

350-201 Dumps

Performing CyberOps Using Core Security Technologies (CBRCOR)

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



NEW QUESTION 1

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 2

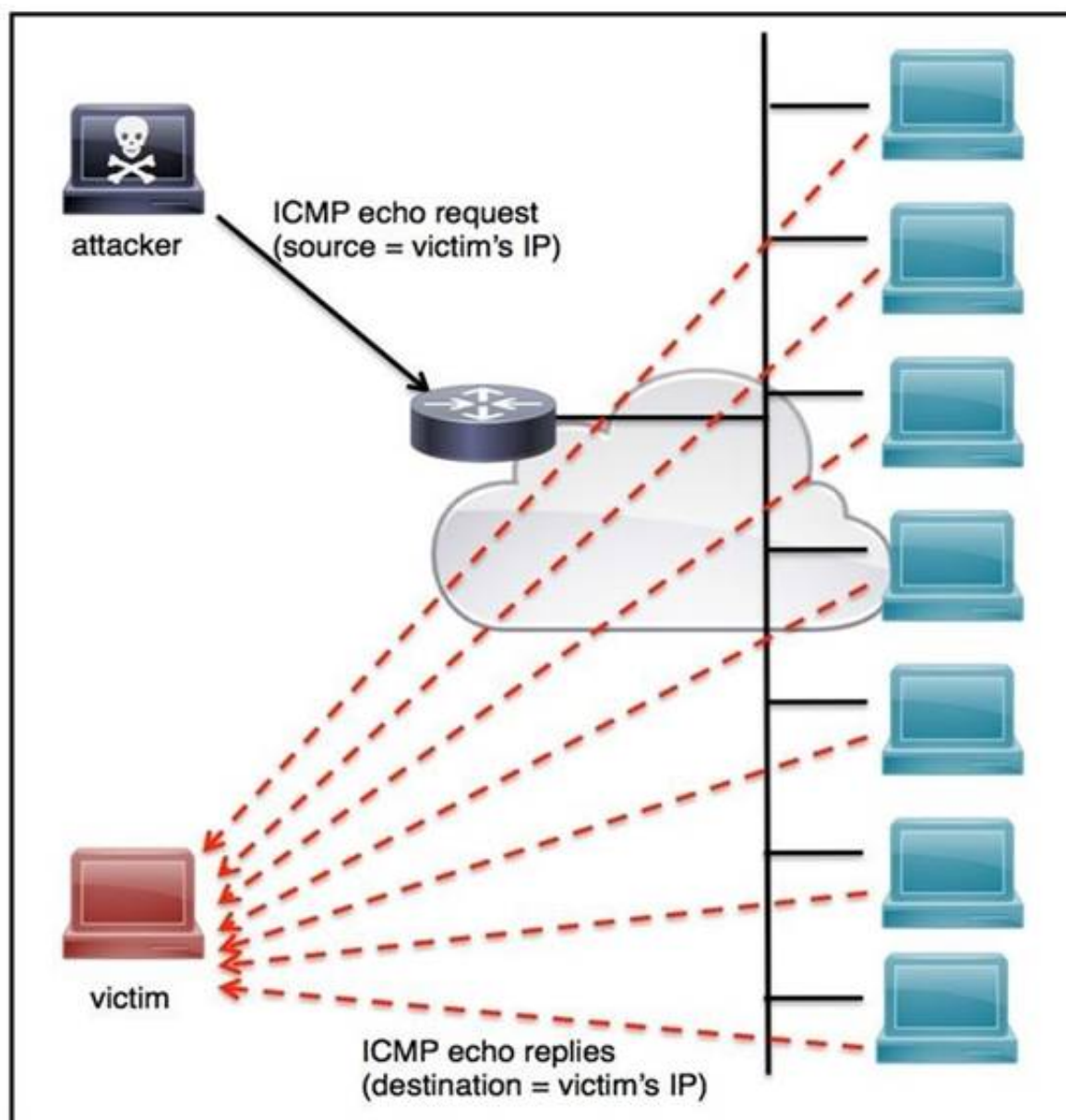
How is a SIEM tool used?

- A. To collect security data from authentication failures and cyber attacks and forward it for analysis
- B. To search and compare security data against acceptance standards and generate reports for analysis
- C. To compare security alerts against configured scenarios and trigger system responses
- D. To collect and analyze security data from network devices and servers and produce alerts

Answer: D

NEW QUESTION 3

Refer to the exhibit.



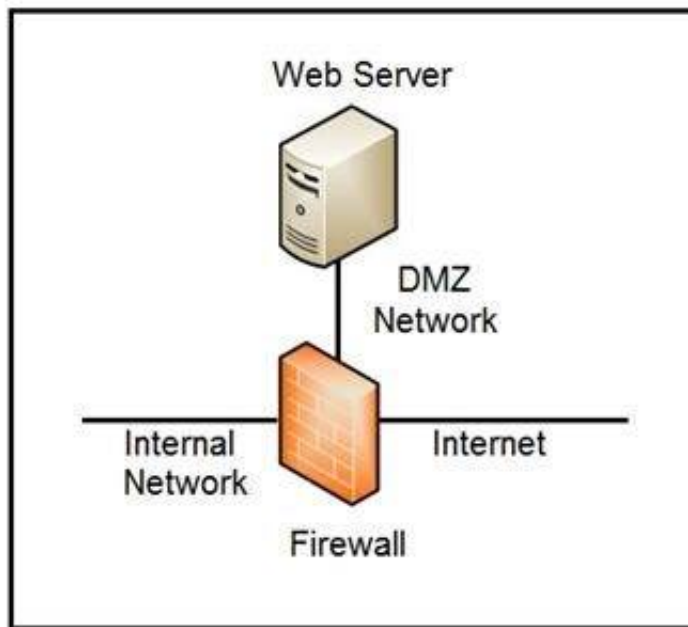
An engineer must tune the Cisco IOS device to mitigate an attack that is broadcasting a large number of ICMP packets. The attack is sending the victim's spoofed source IP to a network using an IP broadcast address that causes devices in the network to respond back to the source IP address. Which action 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 4

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 5

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,
      "kill_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 6

Drag and drop the NIST incident response process steps from the left onto the actions that occur in the steps on the right.

Answer Area

Eradicate	Analyze and document the breach, and strengthen systems against future attacks
Contain	Conduct incident response role training for employees
Post-Incident Handling	Determine where the breach started and prevent the attack from spreading
Recover	Determine how the breach was discovered and the areas that were impacted
Analyze	Eliminate the root cause of the breach and apply updates to the system
Prepare	Get systems and business operations up and running, and ensure that the same type of attack does not occur again

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Eradicate	Contain
Contain	Prepare
Post-Incident Handling	Recover
Recover	Analyze
Analyze	Eradicate
Prepare	Post-Incident Handling

NEW QUESTION 7

Refer to the exhibit.

```
<employees>
  <employee>
    <lastname>Smith</lastname>
    <firstname>Richard</firstname>
  </employee>
  <employee>
    <lastname>Witzel</lastname>
    <firstname>Sevan</firstname>
  </employee>
</employees>
```

Which data format is being used?

- A. JSON
B. HTML
C. XML
D. CSV

Answer: B

NEW QUESTION 8

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 9

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 10

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 10

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 14

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 15

An engineer is going through vulnerability triage with company management because of a recent malware outbreak from which 21 affected assets need to be patched or remediated. Management decides not to prioritize fixing the assets and accepts the vulnerabilities. What is the next step the engineer should take?

- A. Investigate the vulnerability to prevent further spread
- B. Acknowledge the vulnerabilities and document the risk
- C. Apply vendor patches or available hot fixes
- D. Isolate the assets affected in a separate network

Answer: D

NEW QUESTION 18

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 19

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 23

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 28

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 29

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 30

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 32

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 36

Drag and drop the threat from the left onto the scenario that introduces the threat on the right. Not all options are used.

Answer Area

spoofing attack	installing network devices
broken authentication attack	developing new code
injection attack	implementing a new application
man-in-the-middle attack	changing configuration settings
privilege escalation attack	
default credential attack	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

spoofing attack	man-in-the-middle attack
broken authentication attack	injection attack
injection attack	privilege escalation attack
man-in-the-middle attack	default credential attack
privilege escalation attack	
default credential attack	

NEW QUESTION 40
Refer to the exhibit.

```
def get_umbrella_dispos(domains):
    # put in right format to pass as argument in POST request
    values = str(json.dumps(domains))
    req = requests.post(investigate_url, data=values, headers=headers)
    # time for timestamp of verdict domain
    time = datetime.now().isoformat()
    # error handling if true then the request was HTTP 200, so successful
    if(req.status_code == 200):
        print("SUCCESS: request has the following code: 200\n")
        output = req.json()

        if(domain_status == -1):
            print("The domain %(domain)s is found MALICIOUS at %(time)s\n" % {'domain': domain, 'time': time})
        elif(domain_status == 1):
            print("The domain %(domain)s is found CLEAN at %(time)s\n" %
                  {'domain': domain, 'time': time})
        else:
            print("The domain %(domain)s is found UNDEFINED / RISKY at %(time)s\n" %
                  {'domain': domain, 'time': time})
    else:
        print("An error has occurred with the following code %(error)s, please consult the following link:
              https://docs.umbrella.com/investigate-api/" %
              {'error': req.status_code})
```

Which code snippet will parse the response to identify the status of the domain as malicious, clean or undefined?

- A.

```
for domain in domains[:]:
    domain_status = domain_output["status"]
```
- B.

```
while domain in domains:
    domain_status = domain_output["status"]
```
- C.

```
for domain in domains:
    domain_output = output[domain]
    domain_status = domain_output["status"]
```
- D.

```
while domains in domains:
    domain_output = output[domain]
    domain_status = domain_output["status"]
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 42

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 45

An organization is using a PKI management server and a SOAR platform to manage the certificate lifecycle. The SOAR platform queries a certificate management tool to check all endpoints for SSL certificates that have either expired or are nearing expiration. Engineers are struggling to manage problematic certificates outside of PKI management since deploying certificates and tracking them requires searching server owners manually. Which action will improve workflow automation?

- A. Implement a new workflow within SOAR to create tickets in the incident response system, assign problematic certificate update requests to server owners, and register change requests.
- B. Integrate a PKI solution within SOAR to create certificates within the SOAR engines to track, update, and monitor problematic certificates.
- C. Implement a new workflow for SOAR to fetch a report of assets that are outside of the PKI zone, sort assets by certification management leads and automate alerts that updates are needed.
- D. Integrate a SOAR solution with Active Directory to pull server owner details from the AD and send an automated email for problematic certificates requesting updates.

Answer: C

NEW QUESTION 49

Refer to the exhibit.

Analysis Report

ID	12cbdee21b1ea4	Filename	fpzryrf.exe
OS	7601.1898.amd64fre.win7sp1_gdr.150316-1654	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Started	7/29/16 18:44:43	Analyzed As	exe
Ended	7/29/16 18:50:39	SHA256	e9ca08a3cc2f8c9748a9e9b304c9f5a16d830066e5467d3dd5927be36fec47da
Duration	0:05:56	SHA1	a2de85810fd5ebcf29c5da5dd29ce03470772ad
Sandbox	phl-work-02 (pilot-d)	MD5	dd07d778edf8d581ffaadb1610aaa008

Warnings

- Executable Failed Integrity Check

Behavioral Indicators

CTB Locker Detected	Severity: 100	Confidence: 100
Generic Ransomware Detected	Severity: 100	Confidence: 95
Excessive Suspicious Activity Detected	Severity: 90	Confidence: 100
Process Modified a File in a System Directory	Severity: 90	Confidence: 100
Large Amount of High Entropy Artifacts Written	Severity: 100	Confidence: 80
Process Modified a File in the Program Files Directory	Severity: 80	Confidence: 90
Decoy Document Detected	Severity: 70	Confidence: 100
Process Modified an Executable File	Severity: 60	Confidence: 100
Process Modified File in a User Directory	Severity: 70	Confidence: 80
Windows Crash Tool Execution Detected	Severity: 20	Confidence: 80
Hook Procedure Detected in Executable	Severity: 35	Confidence: 40
Ransomware Queried Domain	Severity: 25	Confidence: 25
Executable Imported the IsDebuggerPresent Symbol	Severity: 20	Confidence: 20

Cisco Advanced Malware Protection installed on an end-user desktop has automatically submitted a low prevalence file to the Threat Grid analysis engine for further analysis. What should be concluded from this report?

- A. The prioritized behavioral indicators of compromise do not justify the execution of the “ransomware” because the scores do not indicate the likelihood of malicious ransomware.
- B. The prioritized behavioral indicators of compromise do not justify the execution of the “ransomware” because the scores are high and do not indicate the likelihood of malicious ransomware.
- C. The prioritized behavioral indicators of compromise justify the execution of the “ransomware” because the scores are high and indicate the likelihood that malicious ransomware has been detected.
- D. The prioritized behavioral indicators of compromise justify the execution of the “ransomware” because the scores are low and indicate the likelihood that malicious ransomware has been detected.

Answer: C

NEW QUESTION 52

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 54

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 55

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 56

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 59

Refer to the exhibit.

```
#!/usr/bin/env python3

import re

def (username, minlen):
    if type(username) != str:
        raise TypeError
    if minlen < 3:
        raise ValueError
    if len(username) < minlen:
        return False
    if not re.match('[a-z0-9._]*$', username):
        return False
    if username[0].isnumeric():
        return False
    return True
```

An organization is using an internal application for printing documents that requires a separate registration on the website. The application allows format-free user creation, and users must match these required conditions to comply with the company's user creation policy:

- minimum length: 3
- usernames can only use letters, numbers, dots, and underscores
- usernames cannot begin with a number

The application administrator has to manually change and track these daily to ensure compliance. An engineer is tasked to implement a script to automate the process according to the company user creation policy. The engineer implemented this piece of code within the application, but users are still able to create format-free usernames. Which change is needed to apply the restrictions?

- A. modify code to return error on restrictions def return false_user(username, minlen)
- B. automate the restrictions def automate_user(username, minlen)
- C. validate the restrictions, def validate_user(username, minlen)
- D. modify code to force the restrictions, def force_user(username, minlen)

Answer: B

NEW QUESTION 61

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 63

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

Answer Area

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 64
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 66

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 Ack=61118
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 69

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 70

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, realmDomain=0, shortrealm=0
x-xss-protection: 1; mode=block
```

Where does it signify that a page will be stopped from loading when a scripting attack is detected?

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

Answer: C

NEW QUESTION 72

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 77

.....

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>