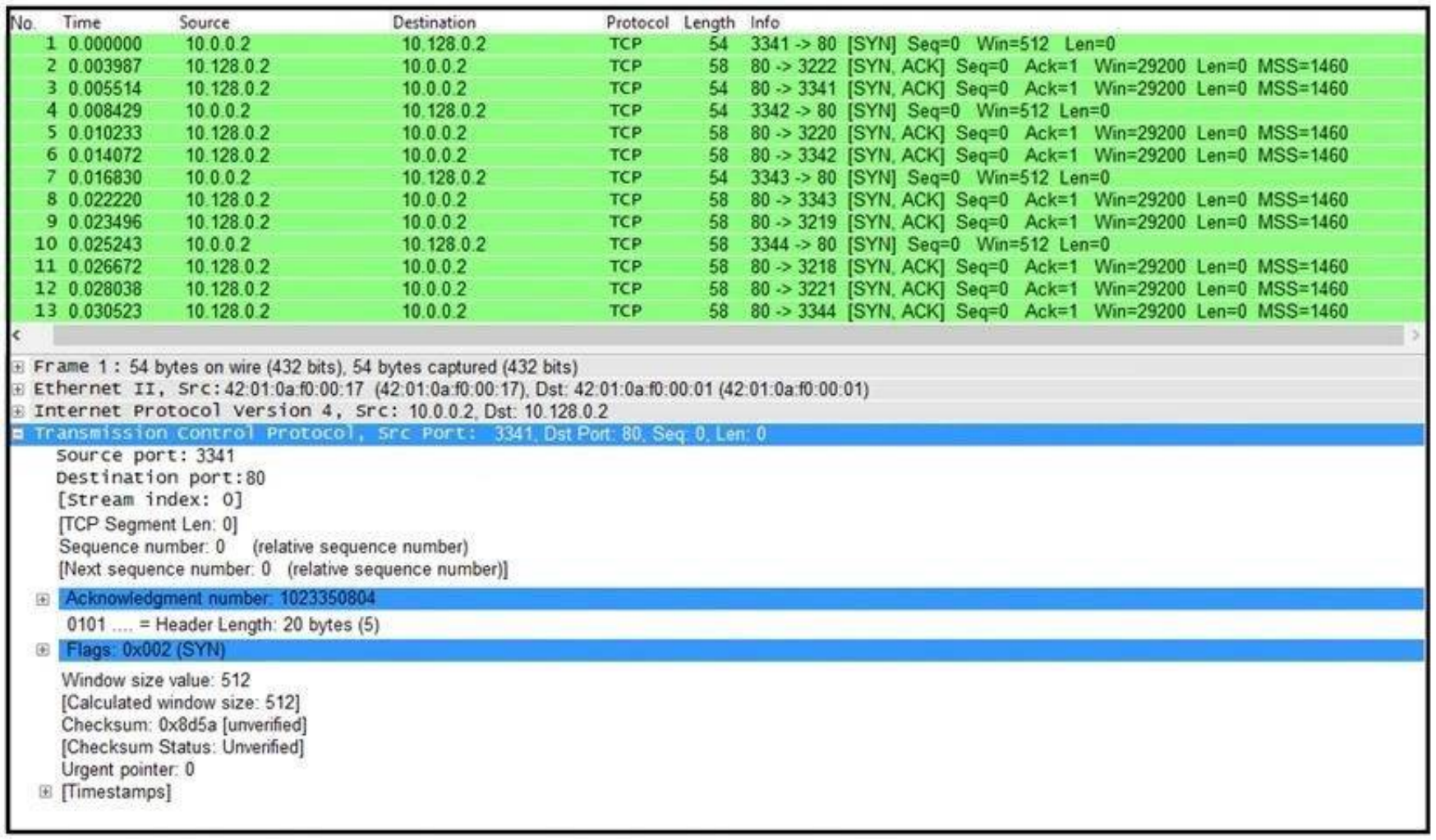
Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)

https://www.2passeasy.com/dumps/350-201/

NEW QUESTION 1
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 2
Drag and drop the mitigation steps from the left onto the vulnerabilities they mitigate on the right.

Answer Area

Restrict administrative access to operating systems and applications in accordance with job duties	End-user desktops allow the execution of non-approved applications that include malicious code
Use multifactor authentication for remote access or accessing sensitive information	Application security vulnerabilities can be used to execute malicious code
Change backup and store software and configuration settings for at least three months	Privilege accounts have full rights to information systems
Patch applications including flash, web browsers, and PDF viewers	User verification is weak and based on a single factor
Utilize application control to stop malware delivery and execution	Data or access loss occurs due to cybersecurity incidents

A. Mastered
B. Not Mastered

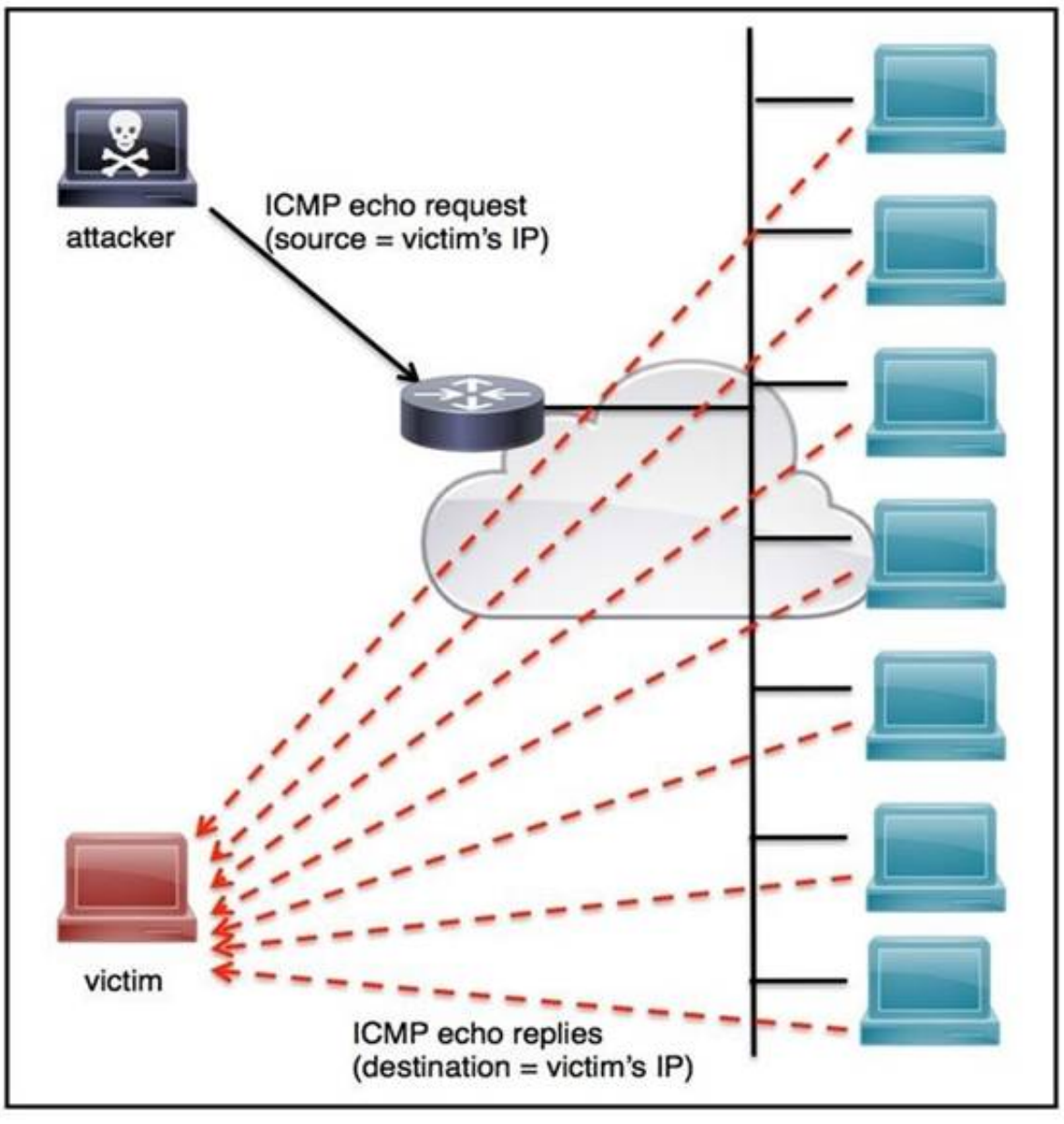
Answer: A

Explanation:

Answer Area

Restrict administrative access to operating systems and applications in accordance with job duties	Utilize application control to stop malware delivery and execution
Use multifactor authentication for remote access or accessing sensitive information	Patch applications including flash, web browsers, and PDF viewers
Change backup and store software and configuration settings for at least three months	Restrict administrative access to operating systems and applications in accordance with job duties
Patch applications including flash, web browsers, and PDF viewers	Use multifactor authentication for remote access or accessing sensitive information
Utilize application control to stop malware delivery and execution	Change backup and store software and configuration settings for at least three months

NEW QUESTION 3
Refer to the exhibit.



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

A. Use command ip verify reverse-path interface
B. Use global configuration command service tcp-keepalives-out
C. Use subinterface command no ip directed-broadcast
D. Use logging trap 6

Answer: A

NEW QUESTION 4
Refer to the exhibit.

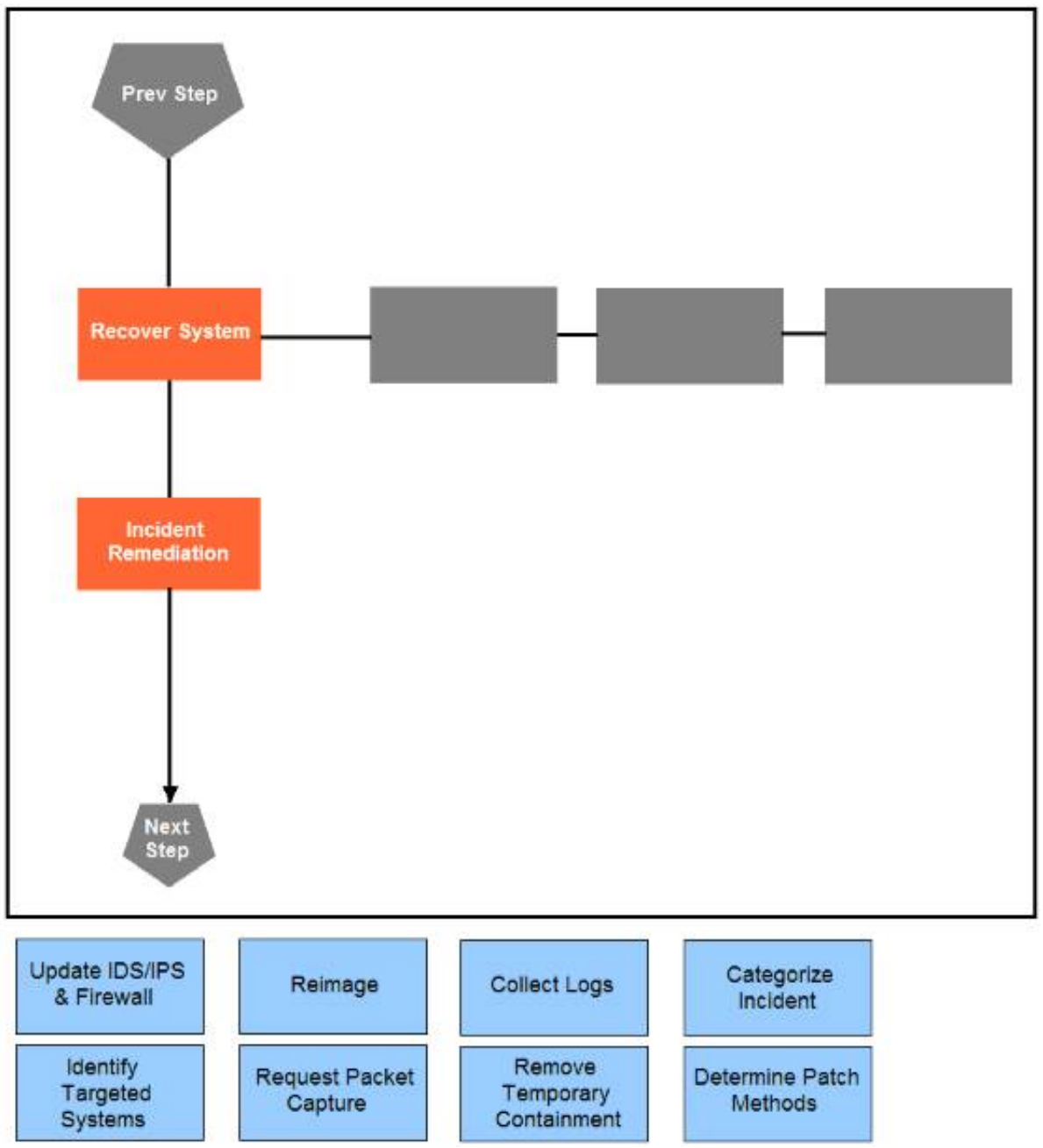

```
{
  "type": "bundle",
  "id": "bundle--56be2a39",
  "objects": [
      {
        "type": "indicator",
        "spec_version": "2.1",
        "id": "indicator--d81f86b9-9f",
        "created": "2020-08-10T13:49:37.079Z",
        "modified": "2020-08-10T13:49:37.079Z",
        "name": "Malicious site 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

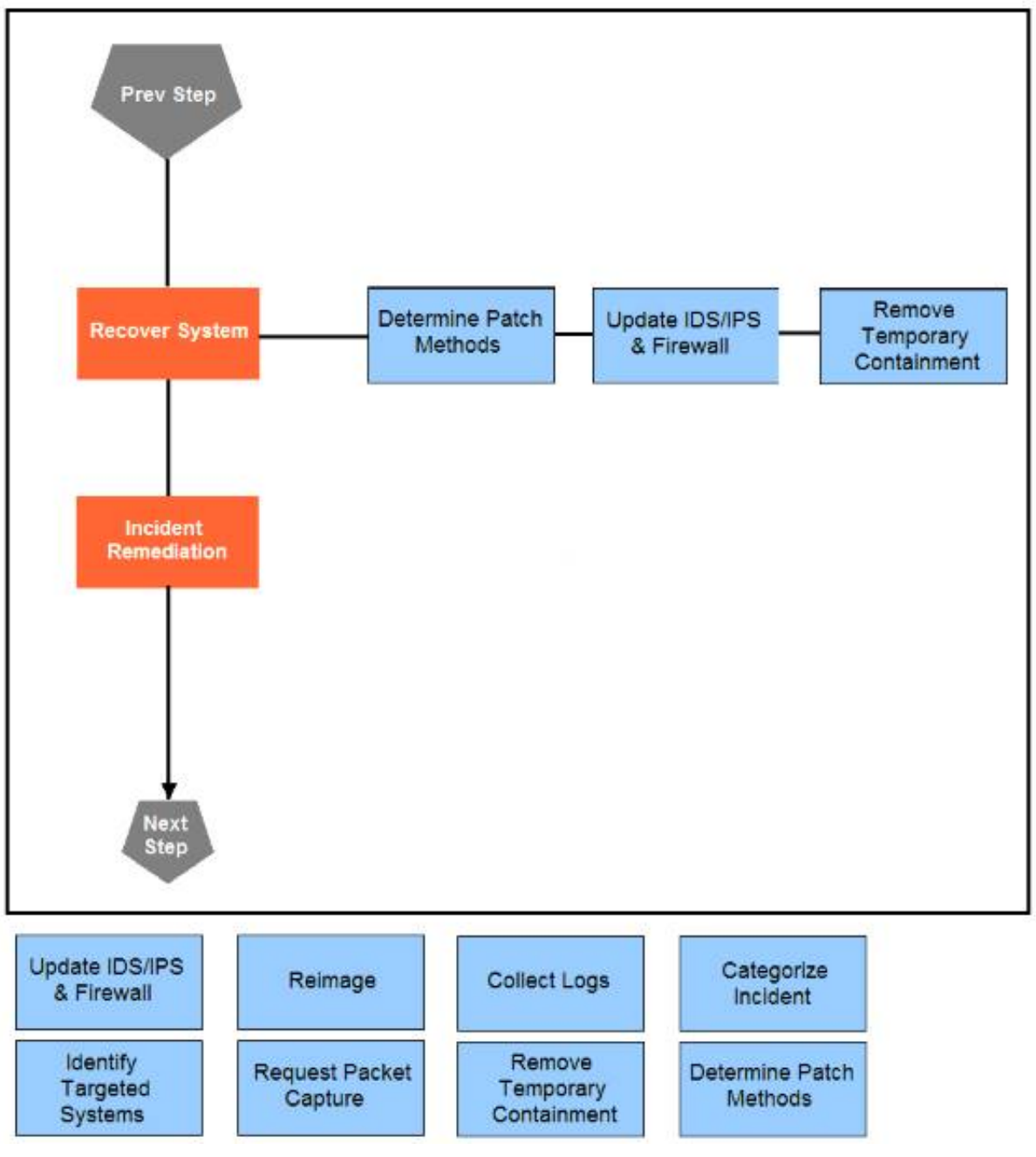
NEW QUESTION 5
Drag and drop the actions below the image onto the boxes in the image for the actions that should be taken during this playbook step. Not all options are used.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 6
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

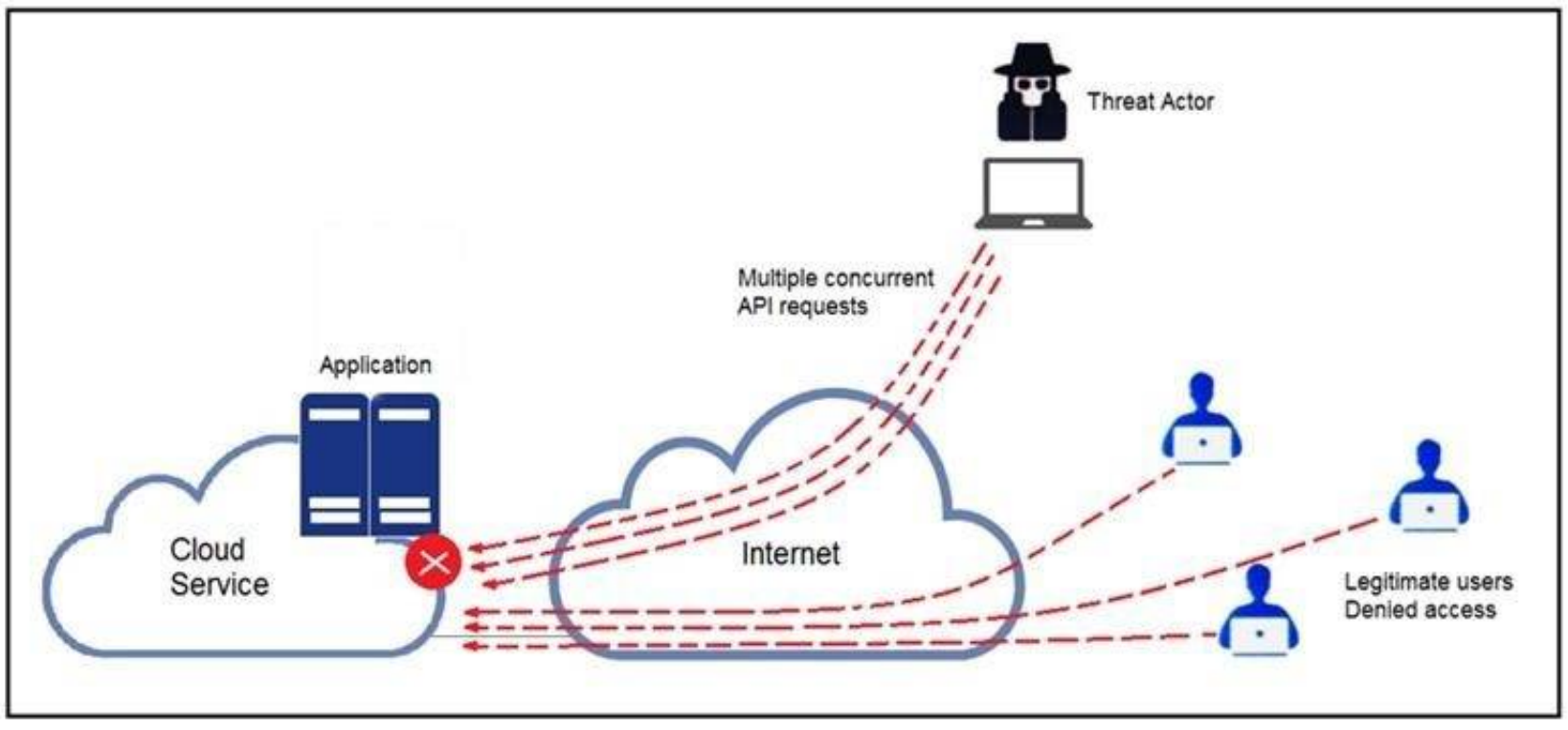
Answer: C

NEW QUESTION 7
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 8
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 9
What is the purpose of hardening systems?

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

Answer: A

NEW QUESTION 10
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 10
An organization installed a new application server for IP phones. An automated process fetched user credentials from the Active Directory server, and the application will have access to on-premises and cloud services. Which security threat should be mitigated first?

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

Answer: B

NEW QUESTION 11
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 15
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 17
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 22
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 26
An analyst is alerted for a malicious file hash. After analysis, the analyst determined that an internal workstation is communicating over port 80 with an external server and that the file hash is associated with Duqu malware. Which tactics, techniques, and procedures align with this analysis?

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

Answer: A

NEW QUESTION 31
An engineer is moving data from NAS servers in different departments to a combined storage database so that the data can be accessed and analyzed by the organization on-demand. Which data management process is being used?

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

Answer: A

NEW QUESTION 36
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 39
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 42
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 44
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 48
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 53
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 56
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 58
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 60
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 64
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 65
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 68

.....

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