

## Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)

<https://www.2passeasy.com/dumps/350-201/>



### NEW QUESTION 1

Refer to the exhibit.

Max (K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

Which command was executed in PowerShell to generate this log?

- A. Get-EventLog -LogName\*
- B. Get-EventLog -List
- C. Get-WinEvent -ListLog\* -ComputerName localhost
- D. Get-WinEvent -ListLog\*

**Answer: A**

### NEW QUESTION 2

Which command does an engineer use to set read/write/execute access on a folder for everyone who reaches the resource?

- A. chmod 666
- B. chmod 774
- C. chmod 775
- D. chmod 777

**Answer: D**

### NEW QUESTION 3

The physical security department received a report that an unauthorized person followed an authorized individual to enter a secured premise. The incident was documented and given to a security specialist to analyze. Which step should be taken at this stage?

- A. Determine the assets to which the attacker has access
- B. Identify assets the attacker handled or acquired
- C. Change access controls to high risk assets in the enterprise
- D. Identify movement of the attacker in the enterprise

**Answer: D**

### NEW QUESTION 4

A patient views information that is not theirs when they sign in to the hospital's online portal. The patient calls the support center at the hospital but continues to be put on hold because other patients are experiencing the same issue. An incident has been declared, and an engineer is now on the incident bridge as the CyberOps Tier 3 Analyst. There is a concern about the disclosure of PII occurring in real-time. What is the first step the analyst should take to address this incident?

- A. Evaluate visibility tools to determine if external access resulted in tampering
- B. Contact the third-party handling provider to respond to the incident as critical
- C. Turn off all access to the patient portal to secure patient records
- D. Review system and application logs to identify errors in the portal code

**Answer: C**

### NEW QUESTION 5

The incident response team receives information about the abnormal behavior of a host. A malicious file is found being executed from an external USB flash drive. The team collects and documents all the necessary evidence from the computing resource. What is the next step?

- A. Conduct a risk assessment of systems and applications
- B. Isolate the infected host from the rest of the subnet
- C. Install malware prevention software on the host
- D. Analyze network traffic on the host's subnet

**Answer: B**

### NEW QUESTION 6

Drag and drop the telemetry-related considerations from the left onto their cloud service models on the right.

## Answer Area

Logs, alerts, and events for application performance monitoring and application health are configurable by the customer	SaaS
The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited	PaaS
Logs, alerts, and events for operating systems are configurable by the customer	IaaS

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

## Answer Area

Logs, alerts, and events for application performance monitoring and application health are configurable by the customer	The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited
The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited	Logs, alerts, and events for operating systems are configurable by the customer
Logs, alerts, and events for operating systems are configurable by the customer	Logs, alerts, and events for application performance monitoring and application health are configurable by the customer

## NEW QUESTION 7

Drag and drop the phases to evaluate the security posture of an asset from the left onto the activity that happens during the phases on the right.

## Answer Area

vulnerability assessment	gathering information on a target for future use
persistence	probing the target to discover operating system details
exploit	confirming the existence of known vulnerabilities in the target system
cover tracks	using previously identified vulnerabilities to gain access to the target system
reconnaissance	inserting backdoor access or covert channels to ensure access to the target system
enumeration	erasing traces of actions in audit logs and registry entries

- A. Mastered  
B. Not Mastered



Answer: A

Explanation:

### Answer Area

vulnerability assessment	persistence
persistence	reconnaissance
exploit	vulnerability assessment
cover tracks	exploit
reconnaissance	enumeration
enumeration	cover tracks

### NEW QUESTION 8

An employee who often travels abroad logs in from a first-seen country during non-working hours. The SIEM tool generates an alert that the user is forwarding an increased amount of emails to an external mail domain and then logs out. The investigation concludes that the external domain belongs to a competitor. Which two behaviors triggered UEBA? (Choose two.)

- A. domain belongs to a competitor
- B. log in during non-working hours
- C. email forwarding to an external domain
- D. log in from a first-seen country
- E. increased number of sent mails

Answer: AB

### NEW QUESTION 9

Employees report computer system crashes within the same week. An analyst is investigating one of the computers that crashed and discovers multiple shortcuts in the system's startup folder. It appears that the shortcuts redirect users to malicious URLs. What is the next step the engineer should take to investigate this case?

- A. Remove the shortcut files
- B. Check the audit logs
- C. Identify affected systems
- D. Investigate the malicious URLs

Answer: C

### NEW QUESTION 10

Refer to the exhibit.

<p>URIs:</p> <ul style="list-style-type: none"> <li>• /invoker/JMXInvokerServlet</li> <li>• /CFIDE/adminapi</li> <li>• /?a=&lt;script&gt;alert%28%22XSS%22%29%3B&lt;/script&gt;&amp;b=UNION+SELECT+ALL+FROM+information_schema+AND+%27+or+SLEEP%285%29+or+%27&amp;c=../../../../etc/passwd</li> </ul>
---

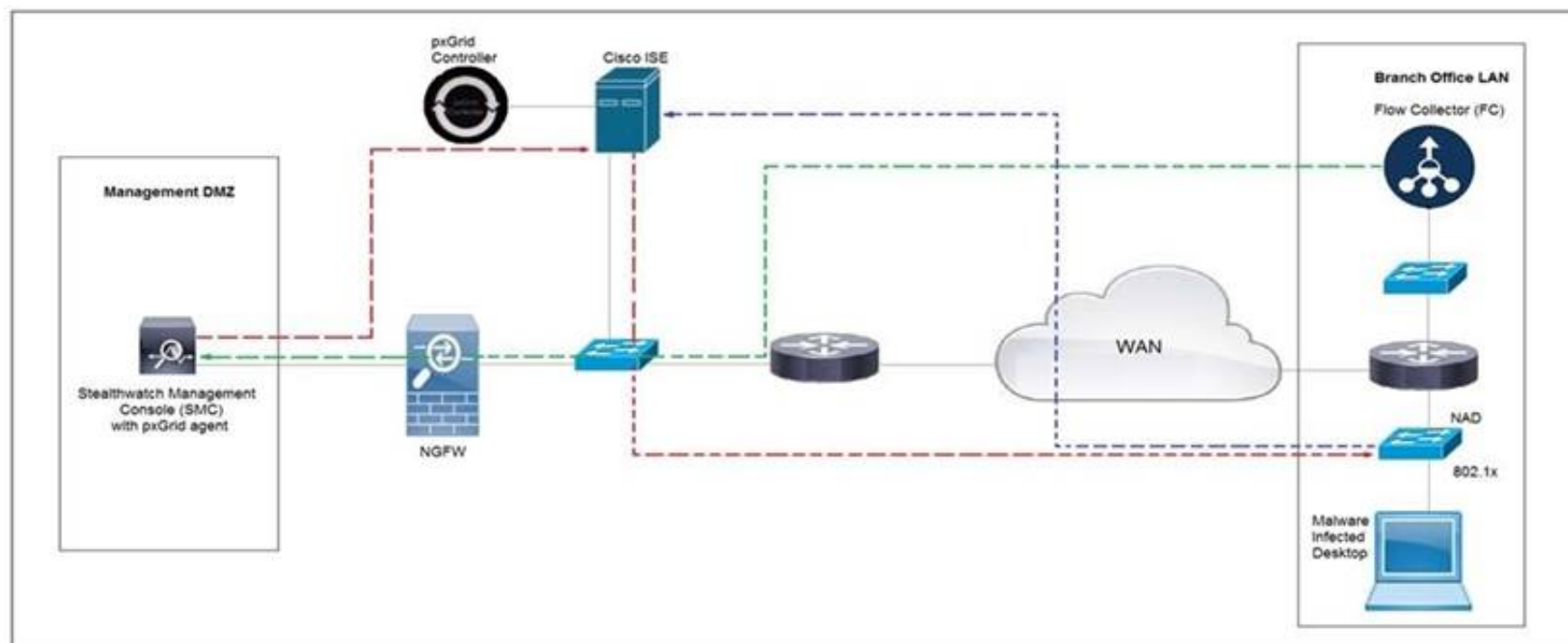
At which stage of the threat kill chain is an attacker, based on these URIs of inbound web requests from known malicious Internet scanners?

- A. exploitation
- B. actions on objectives
- C. delivery
- D. reconnaissance

Answer: C

### NEW QUESTION 10

Refer to the exhibit.



Cisco Rapid Threat Containment using Cisco Secure Network Analytics (Stealthwatch) and ISE detects the threat of malware-infected 802.1x authenticated endpoints and places that endpoint into a Quarantine VLAN using Adaptive Network Control policy. Which telemetry feeds were correlated with SMC to identify the malware?

- A. NetFlow and event data
- B. event data and syslog data
- C. SNMP and syslog data
- D. NetFlow and SNMP

**Answer: B**

#### NEW QUESTION 11

A company recently completed an internal audit and discovered that there is CSRF vulnerability in 20 of its hosted applications. Based on the audit, which recommendation should an engineer make for patching?

- A. Identify the business applications running on the assets
- B. Update software to patch third-party software
- C. Validate CSRF by executing exploits within Metasploit
- D. Fix applications according to the risk scores

**Answer: D**

#### NEW QUESTION 12

What do 2xx HTTP response codes indicate for REST APIs?

- A. additional action must be taken by the client to complete the request
- B. the server takes responsibility for error status codes
- C. communication of transfer protocol-level information
- D. successful acceptance of the client's request

**Answer: D**

#### NEW QUESTION 17

What is a limitation of cyber security risk insurance?

- A. It does not cover the costs to restore stolen identities as a result of a cyber attack
- B. It does not cover the costs to hire forensics experts to analyze the cyber attack
- C. It does not cover the costs of damage done by third parties as a result of a cyber attack
- D. It does not cover the costs to hire a public relations company to help deal with a cyber attack

**Answer: A**

#### NEW QUESTION 21

Refer to the exhibit.



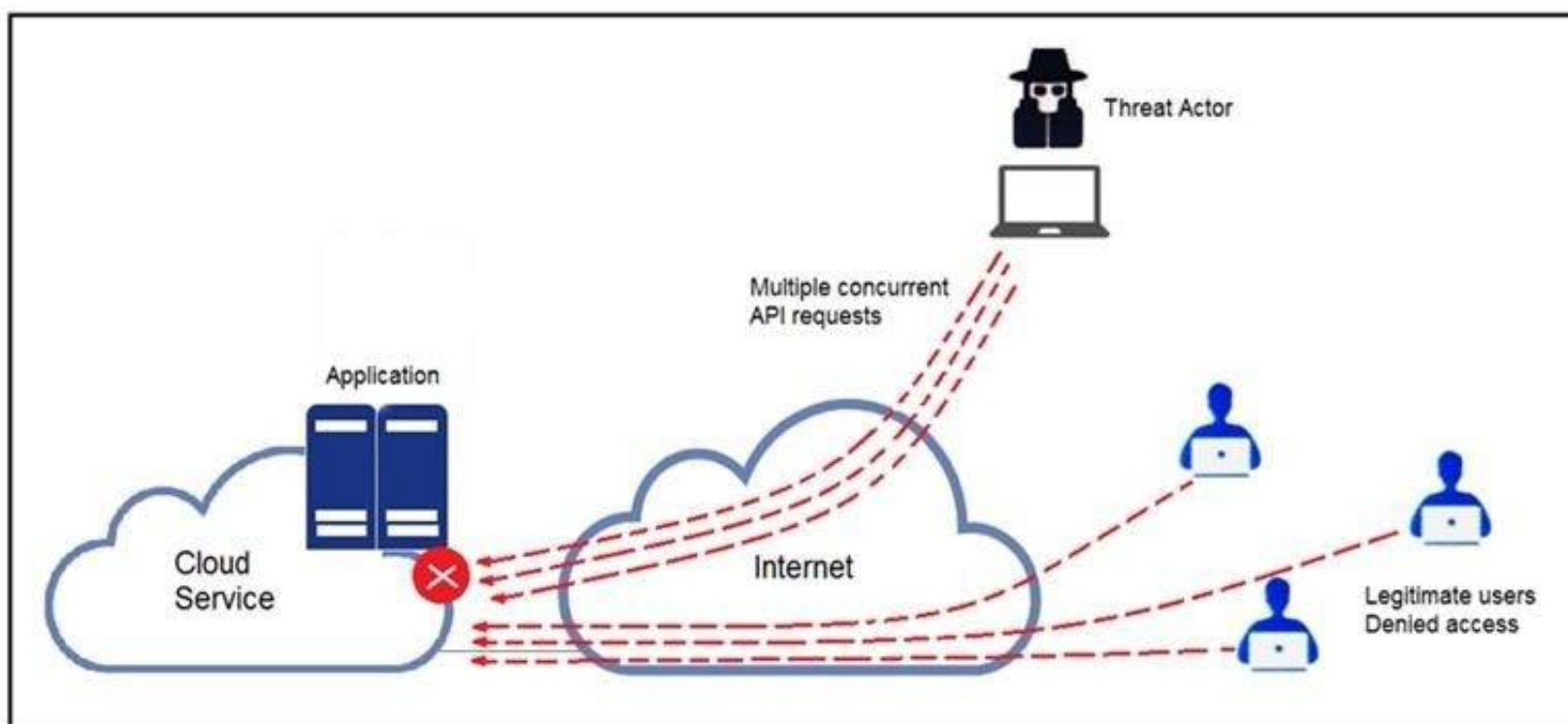
An engineer is investigating a case with suspicious usernames within the active directory. After the engineer investigates and cross-correlates events from other sources, it appears that the 2 users are privileged, and their creation date matches suspicious network traffic that was initiated from the internal network 2 days prior. Which type of compromise is occurring?

- A. compromised insider
- B. compromised root access
- C. compromised database tables
- D. compromised network

Answer: D

#### NEW QUESTION 26

Refer to the exhibit.



A threat actor behind a single computer exploited a cloud-based application by sending multiple concurrent API requests. These requests made the application unresponsive. Which solution protects the application from being overloaded and ensures more equitable application access across the end-user community?

- A. Limit the number of API calls that a single client is allowed to make
- B. Add restrictions on the edge router on how often a single client can access the API
- C. Reduce the amount of data that can be fetched from the total pool of active clients that call the API
- D. Increase the application cache of the total pool of active clients that call the API

Answer: A

#### NEW QUESTION 31

A payroll administrator noticed unexpected changes within a piece of software and reported the incident to the incident response team. Which actions should be taken at this step in the incident response workflow?

- A. Classify the criticality of the information, research the attacker's motives, and identify missing patches
- B. Determine the damage to the business, extract reports, and save evidence according to a chain of custody
- C. Classify the attack vector, understand the scope of the event, and identify the vulnerabilities being exploited
- D. Determine the attack surface, evaluate the risks involved, and communicate the incident according to the escalation plan

Answer: B

#### NEW QUESTION 35



Drag and drop the cloud computing service descriptions from the left onto the cloud service categories on the right.

### Answer Area

triggers a block of code when triggered by a specific event	SaaS
allows renting full servers or virtual machines	PaaS
focuses on developing, testing, and delivering applications	IaaS
allows hosting and managing a virtual environment	FaaS

- A. Mastered  
 B. Not Mastered

Answer: A

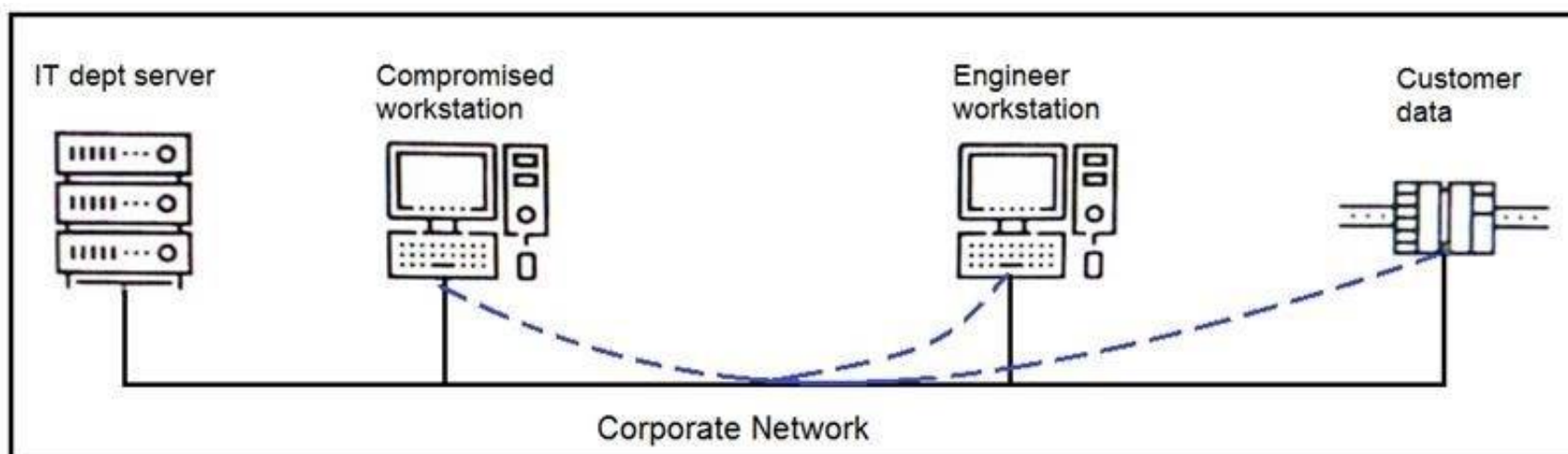
Explanation:

### Answer Area

triggers a block of code when triggered by a specific event	focuses on developing, testing, and delivering applications
allows renting full servers or virtual machines	allows hosting and managing a virtual environment
focuses on developing, testing, and delivering applications	allows renting full servers or virtual machines
allows hosting and managing a virtual environment	triggers a block of code when triggered by a specific event

### NEW QUESTION 39

Refer to the exhibit.



An engineer received a report that an attacker has compromised a workstation and gained access to sensitive customer data from the network using insecure protocols. Which action prevents this type of attack in the future?

- A. Use VLANs to segregate zones and the firewall to allow only required services and secured protocols  
 B. Deploy a SOAR solution and correlate log alerts from customer zones  
 C. Deploy IDS within sensitive areas and continuously update signatures  
 D. Use syslog to gather data from multiple sources and detect intrusion logs for timely responses

Answer: A

### NEW QUESTION 44

An organization lost connectivity to critical servers, and users cannot access business applications and internal websites. An engineer checks the network devices to investigate the outage and determines that all devices are functioning. Drag and drop the steps from the left into the sequence on the right to continue investigating this issue. Not all options are used.

## Answer Area

run show access-list	Step 1
run show config	Step 2
validate the file MD5	Step 3
generate the core file	Step 4
verify the image file hash	
check the memory logs	
verify the memory state	

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

## Answer Area

run show access-list	run show config
run show config	check the memory logs
validate the file MD5	verify the memory state
generate the core file	run show access-list
verify the image file hash	
check the memory logs	
verify the memory state	

### NEW QUESTION 46

What is the HTTP response code when the REST API information requested by the authenticated user cannot be found?

- A. 401B.-402C.403D.404E.405

**Answer:** A

### NEW QUESTION 48

An engineer receives a report that indicates a possible incident of a malicious insider sending company information to outside parties. What is the first action the engineer must take to determine whether an incident has occurred?

- A. Analyze environmental threats and causes  
B. Inform the product security incident response team to investigate further  
C. Analyze the precursors and indicators  
D. Inform the computer security incident response team to investigate further



Answer: C

#### NEW QUESTION 51

An organization had several cyberattacks over the last 6 months and has tasked an engineer with looking for patterns or trends that will help the organization anticipate future attacks and mitigate them. Which data analytic technique should the engineer use to accomplish this task?

- A. diagnostic
- B. qualitative
- C. predictive
- D. statistical

Answer: C

#### NEW QUESTION 53

Refer to the exhibit.

```
pragma: no-cache
server: Apache
status: 200
strict-transport-security: max-age=31536000
vary: Accept-Encoding
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-test-debug: nURL=www.cisco.com, realm=0, isRealm=0, realDomain=0, shortrealm=0
x-xss-protection: 1; mode=block
```

Where are the browser page rendering permissions displayed?

- A. x-frame-options
- B. x-xss-protection
- C. x-content-type-options
- D. x-test-debug

Answer: C

#### NEW QUESTION 55

A company's web server availability was breached by a DDoS attack and was offline for 3 hours because it was not deemed a critical asset in the incident response playbook. Leadership has requested a risk assessment of the asset. An analyst conducted the risk assessment using the threat sources, events, and vulnerabilities. Which additional element is needed to calculate the risk?

- A. assessment scope
- B. event severity and likelihood
- C. incident response playbook
- D. risk model framework

Answer: D

#### NEW QUESTION 57

A SOC analyst is notified by the network monitoring tool that there are unusual types of internal traffic on IP subnet 103.861.2117.0/24. The analyst discovers unexplained encrypted data files on a computer system that belongs on that specific subnet. What is the cause of the issue?

- A. DDoS attack
- B. phishing attack
- C. virus outbreak
- D. malware outbreak

Answer: D

#### NEW QUESTION 58

An API developer is improving an application code to prevent DDoS attacks. The solution needs to accommodate instances of a large number of API requests coming for legitimate purposes from trustworthy services. Which solution should be implemented?

- A. Restrict the number of requests based on a calculation of daily average
- B. If the limit is exceeded, temporarily block access from the IP address and return a 402 HTTP error code.
- C. Implement REST API Security Essentials solution to automatically mitigate limit exhaustio
- D. If the limit is exceeded, temporarily block access from the service and return a 409 HTTP error code.
- E. Increase a limit of replies in a given interval for each AP
- F. If the limit is exceeded, block access from the API key permanently and return a 450 HTTP error code.
- G. Apply a limit to the number of requests in a given time interval for each AP
- H. If the rate is exceeded, block access from the API key temporarily and return a 429 HTTP error code.

Answer: D

#### NEW QUESTION 60

An employee abused PowerShell commands and script interpreters, which lead to an indicator of compromise (IOC) trigger. The IOC event shows that a known malicious file has been executed, and there is an increased likelihood of a breach. Which indicator generated this IOC event?

- A. ExecutedMalware.ioc
- B. Crossrider.ioc
- C. ConnectToSuspiciousDomain.ioc
- D. W32 AccesschkUtility.ioc

Answer: D

NEW QUESTION 63

Refer to the exhibit.

Max (K)	Retain	OverflowAction	Entries	Log
-----	-----	-----	-----	---
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

An employee is a victim of a social engineering phone call and installs remote access software to allow an “MS Support” technician to check his machine for malware. The employee becomes suspicious after the remote technician requests payment in the form of gift cards. The employee has copies of multiple, unencrypted database files, over 400 MB each, on his system and is worried that the scammer copied the files off but has no proof of it. The remote technician was connected sometime between 2:00 pm and 3:00 pm over https. What should be determined regarding data loss between the employee’s laptop and the remote technician’s system?

- A. No database files were disclosed
- B. The database files were disclosed
- C. The database files integrity was violated
- D. The database files were intentionally corrupted, and encryption is possible

Answer: C

NEW QUESTION 67

Drag and drop the function on the left onto the mechanism on the right.

Answer Area

creates the set of executable tasks

minimizes redundancies and steamlines repetitive tasks

organizes components to seamlessly run applications

systematically executes large workflows

Orchestration

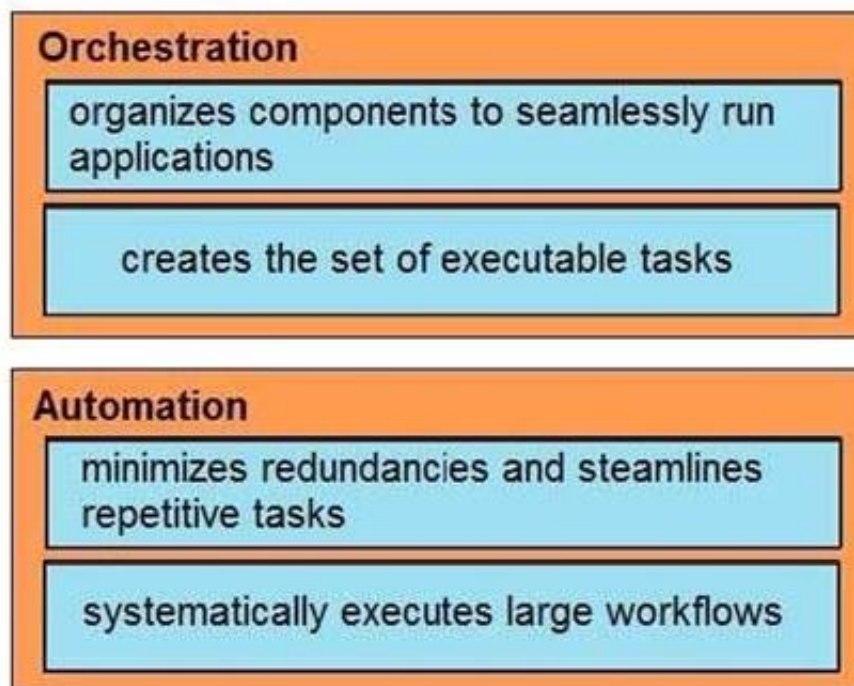
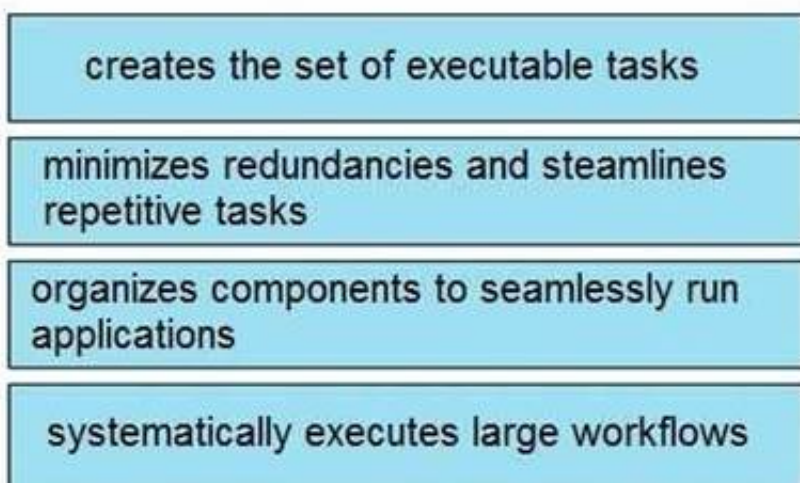
Automation

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Answer Area



### NEW QUESTION 68

Refer to the exhibit.

```

try
{
    using (MemoryStream memoryStream = new MemoryStream())
    {
        memoryStream.Position = 32L;
        using (AesCryptoServiceProvider aesCryptoServiceProvider = new AesCryptoServiceProvider())
        {
            aesCryptoServiceProvider.KeySize = 128;
            aesCryptoServiceProvider.BlockSize = 128;
            aesCryptoServiceProvider.Mode = CipherMode.CBC;
            aesCryptoServiceProvider.Padding = PaddingMode.PKCS7;
            aesCryptoServiceProvider.Key = key;
            aesCryptoServiceProvider.GenerateIV();
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, aesCryptoServiceProvider.CreateEncryptor(), CryptoStreamMode.Write))
            {
                memoryStream.Write(aesCryptoServiceProvider.IV, 0, aesCryptoServiceProvider.IV.Length);
                cryptoStream.Write(input, 0, input.Length);
                cryptoStream.FlushFinalBlock();
                using (HMACSHA256 hMACSHA = new HMACSHA256(bytes))
                {
                    byte[] array = hMACSHA.ComputeHash(memoryStream.ToArray(), 32, memoryStream.ToArray().Length - 32);
                    memoryStream.Position = 0L;
                    memoryStream.Write(array, 0, array.Length);
                }
            }
        }
        result = memoryStream.ToArray();
    }
}
catch
{
}
  
```

An engineer is performing a static analysis on a malware and knows that it is capturing keys and webcam events on a company server. What is the indicator of compromise?

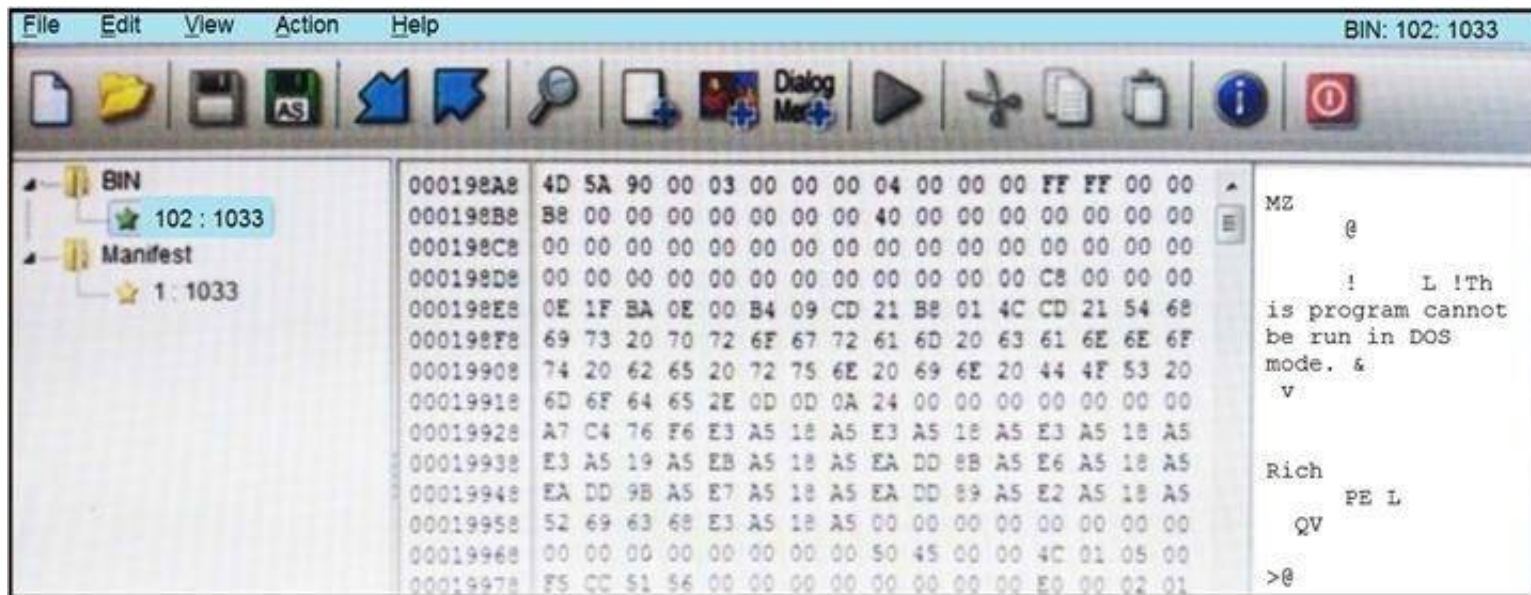
- A. The malware is performing comprehensive fingerprinting of the host, including a processor, motherboard manufacturer, and connected removable storage.
- B. The malware is a ransomware querying for installed anti-virus products and operating systems to encrypt and render unreadable until payment is made for file decryption.
- C. The malware has moved to harvesting cookies and stored account information from major browsers and configuring a reverse proxy for intercepting network activity.
- D. The malware contains an encryption and decryption routine to hide URLs/IP addresses and is storing the output of loggers and webcam captures in locally encrypted files for retrieval.

Answer: B

### NEW QUESTION 69

Refer to the exhibit.





An engineer is reverse engineering a suspicious file by examining its resources. What does this file indicate?

- A. a DOS MZ executable format
- B. a MS-DOS executable archive
- C. an archived malware
- D. a Windows executable file

Answer: D

#### NEW QUESTION 72

What is a benefit of key risk indicators?

- A. clear perspective into the risk position of an organization
- B. improved visibility on quantifiable information
- C. improved mitigation techniques for unknown threats
- D. clear procedures and processes for organizational risk

Answer: C

#### NEW QUESTION 76

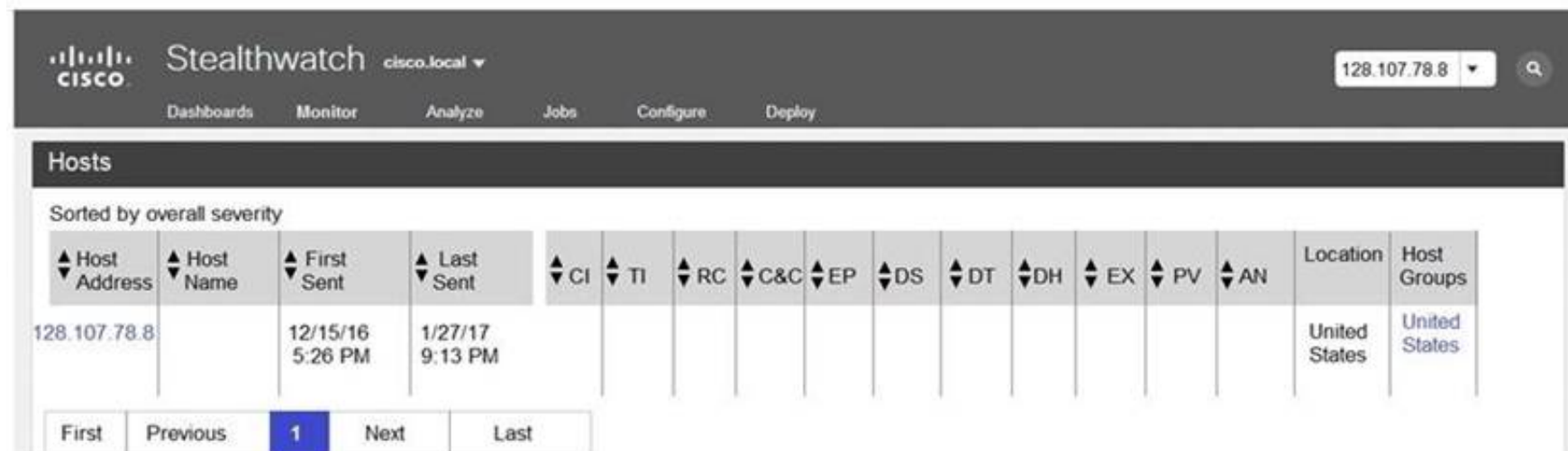
A company launched an e-commerce website with multiple points of sale through internal and external e- stores. Customers access the stores from the public website, and employees access the stores from the intranet with an SSO. Which action is needed to comply with PCI standards for hardening the systems?

- A. Mask PAN numbers
- B. Encrypt personal data
- C. Encrypt access
- D. Mask sales details

Answer: B

#### NEW QUESTION 77

Refer to the exhibit.



The Cisco Secure Network Analytics (Stealthwatch) console alerted with “New Malware Server Discovered” and the IOC indicates communication from an end-user desktop to a Zeus C&C Server. Drag and drop the actions that the analyst should take from the left into the order on the right to investigate and remediate this IOC.

Answer Area

Execute rapid threat containment

Investigate and classify the exposure

Investigate infected hosts

Search for infected hosts

Examine returned results

Step 1

Step 2

Step 3

Step 4

Step 5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Execute rapid threat containment

Investigate and classify the exposure

Investigate infected hosts

Search for infected hosts

Examine returned results

Search for infected hosts

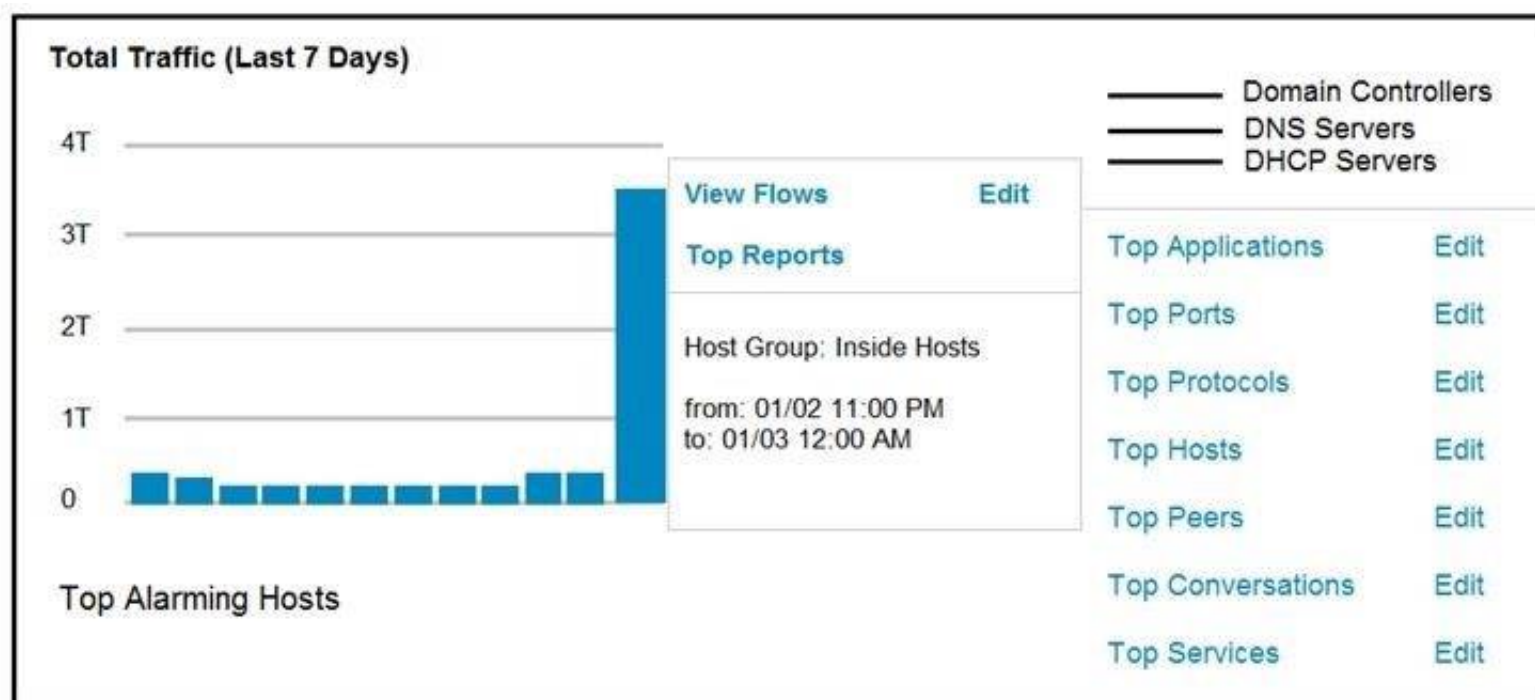
Investigate infected hosts

Investigate and classify the exposure

Examine returned results

Execute rapid threat containment

NEW QUESTION 80  
Refer to the exhibit.



An engineer notices a significant anomaly in the traffic in one of the host groups in Cisco Secure Network Analytics (Stealthwatch) and must analyze the top data transmissions. Which tool accomplishes this task?

- A. Top Peers
- B. Top Hosts
- C. Top Conversations
- D. Top Ports

Answer: B

#### NEW QUESTION 82

Where do threat intelligence tools search for data to identify potential malicious IP addresses, domain names, and URLs?

- A. customer data
- B. internal database
- C. internal cloud
- D. Internet

Answer: D

#### NEW QUESTION 85

An engineer is analyzing a possible compromise that happened a week ago when the company ? (Choose two.)

- A. firewall
- B. Wireshark
- C. autopsy
- D. SHA512
- E. IPS

Answer: AB

#### NEW QUESTION 89

Drag and drop the components from the left onto the phases of the CI/CD pipeline on the right.

##### Answer Area

- build
- release
- deploy
- operate
- monitor
- test
- plan
- develop

- Phase 1
- Phase 2
- Phase 3
- Phase 4
- Phase 5
- Phase 6
- Phase 7
- Phase 8



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

#### Answer Area

build	plan
release	develop
deploy	build
operate	test
monitor	release
test	deploy
plan	operate
develop	monitor

#### NEW QUESTION 92

Refer to the exhibit.

TCP	192.168.1.8:54580	vk-in-f108:imaps	ESTABLISHED
TCP	192.168.1.8:54583	132.245.61.50:https	ESTABLISHED
TCP	192.168.1.8:54916	bay405-m:https	ESTABLISHED
TCP	192.168.1.8:54978	vu-in-f188:5228	ESTABLISHED
TCP	192.168.1.8:55094	72.21.194.109:https	ESTABLISHED
TCP	192.168.1.8:55401	wonderhowto:http	ESTABLISHED
TCP	192.168.1.8:55730	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55824	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55825	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55846	mia07s25-in-f14:https	TIME_WAIT
TCP	192.168.1.8:55847	a184-51-150-89:http	CLOSE_WAIT
TCP	192.168.1.8:55853	157.55.56.154:40028	ESTABLISHED
TCP	192.168.1.8:55879	atl14s38-in-f4:https	ESTABLISHED
TCP	192.168.1.8:55884	208-46-117-174:https	ESTABLISHED
TCP	192.168.1.8:55893	vx-in-f95:https	TIME_WAIT
TCP	192.168.1.8:55947	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55966	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55970	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55972	191.238.241.80:https	TIME_WAIT
TCP	192.168.1.8:55976	54.239.26.242:https	ESTABLISHED
TCP	192.168.1.8:55979	mia07s35-in-f14:https	ESTABLISHED
TCP	192.168.1.8:55986	server11:https	TIME_WAIT
TCP	192.168.1.8:55988	104.16.118.182:http	ESTABLISHED

A security analyst needs to investigate a security incident involving several suspicious connections with a possible attacker. Which tool should the analyst use to identify the source IP of the offender?

- A. packet sniffer
- B. malware analysis
- C. SIEM
- D. firewall manager

**Answer:** A

#### NEW QUESTION 94

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
2389	848.622259	10.31.133.235	10.25.129.5	TCP	66	61118 → 80 [SYN] Seq=0 Win=8192
2389	848.622273	10.25.129.5	10.31.133.235	TCP	66	80 → 61118 [SYN, ACK] Seq=0 Acc=1
2389	848.622351	10.31.133.235	10.25.129.5	TCP	60	30745 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.622719	10.31.133.235	10.25.129.5	TCP	60	30746 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.622889	10.31.133.235	10.25.129.5	TCP	60	30748 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.623250	10.31.133.235	10.25.129.5	TCP	60	30747 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.623545	10.31.133.235	10.25.129.5	TCP	60	30749 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.623882	10.31.133.235	10.25.129.5	TCP	60	30750 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.624295	10.31.133.235	10.25.129.5	TCP	60	30751 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.624880	10.31.133.235	10.25.129.5	TCP	60	30752 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.625424	10.31.133.235	10.25.129.5	TCP	60	30753 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.625729	10.31.133.235	10.25.129.5	TCP	60	30754 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.626842	10.31.133.235	10.25.129.5	TCP	60	30755 → 80 [RST] Seq=1 Win=0 Len=0
2389	848.627352	10.31.133.235	10.25.129.5	TCP	60	30756 → 80 [RST] Seq=1 Win=0 Len=0

What is occurring in this packet capture?

- A. TCP port scan
- B. TCP flood
- C. DNS flood
- D. DNS tunneling

Answer: B

#### NEW QUESTION 98

A threat actor attacked an organization's Active Directory server from a remote location, and in a thirty-minute timeframe, stole the password for the administrator account and attempted to access 3 company servers. The threat actor successfully accessed the first server that contained sales data, but no files were downloaded. A second server was also accessed that contained marketing information and 11 files were downloaded. When the threat actor accessed the third server that contained corporate financial data, the session was disconnected, and the administrator's account was disabled. Which activity triggered the behavior analytics tool?

- A. accessing the Active Directory server
- B. accessing the server with financial data
- C. accessing multiple servers
- D. downloading more than 10 files

Answer: C

#### NEW QUESTION 99

A security expert is investigating a breach that resulted in a \$32 million loss from customer accounts. Hackers were able to steal API keys and two-factor codes due to a vulnerability that was introduced in a new code a few weeks before the attack. Which step was missed that would have prevented this breach?

- A. use of the Nmap tool to identify the vulnerability when the new code was deployed
- B. implementation of a firewall and intrusion detection system
- C. implementation of an endpoint protection system
- D. use of SecDevOps to detect the vulnerability during development

Answer: D

#### NEW QUESTION 104

An engineer wants to review the packet overviews of SNORT alerts. When printing the SNORT alerts, all the packet headers are included, and the file is too large to utilize. Which action is needed to correct this problem?

- A. Modify the alert rule to "output alert\_syslog: output log"
- B. Modify the output module rule to "output alert\_quick: output filename"
- C. Modify the alert rule to "output alert\_syslog: output header"
- D. Modify the output module rule to "output alert\_fast: output filename"

Answer: A

#### NEW QUESTION 108

A SOC team is informed that a UK-based user will be traveling between three countries over the next 60 days. Having the names of the 3 destination countries and the user's working hours, what must the analyst do next to detect an abnormal behavior?

- A. Create a rule triggered by 3 failed VPN connection attempts in an 8-hour period
- B. Create a rule triggered by 1 successful VPN connection from any nondestination country
- C. Create a rule triggered by multiple successful VPN connections from the destination countries
- D. Analyze the logs from all countries related to this user during the traveling period

Answer: D

#### NEW QUESTION 111

Refer to the exhibit.

Asset	Threat	Vulnerability	Likelihood (1-10)	Impact (1-10)
Servers	Natural Disasters – Flooding	Server Room is on the zero floor	3	10
Secretary Workstation	Usage of illegitimate software	Inadequate control of software	7	6
Payment Process	Eavesdropping, Misrouting/re-routing of messages	Unencrypted communications	5	10
Website	Website Intrusion	No IDS/IPS usage	6	8

Which asset has the highest risk value?

- A. servers
- B. website
- C. payment process
- D. secretary workstation

**Answer:** C

**NEW QUESTION 112**

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 350-201 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 350-201 Product From:

<https://www.2passeasy.com/dumps/350-201/>

## Money Back Guarantee

### 350-201 Practice Exam Features:

- \* 350-201 Questions and Answers Updated Frequently
- \* 350-201 Practice Questions Verified by Expert Senior Certified Staff
- \* 350-201 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 350-201 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year