Free Questions for GSEC by actualtestdumps

Shared by Reyes on 12-12-2023

For More Free Questions and Preparation Resources

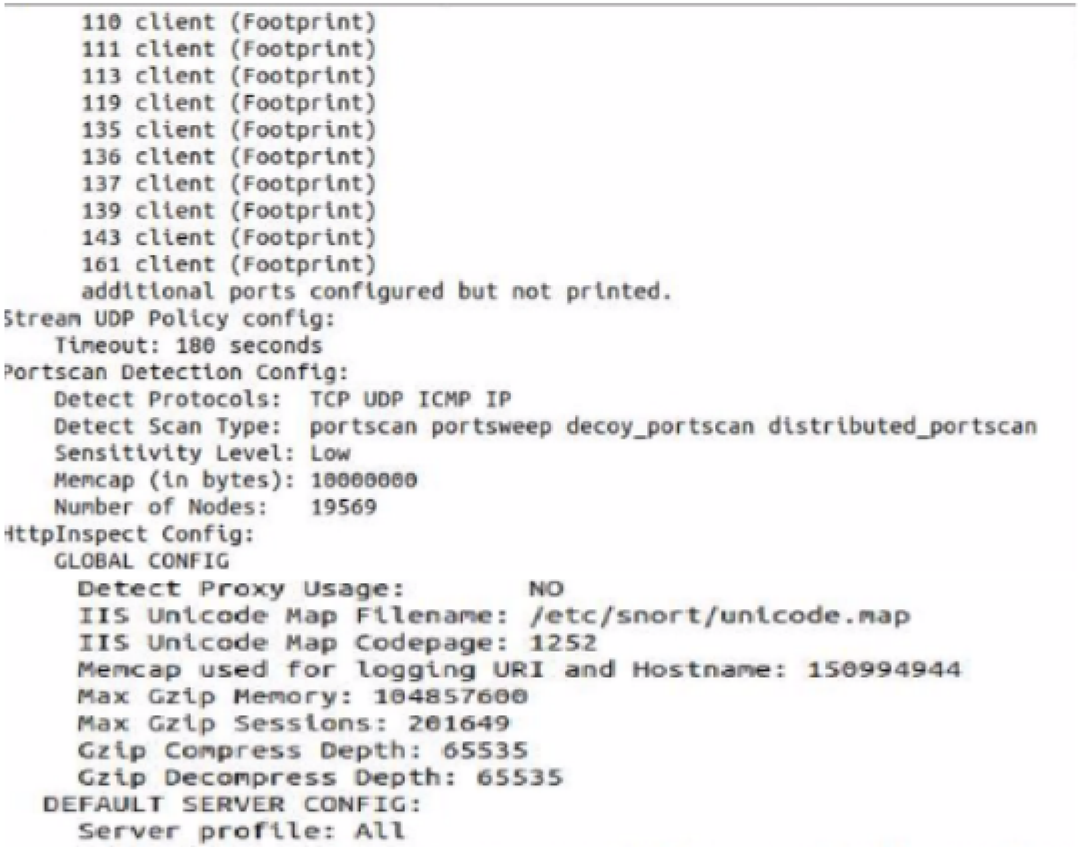
Check the Links on Last Page

Question 1

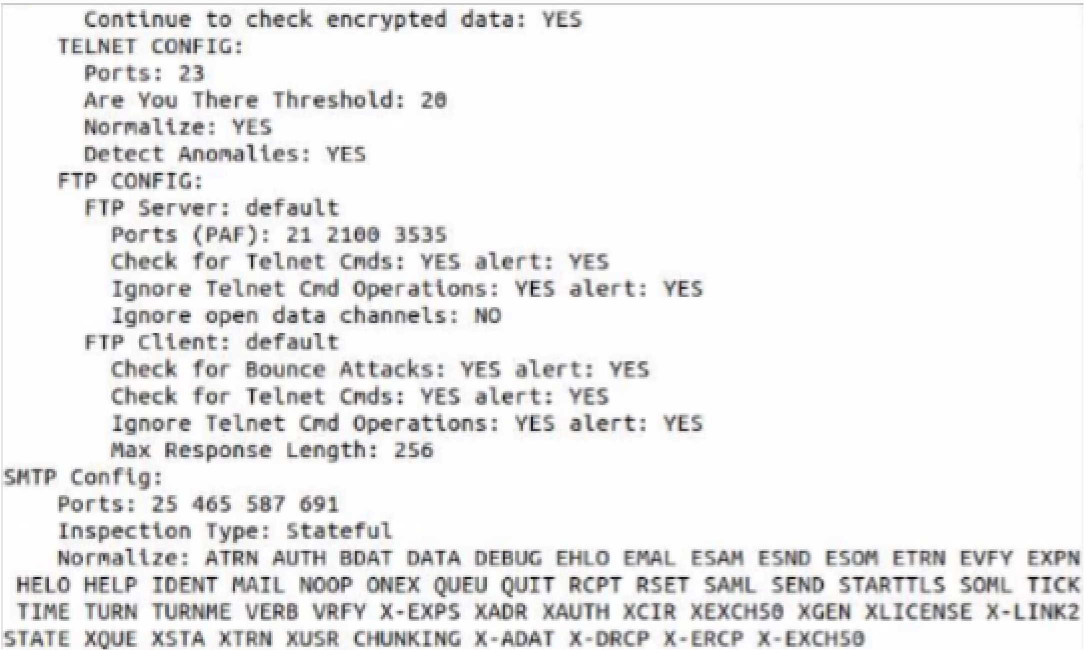
Question Type: MultipleChoice

Use sudo to launch Snort with the, /etc /snort /snort.conf file In full mode to generate alerts based on incoming traffic to echo. What is the source IP address of the traffic triggering an alert with a destination port of 156?

Note: Snort Is configured to exit after It evaluates 50 packets.



```
        110 client (Footprint)
        111 client (Footprint)
        113 client (Footprint)
        119 client (Footprint)
        135 client (Footprint)
        136 client (Footprint)
        137 client (Footprint)
        139 client (Footprint)
        143 client (Footprint)
        161 client (Footprint)
        additional ports configured but not printed.
Stream UDP Policy config:
    Timeout: 180 seconds
Portscan Detection Config:
    Detect Protocols:  TCP UDP ICMP IP
    Detect Scan Type:  portscan portsweep decoy_portscan distributed_portscan
    Sensitivity Level: Low
    Memcap (in bytes): 10000000
    Number of Nodes:   19569
HttpInspect Config:
    GLOBAL CONFIG
      Detect Proxy Usage:       NO
      IIS Unicode Map Filename: /etc/snort/unicode.map
      IIS Unicode Map Codepage: 1252
      Memcap used for logging URI and Hostname: 150994944
      Max Gzip Memory: 104857600
      Max Gzip Sessions: 201649
      Gzip Compress Depth: 65535
      Gzip Decompress Depth: 65535
    DEFAULT SERVER CONFIG:
      Server profile: All
```



```
      Continue to check encrypted data: YES
    TELNET CONFIG:
      Ports: 23
      Are You There Threshold: 20
      Normalize: YES
      Detect Anomalies: YES
    FTP CONFIG:
      FTP Server: default
        Ports (PAF): 21 2100 3535
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: YES alert: YES
        Ignore open data channels: NO
      FTP Client: default
        Check for Bounce Attacks: YES alert: YES
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: YES alert: YES
        Max Response Length: 256
SMTP Config:
    Ports: 25 465 587 691
    Inspection Type: Stateful
    Normalize: ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN
 HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND STARTTLS SOML TICK
 TIME TURN TURNME VERB VRFY X-EXPS XADR XAUTH XCIR XEXCH50 XGEN XLICENSE X-LINK2
STATE XQUE XSTA XTRN XUSR CHUNKING X-ADAT X-DRCP X-ERCP X-EXCH50
```

Options:

A- 192.168.^.30

B- 10.72.101.210

C- 10.10.28.19

D- 10.11.10.11

E- 10.10.10.66

F- 192.168.87.68

G- 10.12.10.112

H- 10.11.12.13

I- 10.10.201.150

J- 10.10.199.146

Answer:

I

Question 2

Question Type: **MultipleChoice**

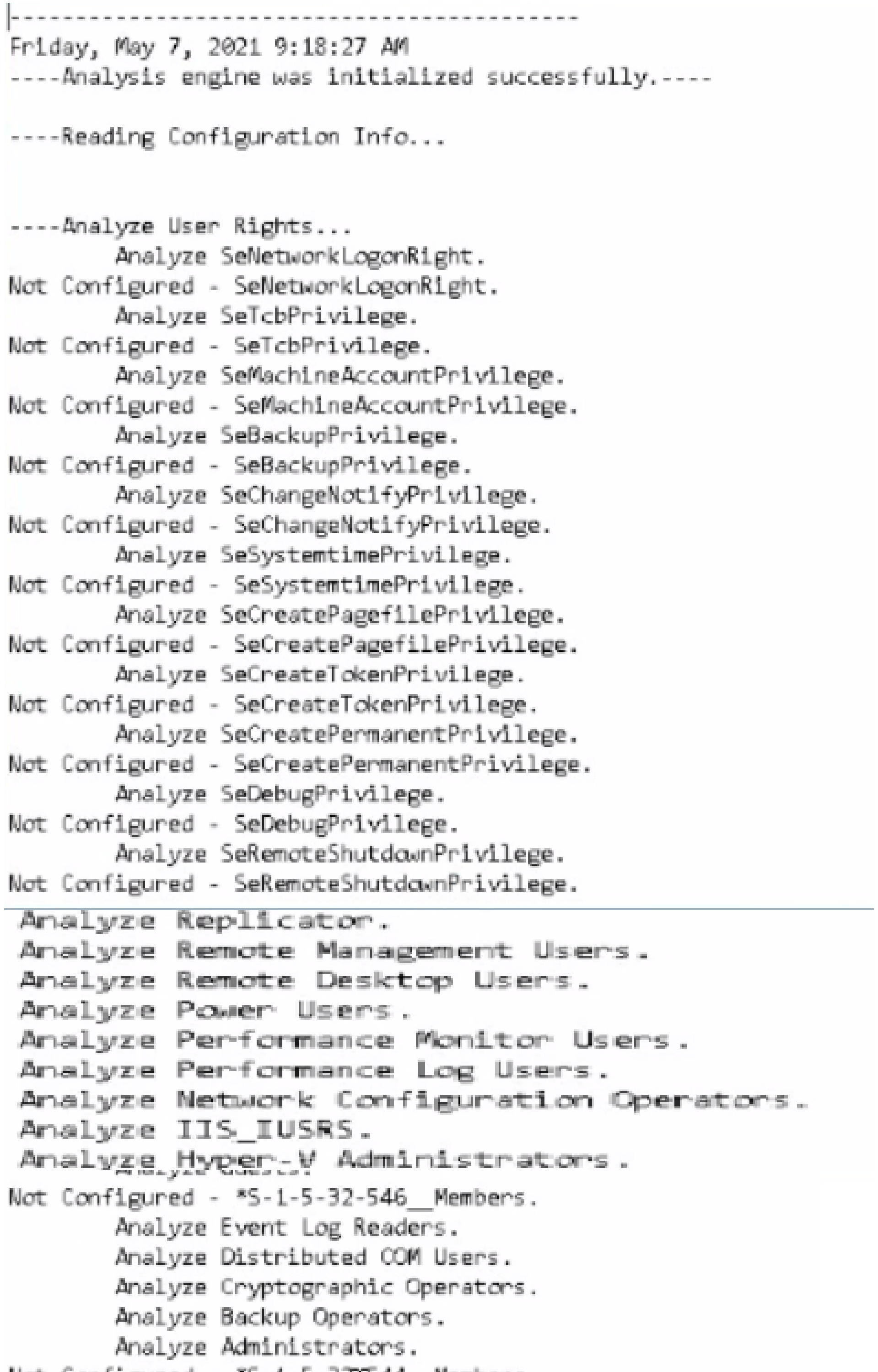
Using PowerShell ISE running as an Administrator, navigate to the

C:\hlindows\security\tevplatesdirectory. Use secedit.exe in analyze mode to compare the temp.sdb and uorkstdtionSecureTmplate.inf files, and output the findings to a file called log.txt. Which configuration setting under Analyze User Rights reports a mismatch?

Hints:

Use files located in the C \windows\security\templates\ directory

The log. txt file will be created in the directory the secedit.exe command is run from



```
----------------------------------------
Friday, May 7, 2021 9:18:27 AM
----Analysis engine was initialized successfully.----

----Reading Configuration Info...


----Analyze User Rights...
        Analyze SeNetworkLogonRight.
Not Configured - SeNetworkLogonRight.
        Analyze SeTcbPrivilege.
Not Configured - SeTcbPrivilege.
        Analyze SeMachineAccountPrivilege.
Not Configured - SeMachineAccountPrivilege.
        Analyze SeBackupPrivilege.
Not Configured - SeBackupPrivilege.
        Analyze SeChangeNotifyPrivilege.
Not Configured - SeChangeNotifyPrivilege.
        Analyze SeSystemtimePrivilege.
Not Configured - SeSystemtimePrivilege.
        Analyze SeCreatePagefilePrivilege.
Not Configured - SeCreatePagefilePrivilege.
        Analyze SeCreateTokenPrivilege.
Not Configured - SeCreateTokenPrivilege.
        Analyze SeCreatePermanentPrivilege.
Not Configured - SeCreatePermanentPrivilege.
        Analyze SeDebugPrivilege.
Not Configured - SeDebugPrivilege.
        Analyze SeRemoteShutdownPrivilege.
Not Configured - SeRemoteShutdownPrivilege.
 Analyze Replicator.
 Analyze Remote Management Users.
 Analyze Remote Desktop Users.
 Analyze Power Users.
 Analyze Performance Monitor Users.
 Analyze Performance Log Users.
 Analyze Network Configuration Operators.
 Analyze IIS_IUSRS.
 Analyze Hyper-V Administrators.
Not Configured - *S-1-5-32-546__Members.
        Analyze Event Log Readers.
        Analyze Distributed COM Users.
        Analyze Cryptographic Operators.
        Analyze Backup Operators.
        Analyze Administrators.
Not Configured - *S-1-5-32544__Members.
```

Options:

A- RemoteAccess

B- *S-l-5-32-544__ Members

C- Enable Admin Account

D- UseManger

E- AuditSystemEvents

F- AuditDSAccess.

G- SeSecurityPrivilege

H- SeinteractivelogonRight

I- SeServiceLogonRight:

J- lockoutBadCount

Answer:

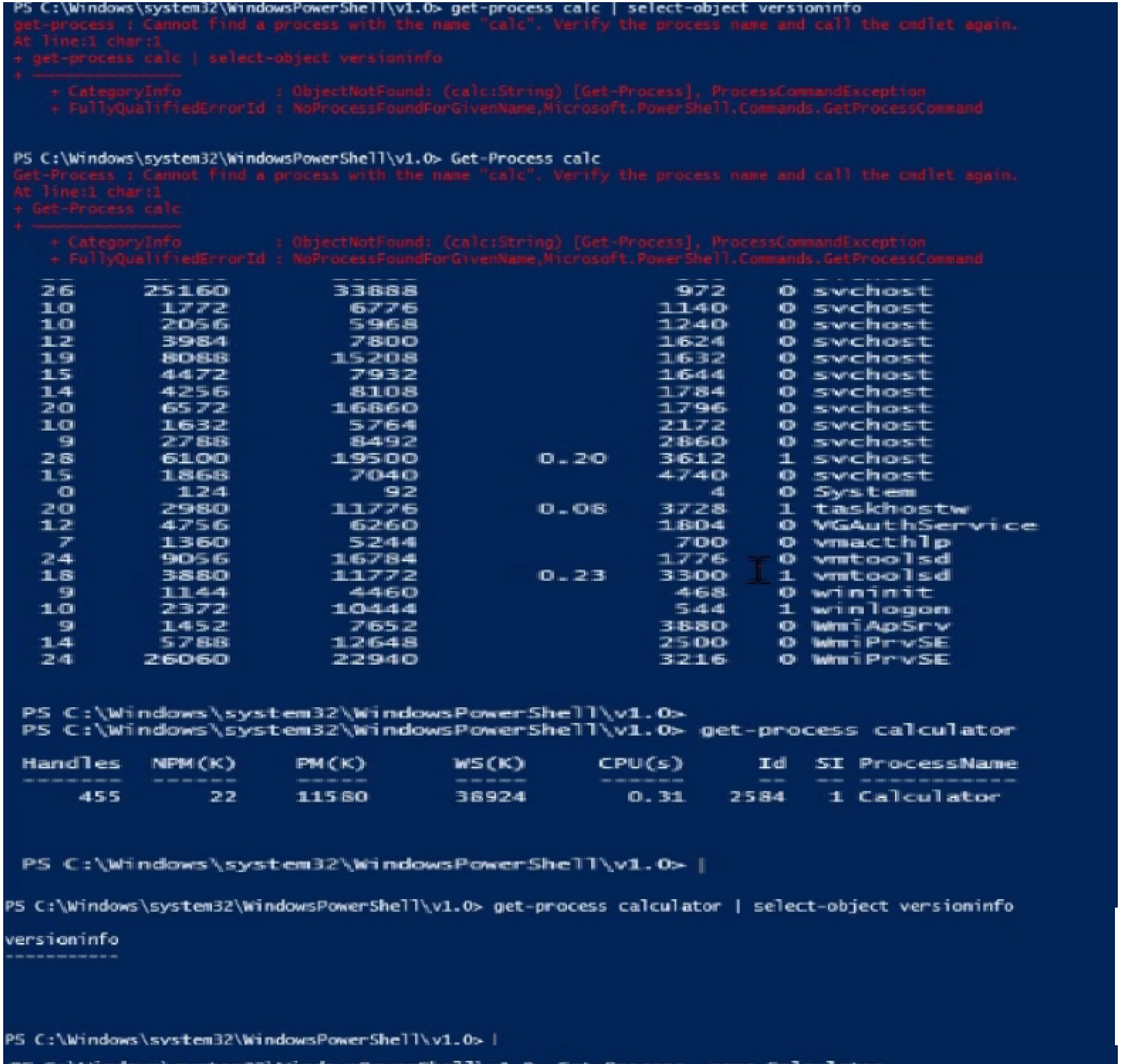
J

Question 3

Question Type: **MultipleChoice**

Launch Calculator (calc.exe). Using PowerShell, retrieve the Calculator Process Information. What is the value of the File Version property?

Hint: The process name of Calculator is calculator



```
PS C:\Windows\system32\WindowsPowerShell\v1.0> get-process calc | select-object versioninfo
get-process : Cannot find a process with the name "calc". Verify the process name and call the cmdlet again.
At line:1 char:1
+ get-process calc | select-object versioninfo
+ ~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (calc:String) [Get-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.GetProcessCommand


PS C:\Windows\system32\WindowsPowerShell\v1.0> Get-Process calc
Get-Process : Cannot find a process with the name "calc". Verify the process name and call the cmdlet again.
At line:1 char:1
+ Get-Process calc
+ ~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (calc:String) [Get-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.GetProcessCommand
     26     25160      33888                   972   0 svchost
     10      1772       6776                  1140   0 svchost
     10      2056       5968                  1240   0 svchost
     12      3984       7800                  1624   0 svchost
     19      8088      15208                  1632   0 svchost
     15      4472       7932                  1644   0 svchost
     14      4256       8108                  1784   0 svchost
     20      6572      16860                  1796   0 svchost
     10      1632       5764                  2172   0 svchost
      9      2788       8492                  2860   0 svchost
     28      6100      19500       0.20       3612   1 svchost
     15      1868       7040                  4740   0 svchost
      0       124         92                     4   0 System
     20      2980      11776       0.08       3728   1 taskhostw
     12      4756       6260                  1804   0 VGAuthService
      7      1360       5244                   700   0 vmacthlp
     24      9056      16784                  1776   0 vmtoolsd
     18      3880      11772       0.23       3300   1 vmtoolsd
      9      1144       4460                   468   0 wininit
     10      2372      10444                   544   1 winlogon
      9      1452       7652                  3880   0 WmiApSrv
     14      5788      12648                  2500   0 WmiPrvSE
     24     26060      22940                  3216   0 WmiPrvSE


PS C:\Windows\system32\WindowsPowerShell\v1.0>
PS C:\Windows\system32\WindowsPowerShell\v1.0> get-process calculator

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    455      22    11580      38924       0.31   2584   1 Calculator


PS C:\Windows\system32\WindowsPowerShell\v1.0> |

PS C:\Windows\system32\WindowsPowerShell\v1.0> get-process calculator | select-object versioninfo

versioninfo
-----------



PS C:\Windows\system32\WindowsPowerShell\v1.0> |
```

Options:

A- 10.1705.12507.0

B- 10.1902.1603.06155

C- 10.0.19041.1

D- 8.1.2017.26587

E- 8.2017.1009.04153

F- 10.1705.1809.07007

G- 8.2017.0908.29102

H- 8.1902.6547.63452

I- 10.0.14395.693

J- 8.1.875.154873

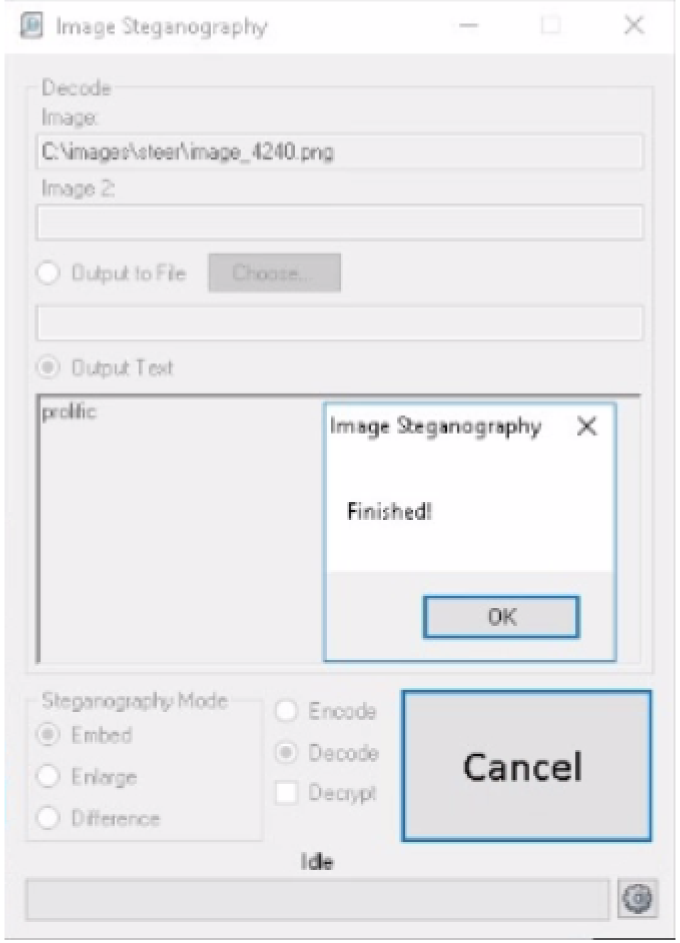
Answer:

F

Question 4

Question Type: MultipleChoice

In the directory C:\Images\steer there Is an Image file Image_4240.png with a data string encoded inside the file. What word is hidden in the file?



Decode

Image:
C:\images\steer\image_4240.png

Image 2:

○ Output to File

● Output Text

prolific

Image Steganography

Finished!

Steganography Mode
● Embed
○ Enlarge
○ Difference

○ Encode
● Decode
□ Decrypt

Idle

Options:

A- pontine

B- prolific

C- abysmal

D- petroleum

E- mushroom

F- Chicago

G- marshmallow

H- flying

I- shocking

Answer:

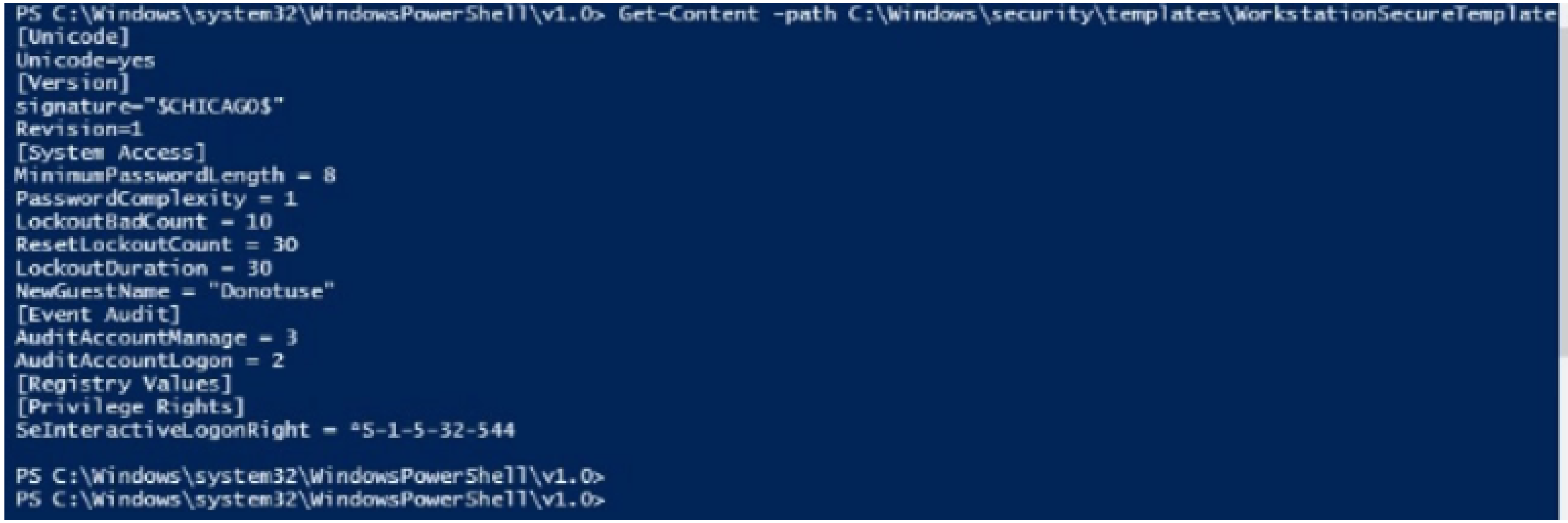
B

Question 5

Question Type: **MultipleChoice**

Use PowerShell ISE to

examineC:\Windows\security\templates\WorkstationSecureTemplate.inf. Which setting is configured in the template?



```
PS C:\Windows\system32\WindowsPowerShell\v1.0> Get-Content -path C:\Windows\security\templates\WorkstationSecureTemplate
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[System Access]
MinimumPasswordLength = 8
PasswordComplexity = 1
LockoutBadCount = 10
ResetLockoutCount = 30
LockoutDuration = 30
NewGuestName = "Donotuse"
[Event Audit]
AuditAccountManage = 3
AuditAccountLogon = 2
[Registry Values]
[Privilege Rights]
SeInteractiveLogonRight = *S-1-5-32-544

PS C:\Windows\system32\WindowsPowerShell\v1.0>
PS C:\Windows\system32\WindowsPowerShell\v1.0>
```

Options:

A- ResetLockoutCount

B- NewAdministratorName

C- MinirnumPasswordAge

D- Require logonToChangoPassword

E- SeRemotPlnteractiveLogonRlght

F- MaxRenewAge

G- AuditSystemEvents

H- EnableGuestAccount

I- AuditPolicyChange

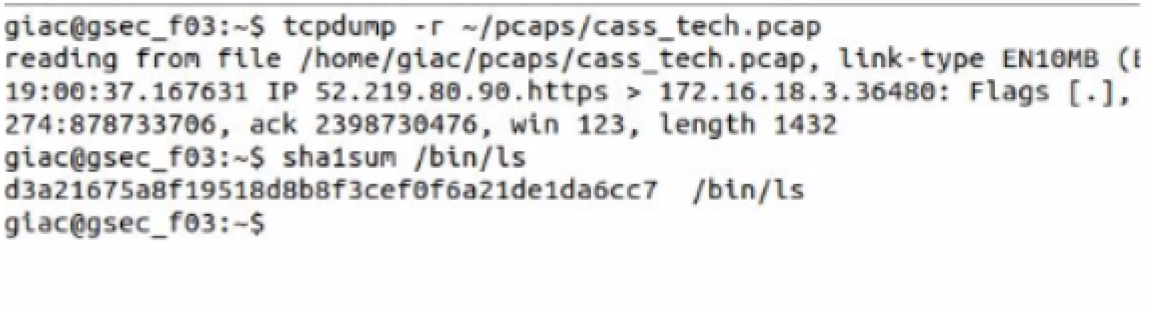
Answer:

A

Question 6

Question Type: **MultipleChoice**

What is the SHA1 hash of the Ale /bin/Is?



```
giac@gsec_f03:~$ tcpdump -r ~/pcaps/cass_tech.pcap
reading from file /home/giac/pcaps/cass_tech.pcap, link-type EN10MB (E
19:00:37.167631 IP 52.219.80.90.https > 172.16.18.3.36480: Flags [.],
274:878733706, ack 2398730476, win 123, length 1432
giac@gsec_f03:~$ sha1sum /bin/ls
d3a21675a8f19518d8b8f3cef0f6a21de1da6cc7  /bin/ls
giac@gsec_f03:~$
```

Options:

A- a895bac9c3<M75d5fa7fb5820b35568cedb5dc23

B- 54771b4r<d7tKb4382e670b4465O265206cf09e9

C- a39bed3C496fC764fc518d3e2d56f7d0f4C625fb

D- 93c1 ffbd22ebcad798886fb4aa46fa 357b23d80a

E- aa40739f465ded2245872b1e4972e33d5bObb1cb

F- 494a 192859f 244c69d5bdc46255d b44l9e 7d051 f

G- d3a21675a8f 19518d8b8f3cefOf6a21 del da6cc7

H- 84611 eOb6d59045bOcf 189fca9bc760afdf b7372

I- 8873 5f5cb7CCf7b2d 137944ab1 2d 116808310500

J- 2cadod58fbd0345c2ced336f9a3ae6f43cf355fi

Answer:

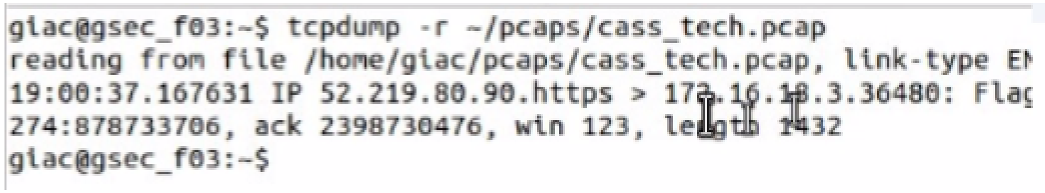
G

Question 7

Question Type: MultipleChoice

Open the MATE terminal and use the tcpdump program to read - /pcaps /cass tech.pcap.

What is the source port number?



```
giac@gsec_f03:~$ tcpdump -r ~/pcaps/cass_tech.pcap
reading from file /home/giac/pcaps/cass_tech.pcap, link-type EN
19:00:37.167631 IP 52.219.80.90.https > 172.16.18.3.36480: Flag
274:878733706, ack 2398730476, win 123, length 1432
giac@gsec_f03:~$
```

Options:

A- 878733706

B- 123

C- 443

D- 878732274

E- 36480

F- 2398730476

G- 1432

H- 80

I- 25

Answer:

E