350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Question 1:

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

Correct Answer: A

Question 2:

An engineer received an alert of a zero-day vulnerability affecting desktop phones through which an attacker sends a crafted packet to a device, resets the credentials, makes the device unavailable, and allows a default administrator account login.

Which step should an engineer take after receiving this alert?

A. Initiate a triage meeting to acknowledge the vulnerability and its potential impact

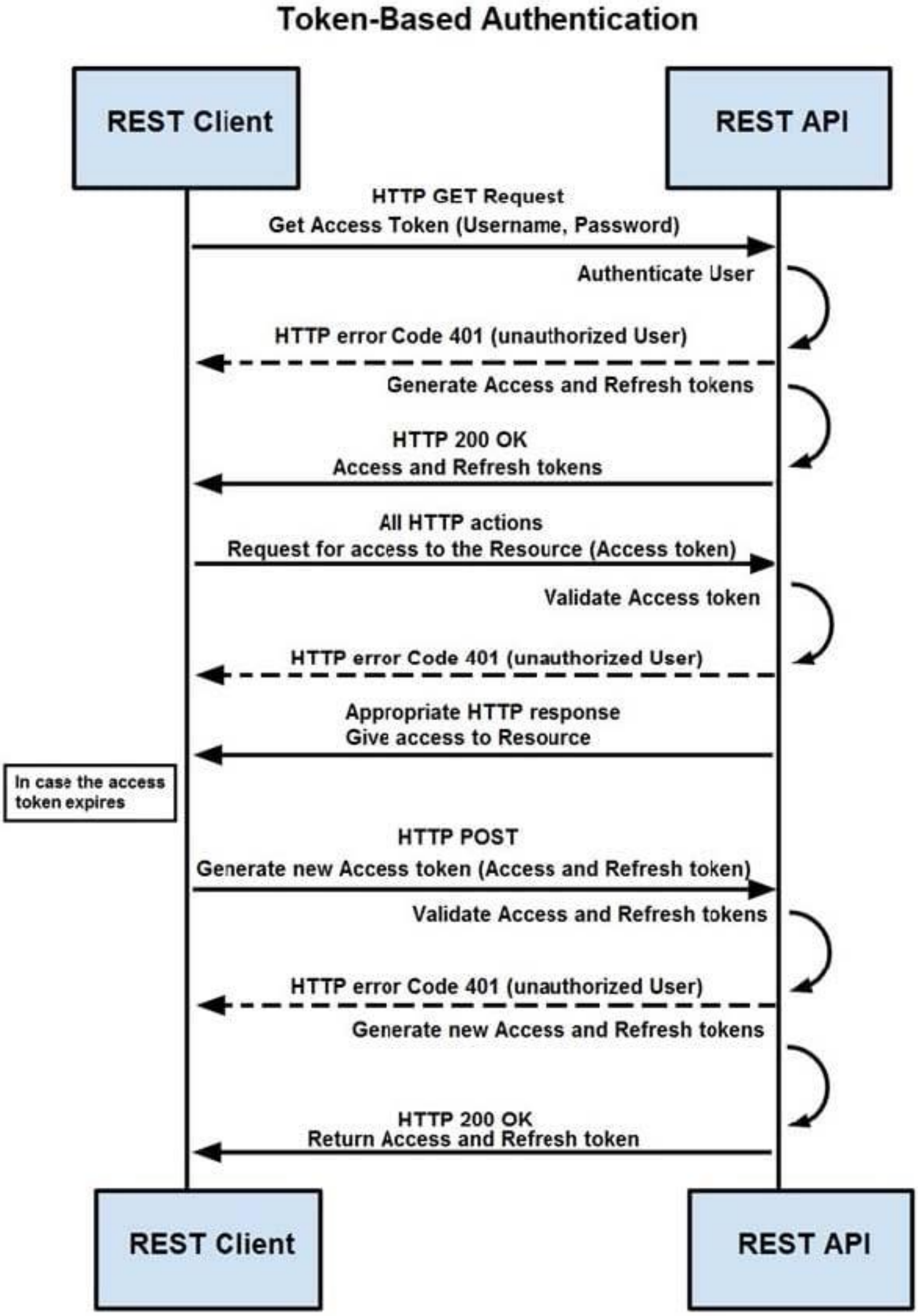
B. Determine company usage of the affected products

C. Search for a patch to install from the vendor

D. Implement restrictions within the VoIP VLANS

Correct Answer: C

Question 3:


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.

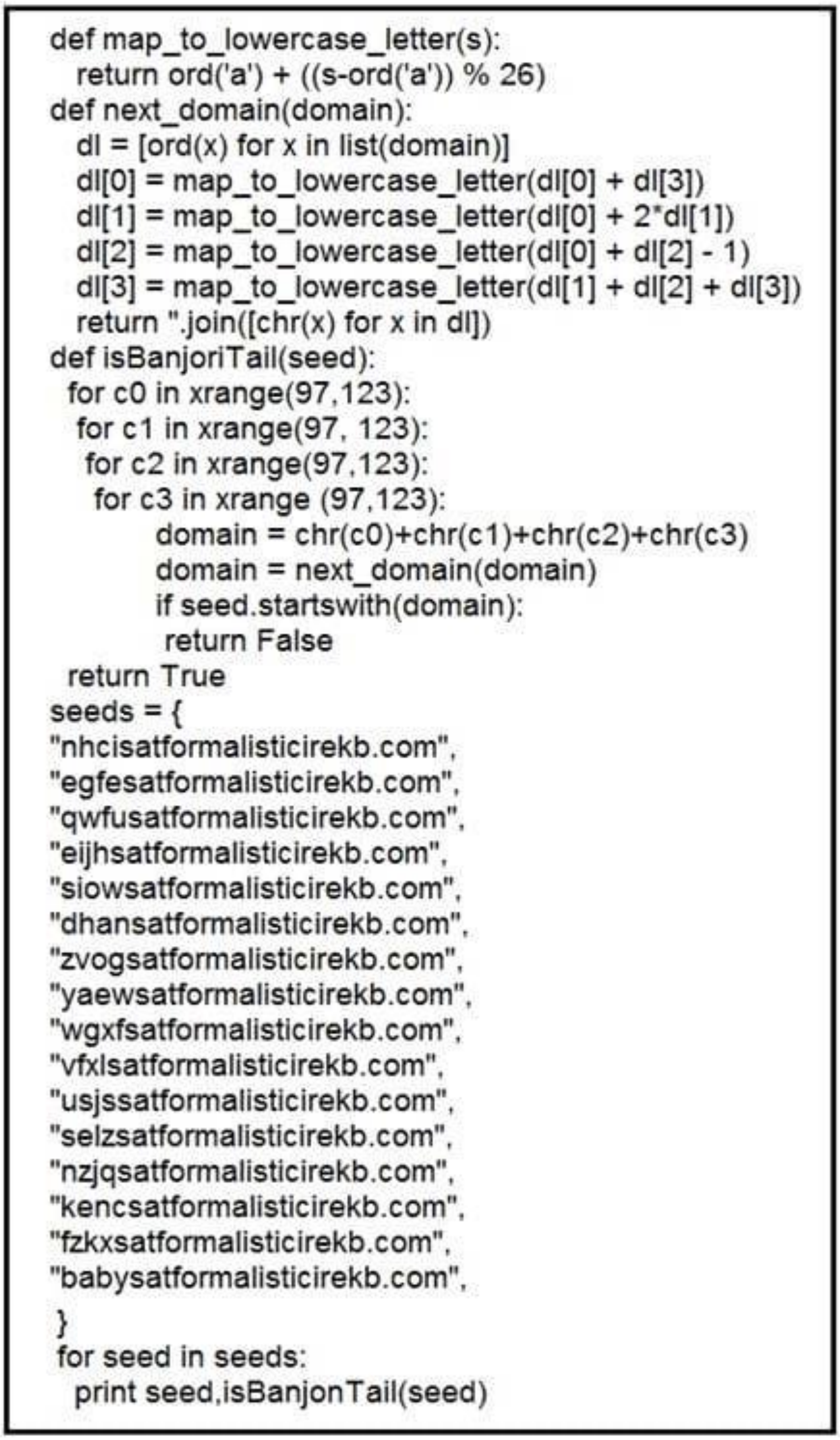
B. The token is obtained by providing a password. The REST API requests access to a resource using the access token, validates the access token, and gives access to the resource.

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 4:



```
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)
```

Refer to the exhibit. What results from this script?

A. Seeds for existing domains are checked

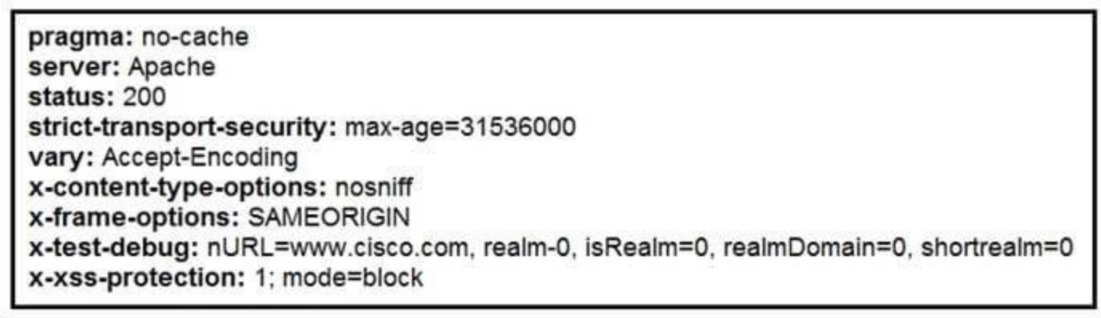
B. A search is conducted for additional seeds

C. Domains are compared to seed rules

D. A list of domains as seeds is blocked

Correct Answer: B

Question 5:



```
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

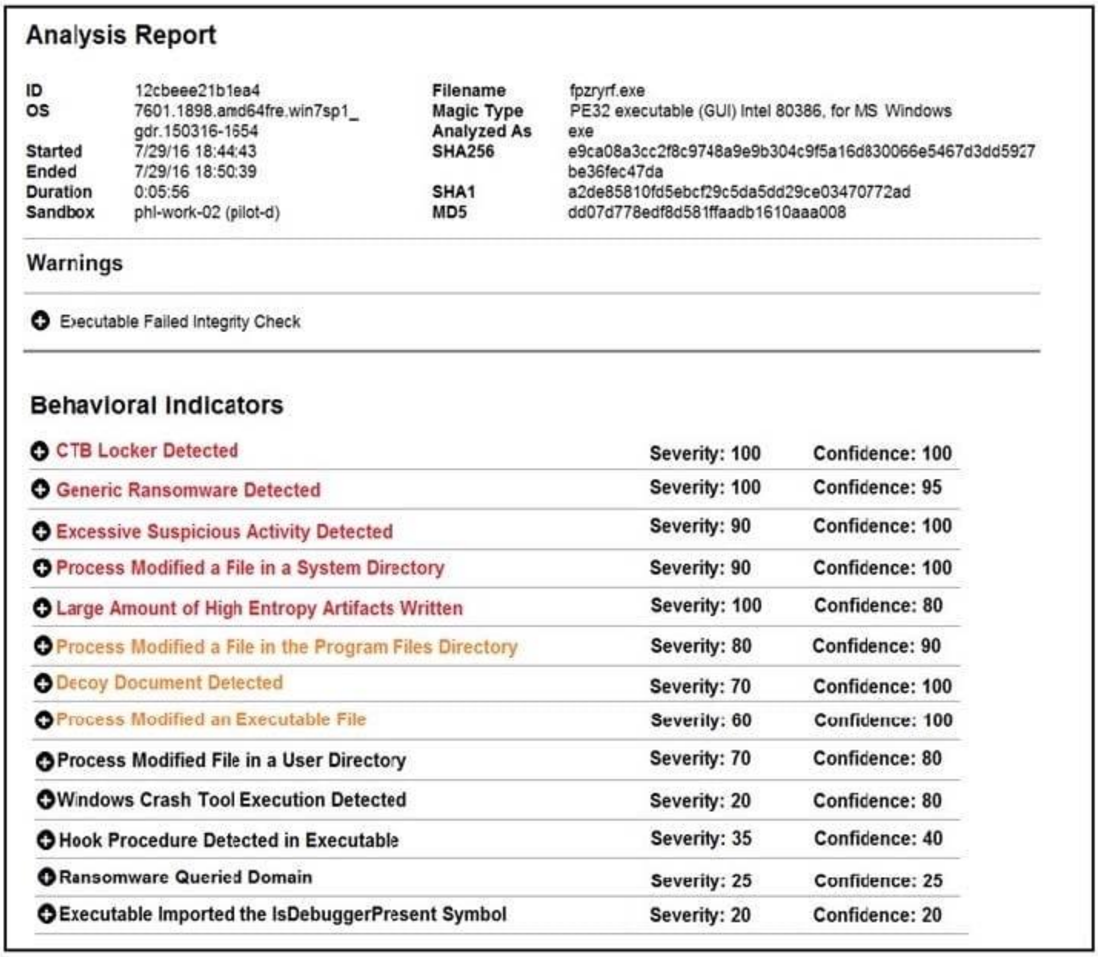
C. x-xss-protection

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 6:



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**	e9ca08a3cc2f8c9748a9e9b304c9f5a16d830066e5467d3dd5927 be36fec47da
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

Refer to the exhibit. 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.

Correct Answer: C

Question 7:
A SOC analyst is investigating a recent email delivered to a high-value user for a customer whose network their organization monitors. The email includes a suspicious attachment titled "Invoice RE: 0004489". The hash of the file is gathered from the Cisco Email Security Appliance. After searching Open Source Intelligence, no available history of this hash is found anywhere on the web.

What is the next step in analyzing this attachment to allow the analyst to gather indicators of compromise?

A. Run and analyze the DLP Incident Summary Report from the Email Security Appliance

B. Ask the company to execute the payload for real time analysis

C. Investigate further in open source repositories using YARA to find matches

D. Obtain a copy of the file for detonation in a sandbox

Correct Answer: D

Question 8:
An engineer is utilizing interactive behavior analysis to test malware in a sandbox environment to see how the malware performs when it is successfully executed. A location is secured to perform reverse engineering on a piece of malware. What is the next step the engineer should take to analyze this malware?

A. Run the program through a debugger to see the sequential actions

B. Unpack the file in a sandbox to see how it reacts

C. Research the malware online to see if there are noted findings

D. Disassemble the malware to understand how it was constructed

Correct Answer: C

Question 9:
An analyst received multiple alerts on the SIEM console of users that are navigating to malicious URLs. The analyst needs to automate the task of receiving alerts and processing the data for further investigations. Three variables are available from the SIEM console to include in an automation script: console_ip, api_token, and reference_set_name. What must be added to this script to receive a successful HTTP response?

#!/usr/bin/pythonimport sysimport requests

A. {1}, {2}

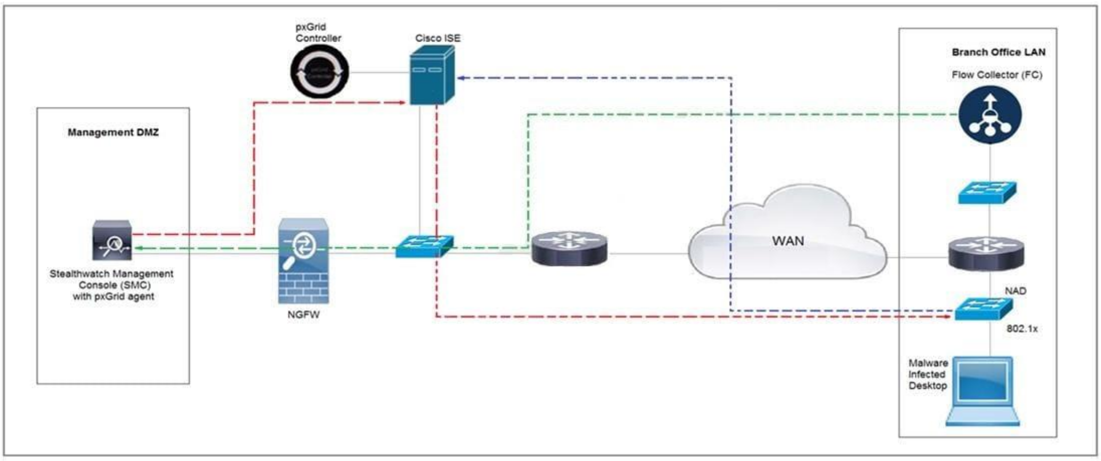
B. {1}, {3}

C. console_ip, api_token

D. console_ip, reference_set_name

Correct Answer: C

Question 10:
Refer to the exhibit. Rapid Threat Containment using Cisco Secure Network Analytics (Stealthwatch) and ISE detects the threat of malware-infected 802.1x authenticated endpoints and places that endpoint into a quarantine VLAN using Adaptive Network Control policy. Which method was used to signal ISE to quarantine the endpoints?



A. SNMP

B. syslog

C. REST API

D. pxGrid

Correct Answer: C

Question 11:
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

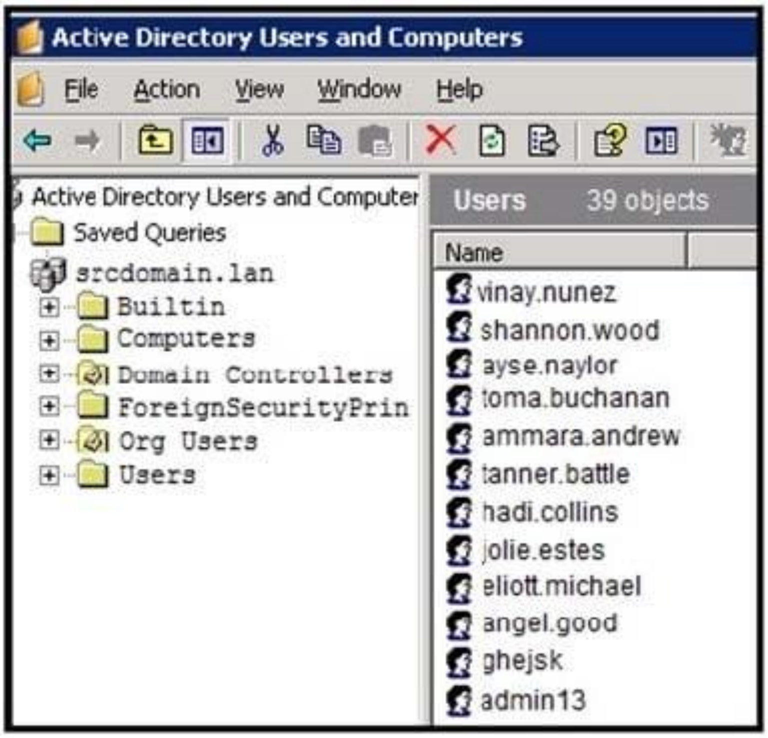
C. Run the w command

D. Run the who command

Correct Answer: A

Reference: https://eclecticlight.co/2016/02/06/the-ultimate-diagnostic-tool-sysdiagnose/

Question 12:



Name
vinay.nunez
shannon.wood
ayse.naylor
toma.buchanan
ammara.andrew
tanner.battle
hadi.collins
jolie.estes
eliott.michael
angel.good
ghejsk
admin13

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

Correct Answer: D

Question 13:
A patient views information that is not theirs when they sign in to the hospital\'s online portal. The patient calls the support center at the hospital but continues to be put on hold because other patients are experiencing the same issue. An incident has been declared, and an engineer is now on the incident bridge as the CyberOps Tier 3 Analyst. There is a concern about the disclosure of PII occurring in real-time.

What is the first step the analyst should take to address this incident?

A. Evaluate visibility tools to determine if external access resulted in tampering

B. Contact the third-party handling provider to respond to the incident as critical

C. Turn off all access to the patient portal to secure patient records

D. Review system and application logs to identify errors in the portal code

Correct Answer: C

Question 14:
What is idempotence?

A. the assurance of system uniformity throughout the whole delivery process

B. the ability to recover from failures while keeping critical services running

C. the necessity of setting maintenance of individual deployment environments

D. the ability to set the target environment configuration regardless of the starting state

Correct Answer: A

Question 15:
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

Correct Answer: C