350-201 Dumps

Performing CyberOps Using Core Security Technologies (CBRCOR)

https://www.certleader.com/350-201-dumps.html

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
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

The incident response team was notified of detected malware. The team identified the infected hosts, removed the malware, restored the functionality and data of infected systems, and planned a company meeting to improve the incident handling capability. Which step was missed according to the NIST incident handling guide?

A. Contain the malware
B. Install IPS software
C. Determine the escalation path
D. Perform vulnerability assessment

Answer: D

NEW QUESTION 8

Refer to the exhibit.

```
{
    "type": "bundle",
    "id": "bundle--56be2a39",
    "objects": [
        {
            "type": "indicator",
            "spec_version": "2.1",
            "id": "indicator--d81f86b9-9f",
            "created": "2020-08-10T13:49:37.079Z",
            "modified": "2020-08-10T13:49:37.079Z",
            "name": "Malicious site hosting downloader",
            "indicator_types":[
                "malicious-activity"
            ],
            "pattern": "[url:value = 'http://y2z7atc.cn/4823/']",
            "pattern_type": "stix",
            "valid_from": "2020-08-10T13:49:37.079Z"
        },
        {
            "type": "malware",
            "spec_version": "2.1",
            "id": "malware- -162d9 a",
            "created": "2020-08-13T09:15:17.182Z",
            "modified": "2020-08-13T09:15:17.182Z",
            "name": "y2z7atc backdoor",
            "malware_types": [
                "backdoor",
                "remote-access-trojan"
            ],
            "is_family": false,
            "kil_chain_phases": [
                {
                    "kill_chain_name": "mandant-attack-lifecycle-model",
                    "phase_name": "establish-foothold"
                }
            ]
        },
        {
            "type": "relationship",
            "spec_version": "2.1",
            "id": "relationship--864af2e5",
            "created": "2020-08-15T18:03:58.029Z",
            "modified": "2020-08-15T18:03:58.029Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4",
            "target_ref": "malware--162d917e07661-4611-b5d6-652791454fca"
        }
    ]
}
```

Which indicator of compromise is represented by this STIX?

A. website redirecting traffic to ransomware server
B. website hosting malware to download files
C. web server vulnerability exploited by malware
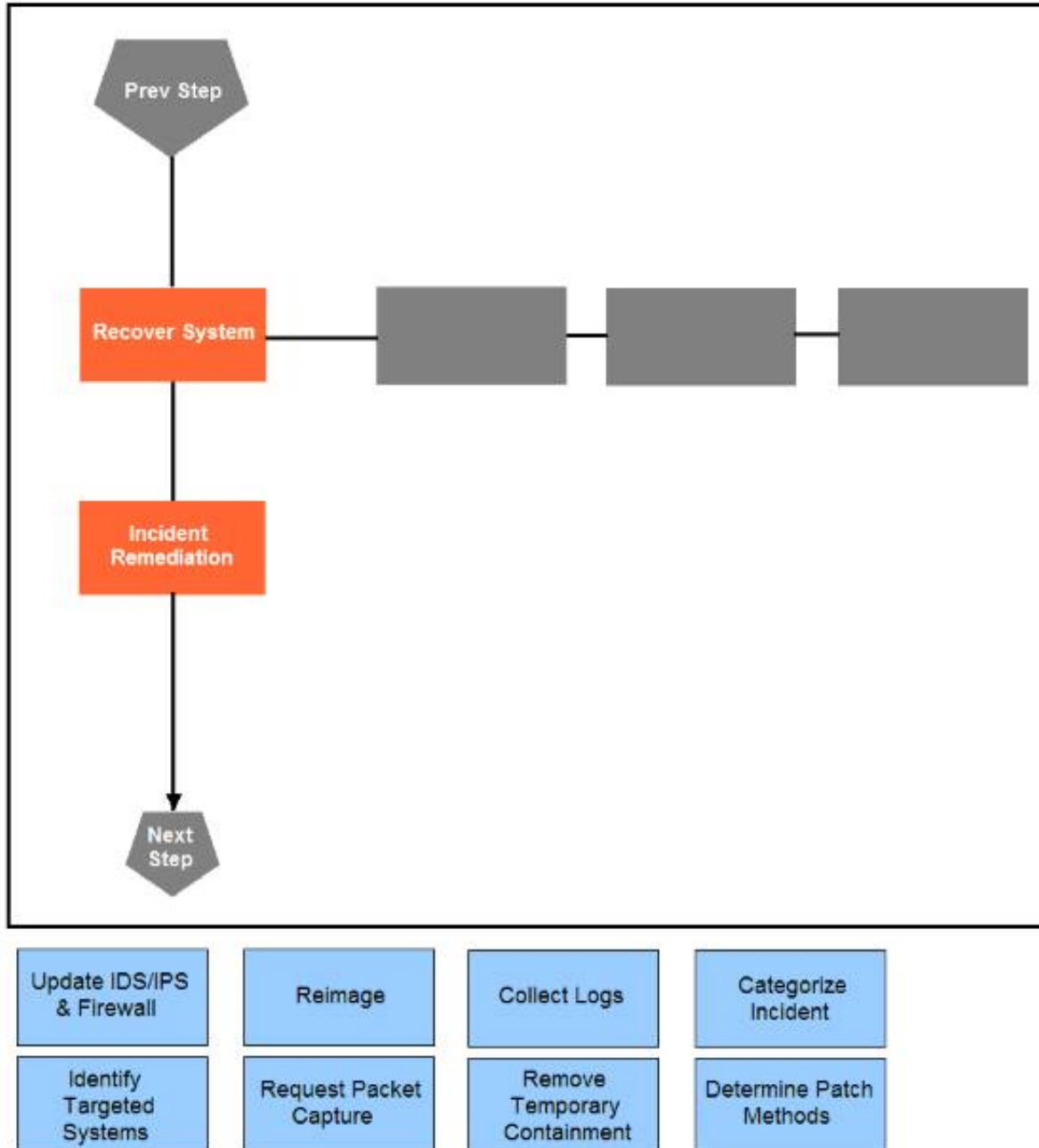D. cross-site scripting vulnerability to backdoor server

Answer: C

NEW QUESTION 9
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
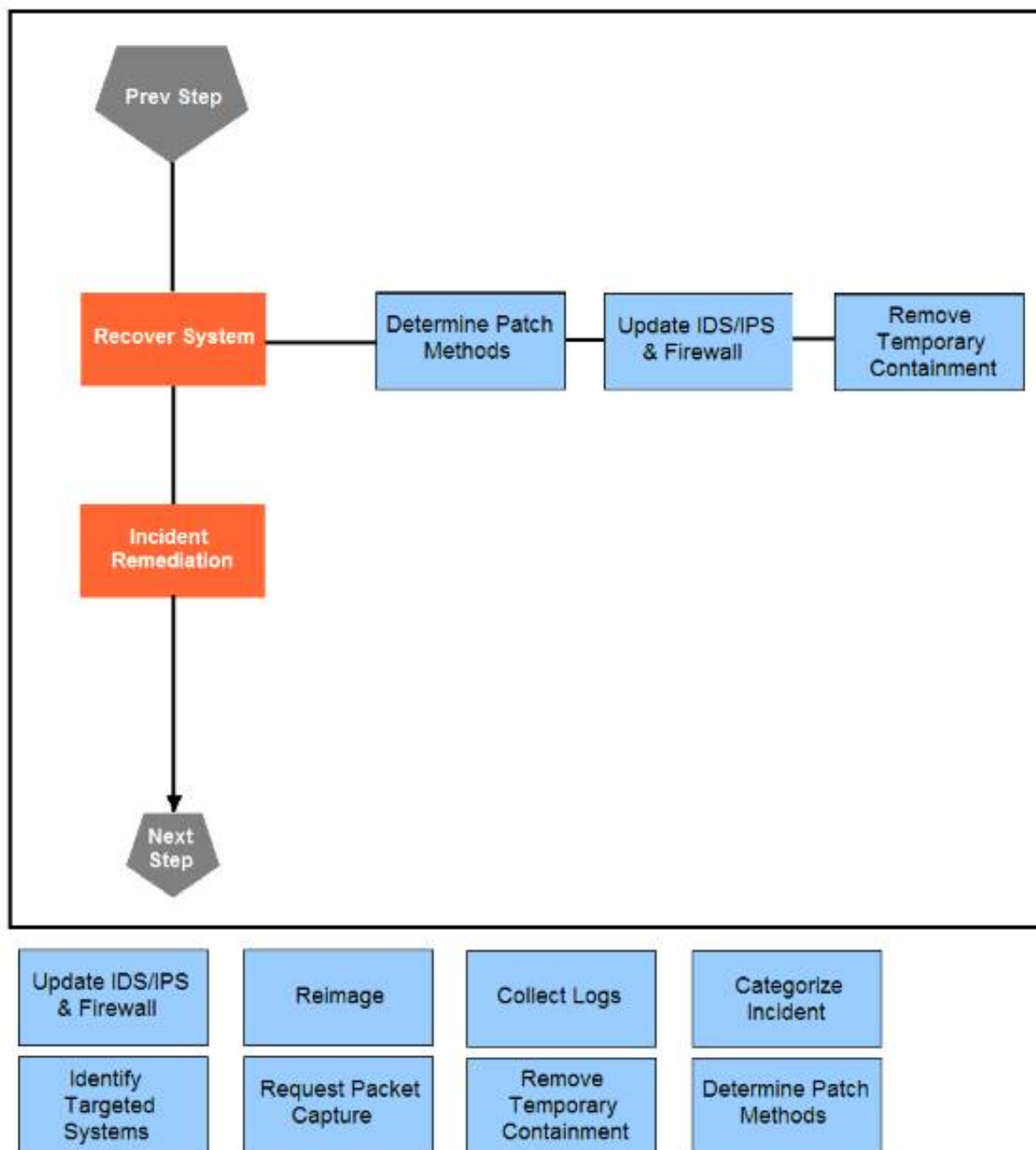
Answer: A

NEW QUESTION 10
Drag and drop the actions below the image onto the boxes in the image for the actions that should be taken during this playbook step. Not all options are used.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 10

A security architect is working in a processing center and must implement a DLP solution to detect and prevent any type of copy and paste attempts of sensitive data within unapproved applications and removable devices. Which technical architecture must be used?

A. DLP for data in motion
B. DLP for removable data
C. DLP for data in use
D. DLP for data at rest

Answer: C

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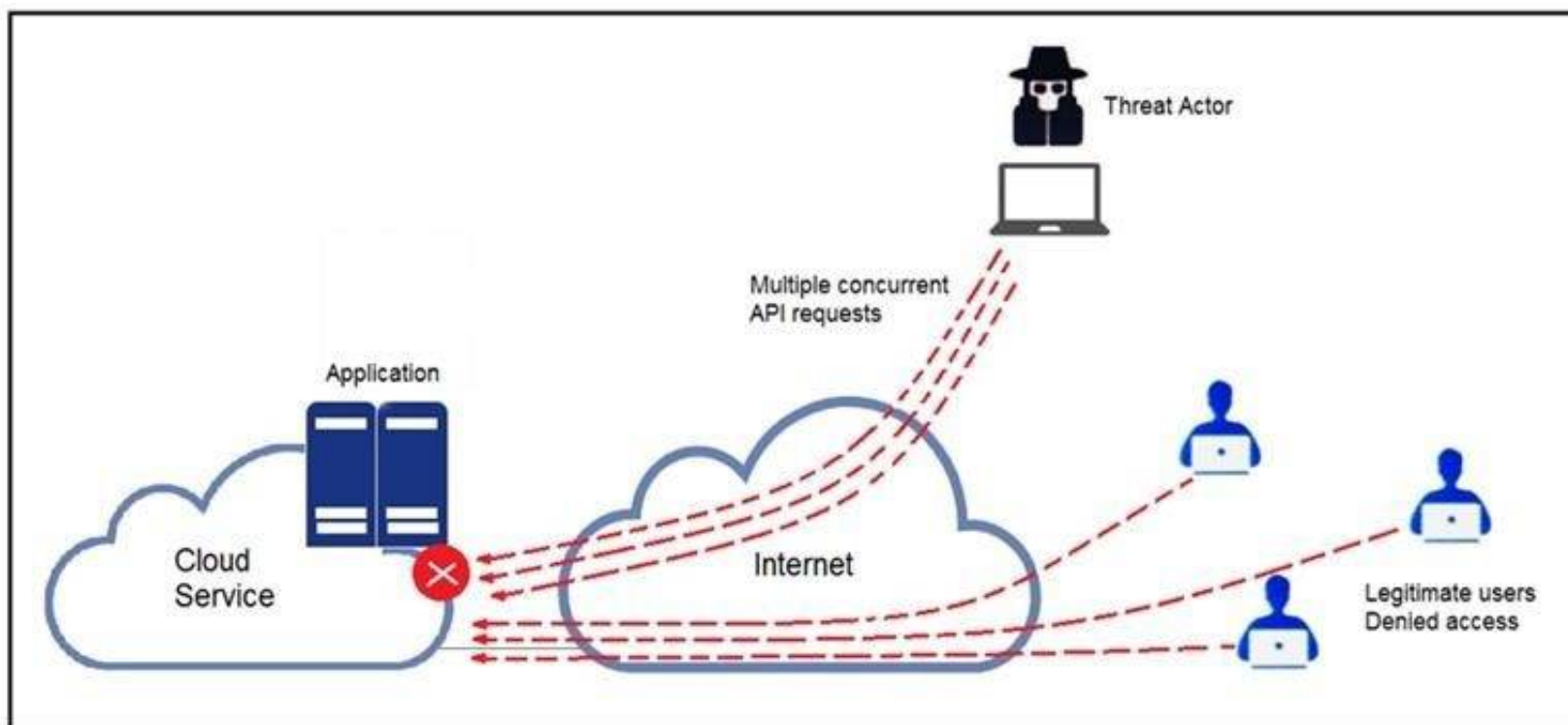
A. Identify the business applications running on the assets
B. Update software to patch third-party software
C. Validate CSRF by executing exploits within Metasploit
D. Fix applications according to the risk scores

Answer: D

NEW QUESTION 14
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 18
An engineer has created a bash script to automate a complicated process. During script execution, this error occurs: permission denied. Which command must be added to execute this script?

A. chmod +x ex.sh
B. source ex.sh
C. chroot ex.sh
D. sh ex.sh

Answer: A

NEW QUESTION 21
What is the purpose of hardening systems?

A. to securely configure machines to limit the attack surface
B. to create the logic that triggers alerts when anomalies occur
C. to identify vulnerabilities within an operating system
D. to analyze attacks to identify threat actors and points of entry

Answer: A

NEW QUESTION 24
A security analyst receives an escalation regarding an unidentified connection on the Accounting A1 server within a monitored zone. The analyst pulls the logs and discovers that a Powershell process and a WMI tool process were started on the server after the connection was established and that a PE format file was created in the system directory. What is the next step the analyst should take?

A. Isolate the server and perform forensic analysis of the file to determine the type and vector of a possible attack
B. Identify the server owner through the CMDB and contact the owner to determine if these were planned and identifiable activities
C. Review the server backup and identify server content and data criticality to assess the intrusion risk
D. Perform behavioral analysis of the processes on an isolated workstation and perform cleaning procedures if the file is malicious

Answer: C

NEW QUESTION 25
An organization installed a new application server for IP phones. An automated process fetched user credentials from the Active Directory server, and the application will have access to on-premises and cloud services. Which security threat should be mitigated first?

A. aligning access control policies
B. exfiltration during data transfer
C. attack using default accounts
D. data exposure from backups

Answer: B

NEW QUESTION 29
A new malware variant is discovered hidden in pirated software that is distributed on the Internet. Executives have asked for an organizational risk assessment.

The security officer is given a list of all assets. According to NIST, which two elements are missing to calculate the risk assessment? (Choose two.)

A. incident response playbooks
B. asset vulnerability assessment
C. report of staff members with asset relations
D. key assets and executives
E. malware analysis report

Answer: BE

NEW QUESTION 31
An engineer is utilizing interactive behavior analysis to test malware in a sandbox environment to see how the malware performs when it is successfully executed. A location is secured to perform reverse engineering on a piece of malware. What is the next step the engineer should take to analyze this malware?

A. Run the program through a debugger to see the sequential actions
B. Unpack the file in a sandbox to see how it reacts
C. Research the malware online to see if there are noted findings
D. Disassemble the malware to understand how it was constructed

Answer: C

NEW QUESTION 34
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 39
Drag and drop the cloud computing service descriptions from the left onto the cloud service categories on the right.

Answer Area

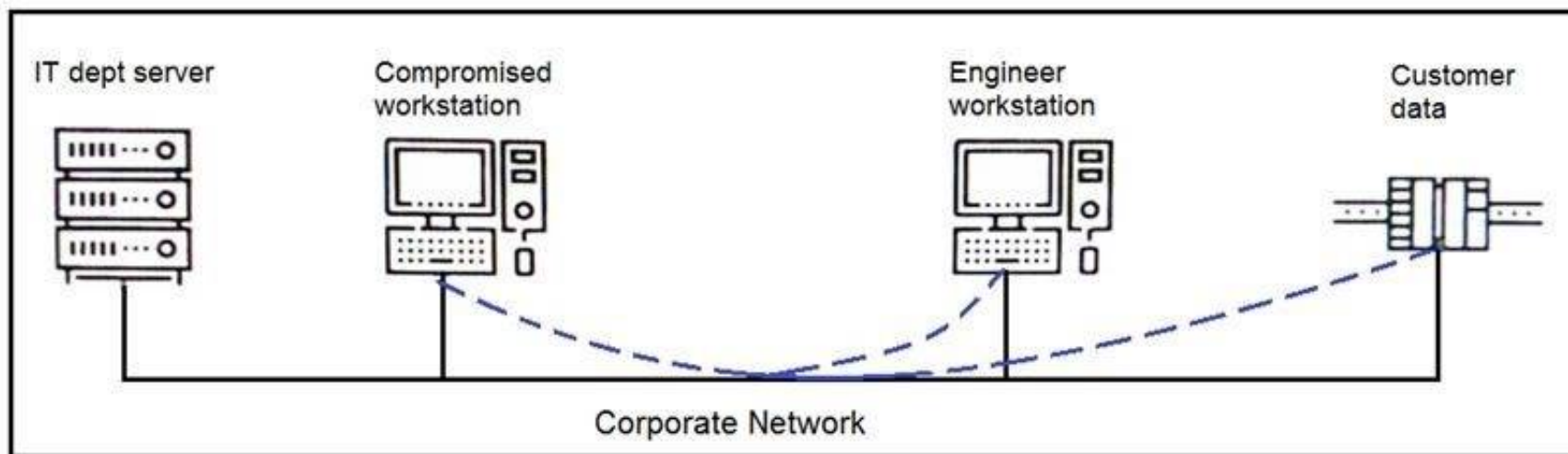| triggers a block of code when triggered by a specific event | | SaaS |
allows renting full servers or virtual machines		PaaS
focuses on developing, testing, and delivering applications		IaaS
allows hosting and managing a virtual environment		FaaS

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 42
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 45
An engineer returned to work and realized that payments that were received over the weekend were sent to the wrong recipient. The engineer discovered that the SaaS tool that processes these payments was down over the weekend. Which step should the engineer take first?

A. Utilize the SaaS tool team to gather more information on the potential breach
B. Contact the incident response team to inform them of a potential breach
C. Organize a meeting to discuss the services that may be affected
D. Request that the purchasing department creates and sends the payments manually

Answer: A

NEW QUESTION 49
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 53
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 56
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 58
An engineer notices that unauthorized software was installed on the network and discovers that it was installed by a dormant user account. The engineer suspects an escalation of privilege attack and responds to the incident. Drag and drop the activities from the left into the order for the response on the right.

Answer Area

Identify systems to be taken offline	Step 1
Conduct content scans	Step 2
Collect log data	Step 3
Request system patch	Step 4
Reimage	Step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Identify systems to be taken offline	Conduct content scans
Conduct content scans	Collect log data
Collect log data	Identify systems to be taken offline
Request system patch	Reimage
Reimage	Request system patch

NEW QUESTION 62
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 66
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 71
An engineer implemented a SOAR workflow to detect and respond to incorrect login attempts and anomalous user behavior. Since the implementation, the security team has received dozens of false positive alerts and negative feedback from system administrators and privileged users. Several legitimate users were tagged as a threat and their accounts blocked, or credentials reset because of unexpected login times and incorrectly typed credentials. How should the workflow be improved to resolve these issues?

A. Meet with privileged users to increase awareness and modify the rules for threat tags and anomalous behavior alerts
B. Change the SOAR configuration flow to remove the automatic remediation that is increasing the false positives and triggering threats
C. Add a confirmation step through which SOAR informs the affected user and asks them to confirm whether they made the attempts
D. Increase incorrect login tries and tune anomalous user behavior not to affect privileged accounts

Answer: B

NEW QUESTION 74
A threat actor used a phishing email to deliver a file with an embedded macro. The file was opened, and a remote code execution attack occurred in a company's infrastructure. Which steps should an engineer take at the recovery stage?

A. Determine the systems involved and deploy available patches
B. Analyze event logs and restrict network access
C. Review access lists and require users to increase password complexity
D. Identify the attack vector and update the IDS signature list

Answer: B

NEW QUESTION 76
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 78
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 79
An audit is assessing a small business that is selling automotive parts and diagnostic services. Due to increased customer demands, the company recently started to accept credit card payments and acquired a POS terminal. Which compliance regulations must the audit apply to the company?

A. HIPAA
B. FISMA
C. COBIT
D. PCI DSS

Answer: D

NEW QUESTION 83
A customer is using a central device to manage network devices over SNMPv2. A remote attacker caused a denial of service condition and can trigger this vulnerability by issuing a GET request for the ciscoFlashMIB OID on an affected device. Which should be disabled to resolve the issue?

A. SNMPv2
B. TCP small services
C. port UDP 161 and 162
D. UDP small services

Answer: A

NEW QUESTION 85
An analyst is alerted for a malicious file hash. After analysis, the analyst determined that an internal workstation is communicating over port 80 with an external server and that the file hash is associated with Duqu malware. Which tactics, techniques, and procedures align with this analysis?

A. Command and Control, Application Layer Protocol, Duqu
B. Discovery, Remote Services: SMB/Windows Admin Shares, Duqu
C. Lateral Movement, Remote Services: SMB/Windows Admin Shares, Duqu
D. Discovery, System Network Configuration Discovery, Duqu

Answer: A

NEW QUESTION 89
Drag and drop the function on the left onto the mechanism on the right.

Answer Area

creates the set of executable tasks	**Orchestration**
minimizes redundancies and steamlines repetitive tasks	
organizes components to seamlessly run applications	**Automation**
systematically executes large workflows	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

creates the set of executable tasks	**Orchestration**
minimizes redundancies and steamlines repetitive tasks	organizes components to seamlessly run applications
organizes components to seamlessly run applications	creates the set of executable tasks
systematically executes large workflows	**Automation**
	minimizes redundancies and steamlines repetitive tasks
	systematically executes large workflows

NEW QUESTION 93
An engineer is moving data from NAS servers in different departments to a combined storage database so that the data can be accessed and analyzed by the organization on-demand. Which data management process is being used?

A. data clustering
B. data regression
C. data ingestion
D. data obfuscation

Answer: A

NEW QUESTION 96
A threat actor has crafted and sent a spear-phishing email with what appears to be a trustworthy link to the site of a conference that an employee recently attended. The employee clicked the link and was redirected to a malicious site through which the employee downloaded a PDF attachment infected with ransomware. The employee opened the attachment, which exploited vulnerabilities on the desktop. The ransomware is now installed and is calling back to its command and control server. Which security solution is needed at this stage to mitigate the attack?

A. web security solution
B. email security solution
C. endpoint security solution
D. network security solution

Answer: D

NEW QUESTION 97

An engineer receives an incident ticket with hundreds of intrusion alerts that require investigation. An analysis of the incident log shows that the alerts are from trusted IP addresses and internal devices. The final incident report stated that these alerts were false positives and that no intrusions were detected. What action should be taken to harden the network?

A. Move the IPS to after the firewall facing the internal network
B. Move the IPS to before the firewall facing the outside network
C. Configure the proxy service on the IPS
D. Configure reverse port forwarding on the IPS

Answer: C

NEW QUESTION 98
Refer to the exhibit.

```
def map_to_lowercase_letter(s):
    return ord('a') + ((s-ord('a')) % 26)
def next_domain(domain):
    dl = [ord(x) for x in list(domain)]
    dl[0] = map_to_lowercase_letter(dl[0] + dl[3])
    dl[1] = map_to_lowercase_letter(dl[0] + 2*dl[1])
    dl[2] = map_to_lowercase_letter(dl[0] + dl[2] - 1)
    dl[3] = map_to_lowercase_letter(dl[1] + dl[2] + dl[3])
    return ''.join([chr(x) for x in dl])
def isBanjoriTail(seed):
    for c0 in xrange(97,123):
        for c1 in xrange(97, 123):
            for c2 in xrange(97,123):
                for c3 in xrange (97,123):
                    domain = chr(c0)+chr(c1)+chr(c2)+chr(c3)
                    domain = next_domain(domain)
                    if seed.startswith(domain):
                        return False
    return True
seeds = {
"nhcisatformalisticirekb.com",
"egfesatformalisticirekb.com",
"qwfusatformalisticirekb.com",
"eijhsatformalisticirekb.com",
"siowsatformalisticirekb.com",
"dhansatformalisticirekb.com",
"zvogsatformalisticirekb.com",
"yaewsatformalisticirekb.com",
"wgxfsatformalisticirekb.com",
"vfxlsatformalisticirekb.com",
"usjssatformalisticirekb.com",
"selzsatformalisticirekb.com",
"nzjqsatformalisticirekb.com",
"kencsatformalisticirekb.com",
"fzkxsatformalisticirekb.com",
"babysatformalisticirekb.com",
}
for seed in seeds:
    print seed,isBanjonTail(seed)
```
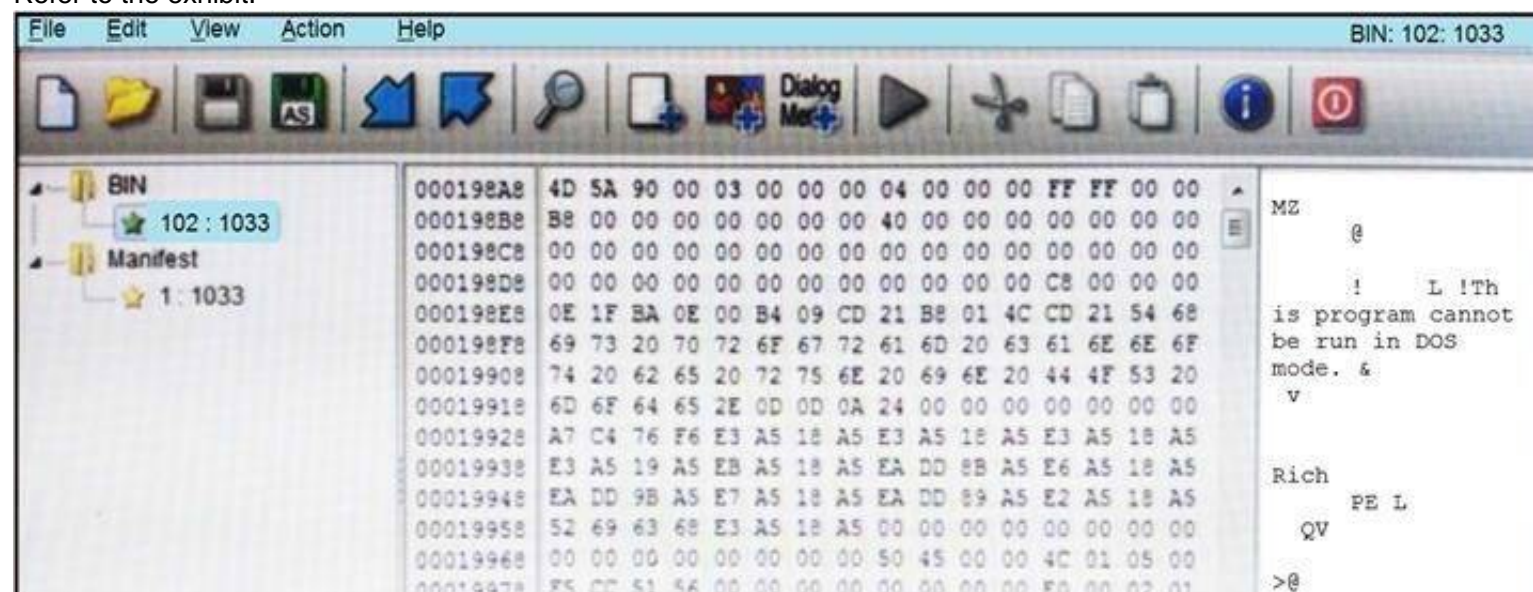
What results from this script?

A. Seeds for existing domains are checked
B. A search is conducted for additional seeds
C. Domains are compared to seed rules
D. A list of domains as seeds is blocked

Answer: B

NEW QUESTION 101
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 104
A European-based advertisement company collects tracking information from partner websites and stores it on a local server to provide tailored ads. Which standard must the company follow to safeguard the resting data?

A. HIPAA
B. PCI-DSS
C. Sarbanes-Oxley
D. GDPR

Answer: D

NEW QUESTION 109
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 110
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 112
Drag and drop the components from the left onto the phases of the CI/CD pipeline on the right.

Answer Area

Components	Phases
build	Phase 1
release	Phase 2
deploy	Phase 3
operate	Phase 4
monitor	Phase 5
test	Phase 6
plan	Phase 7
develop	Phase 8

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

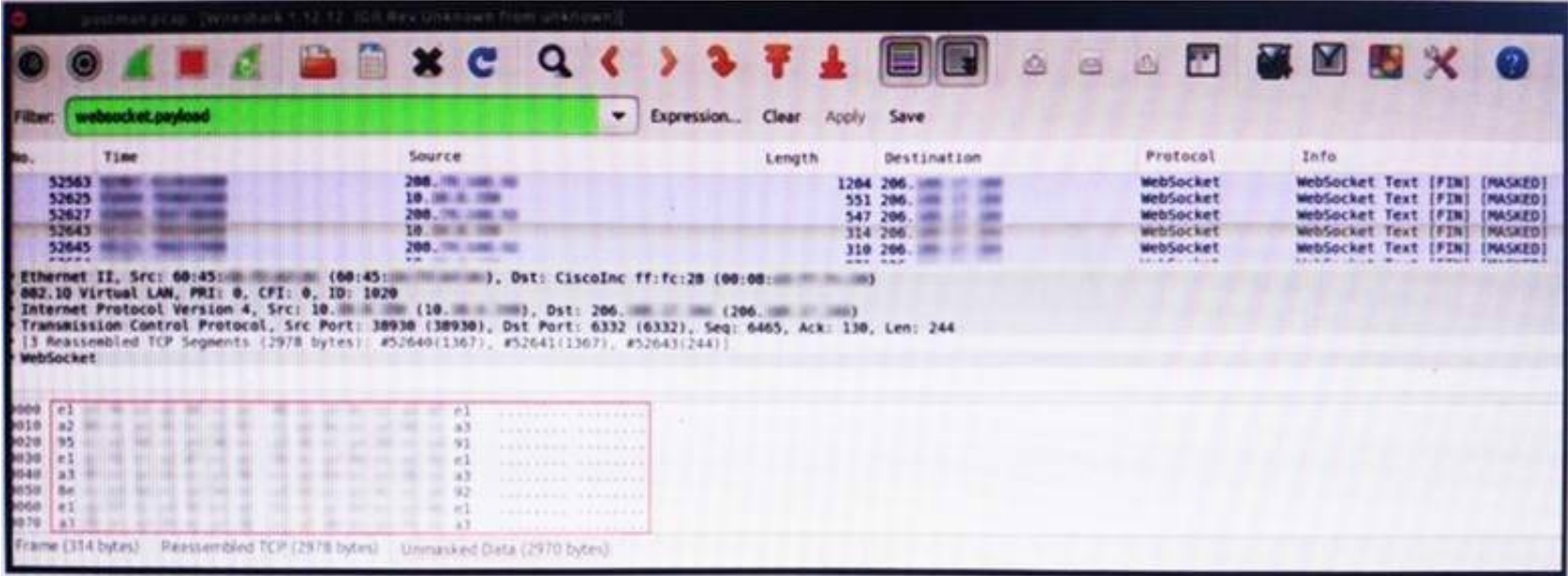|	
build	plan
release	develop
deploy	build
operate	test
monitor	release
test	deploy
plan	operate
develop	monitor

NEW QUESTION 113
Refer to the exhibit.

An engineer is analyzing this Vlan0386-int12-117.pcap file in Wireshark after detecting a suspicious network activity. The origin header for the direct IP connections in the packets was initiated by a google chrome extension on a WebSocket protocol. The engineer checked message payloads to determine what information was being sent off-site but the payloads are obfuscated and unreadable. What does this STIX indicate?

A. The extension is not performing as intended because of restrictions since ports 80 and 443 should be accessible
B. The traffic is legitimate as the google chrome extension is reaching out to check for updates and fetches this information
C. There is a possible data leak because payloads should be encoded as UTF-8 text
D. There is a malware that is communicating via encrypted channels to the command and control server

Answer: C

NEW QUESTION 115
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 116
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 117
......

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 350-201 Exam with Our Prep Materials Via below:

https://www.certleader.com/350-201-dumps.html