# CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

## Pass CompTIA CS0-003 Exam with 100% Guarantee

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

**https://www.pass4itsure.com/cs0-003.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

A systems analyst is limiting user access to system configuration keys and values in a Windows environment. Which of the following describes where the analyst can find these configuration items?

A. config.ini

B. ntds.dit

C. Master boot record

D. Registry

Correct Answer: D

The registry is a database that stores system configuration keys and values in a Windows environment. The registry contains information about the hardware, software, users, and preferences of the system. The registry can be accessed and modified using the Registry Editor tool (regedit.exe) or the command-line tool (reg.exe). The registry is organized into five main sections, called hives, which are further divided into subkeys and values. The other options are not the best descriptions of where the analyst can find system configuration keys and values in a Windows environment. config.ini (A) is a file that stores configuration settings for some applications, but it is not a database that stores system configuration keys and values. ntds.dit (B) is a file that stores the Active Directory data for a domain controller, but it is not a database that stores system configuration keys and values. Master boot record ?is a section of the hard disk that contains information about the partitions and the boot loader, but it is not a database that stores system configuration keys and values.

**QUESTION 2**

A vulnerability analyst is writing a report documenting the newest, most critical vulnerabilities identified in the past month. Which of the following public MITRE repositories would be best to review?

A. Cyber Threat Intelligence

B. Common Vulnerabilities and Exposures

C. Cyber Analytics Repository

D. ATTandCK

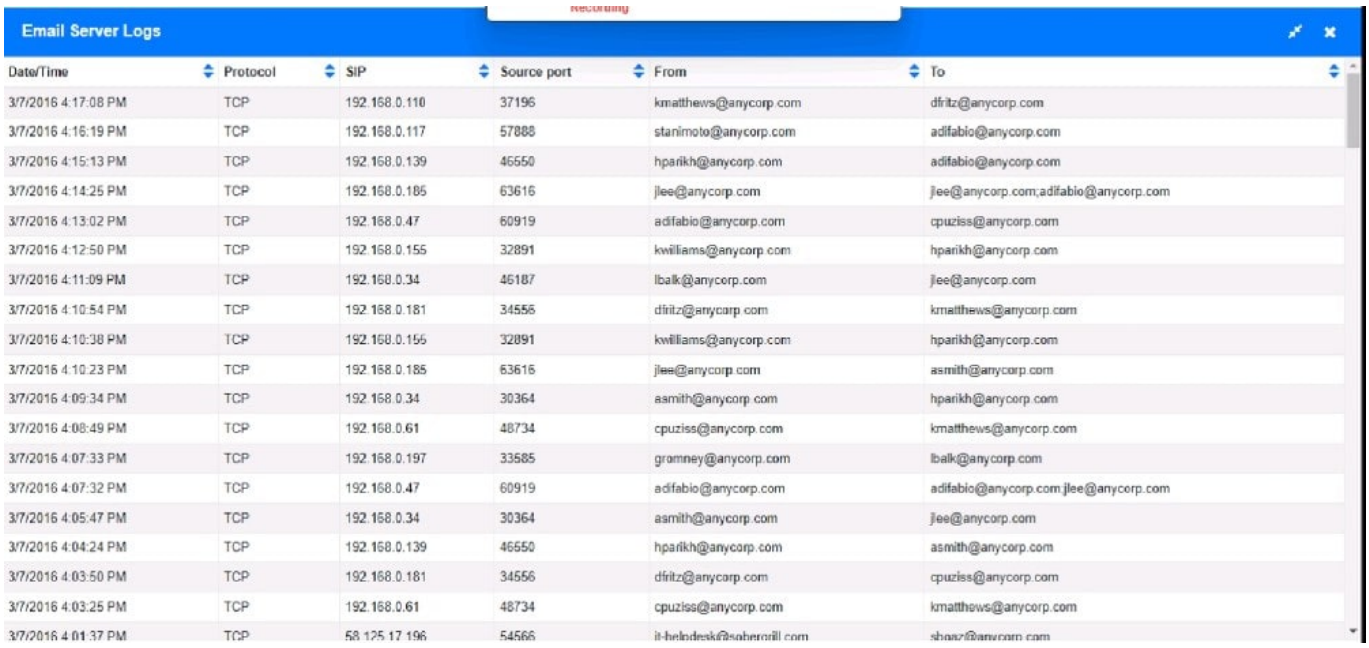
Correct Answer: B

The Common Vulnerabilities and Exposures (CVE) is a public repository of standardized identifiers and descriptions for common cybersecurity vulnerabilities. It helps security analysts to identify, prioritize, and report on the most critical vulnerabilities in their systems and applications. The other options are not relevant for this purpose: Cyber Threat Intelligence (CTI) is a collection of information and analysis on current and emerging cyber threats; Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the ATTandCK adversary model; ATTandCK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.References: According to the CompTIA CySA+ Study Guide: S0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of various cybersecurity frameworks and standards, such as CVE, CTI, CAR, and ATTandCK, in chapter 1. Specifically, it explains the meaning and function of each framework and standard, such as CVE, which provides a common language for describing and sharing information about vulnerabilities1, page 28. Therefore, this is a reliable source to verify the answer to the question.

**QUESTION 3**

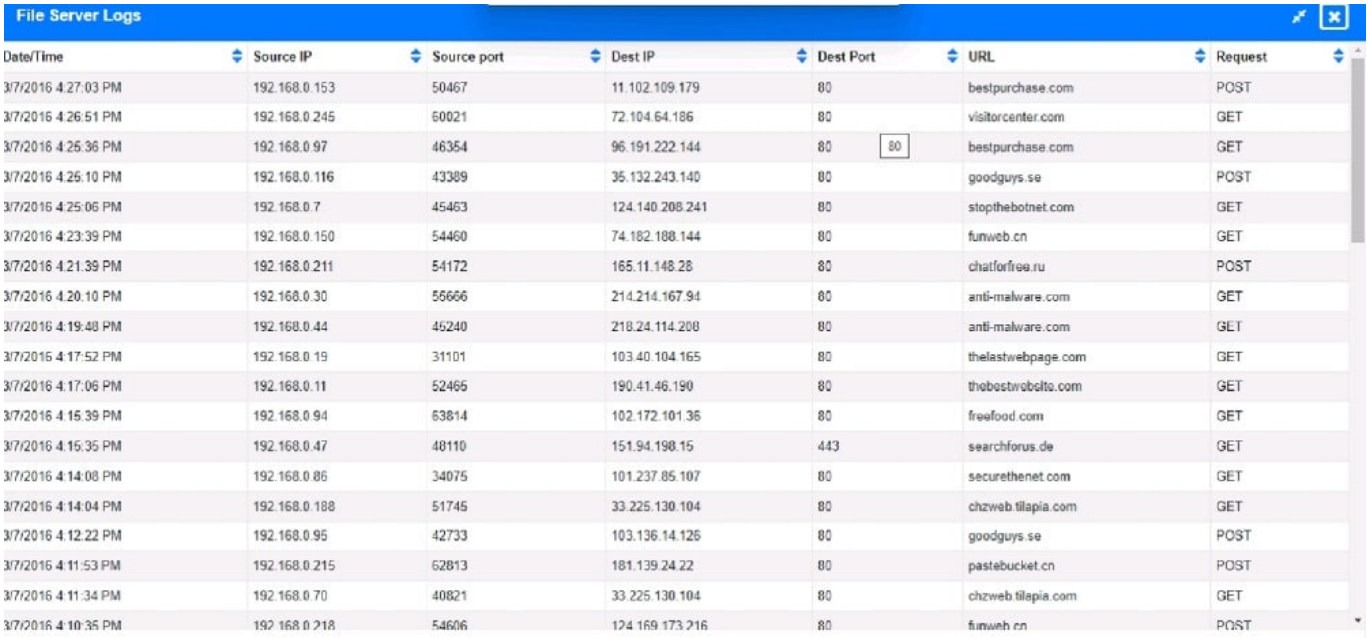
SIMULATION

Approximately 100 employees at your company have received a Phishing email. AS a security analyst. you have been tasked with handling this Situation.



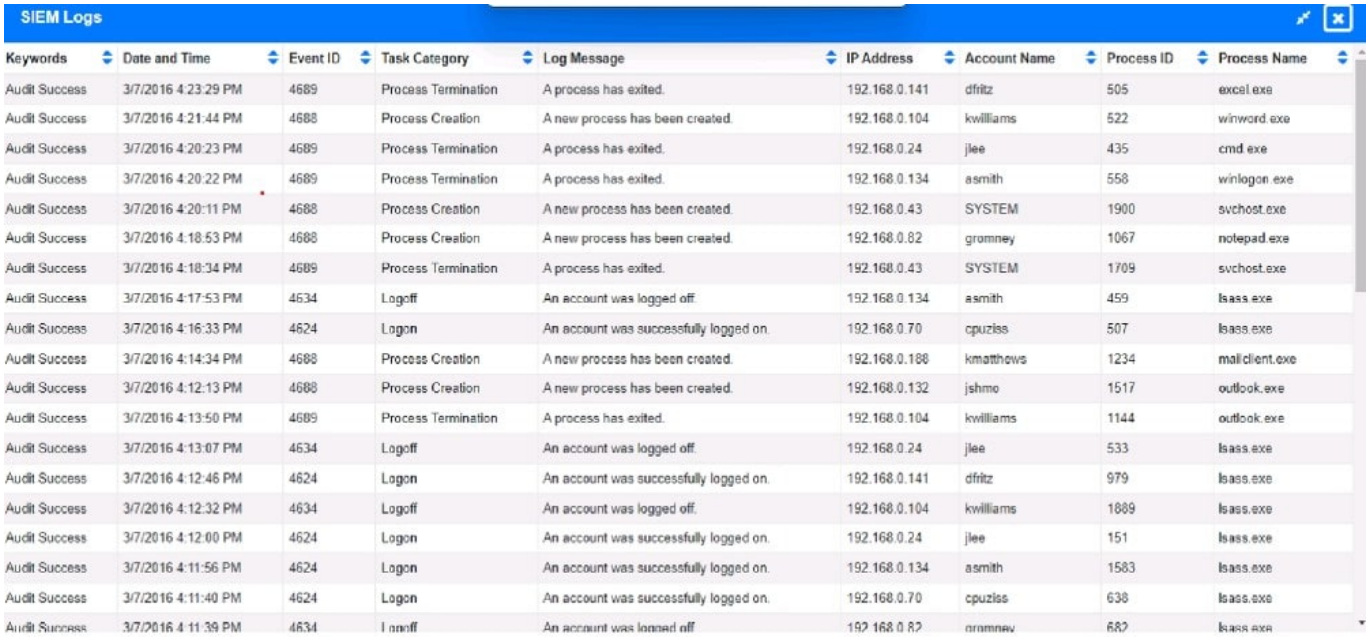
Email Server Logs

| Date/Time | Protocol | SIP | Source port | From | To |
|---|---|---|---|---|---|
| 3/7/2016 4:17:08 PM | TCP | 192.168.0.110 | 37196 | kmatthews@anycorp.com | dfritz@anycorp.com |
| 3/7/2016 4:16:19 PM | TCP | 192.168.0.117 | 57888 | stanimoto@anycorp.com | adifabio@anycorp.com |
| 3/7/2016 4:15:13 PM | TCP | 192.168.0.139 | 46550 | hparikh@anycorp.com | adifabio@anycorp.com |
| 3/7/2016 4:14:25 PM | TCP | 192.168.0.185 | 63616 | jlee@anycorp.com | jlee@anycorp.com;adifabio@anycorp.com |
| 3/7/2016 4:13:02 PM | TCP | 192.168.0.47 | 60919 | adifabio@anycorp.com | cpuziss@anycorp.com |
| 3/7/2016 4:12:50 PM | TCP | 192.168.0.155 | 32891 | kwilliams@anycorp.com | hparikh@anycorp.com |
| 3/7/2016 4:11:09 PM | TCP | 192.168.0.34 | 46187 | lbalk@anycorp.com | jlee@anycorp.com |
| 3/7/2016 4:10:54 PM | TCP | 192.168.0.181 | 34556 | dfritz@anycorp.com | kmatthews@anycorp.com |
| 3/7/2016 4:10:38 PM | TCP | 192.168.0.155 | 32891 | kwilliams@anycorp.com | hparikh@anycorp.com |
| 3/7/2016 4:10:23 PM | TCP | 192.168.0.185 | 63616 | jlee@anycorp.com | asmith@anycorp.com |
| 3/7/2016 4:09:34 PM | TCP | 192.168.0.34 | 30364 | asmith@anycorp.com | hparikh@anycorp.com |
| 3/7/2016 4:08:49 PM | TCP | 192.168.0.61 | 48734 | cpuziss@anycorp.com | kmatthews@anycorp.com |
| 3/7/2016 4:07:33 PM | TCP | 192.168.0.197 | 33585 | gramney@anycorp.com | lbalk@anycorp.com |
| 3/7/2016 4:07:32 PM | TCP | 192.168.0.47 | 60919 | adifabio@anycorp.com | adifabio@anycorp.com;jlee@anycorp.com |
| 3/7/2016 4:05:47 PM | TCP | 192.168.0.34 | 30364 | asmith@anycorp.com | jlee@anycorp.com |
| 3/7/2016 4:04:24 PM | TCP | 192.168.0.139 | 46550 | hparikh@anycorp.com | asmith@anycorp.com |
| 3/7/2016 4:03:50 PM | TCP | 192.168.0.181 | 34556 | dfritz@anycorp.com | cpuziss@anycorp.com |
| 3/7/2016 4:03:25 PM | TCP | 192.168.0.61 | 48734 | cpuziss@anycorp.com | kmatthews@anycorp.com |
| 3/7/2016 4:01:37 PM | TCP | 58.125.17.196 | 54566 | it-helpdesk@soberoill.com | sbenz@anycorp.com |



File Server Logs

| Date/Time | Source IP | Source port | Dest IP | Dest Port | URL | Request |
|---|---|---|---|---|---|---|
| 3/7/2016 4:27:03 PM | 192.168.0.153 | 50467 | 11.102.109.179 | 80 | bestpurchase.com | POST |
| 3/7/2016 4:26:51 PM | 192.168.0.245 | 60021 | 72.104.64.186 | 80 | visitorcenter.com | GET |
| 3/7/2016 4:25:36 PM | 192.168.0.97 | 46354 | 96.191.222.144 | 80 | bestpurchase.com | GET |
| 3/7/2016 4:25:10 PM | 192.168.0.116 | 43389 | 35.132.243.140 | 80 | goodguys.se | POST |
| 3/7/2016 4:25:06 PM | 192.168.0.7 | 45463 | 124.140.208.241 | 80 | stopthebotnet.com | GET |
| 3/7/2016 4:23:39 PM | 192.168.0.150 | 54460 | 74.182.188.144 | 80 | funweb.cn | GET |
| 3/7/2016 4:21:39 PM | 192.168.0.211 | 54172 | 165.11.148.28 | 80 | chatforfree.ru | POST |
| 3/7/2016 4:20:10 PM | 192.168.0.30 | 55666 | 214.214.167.94 | 80 | anti-malware.com | GET |
| 3/7/2016 4:19:48 PM | 192.168.0.44 | 46240 | 218.24.114.208 | 80 | anti-malware.com | GET |
| 3/7/2016 4:17:52 PM | 192.168.0.19 | 31101 | 103.40.104.165 | 80 | thelastwebpage.com | GET |
| 3/7/2016 4:17:06 PM | 192.168.0.11 | 52465 | 190.41.46.190 | 80 | thebestwebsite.com | GET |
| 3/7/2016 4:15:39 PM | 192.168.0.94 | 63814 | 102.172.101.36 | 80 | freefood.com | GET |
| 3/7/2016 4:15:35 PM | 192.168.0.47 | 48110 | 151.94.198.15 | 443 | searchforus.de | GET |
| 3/7/2016 4:14:08 PM | 192.168.0.86 | 34075 | 101.237.85.107 | 80 | securethenet.com | GET |
| 3/7/2016 4:14:04 PM | 192.168.0.188 | 51745 | 33.225.130.104 | 80 | chzweb.tilapia.com | GET |
| 3/7/2016 4:12:22 PM | 192.168.0.95 | 42733 | 103.136.14.125 | 80 | goodguys.se | POST |
| 3/7/2016 4:11:53 PM | 192.168.0.215 | 62813 | 181.139.24.22 | 80 | pastebucket.cn | POST |
| 3/7/2016 4:11:34 PM | 192.168.0.70 | 40821 | 33.225.130.104 | 80 | chzweb.tilapia.com | GET |
| 3/7/2016 4:10:35 PM | 192.168.0.218 | 54606 | 124.169.173.216 | 80 | funweb.cn | POST |



SIEM Logs

| Keywords | Date and Time | Event ID | Task Category | Log Message | IP Address | Account Name | Process ID | Process Name |
|---|---|---|---|---|---|---|---|---|
| Audit Success | 3/7/2016 4:23:29 PM | 4689 | Process Termination | A process has exited. | 192.168.0.141 | dfritz | 505 | excel.exe |
| Audit Success | 3/7/2016 4:21:44 PM | 4688 | Process Creation | A new process has been created. | 192.168.0.104 | kwilliams | 522 | winword.exe |
| Audit Success | 3/7/2016 4:20:23 PM | 4689 | Process Termination | A process has exited. | 192.168.0.24 | jlee | 435 | cmd.exe |
| Audit Success | 3/7/2016 4:20:22 PM | 4689 | Process Termination | A process has exited. | 192.168.0.134 | asmith | 558 | winlogon.exe |
| Audit Success | 3/7/2016 4:20:11 PM | 4688 | Process Creation | A new process has been created. | 192.168.0.43 | SYSTEM | 1900 | svchost.exe |
| Audit Success | 3/7/2016 4:18:53 PM | 4688 | Process Creation | A new process has been created. | 192.168.0.82 | gromney | 1067 | notepad.exe |
| Audit Success | 3/7/2016 4:18:34 PM | 4689 | Process Termination | A process has exited. | 192.168.0.43 | SYSTEM | 1709 | svchost.exe |
| Audit Success | 3/7/2016 4:17:53 PM | 4634 | Logoff | An account was logged off. | 192.168.0.134 | asmith | 459 | lsass.exe |
| Audit Success | 3/7/2016 4:16:33 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.70 | cpuziss | 507 | lsass.exe |
| Audit Success | 3/7/2016 4:14:34 PM | 4688 | Process Creation | A new process has been created. | 192.168.0.188 | kmatthews | 1234 | mailclient.exe |
| Audit Success | 3/7/2016 4:12:13 PM | 4688 | Process Creation | A new process has been created. | 192.168.0.132 | jshmo | 1517 | outlook.exe |
| Audit Success | 3/7/2016 4:13:50 PM | 4689 | Process Termination | A process has exited. | 192.168.0.104 | kwilliams | 1144 | outlook.exe |
| Audit Success | 3/7/2016 4:13:07 PM | 4634 | Logoff | An account was logged off. | 192.168.0.24 | jlee | 533 | lsass.exe |
| Audit Success | 3/7/2016 4:12:46 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.141 | dfritz | 979 | lsass.exe |
| Audit Success | 3/7/2016 4:12:32 PM | 4634 | Logoff | An account was logged off. | 192.168.0.104 | kwilliams | 1889 | lsass.exe |
| Audit Success | 3/7/2016 4:12:00 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.24 | jlee | 151 | lsass.exe |
| Audit Success | 3/7/2016 4:11:56 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.134 | asmith | 1583 | lsass.exe |
| Audit Success | 3/7/2016 4:11:40 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.70 | cpuziss | 638 | lsass.exe |
| Audit Success | 3/7/2016 4:11:39 PM | 4634 | Logoff | An account was logged off. | 192.168.0.82 | gromney | 682 | lsass.exe |

Review the information provided and determine the following:

1.

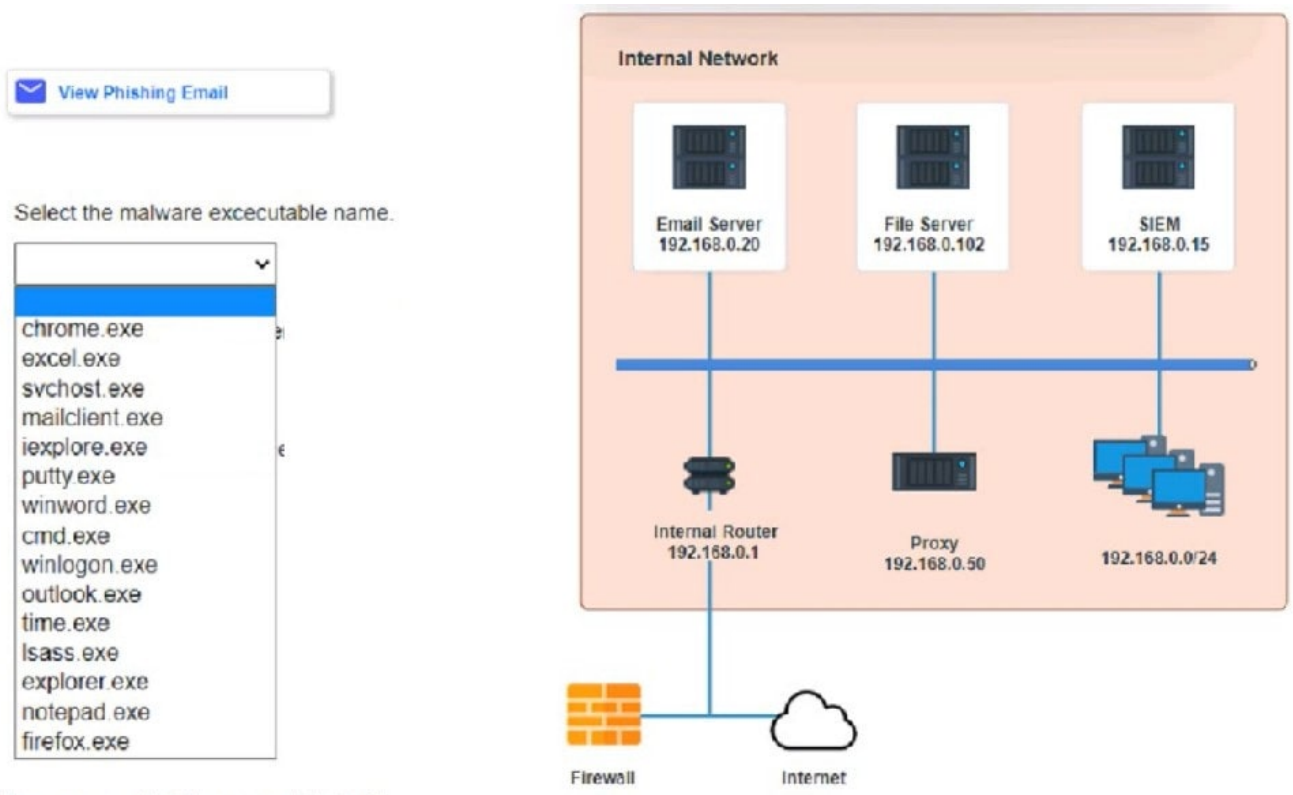
HOW many employees Clicked on the link in the Phishing email?

2.

on how many workstations was the malware installed?

3.

what is the executable file name of the malware?




A. See the answer in explanation for this task.

B. PlaceHoder

C. PlaceHoder

D. PlaceHoder

Correct Answer: A

1.

What is the executable file name of the malware? The executable file name of the malware is svchost.EXE.

2.

On how many workstations was the malware installed? According to the file server logs, the malware was installed on 15 workstations.

3.

How many employees clicked on the link in the phishing email? According to the email server logs, 25 employees clicked on the link in the phishing email.

Answers

1.

svchost.EXE

2.

15

3.

25

**QUESTION 4**

A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network. Which of the following would best aid in decreasing the workload without increasing staff?

A. SIEM

B. XDR

C. SOAR

D. EDR

Correct Answer: C

**QUESTION 5**

An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

A. Hard disk

B. Primary boot partition

C. Malicious tiles

D. Routing table

E. Static IP address

Correct Answer: D

**QUESTION 6**

A security analyst recently joined the team and is trying to determine which scripting language is being used in a

production script to determine if it is malicious. Given the following script:

foreach ($user in Get-Content .\this.txt)

{

Get-ADUser $user -Properties primaryGroupID |select-object pr:

Add-ADGroupMember "Domain Users" -Members $user

Set-ADUser $user -Replace 0(primaryGroupID=513)

}

Which of the following scripting languages was used in the script?

A. PowerShel

B. Ruby

C. Python

D. Shell script

Correct Answer: A

The script uses PowerShell syntax, such as cmdlets, parameters, variables, and comments. PowerShell is a scripting language that can be used to automate tasks and manage systems.

**QUESTION 7**

A security analyst is writing a shell script to identify IP addresses from the same country. Which of the following functions would help the analyst achieve the objective?

A. function w() { info=$(ping -c 1 $1 | awk -F "/" `END{print $1}\\') andand echo "$1 | $info" }

B. function x() { info=$(geoiplookup $1) andand echo "$1 | $info" }

C. function y() { info=$(dig -x $1 | grep PTR | tail -n 1 ) andand echo "$1 | $info" }

D. function z() { info=$(traceroute -m 40 $1 | awk `END{print $1}\\') andand echo "$1 | $info" }

Correct Answer: B

**QUESTION 8**

A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?

A. grep [IP address] packets.pcap

B. cat packets.pcap | grep [IP Address]

C. tcpdump -n -r packets.pcap host [IP address]

D. strings packets.pcap | grep [IP Address]

Correct Answer: C

The -n flag ensures that numeric IP addresses are not resolved to hostnames, and the -r flag specifies the input pcap file. The host [IP address] expression filters packets that involve the specified IP address, helping the security analyst detect connections to the suspicious IP address.

**QUESTION 9**

Which of the following makes STIX and OpenIoC information readable by both humans and machines?

A. XML

B. URL

C. OVAL

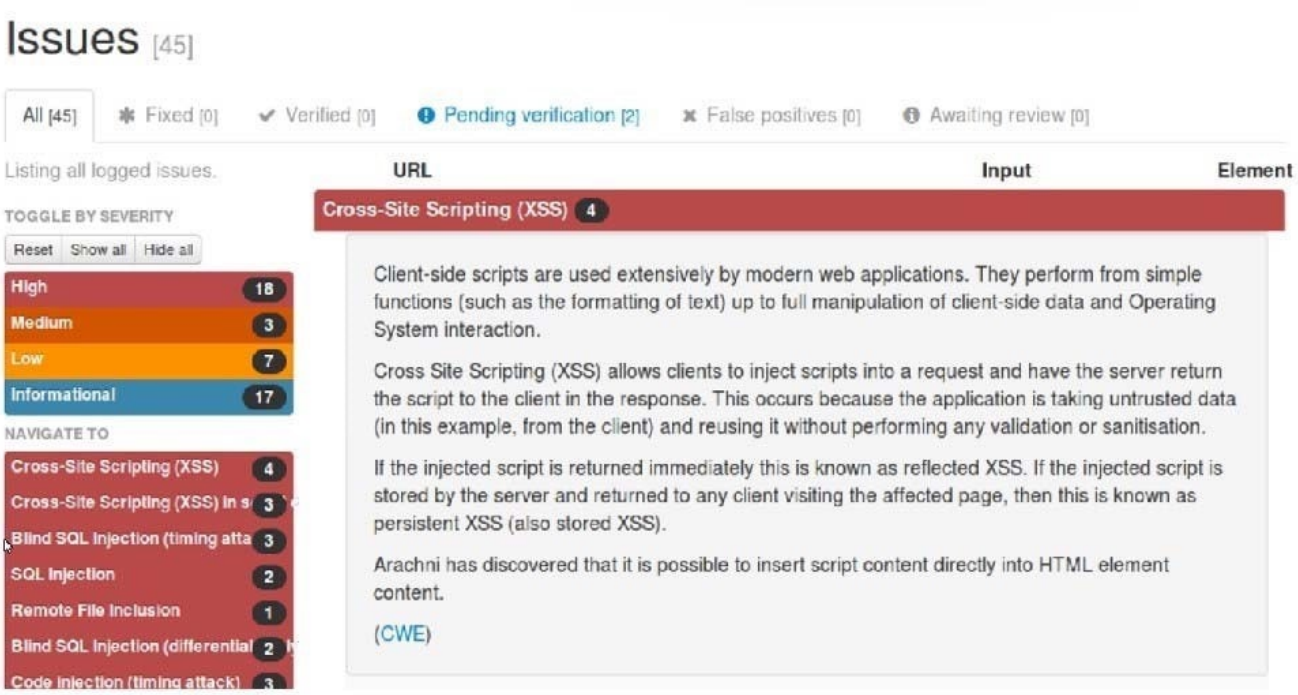
D. TAXII

Correct Answer: A

STIX and OpenIoC are two standards for representing and exchanging cyber threat intelligence (CTI) information. STIX stands for Structured Threat Information Expression and OpenIoC stands for Open Location and Identity Coordinates. Both standards use XML as the underlying data format to encode the information in a structured and machine- readable way. XML stands for Extensible Markup Language and it is a widely used standard for defining and exchanging data on the web. XML uses tags, attributes, and elements to describe the structure and meaning of the data. XML is also human-readable, as it uses plain text and follows a hierarchical and nested structure. XML is not the only format that can be used to make STIX and OpenIoC information readable by both humans and machines, but it is the most common and widely supported one. Other formats that can be used include JSON, CSV, or PDF, depending on the use case and the preferences of the information producers and consumers. However, XML has some advantages over other formats, such as: XML is more expressive and flexible than JSON or CSV, as it can define complex data types, schemas, namespaces, and validation rules. XML is more standardized and interoperable than PDF, as it can be easily parsed, transformed, validated, and queried by various tools and languages. XML is more compatible with existing CTI standards and tools than other formats, as it is the basis for STIX 1.x, TAXII 1.x, MAEC, CybOX, OVAL, and others. References: 1 Introduction to STIX - GitHub Pages 2 5 Best Threat Intelligence Feeds in 2023 (Free and Paid Tools) - Comparitech 3 What Are STIX/TAXII Standards? - Anomali Resources 4 What is STIX/TAXII? | Cloudflare 5 Sample Use | TAXII Project Documentation - GitHub Pages 6 Trying to retrieve xml data with taxii - Stack Overflow 7 CISA AIS TAXII Server Connection Guide 8 CISA AIS TAXII Server Connection Guide v2.0 | CISA

**QUESTION 10**

A security analyst reviews the following Arachni scan results for a web application that stores PII data:




Which of the following should be remediated first?

A. SQL injection

B. RFI

C. XSS

D. Code injection

Correct Answer: A

SQL injection should be remediated first, as it is a high-severity vulnerability that can allow an attacker to execute arbitrary SQL commands on the database server and access, modify, or delete sensitive data, including PII. According to the Arachni scan results, there are two instances of SQL injection and three instances of blind SQL injection (two timing attacks and one differential analysis) in the web application. These vulnerabilities indicate that the web application does not properly validate or sanitize the user input before passing it to the database server, and thus exposes the database to malicious queries12. SQL injection can have serious consequences for the confidentiality, integrity, and availability of the data and the system, and can also lead to further attacks, such as privilege escalation, data exfiltration, or remote code execution34. Therefore, SQL injection should be the highest priority for remediation, and the web application should implement input validation, parameterized queries, and least privilege principle to prevent SQL injection attacks5. References: Web application testing with Arachni | Infosec, How do I create a generated scan report for PDF in Arachni Web ..., Command line user interface ?Arachni/arachni Wiki ?GitHub, SQL Injection - OWASP, Blind SQL Injection - OWASP, SQL Injection Attack: What is it, and how to prevent it., SQL Injection Cheat Sheet and Tutorial | Veracode

---

**QUESTION 11**

HOTSPOT

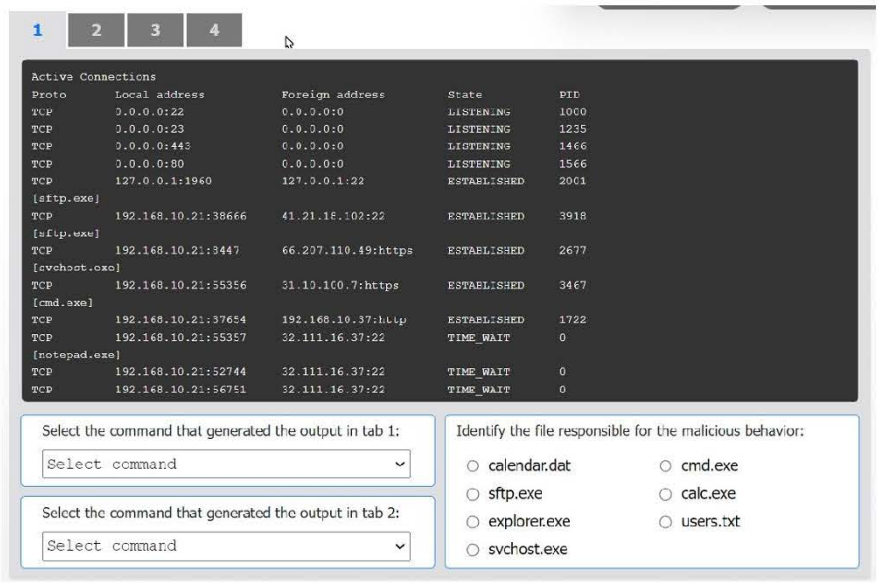
An organization has noticed large amounts of data are being sent out of its network. An analyst is identifying the cause of the data exfiltration.

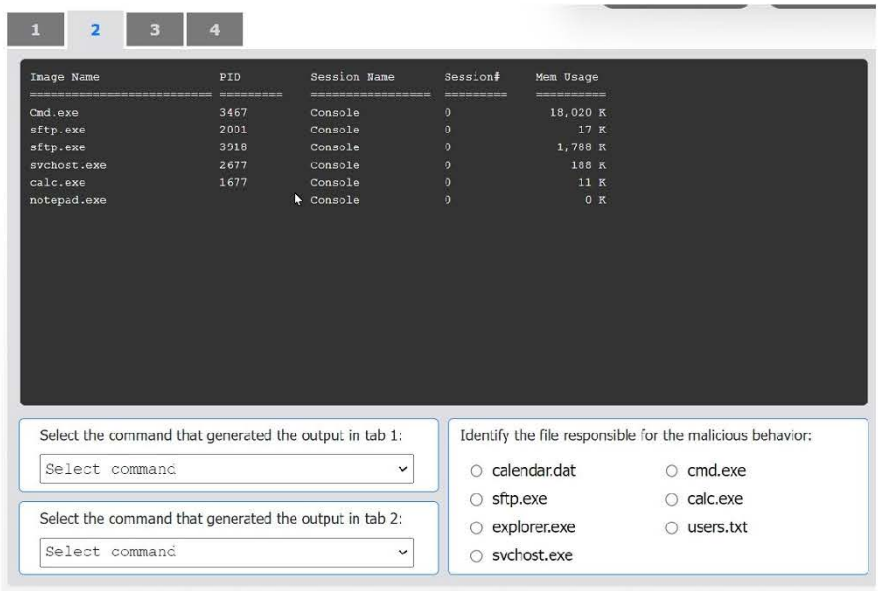
INSTRUCTIONS

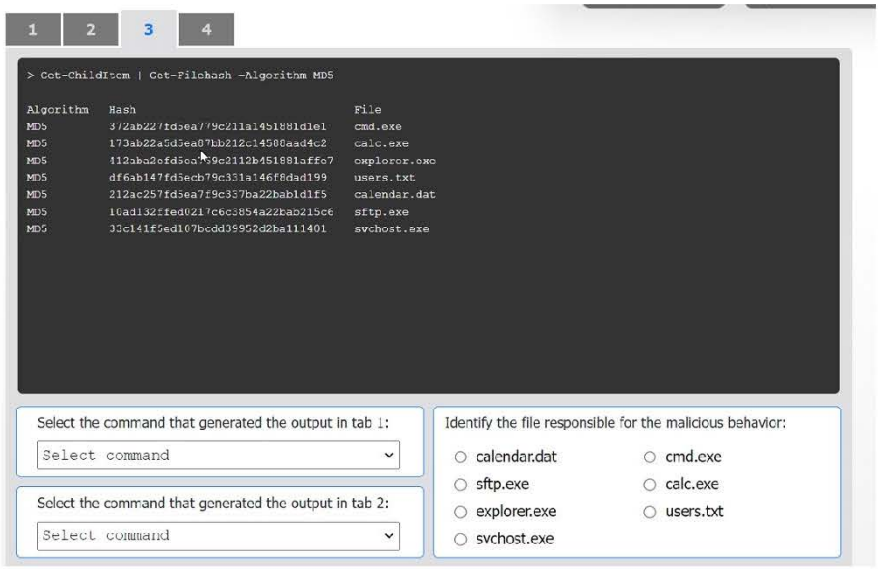
Select the command that generated the output in tabs 1 and 2.

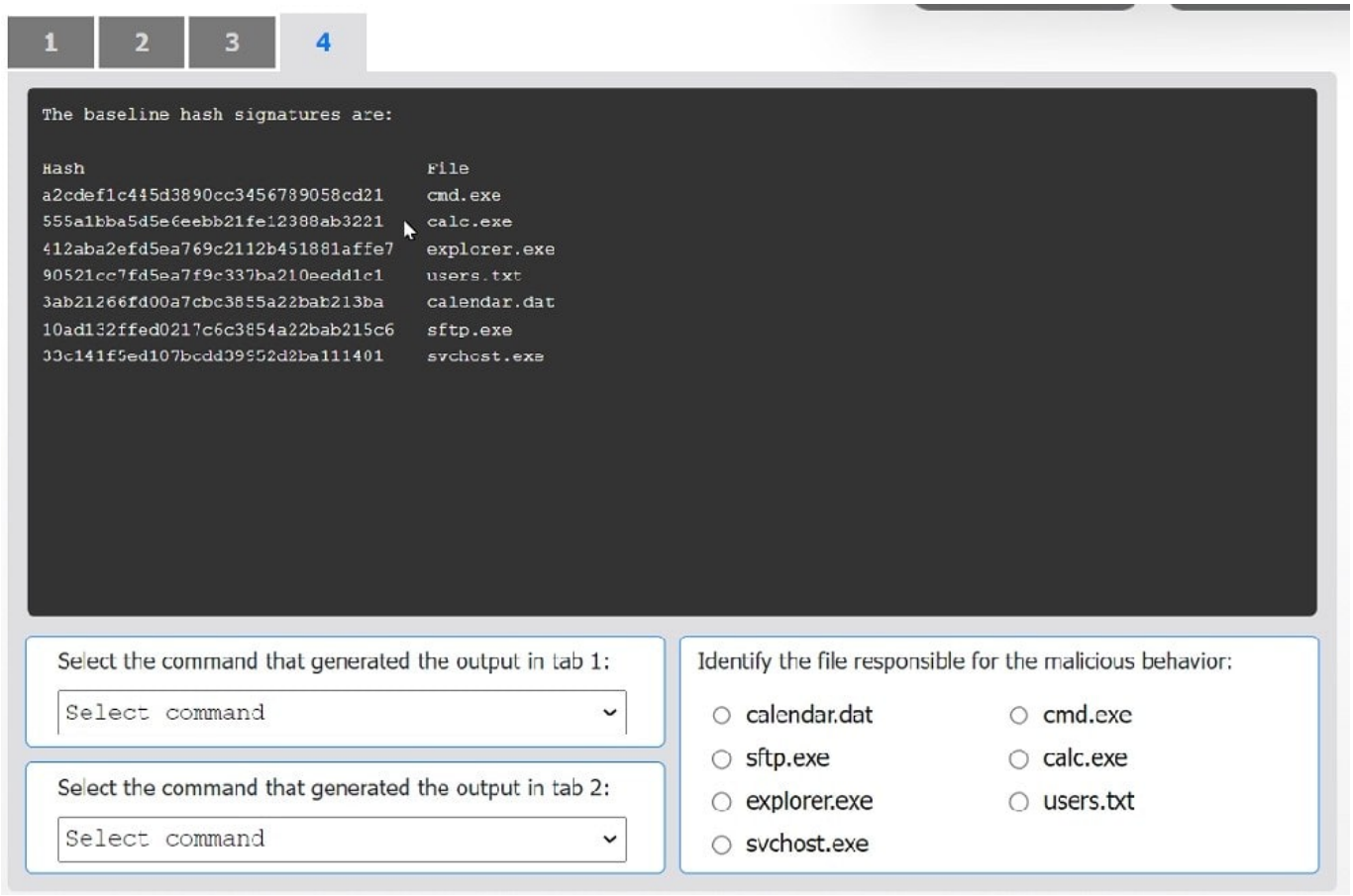
Review the output text in all tabs and identify the file responsible for the malicious behavior.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

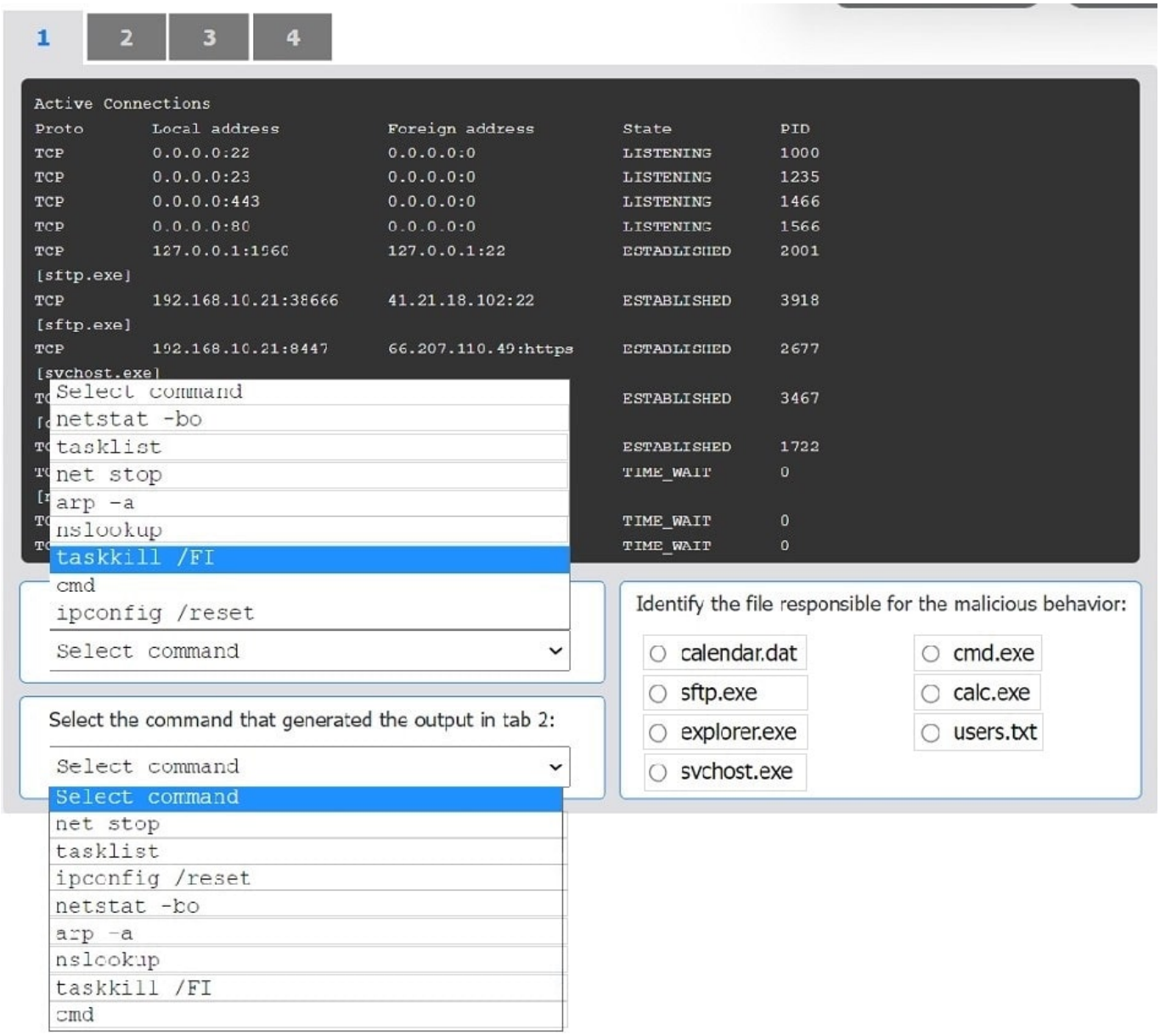

1 2 3 4
Active Connections
Proto Local address Foreign address State PID
TCP 0.0.0.0:22 0.0.0.0:0 LISTENING 1000
TCP 0.0.0.0:23 0.0.0.0:0 LISTENING 1235
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING 1466
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 1566
TCP 127.0.0.1:1960 127.0.0.1:22 ESTABLISHED 2001
[sftp.exe]
TCP 192.168.10.21:38666 41.21.18.102:22 ESTABLISHED 3918
[sftp.exe]
TCP 192.168.10.21:3447 66.207.110.49:https ESTABLISHED 2677
[svchost.exe]
TCP 192.168.10.21:55356 31.10.100.7:https ESTABLISHED 3467
[cmd.exe]
TCP 192.168.10.21:37654 192.168.10.37:http ESTABLISHED 1722
TCP 192.168.10.21:55357 32.111.16.37:22 TIME_WAIT 0
[notepad.exe]
TCP 192.168.10.21:52744 32.111.16.37:22 TIME_WAIT 0
TCP 192.168.10.21:56751 32.111.16.37:22 TIME_WAIT 0
Select the command that generated the output in tab 1:
Select command
Select the command that generated the output in tab 2:
Select command
Identify the file responsible for the malicious behavior:
calendar.dat
sftp.exe
explorer.exe
svchost.exe
cmd.exe
calc.exe
users.txt


1 2 3 4
Image Name PID Session Name Session# Mem Usage
Cmd.exe 3467 Console 0 18,020 K
sftp.exe 2001 Console 0 17 K
sftp.exe 3918 Console 0 1,788 K
svchost.exe 2677 Console 0 188 K
calc.exe 1677 Console 0 11 K
notepad.exe Console 0 0 K
Select the command that generated the output in tab 1:
Select command
Select the command that generated the output in tab 2:
Select command
Identify the file responsible for the malicious behavior:
calendar.dat
sftp.exe
explorer.exe
svchost.exe
cmd.exe
calc.exe
users.txt

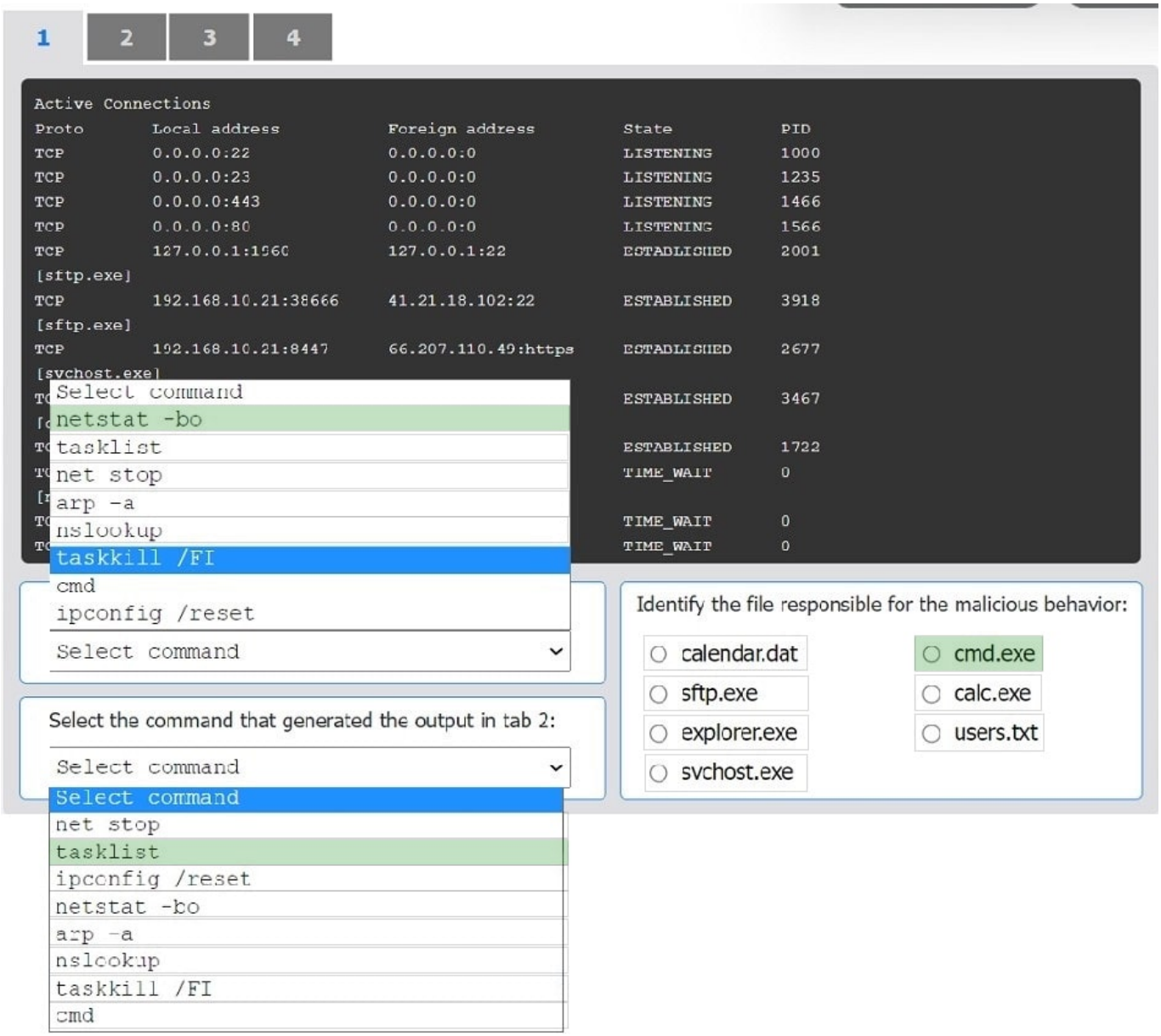

1 2 3 4
> Get-ChildItem | Get-FileHash -Algorithm MD5
Algorithm Hash File
MD5 372ab227fd3ea779c211a145181d1e1 cmd.exe
MD5 173ab22a5d3ea07bb212c14586aad4c2 calc.exe
MD5 412aba2ofd3ea39c2112b451881affe7 explorer.exe
MD5 df6ab147fd3ecb79c331a146f8dad199 users.txt
MD5 212ac257fd3ea7f9c337ba22bab1d1f5 calendar.dat
MD5 10ad132ffed0217c6c3854a22bab215c6 sftp.exe
MD5 33c141f3ed107bcdd39952d2ba111401 svchost.exe
Select the command that generated the output in tab 1:
Select command
Select the command that generated the output in tab 2:
Select command
Identify the file responsible for the malicious behavior:
calendar.dat
sftp.exe
explorer.exe
svchost.exe
cmd.exe
calc.exe
users.txt


1
2
3
4
The baseline hash signatures are:
Hash File
a2cdef1c445d3890cc3456789058cd21 cmd.exe
555a1bba5d5e6eebb21fe12388ab3221 calc.exe
412aba2efd5ea769c2112b451881affe7 explorer.exe
90521cc7fd5ea7f9c337ba210eedd1c1 users.txt
3ab21266fd00a7cbc3855a22bab213ba calendar.dat
10ad132ffed0217c6c3854a22bab215c6 sftp.exe
33c141f5ed107bcdd39552d2ba111401 svchost.exe
Select the command that generated the output in tab 1:
Select command
Select the command that generated the output in tab 2:
Select command
Identify the file responsible for the malicious behavior:
calendar.dat
cmd.exe
sftp.exe
calc.exe
explorer.exe
users.txt
svchost.exe

Hot Area:




Correct Answer:




**QUESTION 12**

A systems administrator receives reports of an internet-accessible Linux server that is running very sluggishly. The administrator examines the server, sees a high amount of memory utilization, and suspects a DoS attack related to half-open TCP sessions consuming memory. Which of the following tools would best help to prove whether this server was experiencing this behavior?

A. Nmap

B. TCPDump

C. SIEM

D. EDR

Correct Answer: B

In this scenario, where the administrator suspects a DoS attack related to half-open TCP sessions consuming memory, TCPDump would be the best tool to use. It can help prove whether the server is experiencing this behavior by capturing and analyzing the network packets to identify patterns consistent with half-open TCP sessions.

**QUESTION 13**

A company has the following security requirements:

1.

No public IPs

2.

All data secured at rest

3.

No insecure ports/protocols

After a cloud scan is completed, a security analyst receives reports that several misconfigurations are putting the company at risk. Given the following cloud scanner output:

| VM name | VM_DEV_DB | VM_PRD_Web01 | VM_DEV_Web02 | VM_PRD_DB |
|---|---|---|---|---|
| IP config | private | public | public | public |
| Encrypt | no | yes | yes | no |
| Ingress port | 443, open | 3389, open | 22, open | 80, open |

Which of the following should the analyst recommend be updated first to meet the security requirements and reduce risks?

A. VM_PRD_DB

B. VM_DEV_DB

C. VM_DEV_Web02

D. VM_PRD_Web01

Correct Answer: A

**QUESTION 14**

After updating the email client to the latest patch, only about 15% of the workforce is able to use email. Windows 10

users do not experience issues, but Windows 11 users have constant issues. Which of the following did the change management team fail to do?

A. Implementation

B. Testing

C. Rollback

D. Validation

Correct Answer: B

Testing is a crucial step in any change management process, as it ensures that the change is compatible with the existing systems and does not cause any errors or disruptions. In this case, the change management team failed to test the email client patch on Windows 11 devices, which resulted in a widespread issue for the users. Testing would have revealed the problem before the patch was deployed, and allowed the team to fix it or postpone the change.
References: 7 Reasons Why Change Management Strategies Fail and How to Avoid Them, CompTIA CySA+ CS0-003 Certification Study Guide

**QUESTION 15**

A security analyst has received an incident case regarding malware spreading out of control on a customer\\'s network. The analyst is unsure how to respond. The configured EDR has automatically obtained a sample of the malware and its signature. Which of the following should the analyst perform next to determine the type of malware, based on its telemetry?

A. Cross-reference the signature with open-source threat intelligence.

B. Configure the EDR to perform a full scan.

C. Transfer the malware to a sandbox environment.

D. Log in to the affected systems and run necstat.

Correct Answer: A