Cisco

Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)

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
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
Refer to the exhibit.

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

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

What is the threat in this Wireshark traffic capture?

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

Answer: D

NEW QUESTION 4
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 5
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 6
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 7
A SOC analyst is investigating a recent email delivered to a high-value user for a customer whose network their organization monitors. The email includes a suspicious attachment titled "Invoice RE: 0004489". The hash of the file is gathered from the Cisco Email Security Appliance. After searching Open Source Intelligence, no available history of this hash is found anywhere on the web. What is the next step in analyzing this attachment to allow the analyst to gather indicators of compromise?

A. Run and analyze the DLP Incident Summary Report from the Email Security Appliance
B. Ask the company to execute the payload for real time analysis
C. Investigate further in open source repositories using YARA to find matches
D. Obtain a copy of the file for detonation in a sandbox

Answer: D

NEW QUESTION 8
Refer to the exhibit.

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

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

Answer: C

NEW QUESTION 9
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 runnning, 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 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 10
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.

```
<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 19
According to GDPR, what should be done with data to ensure its confidentiality, integrity, and availability?

A. Perform a vulnerability assessment
B. Conduct a data protection impact assessment
C. Conduct penetration testing
D. Perform awareness testing

Answer: B

NEW QUESTION 24
Refer to the exhibit.

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

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

Answer: D

NEW QUESTION 26
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 30

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 33

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 36

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 37

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 41

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 44

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 46

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 48
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 51
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 52
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			
systematically executes large workflows		Automation	

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 57
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 62
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 66
Refer to the exhibit.

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

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

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

Answer: B

NEW QUESTION 68
Refer to the exhibit.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 143 ( msg:"PROTOCOL-
IMAP login brute force attempt";
flow:to_server,established,no_stream;
content:"LOGIN",fast_pattern,nocase; detection_filter:track
by_dst, count 5, seconds 900; metadata:ruleset community;
service:imap; reference:url,attack.mitre.org/techniques/T1110;
classtype:suspicious-login; sid:2273; rev:12; )
```

IDS is producing an increased amount of false positive events about brute force attempts on the organization's mail server. How should the Snort rule be modified to improve performance?

A. Block list of internal IPs from the rule
B. Change the rule content match to case sensitive
C. Set the rule to track the source IP
D. Tune the count and seconds threshold of the rule

Answer: B

NEW QUESTION 69
Drag and drop the type of attacks from the left onto the cyber kill chain stages at which the attacks are seen on the right.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 71
Refer to the exhibit.

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

Answer Area

Execute rapid threat containment	Step 1
Investigate and classify the exposure	Step 2
Investigate infected hosts	Step 3
Search for infected hosts	Step 4
Examine returned results	Step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Execute rapid threat containment	Search for infected hosts
Investigate and classify the exposure	Investigate infected hosts
Investigate infected hosts	Investigate and classify the exposure
Search for infected hosts	Examine returned results
Examine returned results	Execute rapid threat containment

NEW QUESTION 76
Refer to the exhibit.
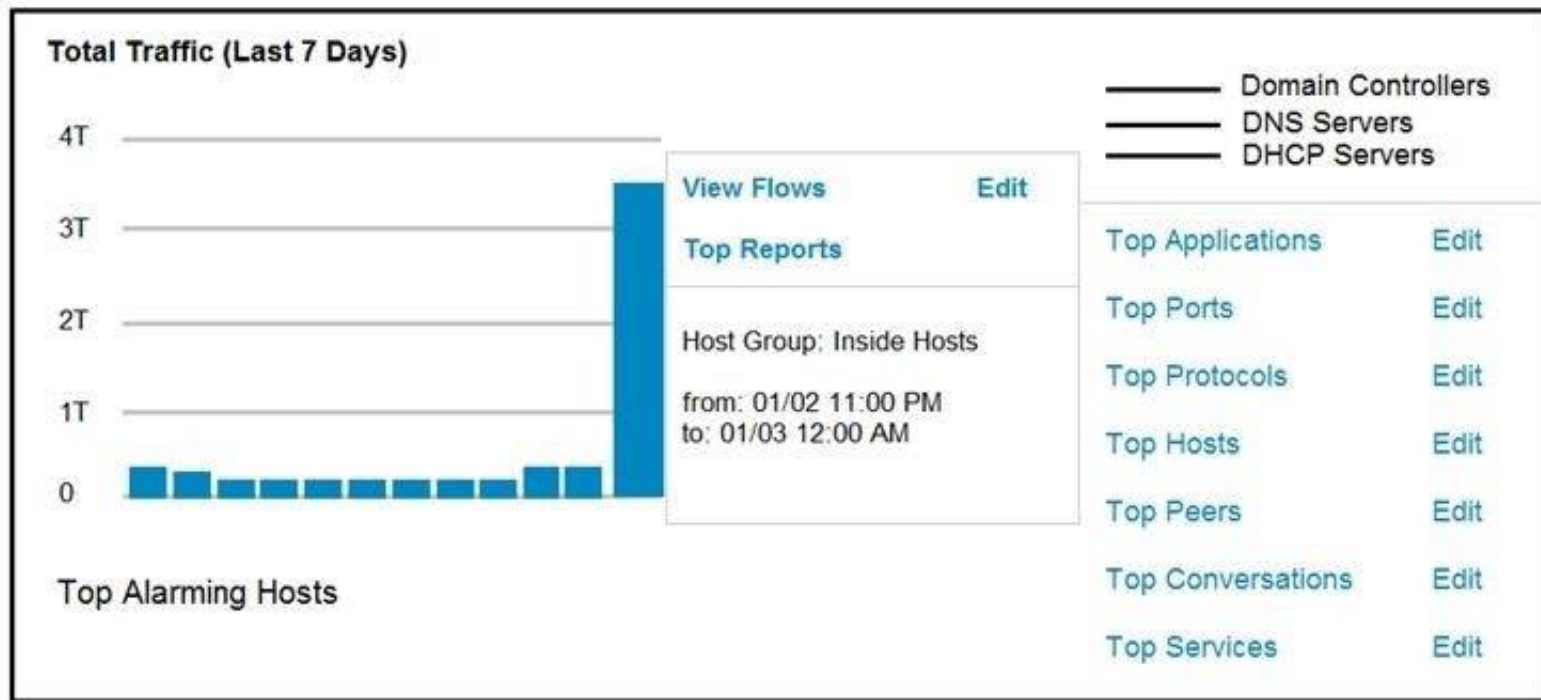
An engineer notices a significant anomaly in the traffic in one of the host groups in Cisco Secure Network Analytics (Stealthwatch) and must analyze the top data transmissions. Which tool accomplishes this task?

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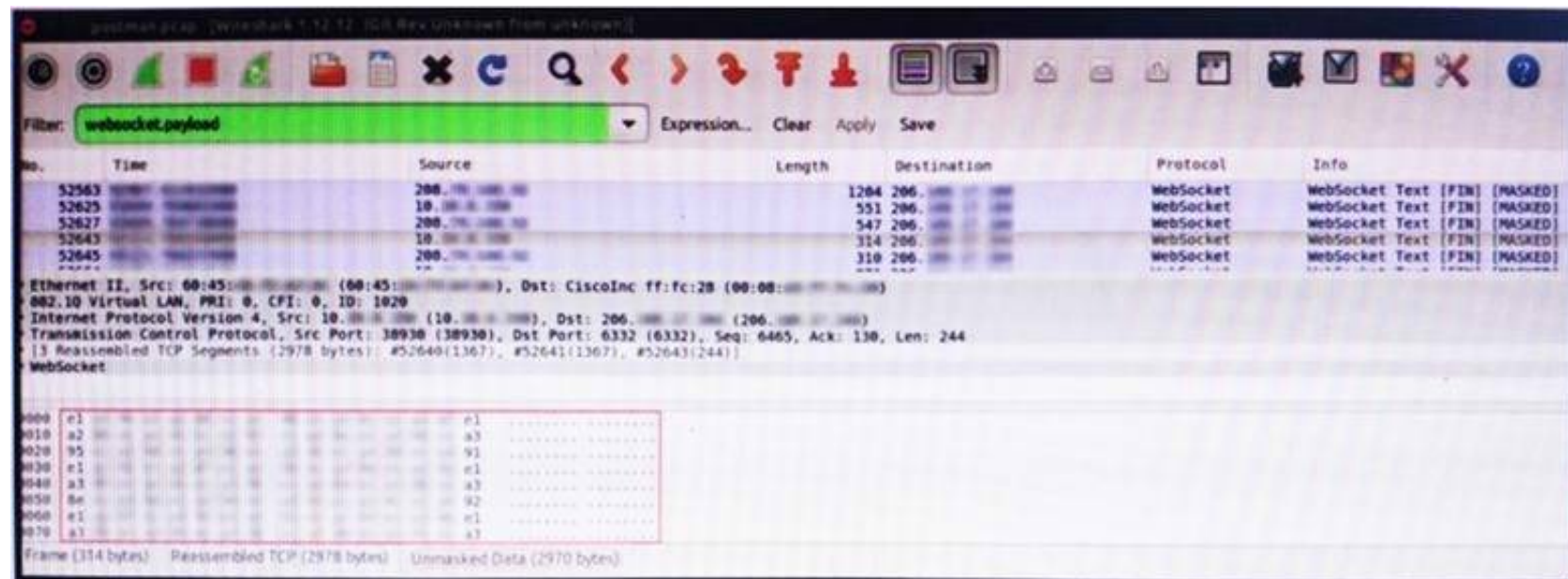C. Top Conversations
D. Top Ports

Answer: B

NEW QUESTION 78
Where do threat intelligence tools search for data to identify potential malicious IP addresses, domain names, and URLs?

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

Answer: D

NEW QUESTION 79
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 80
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 84
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 86
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 89
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 94
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 96
......

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

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
Order The 350-201 Practice Test Here