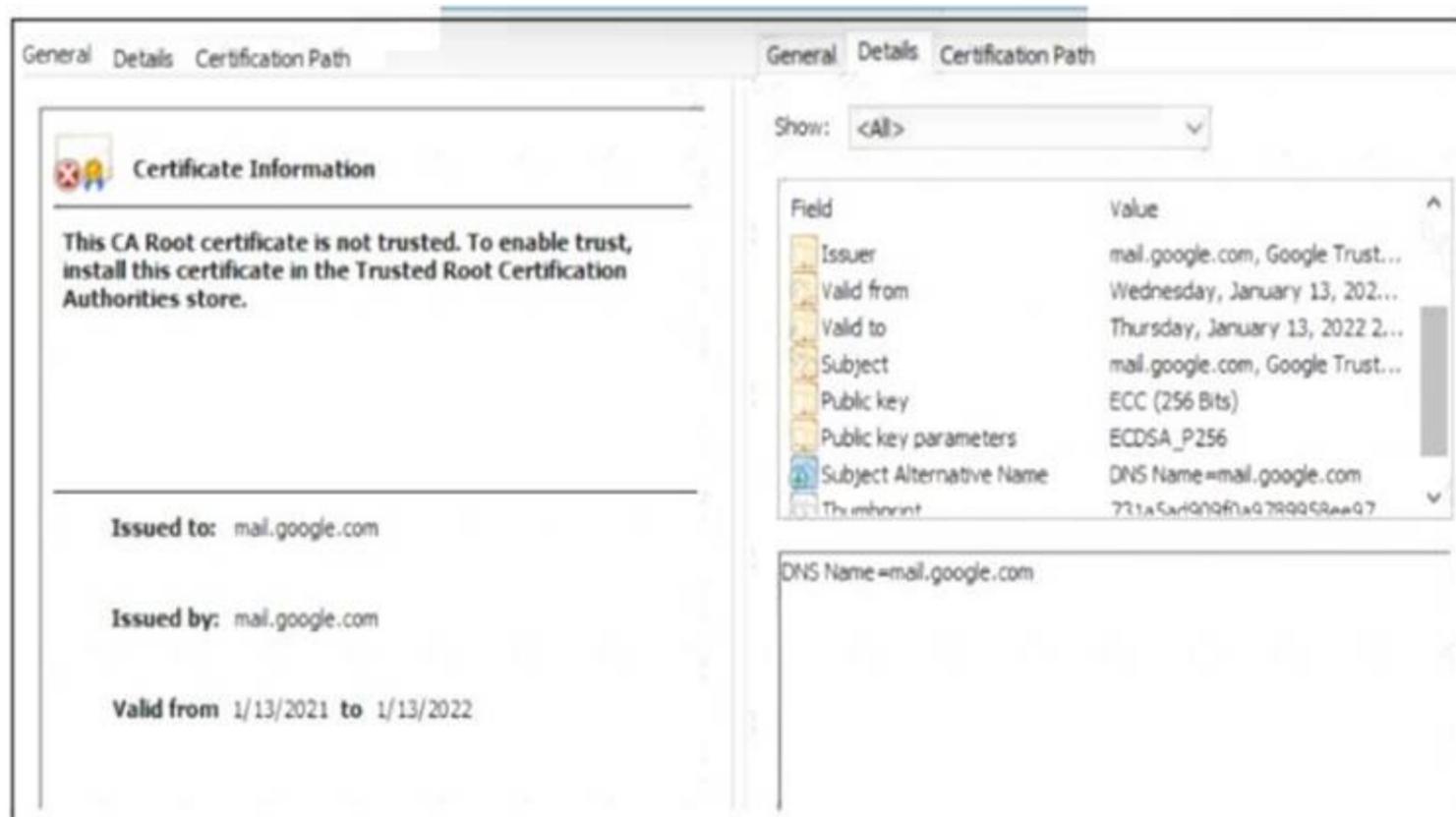
**Answer:** D

**Explanation:**

Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

**NEW QUESTION 202**

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 205**

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 209**

A developer is working on a project using a Linux tool that enables writing processes to obtain these required results:

- > If the process is unsuccessful, a negative value is returned.
- > If the process is successful, 0 value is returned to the child process, and the process ID is sent to the parent process.

Which component results from this operation?

- A. parent directory name of a file pathname
- B. process spawn scheduled
- C. macros for managing CPU sets
- D. new process created by parent process

**Answer: D**

**Explanation:**

There are two tasks with specially distinguished process IDs: swapper or sched has process ID 0 and is responsible for paging, and is actually part of the kernel rather than a normal user-mode process. Process ID 1 is usually the init process primarily responsible for starting and shutting down the system. Originally, process ID 1 was not specifically reserved for init by any technical measures: it simply had this ID as a natural consequence of being the first process invoked by the kernel. More recent Unix systems typically have additional kernel components visible as 'processes', in which case PID 1 is actively reserved for the init process to maintain consistency with older systems

**NEW QUESTION 211**

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 215**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your 200-201 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/200-201-dumps.html>