Free Questions for CS0-002 by go4braindumps

Shared by Casey on 05-09-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

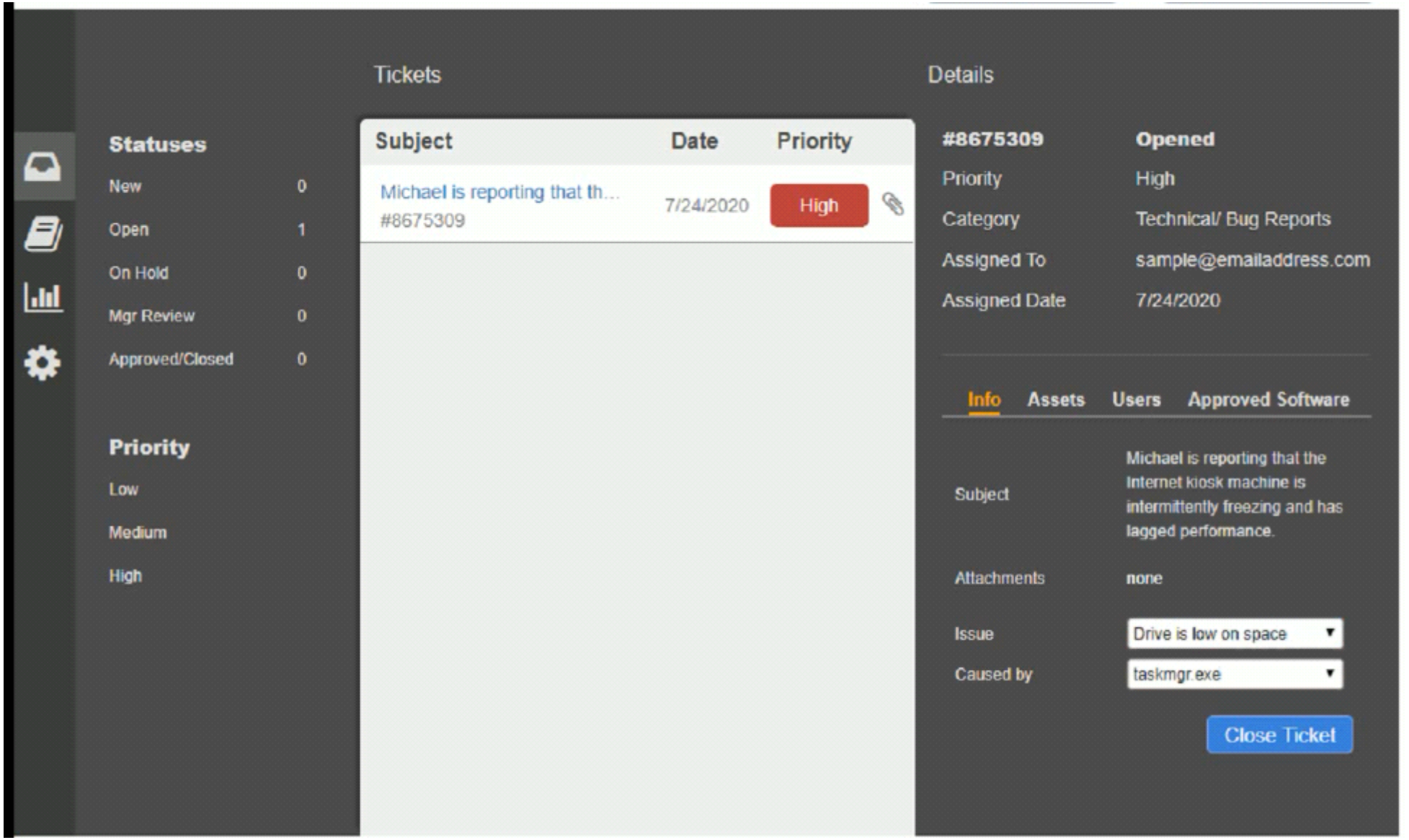
Question Type: MultipleChoice

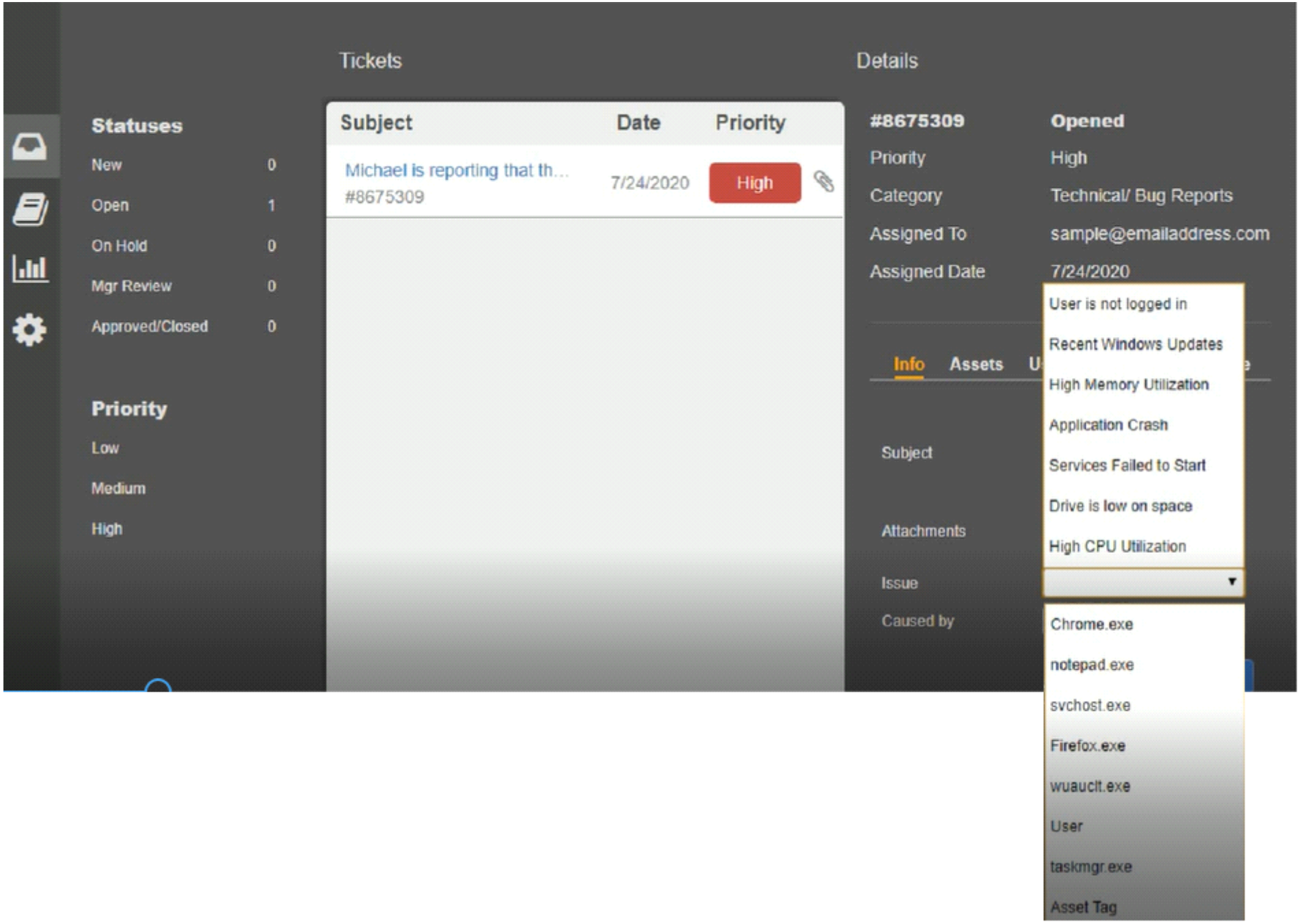
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue.

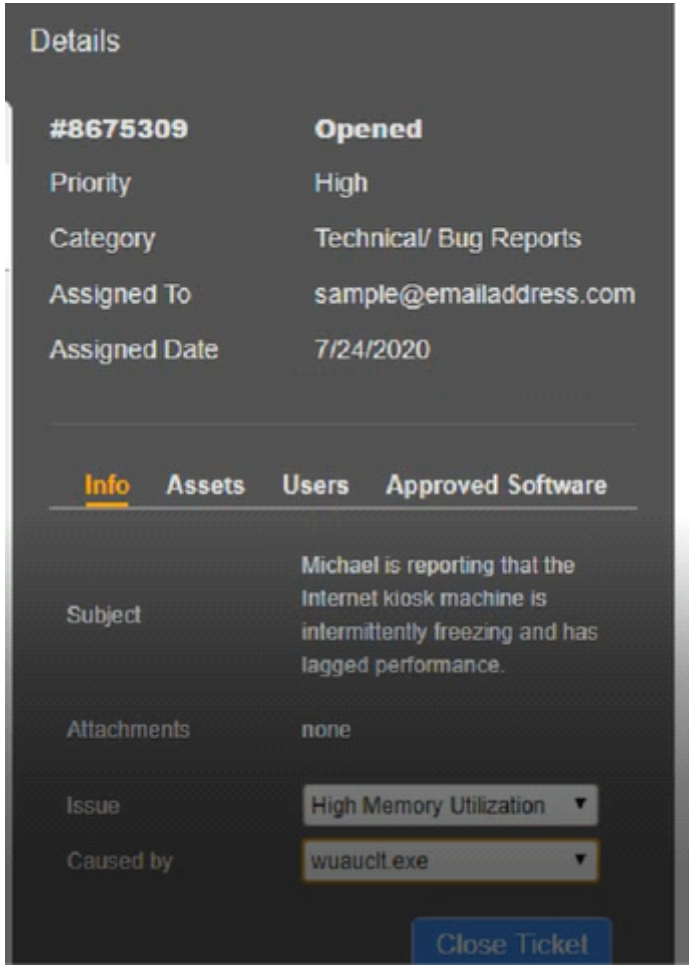
INSTRUCTIONS

Options:

A) Click on me ticket to see the ticket details Additional content is available on tabs within the ticket
First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button


Statuses
New 0
Open 1
On Hold 0
Mgr Review 0
Approved/Closed 0
Priority
Low
Medium
High
Tickets
Subject
Date
Priority
Michael is reporting that th...
#8675309
7/24/2020
High
Details
#8675309
Opened
Priority
High
Category
Technical/ Bug Reports
Assigned To
sample@emailaddress.com
Assigned Date
7/24/2020
Info
Assets
Users
Approved Software
Subject
Michael is reporting that the Internet kiosk machine is intermittently freezing and has lagged performance.
Attachments
none
Issue
Drive is low on space
Caused by
taskmgr.exe
Close Ticket


Tickets
Details
Statuses
New 0
Open 1
On Hold 0
Mgr Review 0
Approved/Closed 0
Priority
Low
Medium
High
Subject
Date
Priority
Michael is reporting that th...
#8675309
7/24/2020
High
#8675309
Opened
Priority
High
Category
Technical/ Bug Reports
Assigned To
sample@emailaddress.com
Assigned Date
7/24/2020
Info
Assets
Subject
Attachments
Issue
Caused by
User is not logged in
Recent Windows Updates
High Memory Utilization
Application Crash
Services Failed to Start
Drive is low on space
High CPU Utilization
Chrome.exe
notepad.exe
svchost.exe
Firefox.exe
wuauclt.exe
User
taskmgr.exe
Asset Tag


Details
#8675309
Opened
Priority
High
Category
Technical/ Bug Reports
Assigned To
sample@emailaddress.com
Assigned Date
7/24/2020
Info
Assets
Users
Approved Software
Subject
Michael is reporting that the Internet kiosk machine is intermittently freezing and has lagged performance.
Attachments
none
Issue
High Memory Utilization
Caused by
wuauclt.exe
Close Ticket

Answer:

A

Question 2

Question Type: MultipleChoice

A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer dat

a. Developers use personal workstations, giving the company little to no visibility into the development activities.

Which of the following would be BEST to implement to alleviate the CISO's concern?

Options:

A) DLP

B) Encryption

C) Test data

D) NDA

Answer:

D

Question 3

Question Type: MultipleChoice

An organization has several system that require specific logons Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?

Options:

A) Use SSO across all applications

B) Perform a manual privilege review

C) Adjust the current monitoring and logging rules

D) Implement multifactor authentication

Answer:

B

Question 4

Question Type: MultipleChoice

Ann, a user, reports to the security team that her browser began redirecting her to random sites while using her Windows laptop. Ann further reports that the OS shows the C: drive is out of space despite having plenty of space recently. Ann claims she not downloaded anything. The security team obtains the laptop and begins to investigate, noting the following:

* File access auditing is turned off.

* When clearing up disk space to make the laptop functional, files that appear to be cached web pages are immediately created in a temporary directory, filling up the available drive space.

* All processes running appear to be legitimate processes for this user and machine.

* Network traffic spikes when the space is cleared on the laptop.

* No browser is open.

Which of the following initial actions and tools would provide the BEST approach to determining what is happening?

Options:

A) Delete the temporary files, run an Nmap scan, and utilize Burp Suite.

B) Disable the network connection, check Sysinternals Process Explorer, and review netstat output.

C) Perform a hard power down of the laptop, take a dd image, and analyze with FTK.

D) Review logins to the laptop, search Windows Event Viewer, and review Wireshark captures.

Answer:

B

Question 5

Question Type: **MultipleChoice**

SIMULATION

Approximately 100 employees at your company have received a phishing email. As a security analyst you have been tasked with handling this situation.

INSTRUCTIONS

Review the information provided and determine the following:

1. How many employees clicked on the link in the phishing email?

2. On how many workstations was the malware installed?

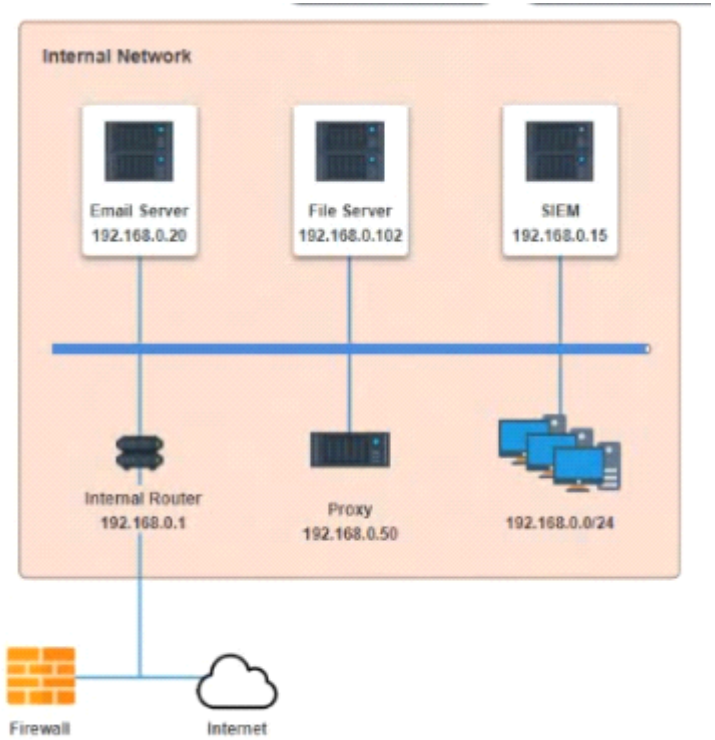
3. What is the executable file name or the malware?

View Phishing Email

How many workstations were infected?

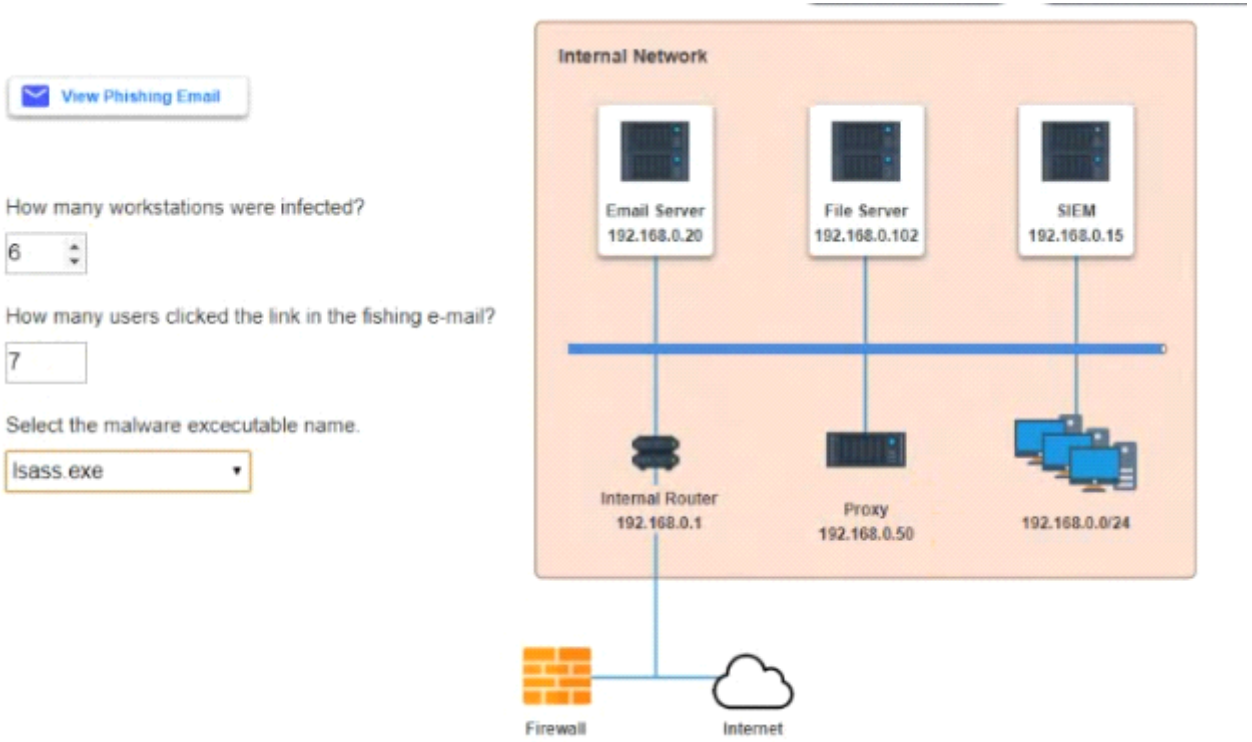
How many users clicked the link in the fishing e-mail?

Select the malware excecutable name.



Options:

A) Select the following answer as per diagram below:



Answer:

A

Question 6

Question Type: MultipleChoice

Which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:

Which of the following should the analyst review to find out how the data was exfilltrated?

Options:

A) Monday's logs

B) Tuesday's logs

C) Wednesday's logs

D) Thursday's logs

Answer:

D

Question 7

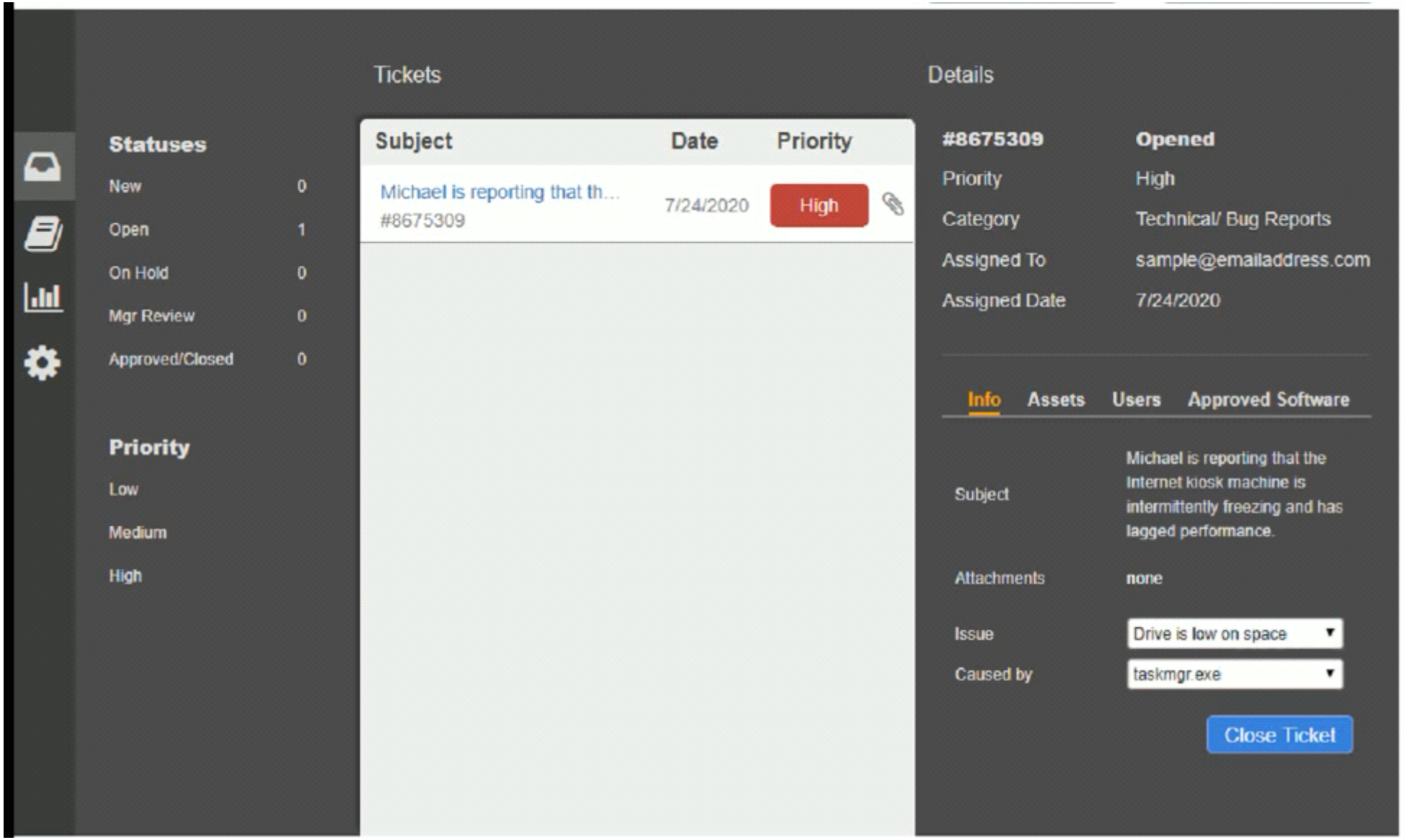
Question Type: MultipleChoice

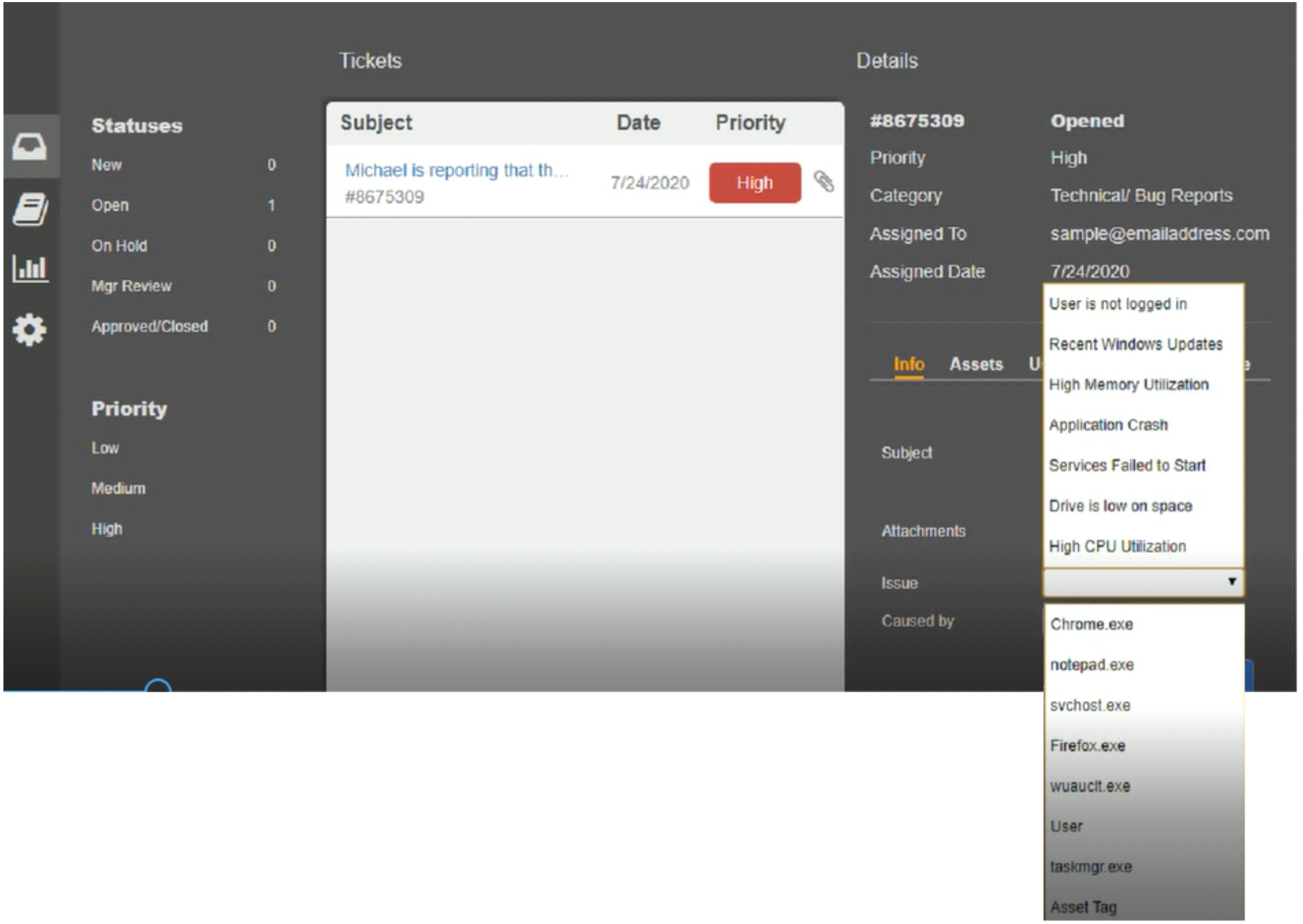
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue.

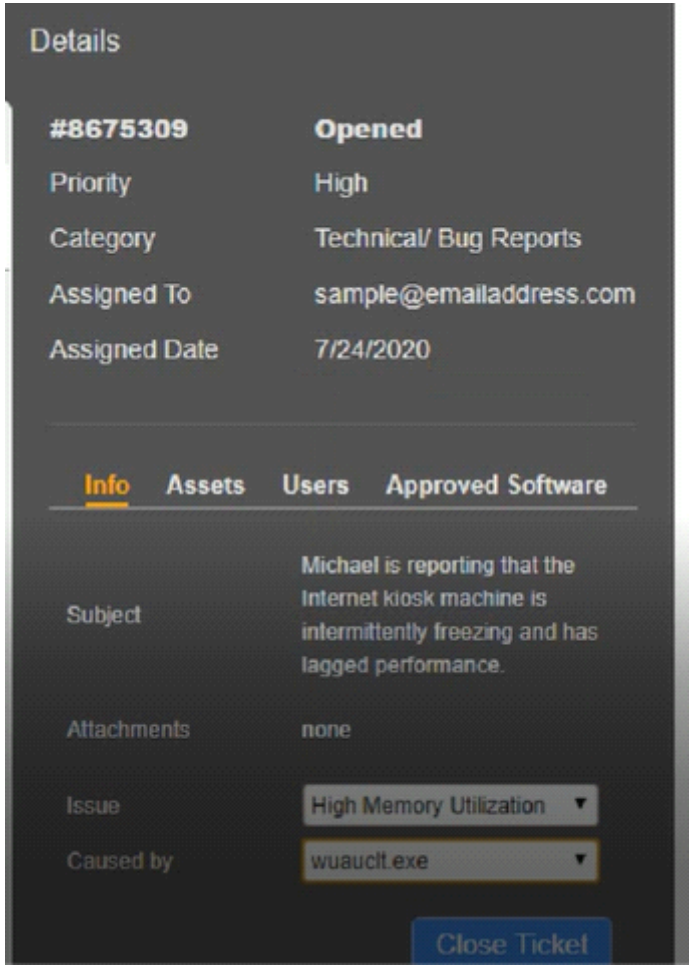
INSTRUCTIONS

Options:

A) Click on me ticket to see the ticket details Additional content is available on tabs within the ticket
First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button


Statuses
New 0
Open 1
On Hold 0
Mgr Review 0
Approved/Closed 0
Priority
Low
Medium
High
Tickets
Subject
Date
Priority
Michael is reporting that th...
#8675309
7/24/2020
High
Details
#8675309
Opened
Priority
High
Category
Technical/ Bug Reports
Assigned To
sample@emailaddress.com
Assigned Date
7/24/2020
Info
Assets
Users
Approved Software
Subject
Michael is reporting that the Internet kiosk machine is intermittently freezing and has lagged performance.
Attachments
none
Issue
Drive is low on space
Caused by
taskmgr.exe
Close Ticket


Tickets
Details
Statuses
New 0
Open 1
On Hold 0
Mgr Review 0
Approved/Closed 0
Priority
Low
Medium
High
Subject
Date
Priority
Michael is reporting that th...
#8675309
7/24/2020
High
#8675309
Opened
Priority
High
Category
Technical/ Bug Reports
Assigned To
sample@emailaddress.com
Assigned Date
7/24/2020
Info
Assets
Subject
Attachments
Issue
Caused by
User is not logged in
Recent Windows Updates
High Memory Utilization
Application Crash
Services Failed to Start
Drive is low on space
High CPU Utilization
Chrome.exe
notepad.exe
svchost.exe
Firefox.exe
wuauclt.exe
User
taskmgr.exe
Asset Tag


Details
#8675309
Opened
Priority
High
Category
Technical/ Bug Reports
Assigned To
sample@emailaddress.com
Assigned Date
7/24/2020
Info
Assets
Users
Approved Software
Subject
Michael is reporting that the Internet kiosk machine is intermittently freezing and has lagged performance.
Attachments
none
Issue
High Memory Utilization
Caused by
wuauclt.exe
Close Ticket

Answer:

A

Question 8

Question Type: MultipleChoice

A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability Company policy prohibits using portable media or mobile storage The security analyst is trying to determine which user caused the malware to get onto the system Which of the following registry keys would MOST likely have this information?

A)

```
HKEY_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run
```

B)

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

C)

```
HKEY_USERS\<user SID>\Software\Microsoft\Windows\explorer\MountPoints2
```

D)

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub
```

Options:

A) Option A

B) Option B

C) Option C

D) Option D

Answer:

C