# Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

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

**NEW QUESTION 1**
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

**NEW QUESTION 2**
What is the difference between deep packet inspection and stateful inspection?

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

**Answer:** D

**NEW QUESTION 3**
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 4**
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 5**
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


**NEW QUESTION 6**
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 7**
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. IP address 179.179.69/50272/192.168.122.100/80/6 is sending a packet from port 80 of IP address 192.168.122.100 that is going to port 50272 of IP address 81.179.179.69 using IP protocol 6.
B. IP address 192.168.122.100/50272/81.179.179.69/80/6 is sending a packet from port 50272 of IP address 192.168.122.100 that is going to port 80 of IP address 81.179.179.69 using IP protocol 6.
C. IP address 192.168.122.100/50272/81.179.179.69/80/6 is sending a packet from port 80 of IP address 192.168.122.100 that is going to port 50272 of IP address 81.179.179.69 using IP protocol 6.7E503B693763E0113BE0CD2E4A16C9C4
D. IP address 179.179.69/50272/192.168.122.100/80/6 is sending a packet from port 50272 of IP address 192.168.122.100 that is going to port 80 of IP address 81.179.179.69 using IP protocol 6.

**Answer:** B


**NEW QUESTION 8**
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 9**
What is the practice of giving an employee access to only the resources needed to accomplish their job?

A. principle of least privilege
B. organizational separation
C. separation of duties
D. need to know principle

**Answer:** A

**NEW QUESTION 10**
Which metric is used to capture the level of access needed to launch a successful attack?

A. privileges required
B. user interaction
C. attack complexity
D. attack vector

**Answer:** A

**NEW QUESTION 10**
Refer to the exhibit.

| File name | CVE-2009-4324 PDF 2009-11-30 note200911.pdf |
|---|---|
| File size | 400918 bytes |
| File type | PDF document, version 1.6 |
| CRC32 | 11638A9B |
| MD5 | 61baabd6fc12e01ff73ceacc07c84f9a |
| SHA1 | 0805d0ae62f5358b9a3f4c1868d552fc3561b17 |
| SHA256 | 27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c |
| SHA512 | 5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a |
| Ssdeep | 1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/QR/875+.prahGV6B |
| PEID | None matched |
| Yara | • embedded_pe (Contains an embedded PE32 file)<br>• embedded_win_api (A non-Windows executable contains win32 API<br>• vmdetect (Possibly employs anti-virtualization techniques) |
| VirusTotal | Permalink<br>VirusTotal Scan Date: 2013-12-27 06:51:52<br>Detection Rate: 32/46 (collapse) |

An engineer is analyzing this Cuckoo Sandbox report for a PDF file that has been downloaded from an email. What is the state of this file?

A. The file has an embedded executable and was matched by PEiD threat signatures for further analysis.
B. The file has an embedded non-Windows executable but no suspicious features are identified.
C. The file has an embedded Windows 32 executable and the Yara field lists suspicious features for further analysis.
D. The file was matched by PEiD threat signatures but no suspicious features are identified since the signature list is up to date.

**Answer:** C

**NEW QUESTION 12**
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

**NEW QUESTION 15**
Refer to the exhibit.

```
10.44.101.23 - - [20/Nov/2017:14:18:06 -0500] "GET / HTTP/1.1"
200 1254 "-" "Mozilla/5.0(X11; Ubuntu; Linux x86_64; rv:54.0)
Gecko/20100101 Firefox/54.0"
```

What does the message indicate?

A. an access attempt was made from the Mosaic web browser
B. a successful access attempt was made to retrieve the password file
C. a successful access attempt was made to retrieve the root of the website
D. a denied access attempt was made to retrieve the password file

**Answer:** C

**NEW QUESTION 19**
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 21**
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 22**
A security engineer deploys an enterprise-wide host/endpoint technology for all of the company's corporate PCs. Management requests the engineer to block a selected set of applications on all PCs.
Which technology should be used to accomplish this task?

A. application whitelisting/blacklisting
B. network NGFW
C. host-based IDS
D. antivirus/antispyware software

**Answer:** A


**NEW QUESTION 23**
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 28**
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 33**
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
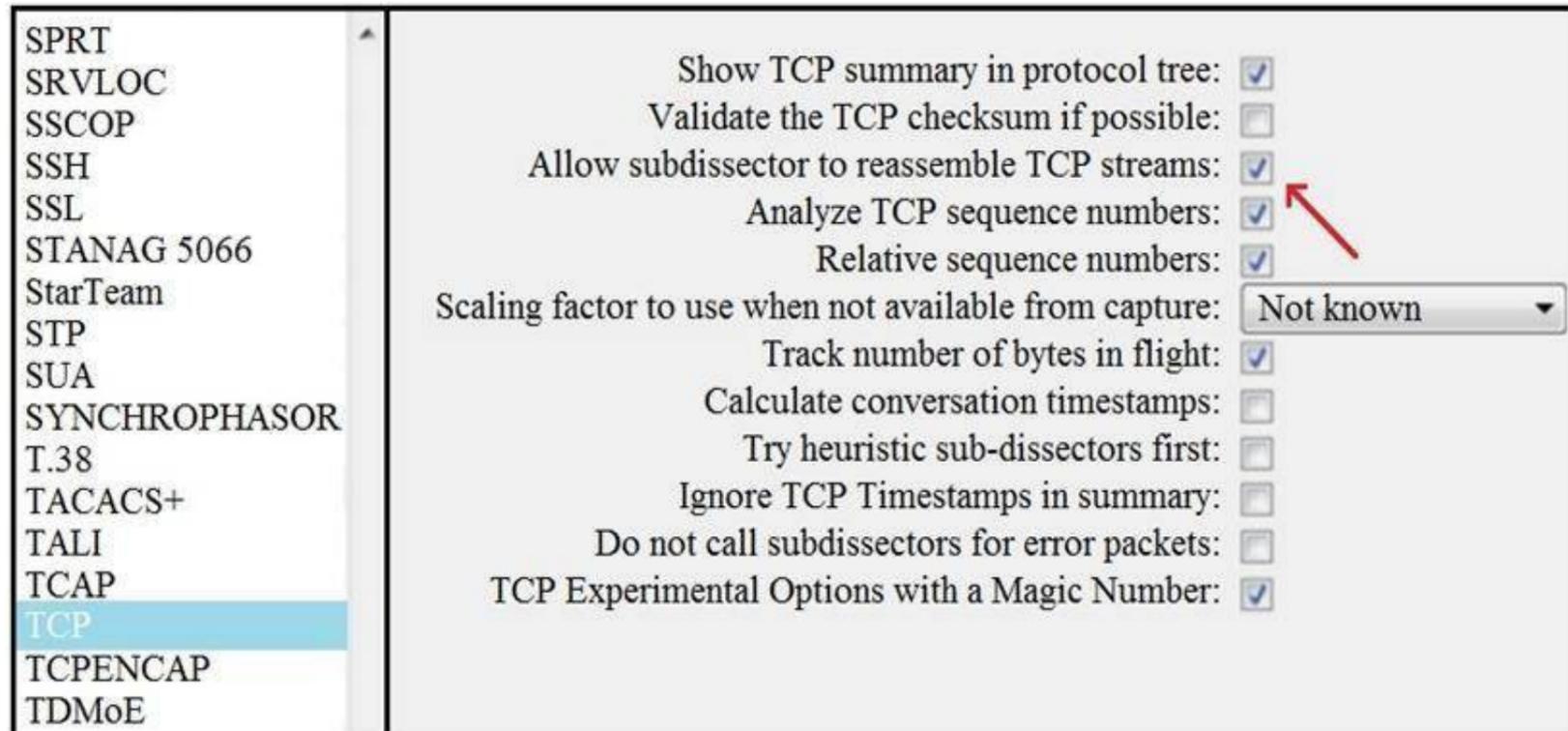
**Answer:** B


**NEW QUESTION 36**
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 39**

Refer to the exhibit.



What is the expected result when the "Allow subdissector to reassemble TCP streams" feature is enabled?

A. insert TCP subdissectors
B. extract a file from a packet capture
C. disable TCP streams
D. unfragment TCP

**Answer:** D

**NEW QUESTION 43**
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 46**
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 47**
How is NetFlow different than 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 50**
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 53**
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 58**
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:** D

**NEW QUESTION 62**
......

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

# Money Back Guarantee

## 200-201 Practice Exam Features:

* 200-201 Questions and Answers Updated Frequently

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

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

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