Cisco

Exam Questions 350-201

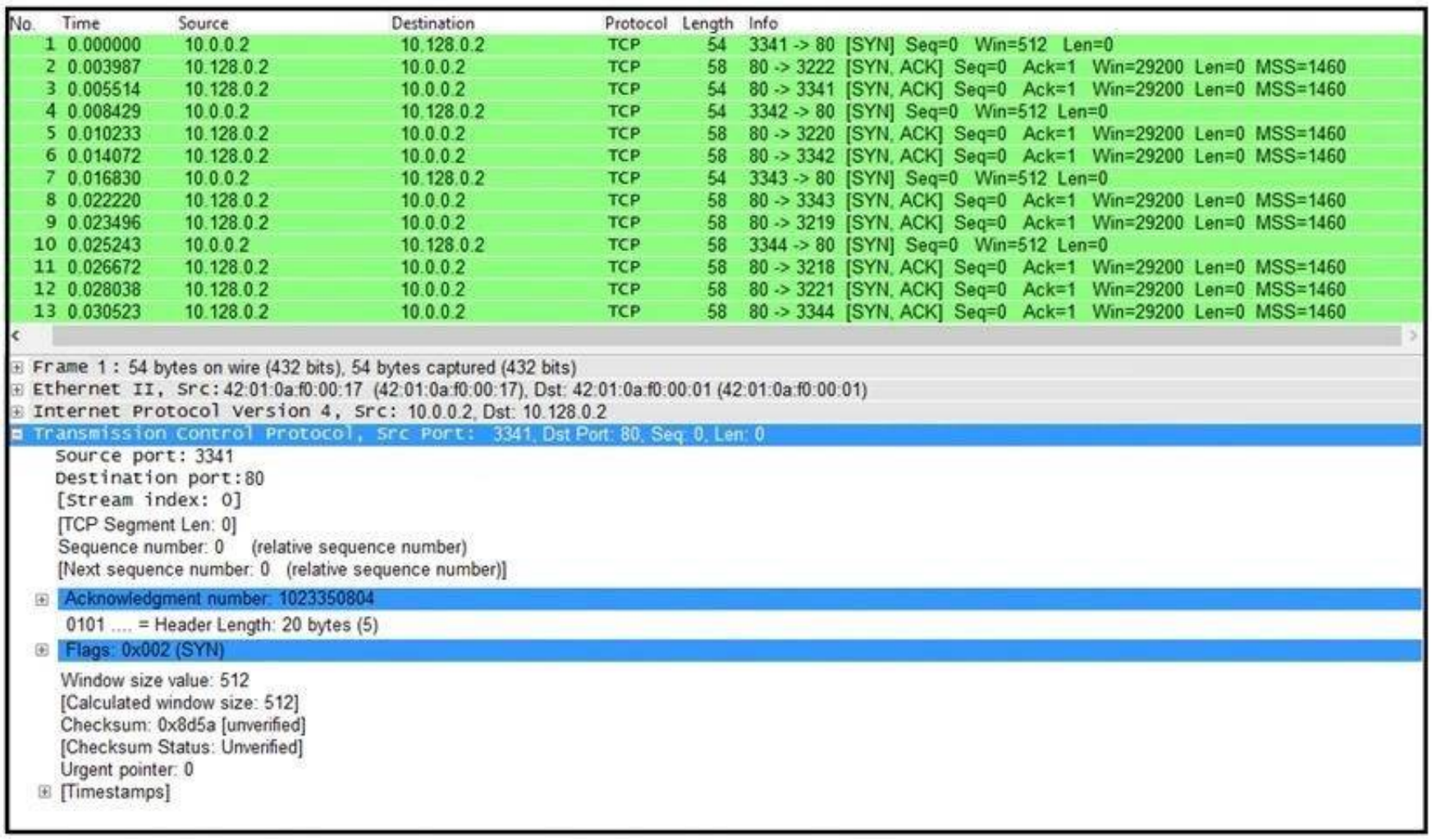
Performing CyberOps Using Core Security Technologies (CBRCOR)

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
Refer to the exhibit.



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 3
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 4
An engineer is investigating several cases of increased incoming spam emails and suspicious emails from the HR and service departments. While checking the event sources, the website monitoring tool showed several web scraping alerts overnight. Which type of compromise is indicated?

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

Answer: C

NEW QUESTION 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

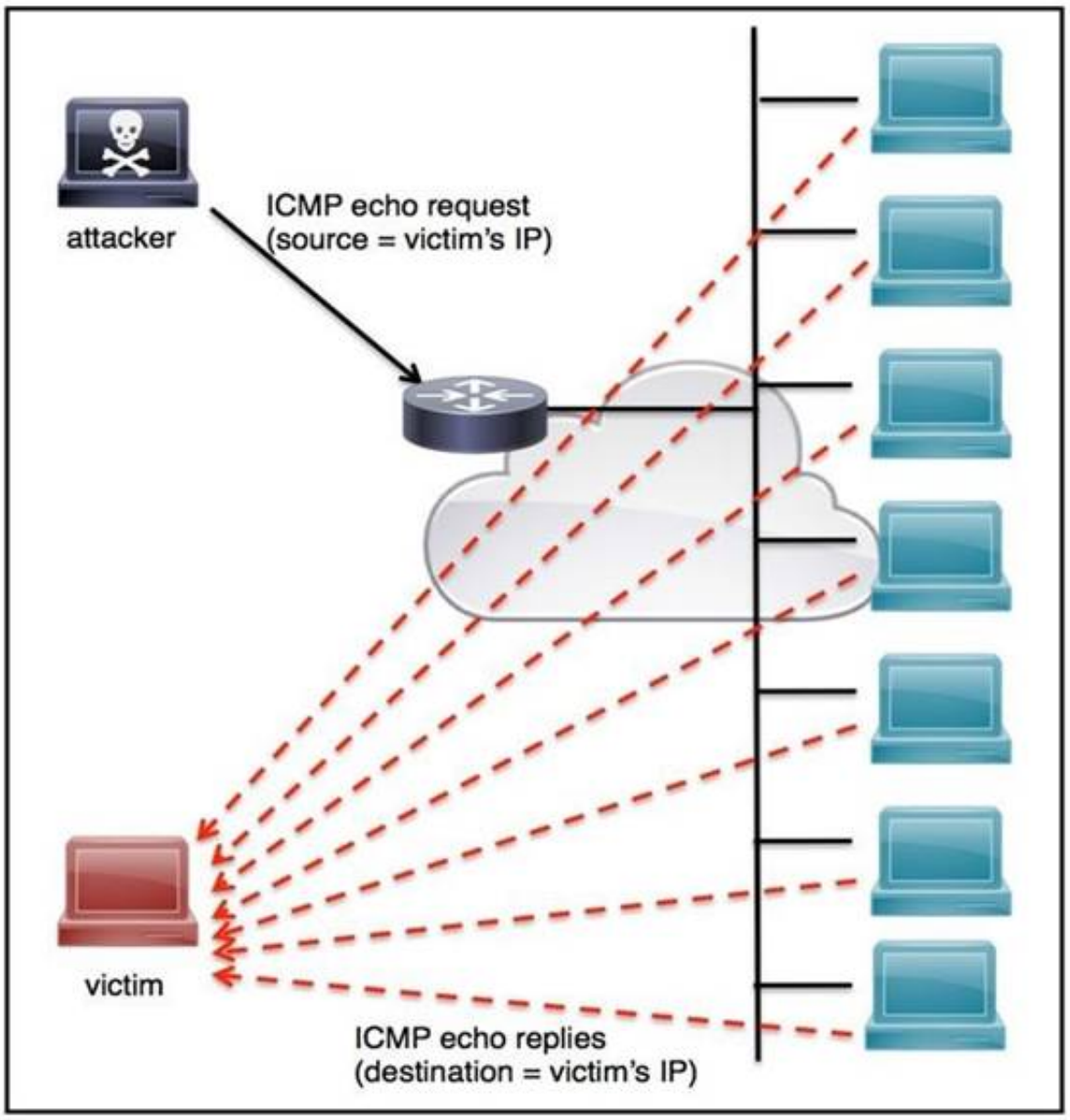
Answer: AB

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
Refer to the exhibit.

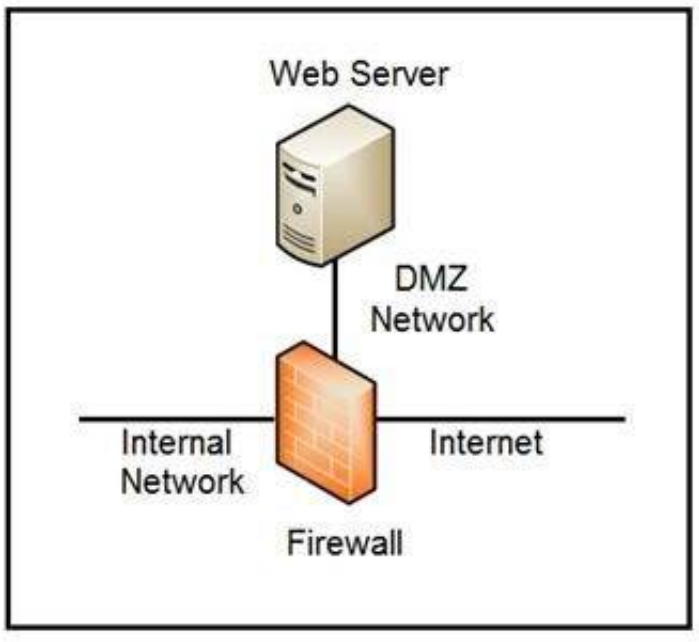


An engineer must tune the Cisco IOS device to mitigate an attack that is broadcasting a large number of ICMP packets. The attack is sending the victim's spoofed source IP to a network using an IP broadcast address that causes devices in the network to respond back to the source IP address. Which action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

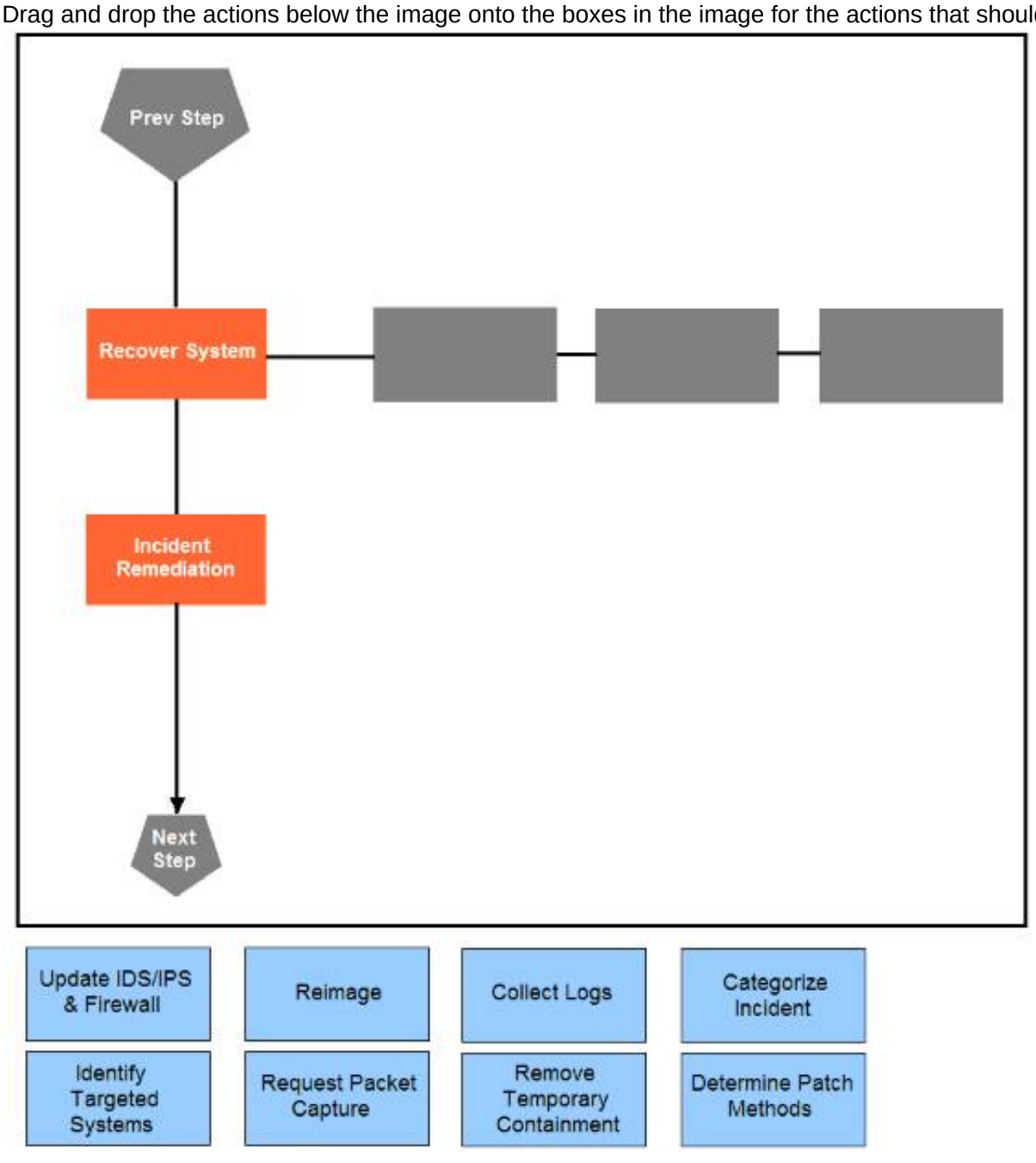
Answer: BD

NEW QUESTION 9
How does Wireshark decrypt TLS network traffic?

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

Answer: A

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

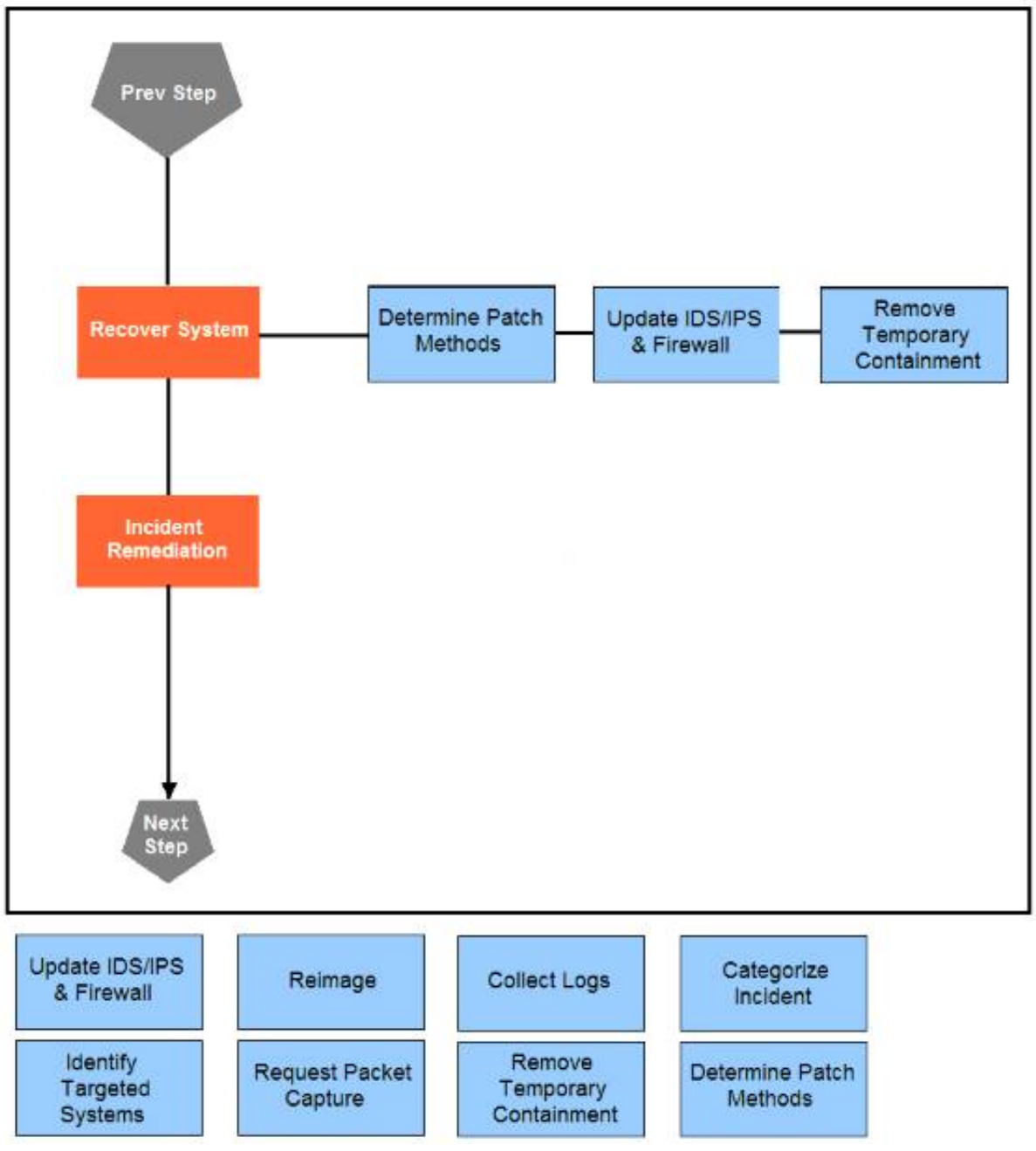


A. Mastered

B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 10
A 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

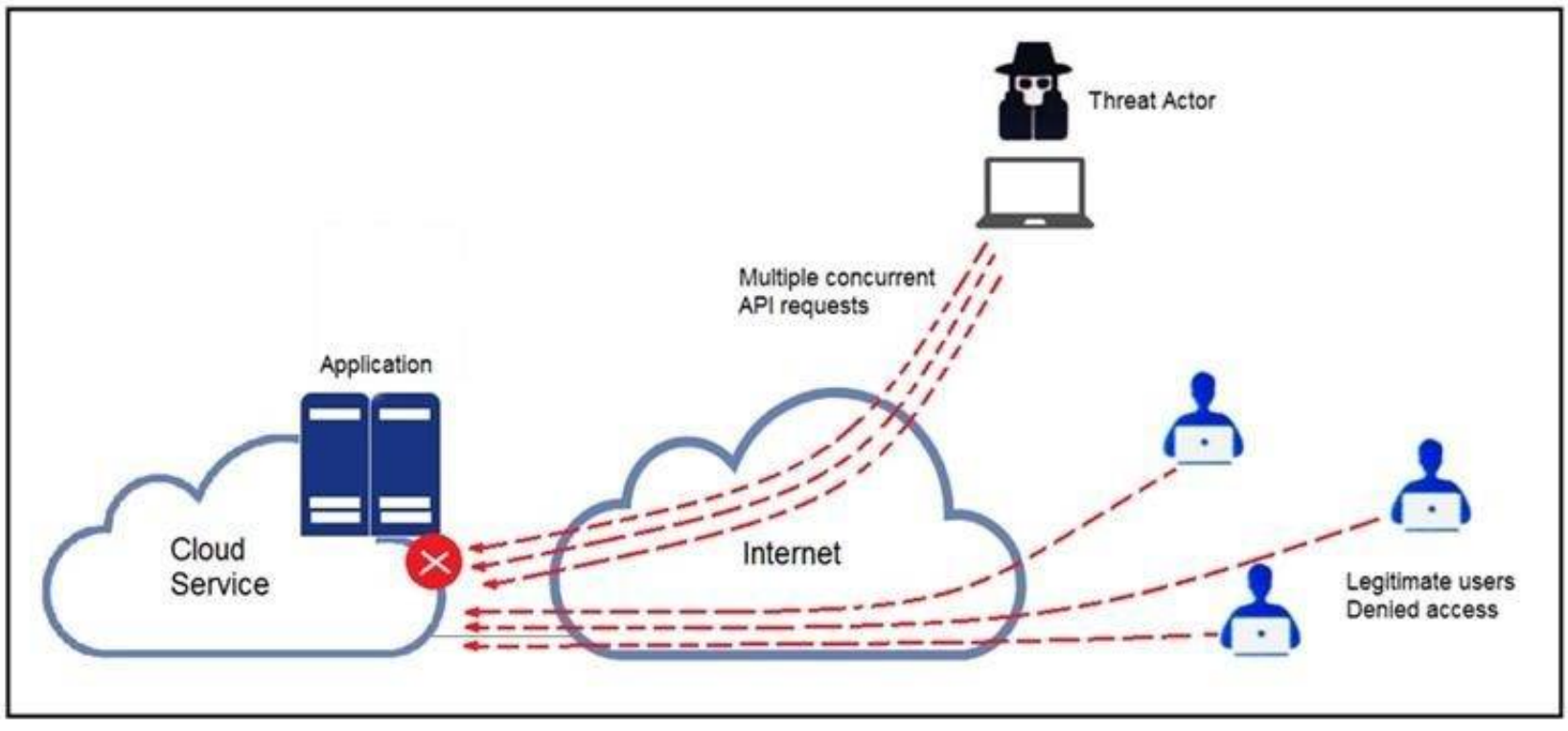
NEW QUESTION 11
Refer to the exhibit.

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 12
Refer to the exhibit.



A threat actor behind a single computer exploited a cloud-based application by sending multiple concurrent API requests. These requests made the application unresponsive. Which solution protects the application from being overloaded and ensures more equitable application access across the end-user community?

A. Limit the number of API calls that a single client is allowed to make
B. Add restrictions on the edge router on how often a single client can access the API
C. Reduce the amount of data that can be fetched from the total pool of active clients that call the API
D. Increase the application cache of the total pool of active clients that call the API

Answer: A

NEW QUESTION 13
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 16
An organization had a breach due to a phishing attack. An engineer leads a team through the recovery phase of the incident response process. Which action should be taken during this phase?

A. Host a discovery meeting and define configuration and policy updates
B. Update the IDS/IPS signatures and reimage the affected hosts
C. Identify the systems that have been affected and tools used to detect the attack
D. Identify the traffic with data capture using Wireshark and review email filters

Answer: C

NEW QUESTION 21
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

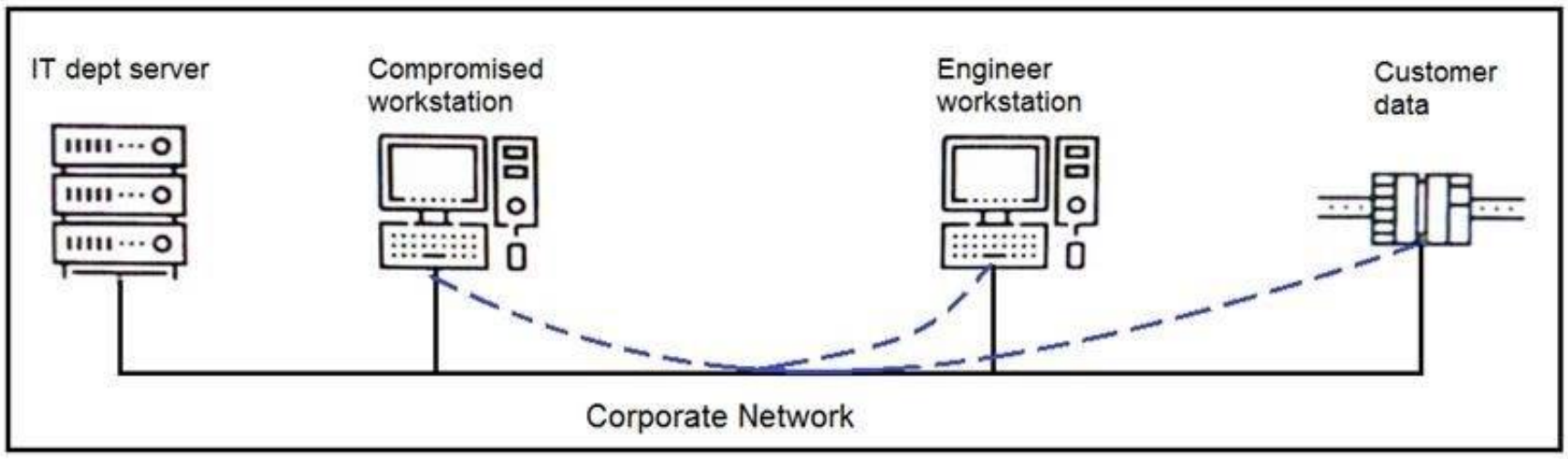
Answer: A

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 24
Refer to the exhibit.



An engineer received a report that an attacker has compromised a workstation and gained access to sensitive customer data from the network using insecure protocols. Which action prevents this type of attack in the future?

A. Use VLANs to segregate zones and the firewall to allow only required services and secured protocols
B. Deploy a SOAR solution and correlate log alerts from customer zones
C. Deploy IDS within sensitive areas and continuously update signatures
D. Use syslog to gather data from multiple sources and detect intrusion logs for timely responses

Answer: A

NEW QUESTION 27
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 30
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 32
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
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 42
A SOC analyst is notified by the network monitoring tool that there are unusual types of internal traffic on IP subnet 103.861.2117.0/24. The analyst discovers unexplained encrypted data files on a computer system that belongs on that specific subnet. What is the cause of the issue?

A. DDoS attack
B. phishing attack
C. virus outbreak
D. malware outbreak

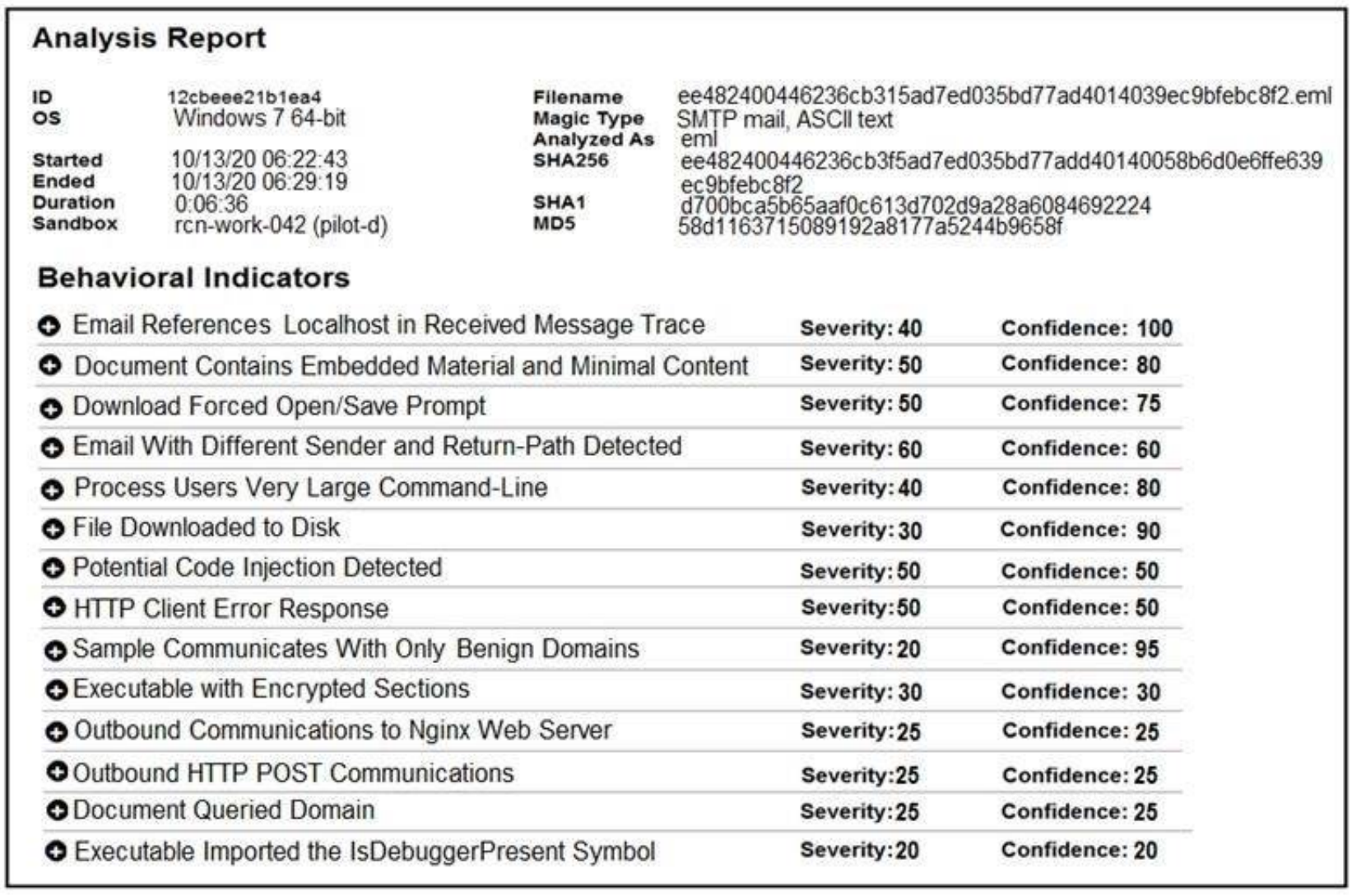
Answer: D

NEW QUESTION 45
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 48
Refer to the exhibit.



Analysis Report

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

Behavioral Indicators

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

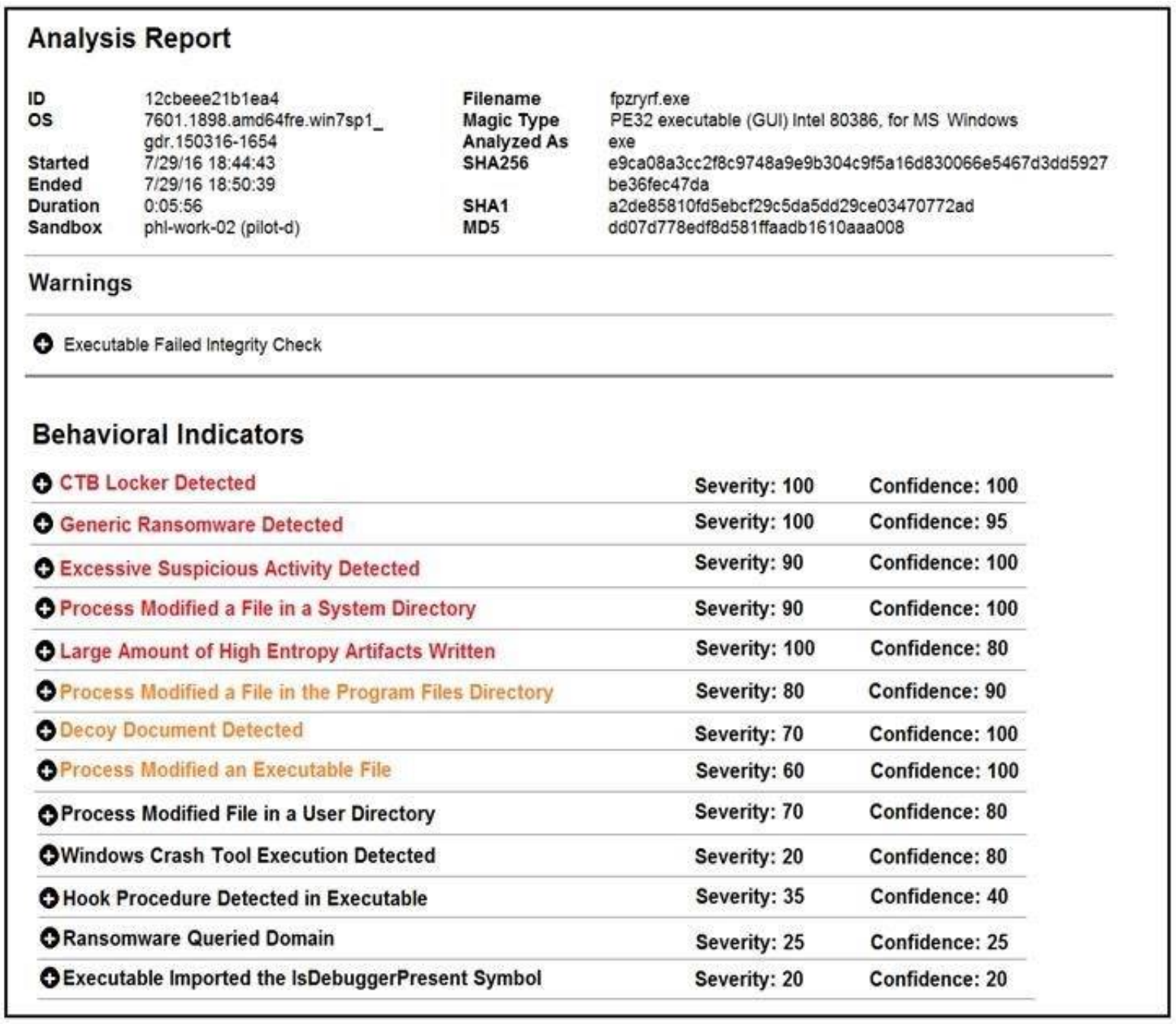
Answer: B

NEW QUESTION 53
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 56
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
		Analyzed As	exe
Started	7/29/16 18:44:43	**SHA256**	e9ca08a3cc2f8c9748a9e9b304c9f5a16d830066e5467d3dd5927be36fec47da
Ended	7/29/16 18:50:39		
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 61
An employee abused PowerShell commands and script interpreters, which lead to an indicator of compromise (IOC) trigger. The IOC event shows that a known malicious file has been executed, and there is an increased likelihood of a breach. Which indicator generated this IOC event?

A. ExecutedMalware.ioc
B. Crossrider.ioc
C. ConnectToSuspiciousDomain.ioc
D. W32 AccesschkUtility.ioc

Answer: D

NEW QUESTION 62
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
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

An employee is a victim of a social engineering phone call and installs remote access software to allow an "MS Support" technician to check his machine for malware. The employee becomes suspicious after the remote technician requests payment in the form of gift cards. The employee has copies of multiple, unencrypted database files, over 400 MB each, on his system and is worried that the scammer copied the files off but has no proof of it. The remote technician was connected sometime between 2:00 pm and 3:00 pm over https. What should be determined regarding data loss between the employee's laptop and the remote technician's system?

A. No database files were disclosed
B. The database files were disclosed
C. The database files integrity was violated
D. The database files were intentionally corrupted, and encryption is possible

Answer: C

NEW QUESTION 66
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 69
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 72
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 74
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 76
Refer to the exhibit.

Vulnerability #1	Vulnerability #2
A vulnerability in the Command Line Interpreter (CLI) of ACME Super Firewall (all models) could allow an attacker to execute a command which would overflow a buffer in memory. In order to carry out this attack, the attacker needs to fulfill all of the following conditions: a) Be logged in to the device over telnet or SSH, or through the local console b) Be logged in as a high-privileges administrative user In order to trigger the vulnerability, the attacker has to execute a command on the device and supply a specially crafted argument to such command. Once the command is executed, an internal stack-based buffer overflow will be triggered. This buffer overflow may lead to code execution within the process space of the CLI parser, or may crash the device. All software versions are affected Fixes are available now There are no workarounds or mitigations	A vulnerability in the web-based management interface of the ACME Big Router models 1010 and 1020 could allow an attacker to bypass authorization checks and then access sensitive information on the device, modify the device's configuration, impact the availability of the system, create administrative level and regular level users on the device. In order to exploit this vulnerability, the attacker needs to: a) Be able to reach port 80/tcp on an affected device b) The web-based management interface needs to be enabled on the device The attacker would then need to send a specially formed HTTP request to the web-based management interface of an affected system. The attacker does not need to log-in to the device before launching the attack. All software versions are affected There are no fixes available now Customers can disable the web-based management interface to prevent exploitation. Customers will still be able to manage, configure and monitor the device by using the Command Line Interface (CLI), but with reduced capabilities for monitoring.

How must these advisories be prioritized for handling?

A. The highest priority for handling depends on the type of institution deploying the devices
B. Vulnerability #2 is the highest priority for every type of institution
C. Vulnerability #1 and vulnerability #2 have the same priority
D. Vulnerability #1 is the highest priority for every type of institution

Answer: D

NEW QUESTION 81
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)

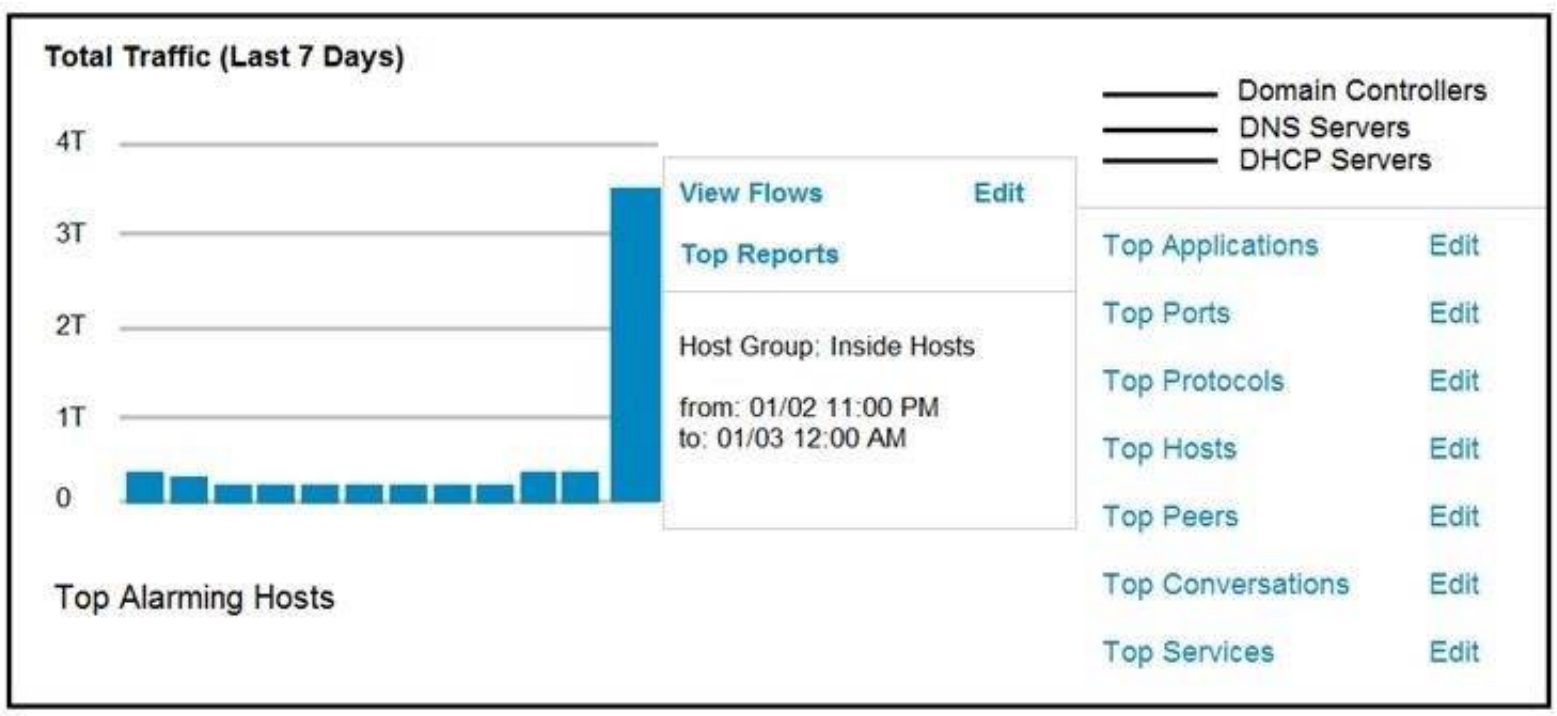
Answer: B

NEW QUESTION 86
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 89
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 93
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 96
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 99
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 104
Refer to the exhibit.

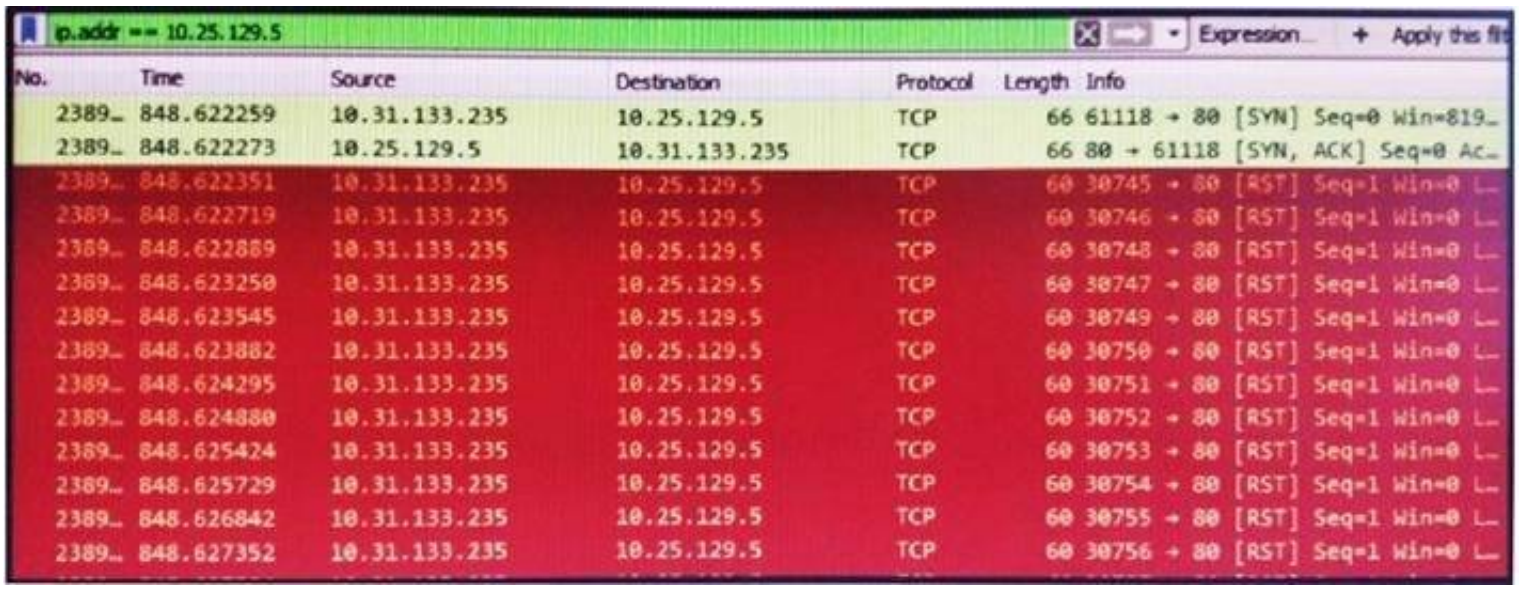
TCP	192.168.1.8:54580	vk-in-f108:imaps	ESTABLISHED
TCP	192.168.1.8:54583	132.245.61.50:https	ESTABLISHED
TCP	192.168.1.8:54916	bay405-m:https	ESTABLISHED
TCP	192.168.1.8:54978	vu-in-f188:5228	ESTABLISHED
TCP	192.168.1.8:55094	72.21.194.109:https	ESTABLISHED
TCP	192.168.1.8:55401	wonderhowto:http	ESTABLISHED
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 107
Refer to the exhibit.



What is occurring in this packet capture?

A. TCP port scan
B. TCP flood
C. DNS flood
D. DNS tunneling

Answer: B

NEW QUESTION 112
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 114
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 116
Refer to the exhibit.

Asset	Threat	Vulnerability	Likelihood (1-10)	Impact (1-10)
Servers	Natural Disasters – Flooding	Server Room is on the zero floor	3	10
Secretary Workstation	Usage of illegitimate software	Inadequate control of software	7	6
Payment Process	Eavesdropping, Misrouting/re-routing of messages	Unencrypted communications	5	10
Website	Website Intrusion	No IDS/IPS usage	6	8

Which asset has the highest risk value?

A. servers
B. website
C. payment process
D. secretary workstation

Answer: C

NEW QUESTION 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 125
.....

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