CYBER RANGERS

ARMORING YOUR BUSINESS

POWERSHELL BASIC SCRIPTING
MODULE 5: POWERSHELL AND WMI

Jan Marek | Cyber Rangers

OSCP | eCPPT | CEH | CHFI | CompTIA Pentest+ | CEI | MVP | MCT | MCC | MCSA | MCSE

Ethical Hacker, Forensic Investigator & Security Engineer

jan@cyber-rangers.com | www.cyber-rangers.com

AGENDA

- How to query data using WMI and CIM
- How to invoke WMI and CIM methods
- WMI/CIM Remoting

WMI VS. CIM CMDLETS

```
Get-Command -Noun *CIM* #CIM cmdlets (WinRM for remote connection)
Get-Command -Noun *WMI* #WMI cmdlets (RPC for remote connection
```

LOOKUP THE CLASS

- Find the right WMI class
  - Using **WMI Explorer**
  - Using **WMI Explorer v2**
  - Using Powershell

```
Get-WmiObject -List -Class win32_bios
Get-CimClass -ClassName win32_bios
```

ENUMERATE INSTANCES

- Use cmdlet

```
Get-WmiObject -Class win32_Bios
Get-CimInstance -ClassName win32_Bios
```

- Use cmdlet filter

```
Get-WmiObject -Class win32_logicaldisk -Filter "DeviceID='C:'"
Get-CimInstance -ClassName Win32_LogicalDisk -Filter "DeviceID='C:'"
```

- Use query (WQL)

```
Get-WmiObject -Query "select * from win32_logicaldisk where DeviceID='C:'"
Get-CimInstance -Query "select * from win32_logicaldisk where DeviceID='C:'"
```

INVOKE METHODS

- WMI

```
Invoke-WmiMethod -Class win32_process -Name create -ArgumentList notepad.exe
```

- CIM

```
Invoke-CimMethod -ClassName win32_process -MethodName create `
-Arguments @{commandline='notepad.exe'}
```

WMI REMOTING

- Enumerate

```
Get-WmiObject -Class win32_computersystem -ComputerName dc
#network communication done over RPC (TCP135, dynamic port range)

Get-CimInstance -ClassName win32_computersystem -ComputerName dc
#network communication done over WinRM (TCP80, TCP443)
```

- Modify

```
$cimsession = New-CimSession -ComputerName dc -Credential (Get-Credential)
Invoke-CimMethod -CimSession $cimsession -ClassName win32_process `
-MethodName create -Arguments @{commandline='notepad.exe'}
```

LAB

POWERSHELL BASIC SCRIPTING
MODULE 5: POWERSHELL AND WMI

Jan Marek | Cyber Rangers

OSCP | eCPPT | CEH | CHFI | CompTIA Pentest+ | CEI | MVP | MCT | MCC | MCSA | MCSE

Ethical Hacker, Forensic Investigator & Security Engineer

jan@cyber-rangers.com | www.cyber-rangers.com

CYBER RANGERS

ARMORING YOUR BUSINESS