

Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)

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



NEW QUESTION 1

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 2

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 3

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 4

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 5

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.2	10.128.0.2	TCP	54	3341 -> 80 [SYN] Seq=0 Win=512 Len=0
2	0.003987	10.128.0.2	10.0.0.2	TCP	58	80 -> 3222 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
3	0.005514	10.128.0.2	10.0.0.2	TCP	54	80 -> 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
4	0.008429	10.0.0.2	10.128.0.2	TCP	54	3342 -> 80 [SYN] Seq=0 Win=512 Len=0
5	0.010233	10.128.0.2	10.0.0.2	TCP	58	80 -> 3220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
6	0.014072	10.128.0.2	10.0.0.2	TCP	58	80 -> 3342 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
7	0.016830	10.0.0.2	10.128.0.2	TCP	54	3343 -> 80 [SYN] Seq=0 Win=512 Len=0
8	0.022220	10.128.0.2	10.0.0.2	TCP	58	80 -> 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
9	0.023496	10.128.0.2	10.0.0.2	TCP	58	80 -> 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
10	0.025243	10.0.0.2	10.128.0.2	TCP	58	3344 -> 80 [SYN] Seq=0 Win=512 Len=0
11	0.026672	10.128.0.2	10.0.0.2	TCP	58	80 -> 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
12	0.028038	10.128.0.2	10.0.0.2	TCP	58	80 -> 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
13	0.030523	10.128.0.2	10.0.0.2	TCP	58	80 -> 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

Frame 1 : 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)
Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.128.0.2
Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0
Source port: 3341
Destination port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 1023350804
0101 = Header Length: 20 bytes (5)
Flags: 0x002 (SYN)
Window size value: 512
[Calculated window size: 512]
Checksum: 0x8d5a [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[Timestamps]

What is the threat in this Wireshark traffic capture?

- A. A high rate of SYN packets being sent from multiple sources toward a single destination IP
- B. A flood of ACK packets coming from a single source IP to multiple destination IPs
- C. A high rate of SYN packets being sent from a single source IP toward multiple destination IPs
- D. A flood of SYN packets coming from a single source IP to a single destination IP

Answer: D

NEW QUESTION 6

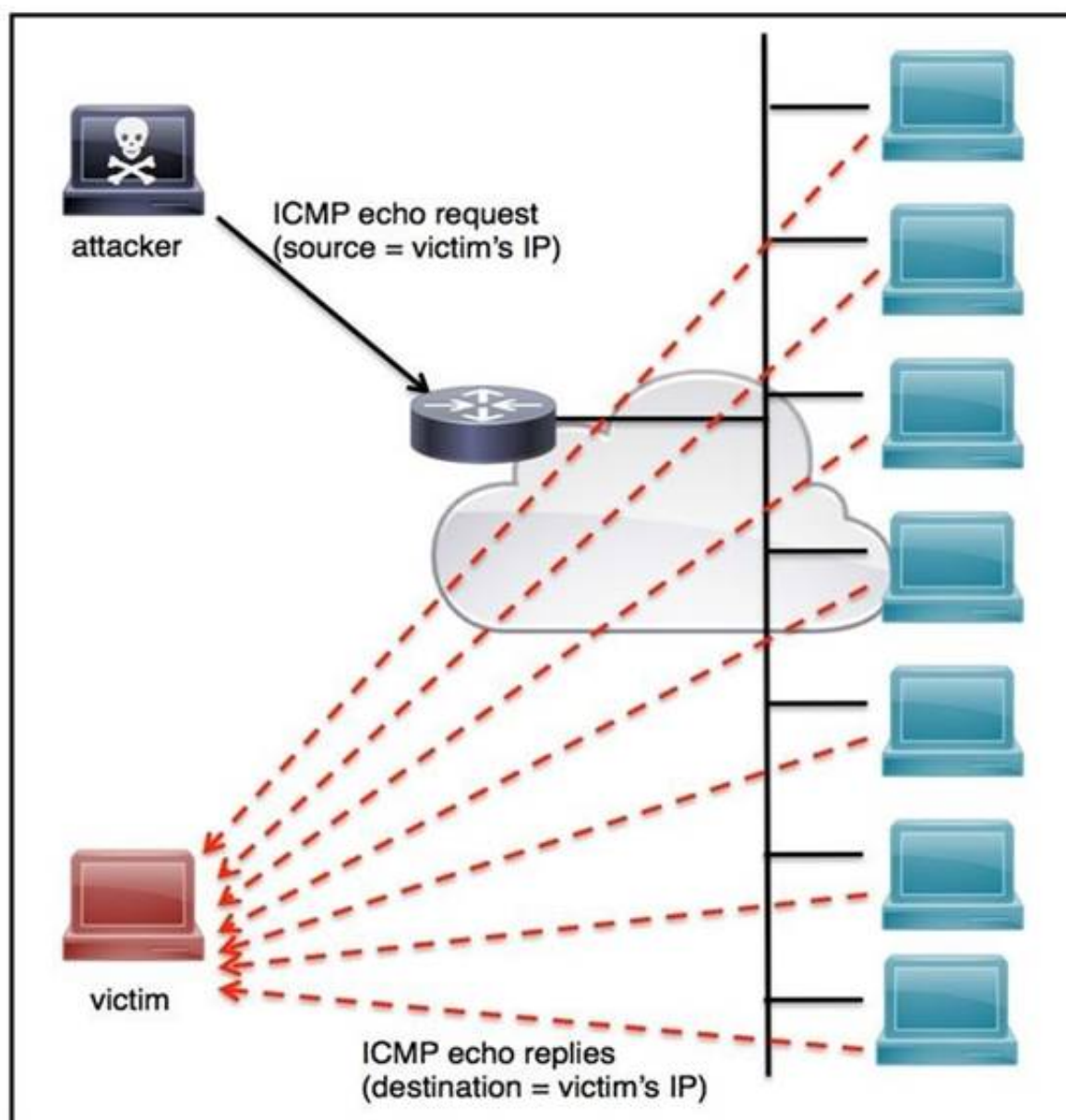
An engineer is investigating several cases of increased incoming spam emails and suspicious emails from the HR and service departments. While checking the event sources, the website monitoring tool showed several web scraping alerts overnight. Which type of compromise is indicated?

- A. phishing
- B. dumpster diving
- C. social engineering
- D. privilege escalation

Answer: C

NEW QUESTION 7

Refer to the exhibit.



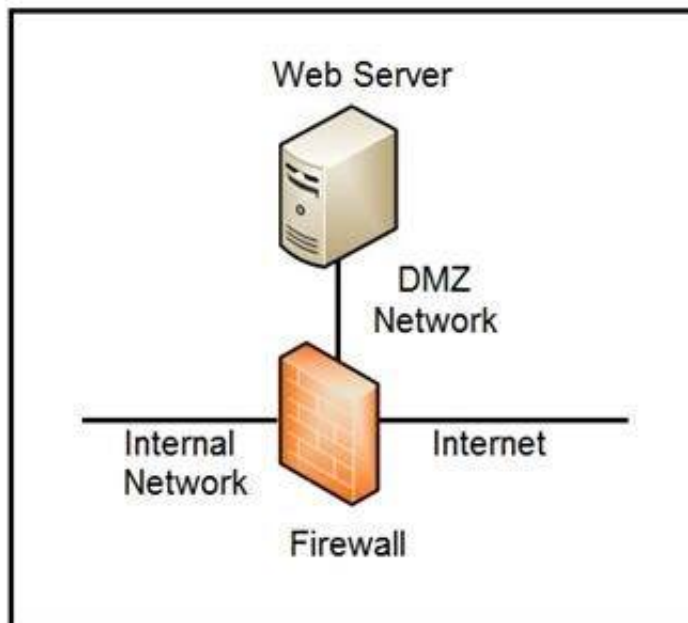
An engineer must tune the Cisco IOS device to mitigate an attack that is broadcasting a large number of ICMP packets. The attack is sending the victim's spoofed source IP to a network using an IP broadcast address that causes devices in the network to respond back to the source IP address. Which action does the engineer recommend?

- A. Use command `ip verify reverse-path interface`
- B. Use global configuration command `service tcp-keepalives-out`
- C. Use subinterface command `no ip directed-broadcast`
- D. Use logging trap 6

Answer: A

NEW QUESTION 8

Refer to the exhibit.



Which two steps mitigate attacks on the webserver from the Internet? (Choose two.)

- A. Create an ACL on the firewall to allow only TLS 1.3
- B. Implement a proxy server in the DMZ network
- C. Create an ACL on the firewall to allow only external connections
- D. Move the webserver to the internal network

Answer: BD

NEW QUESTION 9

Refer to the exhibit.

URIs:

- /invoker/JMXInvokerServlet
- /CFIDE/adminapi
- /?a=<script>alert%28%22XSS%22%29%3B</script>&b=UNION+SELECT+ALL+FROM+information_schema+AND+%27+or+SLEEP%285%29+or+%27&c=../../../../etc/passwd

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

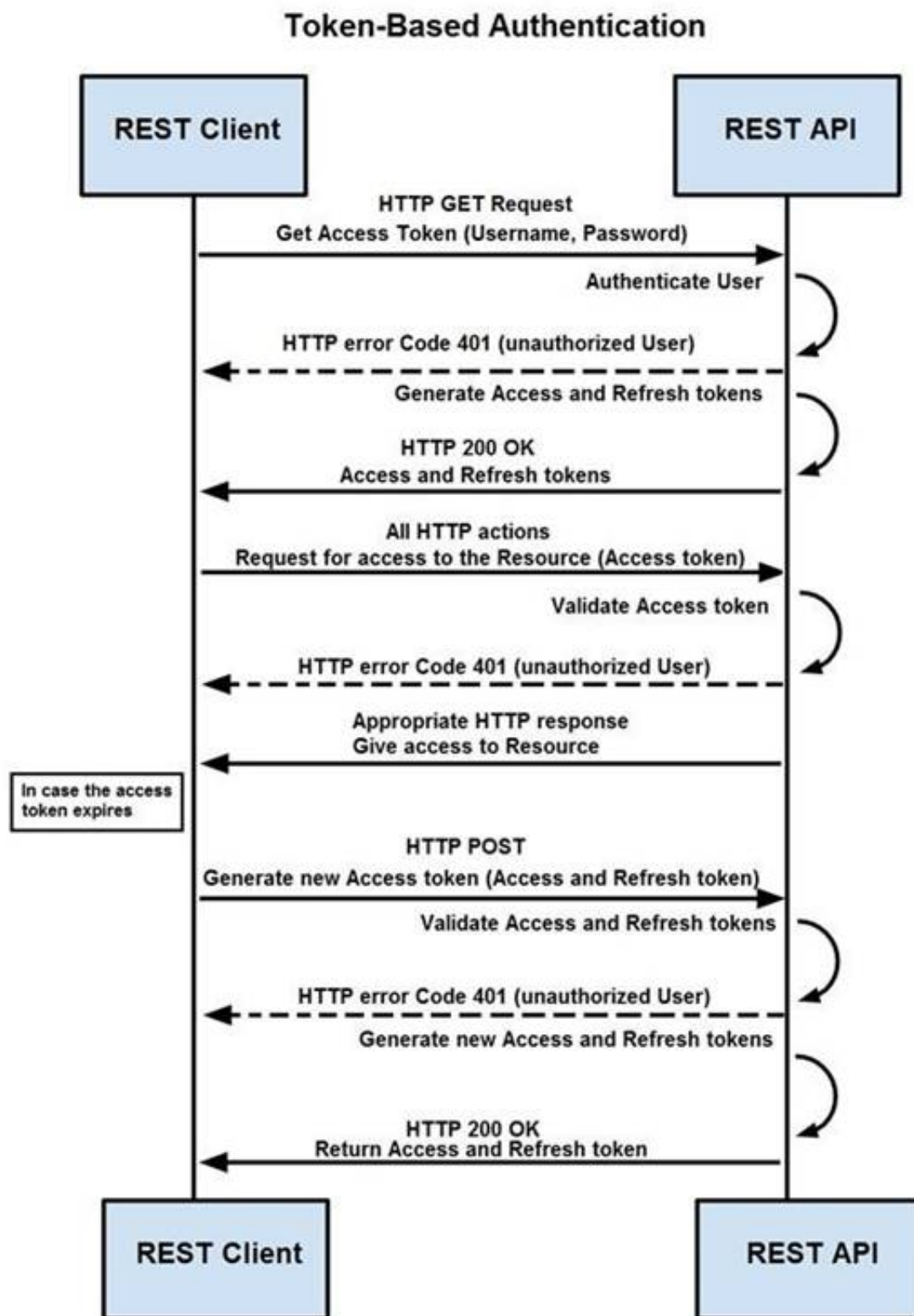
How does Wireshark decrypt TLS network traffic?

- A. with a key log file using per-session secrets
- B. using an RSA public key
- C. by observing DH key exchange
- D. by defining a user-specified decode-as

Answer: A

NEW QUESTION 10

Refer to the exhibit.



How are tokens authenticated when the REST API on a device is accessed from a REST API client?

- A. The token is obtained by providing a password
- B. The REST client requests access to a resource using the access token
- C. The REST API validates the access token and gives access to the resource.
- D. The token is obtained by providing a password
- E. The REST API requests access to a resource using the access token, validates the access token, and gives access to the resource.
- F. The token is obtained before providing a password
- G. The REST API provides resource access, refreshes tokens, and returns them to the REST client
- H. The REST client requests access to a resource using the access token.
- I. The token is obtained before providing a password
- J. The REST client provides access to a resource using the access token
- K. The REST API encrypts the access token and gives access to the resource.

Answer: D

NEW QUESTION 11

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 13

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 17

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 22

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 25

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 29

An engineer is developing an application that requires frequent updates to close feedback loops and enable teams to quickly apply patches. The team wants their code updates to get to market as often as possible. Which software development approach should be used to accomplish these goals?

A. continuous delivery
B. continuous integration
C. continuous deployment
D. continuous monitoring

Answer: A

NEW QUESTION 32

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 35

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 38

Drag and drop the type of attacks from the left onto the cyber kill chain stages at which the attacks are seen on the right.

Answer Area

not visible to the victim
virus scanner turning off
malware placed on the targeted system
open port scans and multiple failed logins from the website
large amount of data leaving the network through unusual ports
system phones connecting to countries where no staff are located
USB with infected files inserted into company laptop

reconnaissance
weaponization
delivery
exploitation
installation
command & control
actions on objectives

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

not visible to the victim
virus scanner turning off
malware placed on the targeted system
open port scans and multiple failed logins from the website
large amount of data leaving the network through unusual ports
system phones connecting to countries where no staff are located
USB with infected files inserted into company laptop

system phones connecting to countries where no staff are located
malware placed on the targeted system
not visible to the victim
large amount of data leaving the network through unusual ports
USB with infected files inserted into company laptop
virus scanner turning off
open port scans and multiple failed logins from the website

NEW QUESTION 42

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 47

.....

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