

## 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**

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 3**

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 4**

A malware outbreak is detected by the SIEM and is confirmed as a true positive. The incident response team follows the playbook to mitigate the threat. What is the first action for the incident response team?

- A. Assess the network for unexpected behavior
- B. Isolate critical hosts from the network
- C. Patch detected vulnerabilities from critical hosts
- D. Perform analysis based on the established risk factors

**Answer: B**

**NEW QUESTION 5**

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 6**

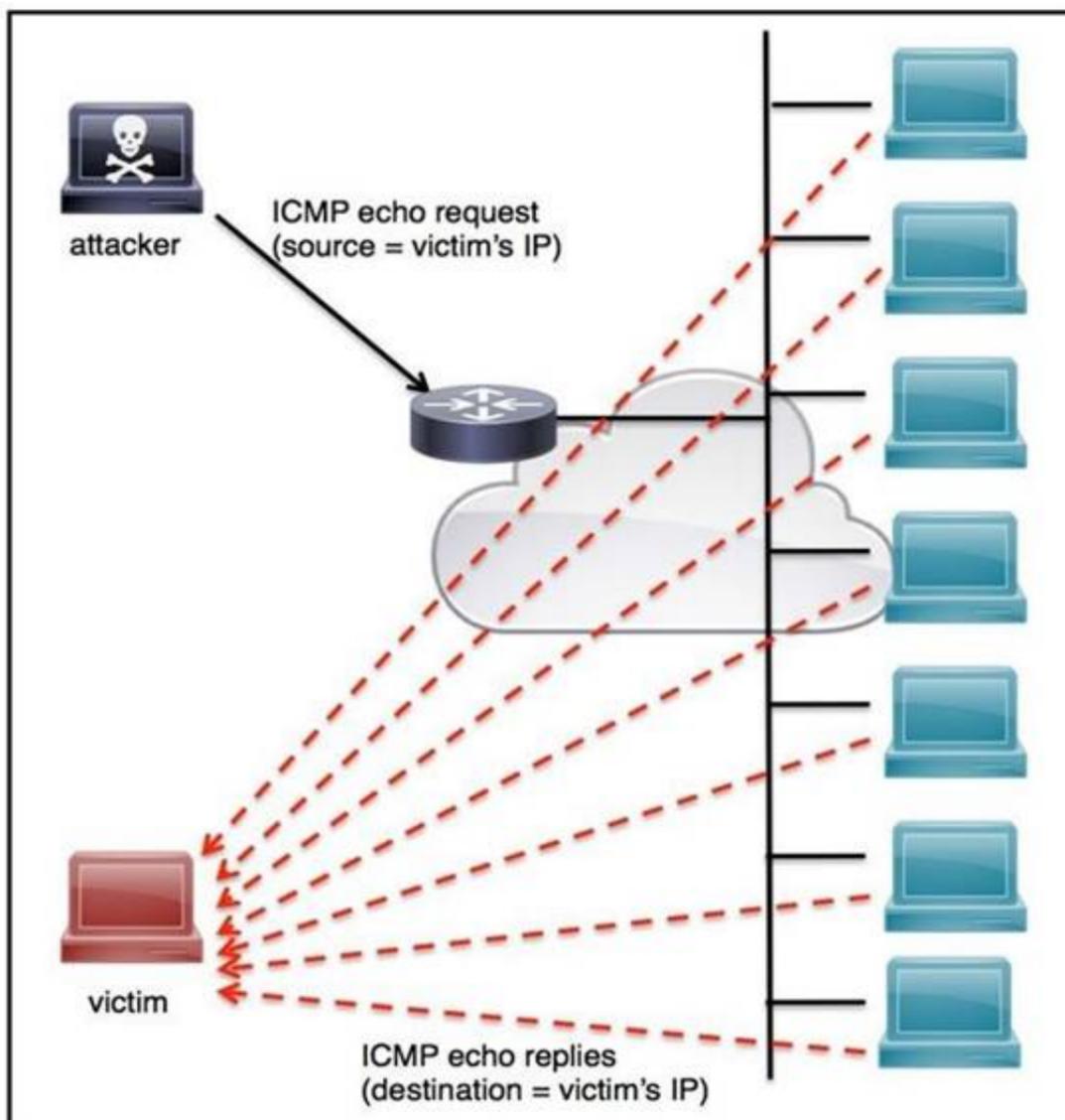
An employee who often travels abroad logs in from a first-seen country during non-working hours. The SIEM tool generates an alert that the user is forwarding an increased amount of emails to an external mail domain and then logs out. The investigation concludes that the external domain belongs to a competitor. 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 7**

Refer to the exhibit.



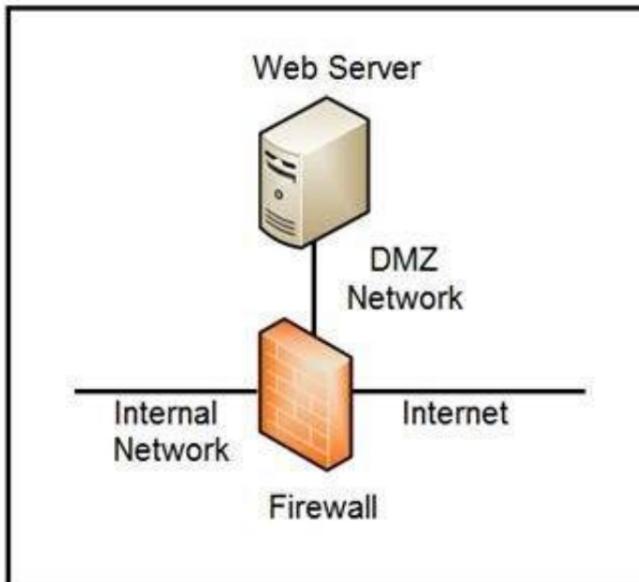
An engineer must tune the Cisco IOS device to mitigate an attack that is broadcasting a large number of ICMP packets. The attack is sending the victim's spoofed source IP to a network using an IP broadcast address that causes devices in the network to respond back to the source IP address. Which action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

```

{
  "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 10

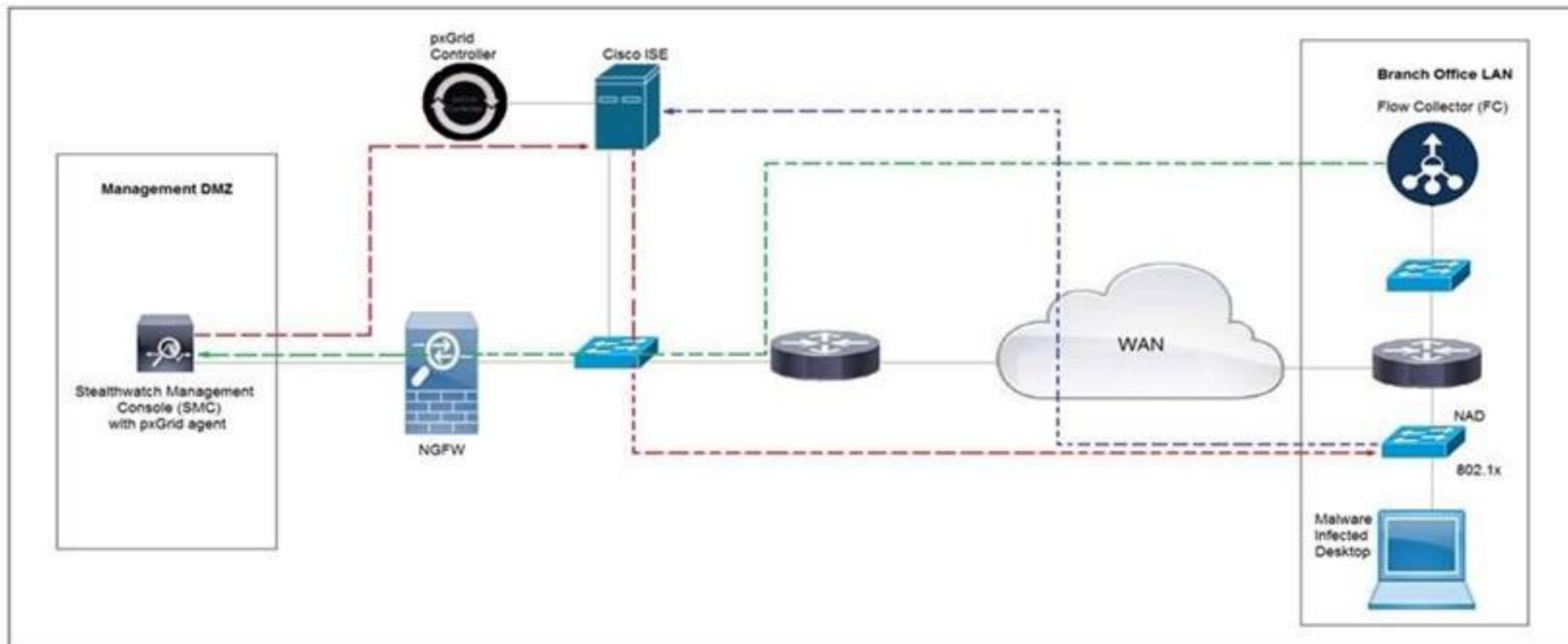
How does Wireshark decrypt TLS network traffic?

- 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.



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 15**

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 18**

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 23**

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 27**

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 29**

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 34**

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 39**

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 44**

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 46

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 50

A SIEM tool fires an alert about a VPN connection attempt from an unusual location. The incident response team validates that an attacker has installed a remote access tool on a user's laptop while traveling. The attacker has the user's credentials and is attempting to connect to the network. What is the next step in handling the incident?

- A. Block the source IP from the firewall
- B. Perform an antivirus scan on the laptop
- C. Identify systems or services at risk
- D. Identify lateral movement

Answer: C

#### NEW QUESTION 51

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 52

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 54

Refer to the exhibit.

Analysis Report			
<b>ID</b>	12cbeee21b1ea4	<b>Filename</b>	ee482400446236cb315ad7ed035bd77ad4014039ec9bfebc8f2.eml
<b>OS</b>	Windows 7 64-bit	<b>Magic Type</b>	SMTP mail, ASCII text
<b>Started</b>	10/13/20 06:22:43	<b>Analyzed As</b>	eml
<b>Ended</b>	10/13/20 06:29:19	<b>SHA256</b>	ee482400446236cb3f5ad7ed035bd77add40140058b6d0e6ffe639ec9bfebc8f2
<b>Duration</b>	0:06:36	<b>SHA1</b>	d700bca5b65aaf0c613d702d9a28a6084692224
<b>Sandbox</b>	rcn-work-042 (pilot-d)	<b>MD5</b>	58d1163715089192a8177a5244b9658f

Behavioral Indicators		
⊕ Email References Localhost in Received Message Trace	<b>Severity: 40</b>	<b>Confidence: 100</b>
⊕ Document Contains Embedded Material and Minimal Content	<b>Severity: 50</b>	<b>Confidence: 80</b>
⊕ Download Forced Open/Save Prompt	<b>Severity: 50</b>	<b>Confidence: 75</b>
⊕ Email With Different Sender and Return-Path Detected	<b>Severity: 60</b>	<b>Confidence: 60</b>
⊕ Process Users Very Large Command-Line	<b>Severity: 40</b>	<b>Confidence: 80</b>
⊕ File Downloaded to Disk	<b>Severity: 30</b>	<b>Confidence: 90</b>
⊕ Potential Code Injection Detected	<b>Severity: 50</b>	<b>Confidence: 50</b>
⊕ HTTP Client Error Response	<b>Severity: 50</b>	<b>Confidence: 50</b>
⊕ Sample Communicates With Only Benign Domains	<b>Severity: 20</b>	<b>Confidence: 95</b>
⊕ Executable with Encrypted Sections	<b>Severity: 30</b>	<b>Confidence: 30</b>
⊕ Outbound Communications to Nginx Web Server	<b>Severity: 25</b>	<b>Confidence: 25</b>
⊕ Outbound HTTP POST Communications	<b>Severity: 25</b>	<b>Confidence: 25</b>
⊕ Document Queried Domain	<b>Severity: 25</b>	<b>Confidence: 25</b>
⊕ Executable Imported the IsDebuggerPresent Symbol	<b>Severity: 20</b>	<b>Confidence: 20</b>

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

- A. Threat scores are high, malicious ransomware has been detected, and files have been modified
- B. Threat scores are low, malicious ransomware has been detected, and files have been modified
- C. Threat scores are high, malicious activity is detected, but files have not been modified
- D. Threat scores are low and no malicious file activity is detected

Answer: B

**NEW QUESTION 56**

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 60**

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 62**

Refer to the exhibit.

### Analysis Report

ID	12cbeee21b1ea4	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 63**

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 64**

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 65**

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 66

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 69

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)
```

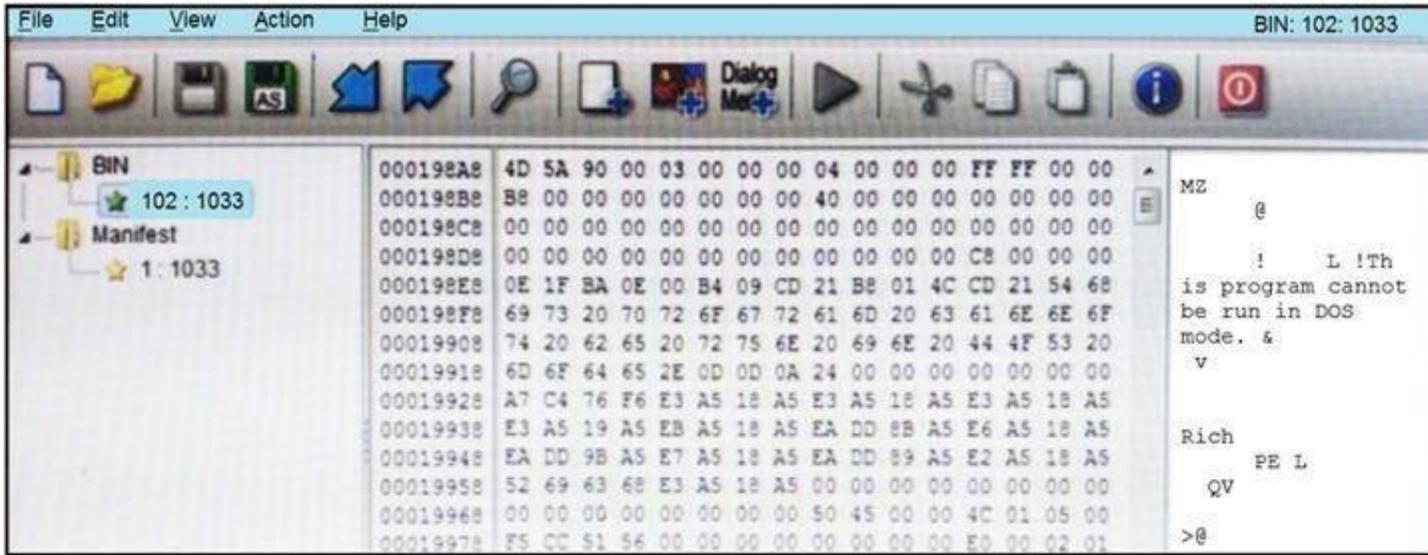
What results from this script?

- 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 73

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 77**

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 81**

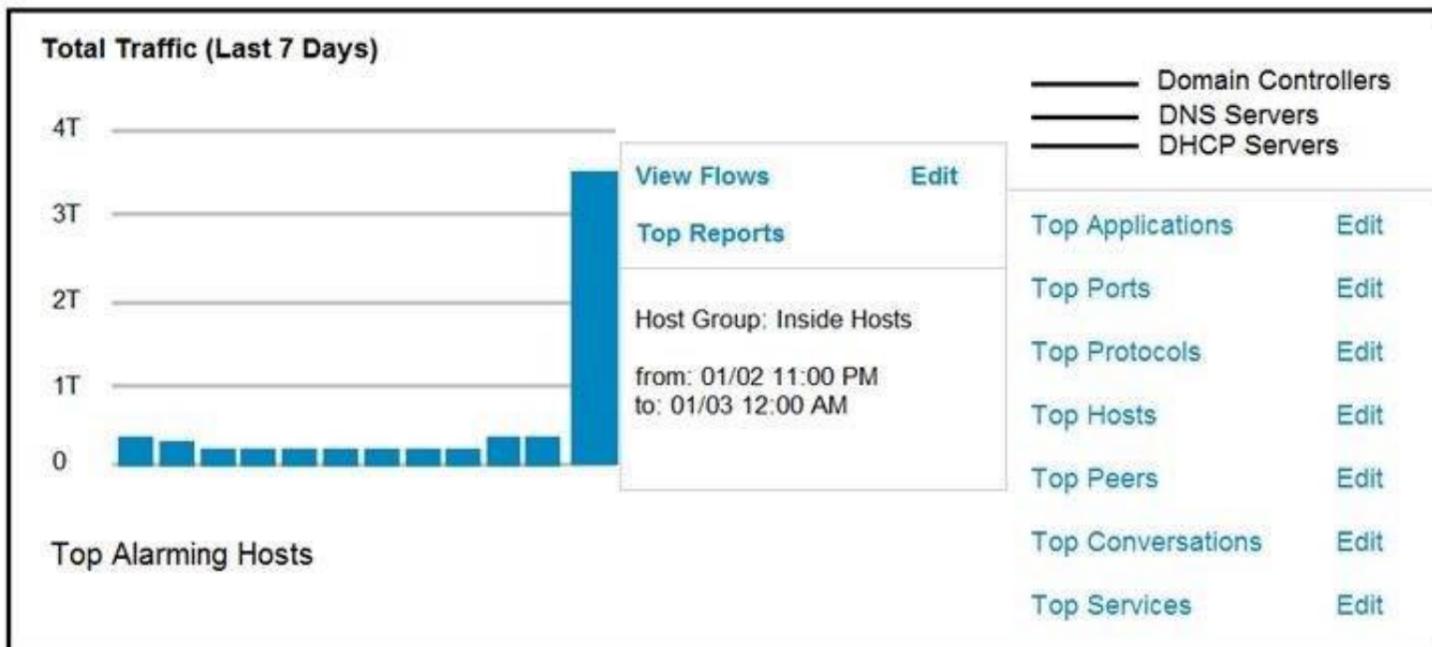
A company launched an e-commerce website with multiple points of sale through internal and external e- stores. Customers access the stores from the public website, and employees access the stores from the intranet with an SSO. Which action is needed to comply with PCI standards for hardening the systems?

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

Answer: B

**NEW QUESTION 86**

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 90**

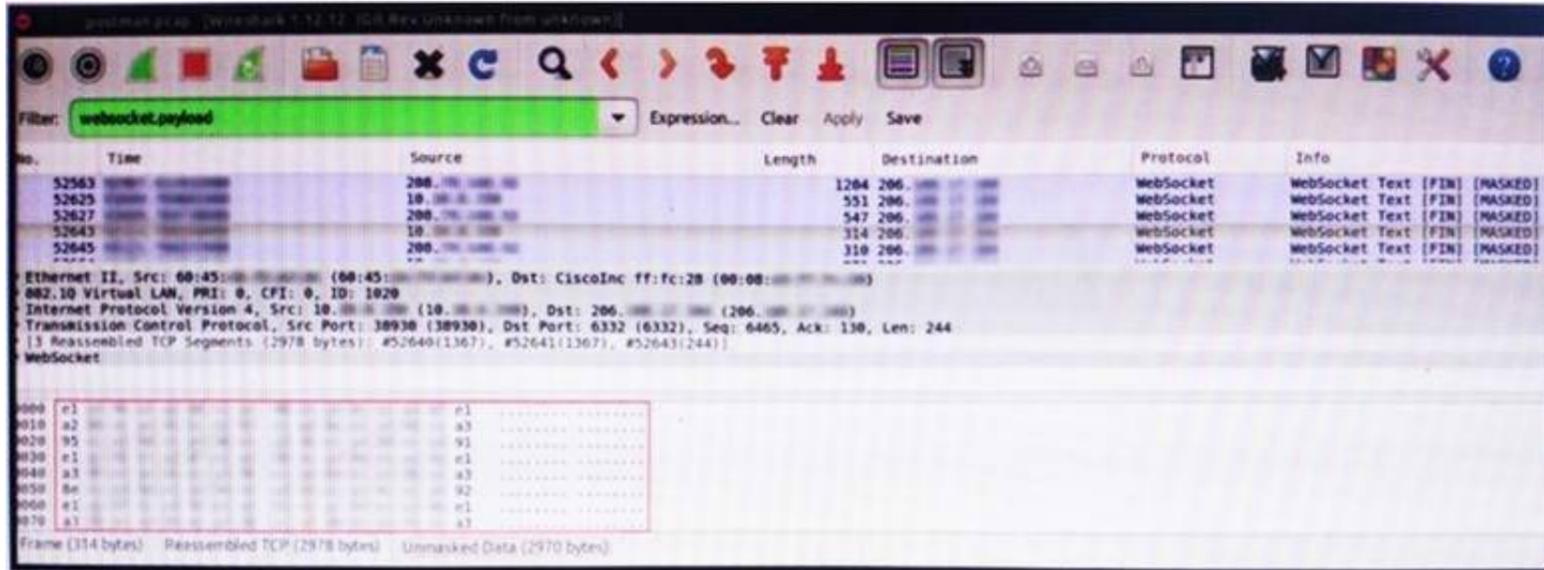
An engineer is analyzing a possible compromise that happened a week ago when the company ? (Choose two.)

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

**Answer: AB**

**NEW QUESTION 93**

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 95**

What is a principle of Infrastructure as Code?

- A. System maintenance is delegated to software systems
- B. Comprehensive initial designs support robust systems
- C. Scripts and manual configurations work together to ensure repeatable routines
- D. System downtime is grouped and scheduled across the infrastructure

**Answer: B**

**NEW QUESTION 100**

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 105**

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 107**

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 111**

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 113**

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 117**

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 121**

A Mac laptop user notices that several files have disappeared from their laptop documents folder. While looking for the files, the user notices that the browser history was recently cleared. The user raises a case, and an analyst reviews the network usage and discovers that it is abnormally high. Which step should be taken to continue the investigation?

- A. Run the sudo sysdiagnose command
- B. Run the sh command
- C. Run the w command
- D. Run the who command

Answer: A

NEW QUESTION 126

.....

## 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