350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.lead4pass.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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

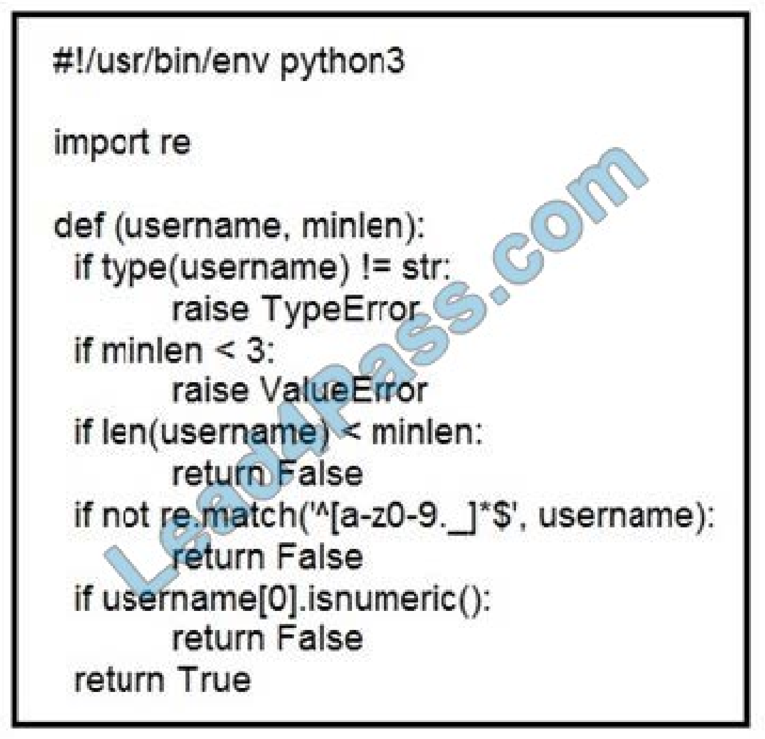
C. Conduct penetration testing

D. Perform awareness testing

Correct Answer: B

Reference: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/DPIA-Guide.pdf

QUESTION 2



```
#!/usr/bin/env python3

impcrt 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
```

Refer to the exhibit. 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)

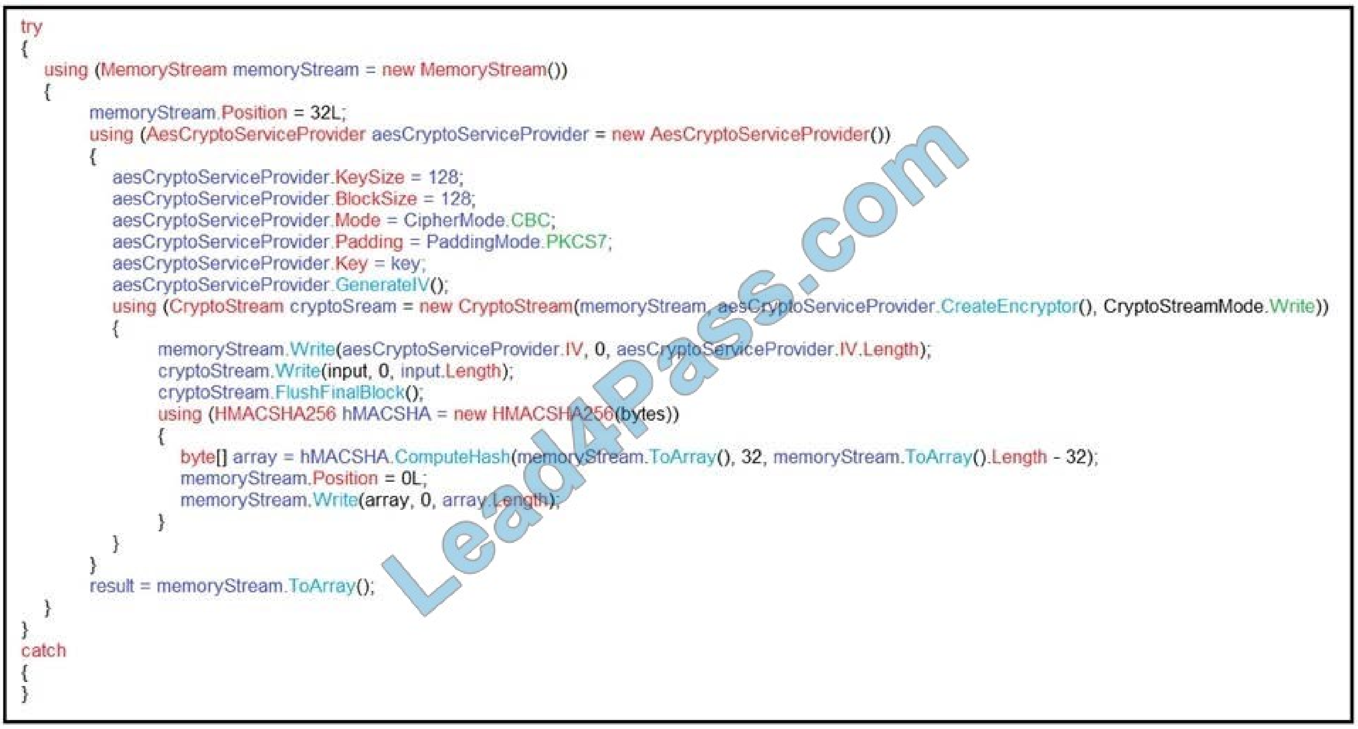
B. automate the restrictions def automate_user(username, minlen)

C. validate the restrictions, def validate_user(username, minlen)

D. modify code to force the restrictions, def force_user(username, minlen)

Correct Answer: B

QUESTION 3



```
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
{
}
```

Refer to the exhibit. 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.

Correct Answer: B

QUESTION 4

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

A. Assess the network for unexpected behavior

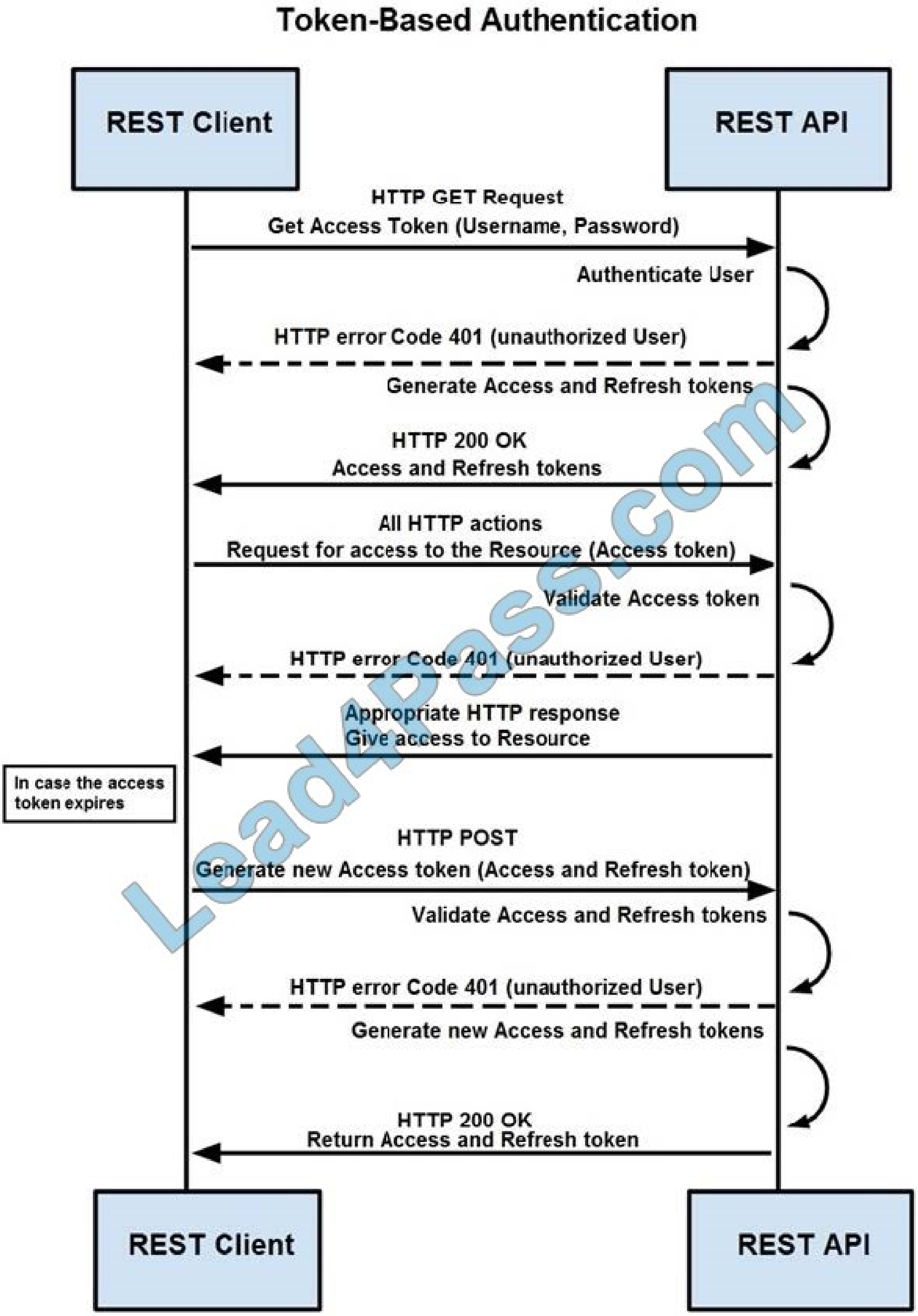
B. Isolate critical hosts from the network

C. Patch detected vulnerabilities from critical hosts

D. Perform analysis based on the established risk factors

Correct Answer: B

QUESTION 5


Token-Based Authentication
REST Client
REST API
HTTP GET Request
Get Access Token (Username, Password)
Authenticate User
HTTP error Code 401 (unauthorized User)
Generate Access and Refresh tokens
HTTP 200 OK
Access and Refresh tokens
All HTTP actions
Request for access to the Resource (Access token)
Validate Access token
HTTP error Code 401 (unauthorized User)
Appropriate HTTP response
Give access to Resource
In case the access token expires
HTTP POST
Generate new Access token (Access and Refresh token)
Validate Access and Refresh tokens
HTTP error Code 401 (unauthorized User)
Generate new Access and Refresh tokens
HTTP 200 OK
Return Access and Refresh token
REST Client
REST API

Refer to the exhibit. How are tokens authenticated when the REST API on a device is accessed from a REST API client?

A. The token is obtained by providing a password. The REST client requests access to a resource using the access token. The REST API validates the access token and gives access to the resource.

B. The token is obtained by providing a password. The REST API requests access to a resource using the access token, validates the access token, and gives access to the resource.

C. The token is obtained before providing a password. The REST API provides resource access, refreshes tokens, and returns them to the REST client. The REST client requests access to a resource using the access token.

D. The token is obtained before providing a password. The REST client provides access to a resource using the access token. The REST API encrypts the access token and gives access to the resource.

Correct Answer: D

QUESTION 6

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

Correct Answer: C

QUESTION 7

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

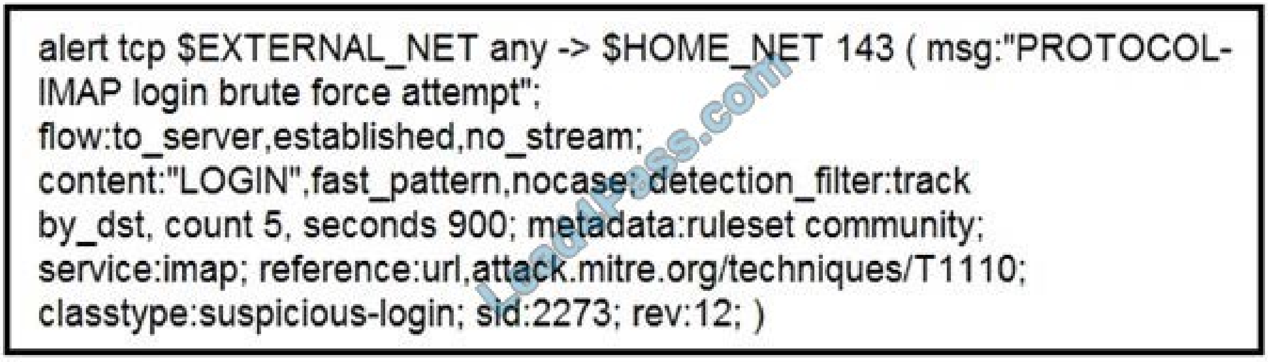
C. DLP for data in use

D. DLP for data at rest

Correct Answer: C

Reference: https://www.endpointprotector.com/blog/what-is-data-loss-prevention-dlp/

QUESTION 8



```
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; )
```

Refer to the exhibit. 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

Correct Answer: B

QUESTION 9

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

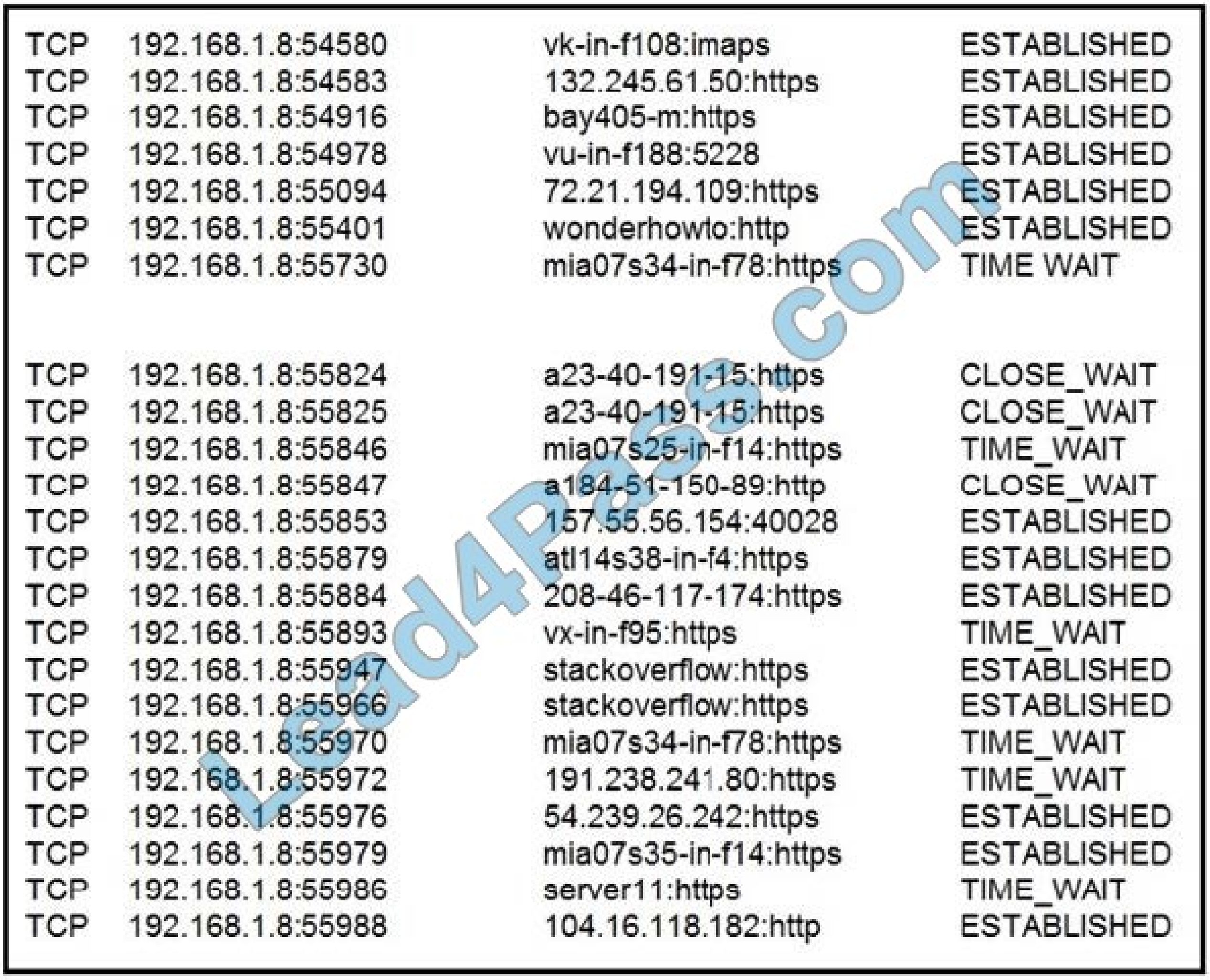
D. It does not cover the costs to hire a public relations company to help deal with a cyber attack

Correct Answer: A

Reference: https://tplinsurance.com/products/cyber-risk-insurance/

QUESTION 10

Refer to the exhibit. 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?



```
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. packet sniffer

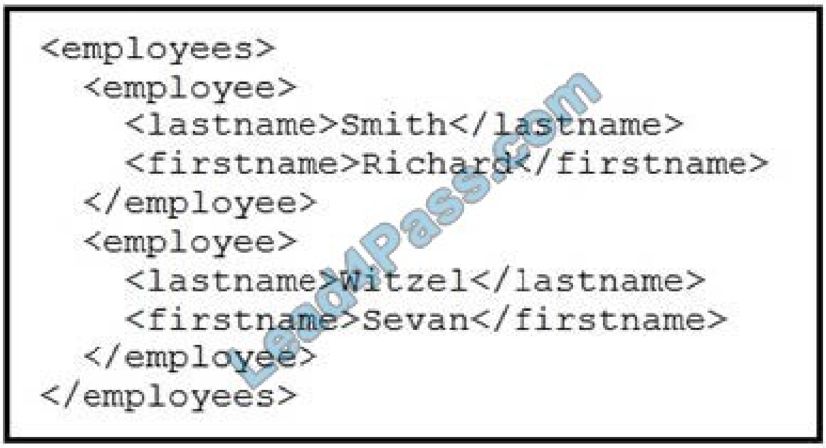
B. malware analysis

C. SIEM

D. firewall manager

Correct Answer: A

QUESTION 11



```
<employees>
  <employee>
    <lastname>Smith</lastname>
    <firstname>Richard</firstname>
  </employee>
  <employee>
    <lastname>Witzel</lastname>
    <firstname>Sevan</firstname>
  </employee>
</employees>
```

Refer to the exhibit. Which data format is being used?

A. JSON

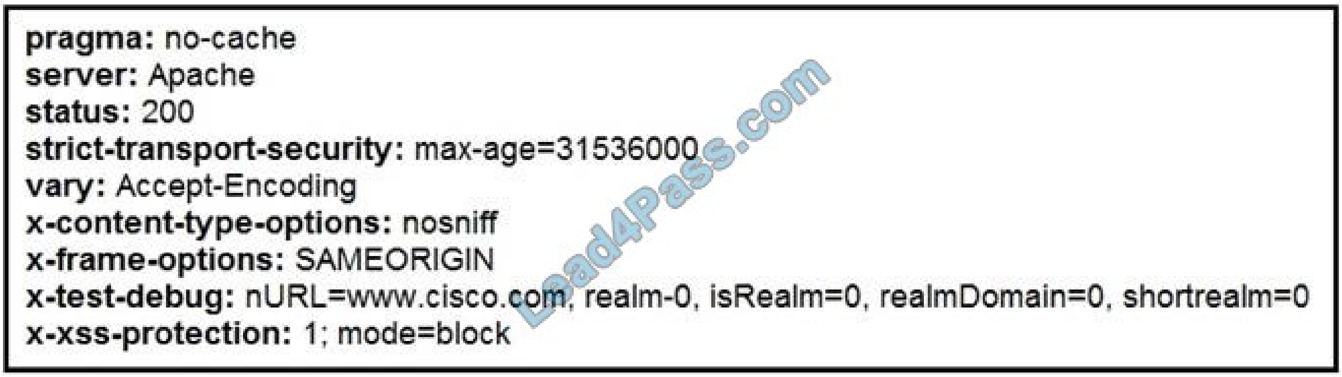
B. HTML

C. XML

D. CSV

Correct Answer: B

QUESTION 12



```
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
```

Refer to the exhibit. 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

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/customize-http-security-headers-ad-fs

QUESTION 13

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

Correct Answer: B

QUESTION 14

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

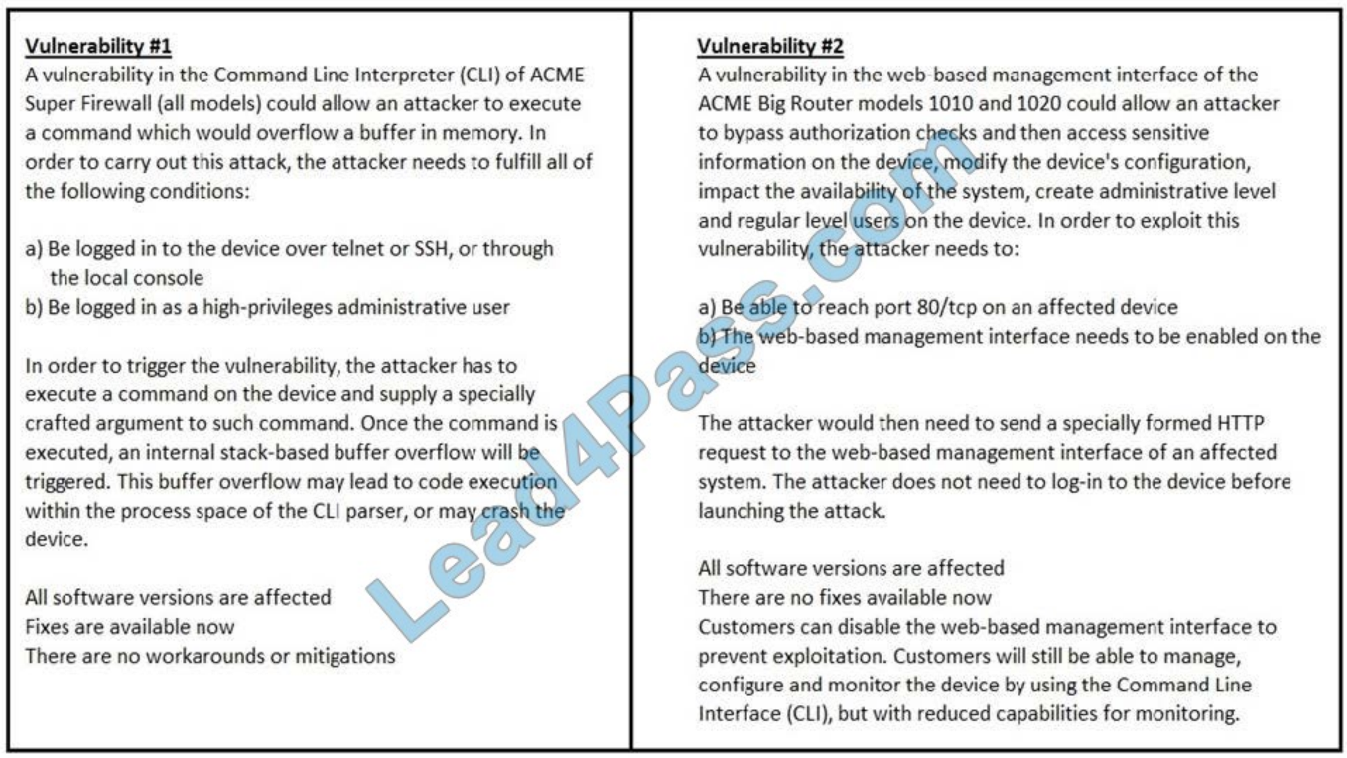
C. port UDP 161 and 162

D. UDP small services

Correct Answer: A

Reference: https://nvd.nist.gov/vuln/detail/CVE-2018-0161

QUESTION 15



Vulnerability #1

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

Vulnerability #2

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.

Refer to the exhibit. How must these advisories be prioritized for handling?

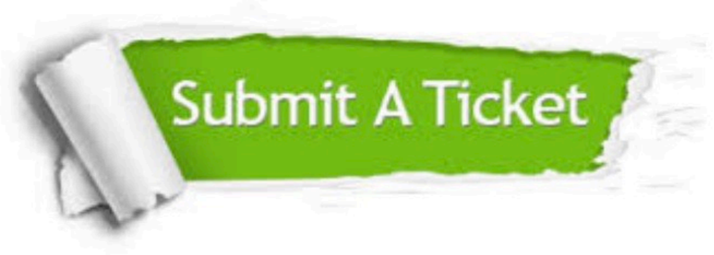
A. The highest priority for handling depends on the type of institution deploying the devices

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

Correct Answer: D


Submit A Ticket