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.

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
How is a SIEM tool used?

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

Answer: D

NEW QUESTION 3
Drag and drop the telemetry-related considerations from the left onto their cloud service models on the right.

Answer Area

Logs, alerts, and events for application performance monitoring and application health are configurable by the customer	SaaS
The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited	PaaS
Logs, alerts, and events for operating systems are configurable by the customer	IaaS

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Logs, alerts, and events for application performance monitoring and application health are configurable by the customer	The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited
The customer controls limited application configuration settings and obtaining logs for security monitoring may be limited	Logs, alerts, and events for operating systems are configurable by the customer
Logs, alerts, and events for operating systems are configurable by the customer	Logs, alerts, and events for application performance monitoring and application health are configurable by the customer

NEW QUESTION 4
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 previoulsy 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

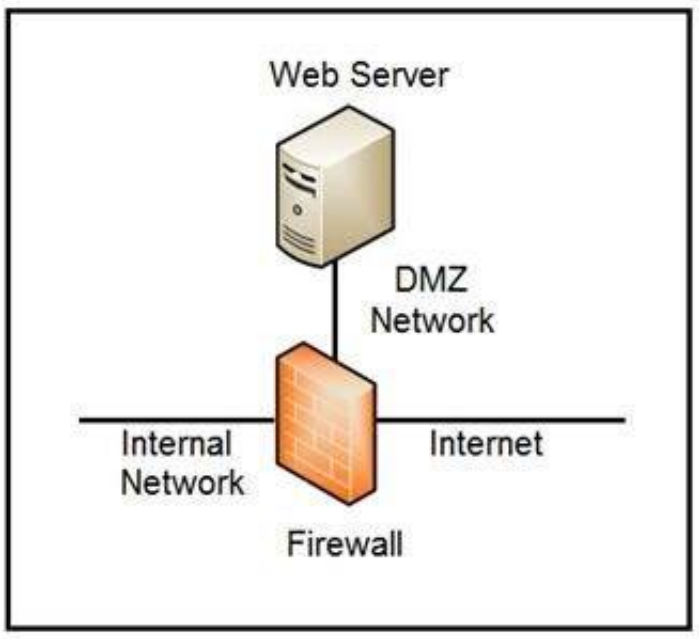
vulnerability assessment	persistence
persistence	reconnaissance
exploit	vulnerability assessment
cover tracks	exploit
reconnaissance	enumeration
enumeration	cover tracks

NEW QUESTION 5
Employees report computer system crashes within the same week. An analyst is investigating one of the computers that crashed and discovers multiple shortcuts in the system's startup folder. It appears that the shortcuts redirect users to malicious URLs. What is the next step the engineer should take to investigate this case?

A. Remove the shortcut files
B. Check the audit logs
C. Identify affected systems
D. Investigate the malicious URLs

Answer: C

NEW QUESTION 6
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 7
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

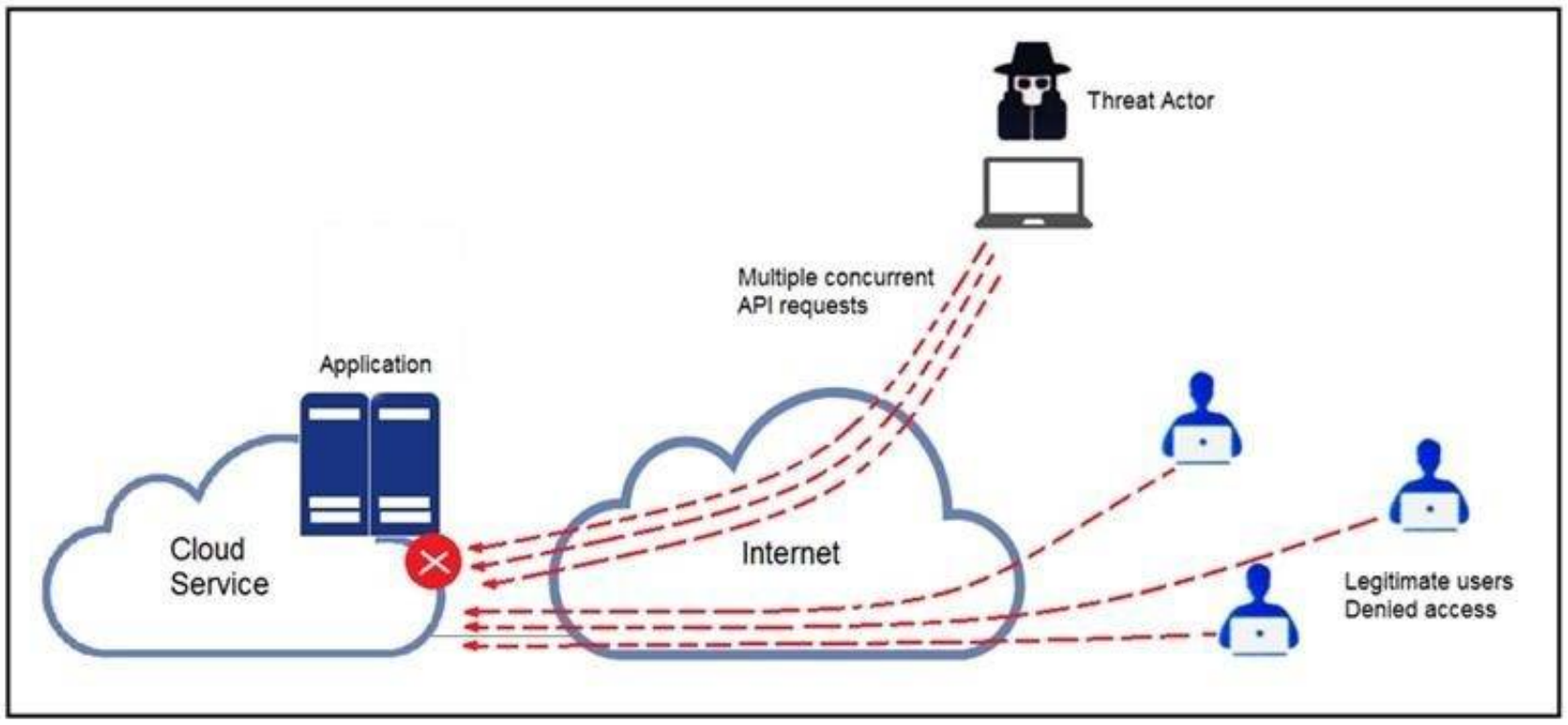
Answer: A

NEW QUESTION 8
What is a limitation of cyber security risk insurance?

A. It does not cover the costs to restore stolen identities as a result of a cyber attack
B. It does not cover the costs to hire forensics experts to analyze the cyber attack
C. It does not cover the costs of damage done by third parties as a result of a cyber attack
D. It does not cover the costs to hire a public relations company to help deal with a cyber attack

Answer: A

NEW QUESTION 9
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 10
An engineer has created a bash script to automate a complicated process. During script execution, this error occurs: permission denied. Which command must be added to execute this script?

A. chmod +x ex.sh
B. source ex.sh
C. chroot ex.sh
D. sh ex.sh

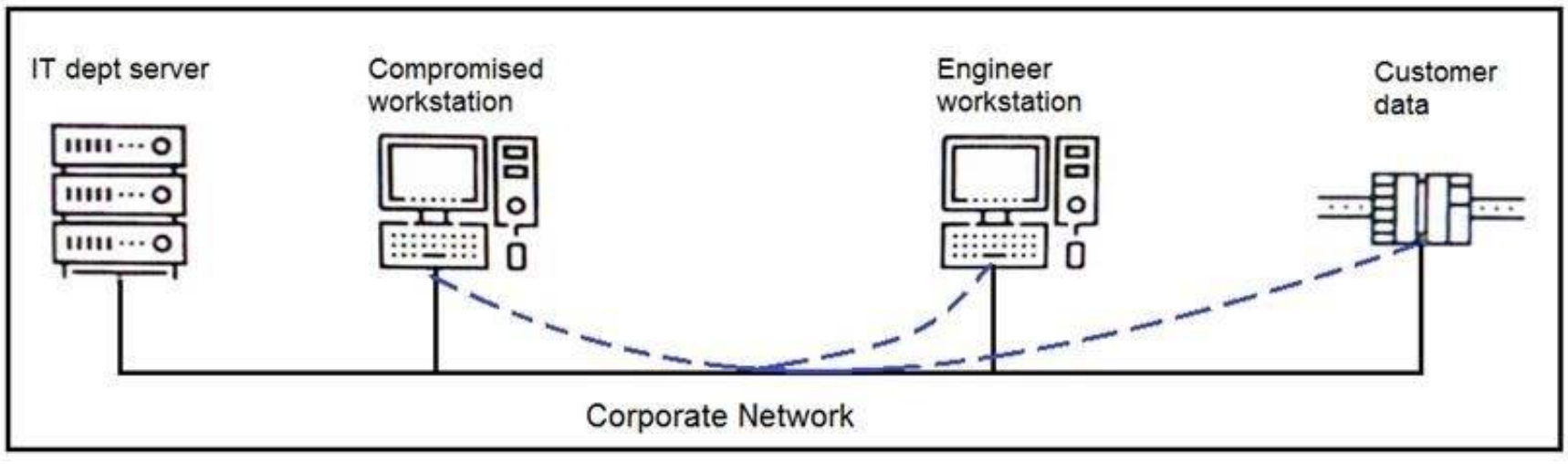
Answer: A

NEW QUESTION 10
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 14
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 16
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 19
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 23
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 27
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 29
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 33
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 35
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 38
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

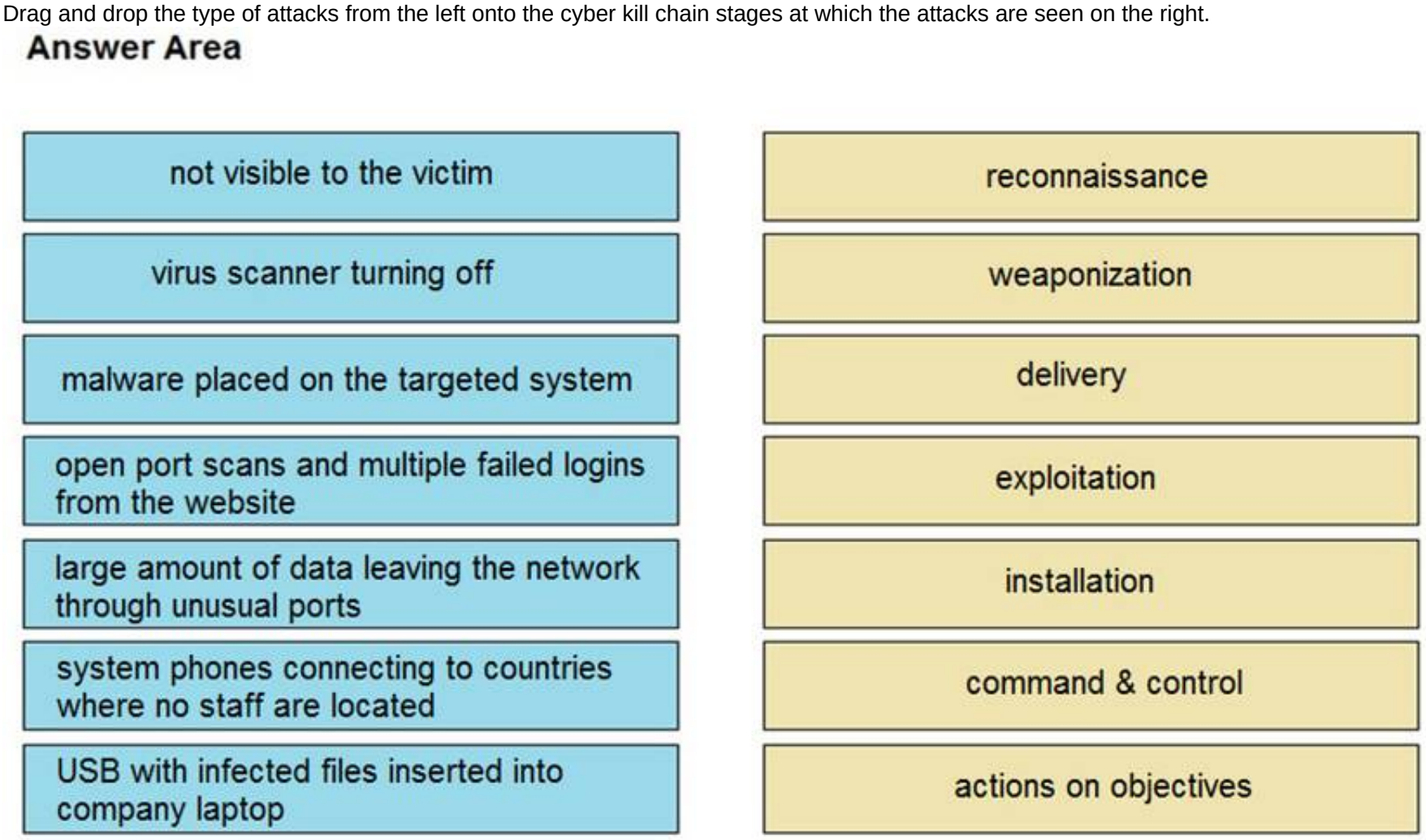
The application administrator has to manually change and track these daily to ensure compliance. An engineer is tasked to implement a script to automate the process according to the company user creation policy. The engineer implemented this piece of code within the application, but users are still able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

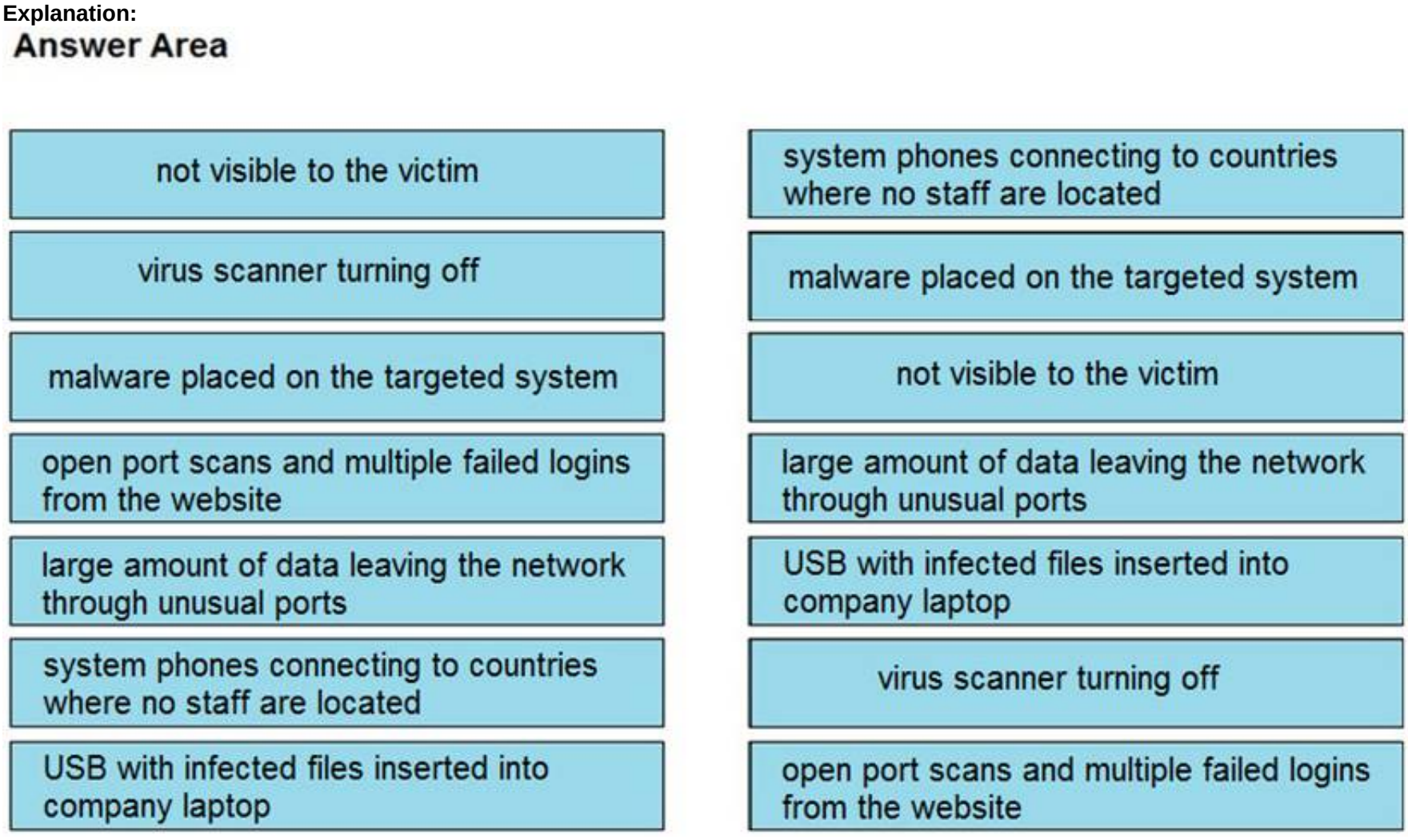
NEW QUESTION 40
Drag and drop the type of attacks from the left onto the cyber kill chain stages at which the attacks are seen on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 42
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 44
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 48
.....

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