LEXSI INNOVATIVE SECURITY. FOR BUSINESS
Conseil / Audit / Formations
Veille et lutte contre la cybercriminalité

WMI SHELL

A new way to get shells on remote Windows machines

using only the WMI service

Andrei Dumitrescu
Security Consultant, LEXSI

SUMMARY

- Introduction
- Authenticated remote code execution (RCE) methods on Windows
- WMI basics & existing tools
- WMI Shell tool: research & implementation
- Demo
- Conclusion

PLAN

Introduction

Authenticated RCE methods on Windows

WMI basics & existing tools

WMI Shell tool: research & implementation

Demo

Conclusion

Questions ?

INTRODUCTION

- **whoami**
  - Andrei Dumitrescu
  - M.Sc. in Information Security (Versailles, France), B.Sc. in Computer Science (Timisoara, Romania)
  - Internship at LEXSI in 2013 → this research!
  - Pentester for LEXSI and occasional CTF player with HZV
  - email: adumitrescu@lexsi.com, twitter: @_dracu_
- **whois** LEXSI

INTRODUCTION

LEXSI

INNOVATIVE SECURITY. FOR BUSINESS

Conseil / Audit / Formations

Veille et lutte contre la cybercriminalité

- IT security consulting
- Founded in 1999
- 600 clients
- 75% of CAC 40 companies
- More than 300 audits per year
- Certified CERT team

Paris
Lyon
Lille
Montréal
Singapour

INTRODUCTION

WMI Shell – **how** ?

- Internship research subject
- Original idea by Nicolas Kerschenbaum

WMI Shell – **why ?**

- You can’t PsExec your way into everything
- Missing piece of the puzzle
- Fully exploit the WMI infrastructure

PLAN

- Introduction
- **Authenticated RCE methods on Windows**
- WMI basics & existing tools
- WMI Shell tool: research & implementation
- Demo
- Conclusion
- Questions ?

LEXSI

AUTHENTICATED RCE METHODS IN WINDOWS

PsExec (& clones)

How it works

Copies the Psexesvc service on the Admin$ share of the remote system, activates it using the Service Control Manager (SCM) and communicates with it via a named pipe.

Requirements & limitations

- Access to the Admin$ share (port 445)
- Active User Account Control (UAC) means only domain accounts can use PsExec.

AUTHENTICATED RCE METHODS IN WINDOWS

Remote File Access

How it works

Copy a file to the remote computer in:

- c:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\
- %WINDIR%\system32\wbem\mof\ ← for MOF files

Command is executed on login or boot.

MOF Files can be automatically compiled and registered by WMI on old Windows (before Vista). Running as SYSTEM. « Stuxnet style ».

Requirements & limitations

- Access to the hidden administrative share C$ (port 445).

AUTHENTICATED RCE METHODS IN WINDOWS

WinRM (Windows Remote Management)

How it works

- The WinRM server listens on ports 80,443 (old versions) and 5985, 5986 (new versions).
- Accepts WMI queries (WQL).

Requirements & limitations

- Installed but not enabled by default on Windows XP+
- 5 minutes time-to-live for WinRS shells.

PLAN

- Introduction
- Authenticated RCE methods on Windows
- **WMI basics & existing tools**
- WMI Shell tool: research & implementation
- Demo
- Conclusion
- Questions ?

WMI BASICS

Definition

Windows Management Instrumentation (WMI) is the infrastructure for management data and operations on Windows-based operating systems.

Get management data like:

- User account information, process list, environment variables, network configuration etc.

Execute operations:

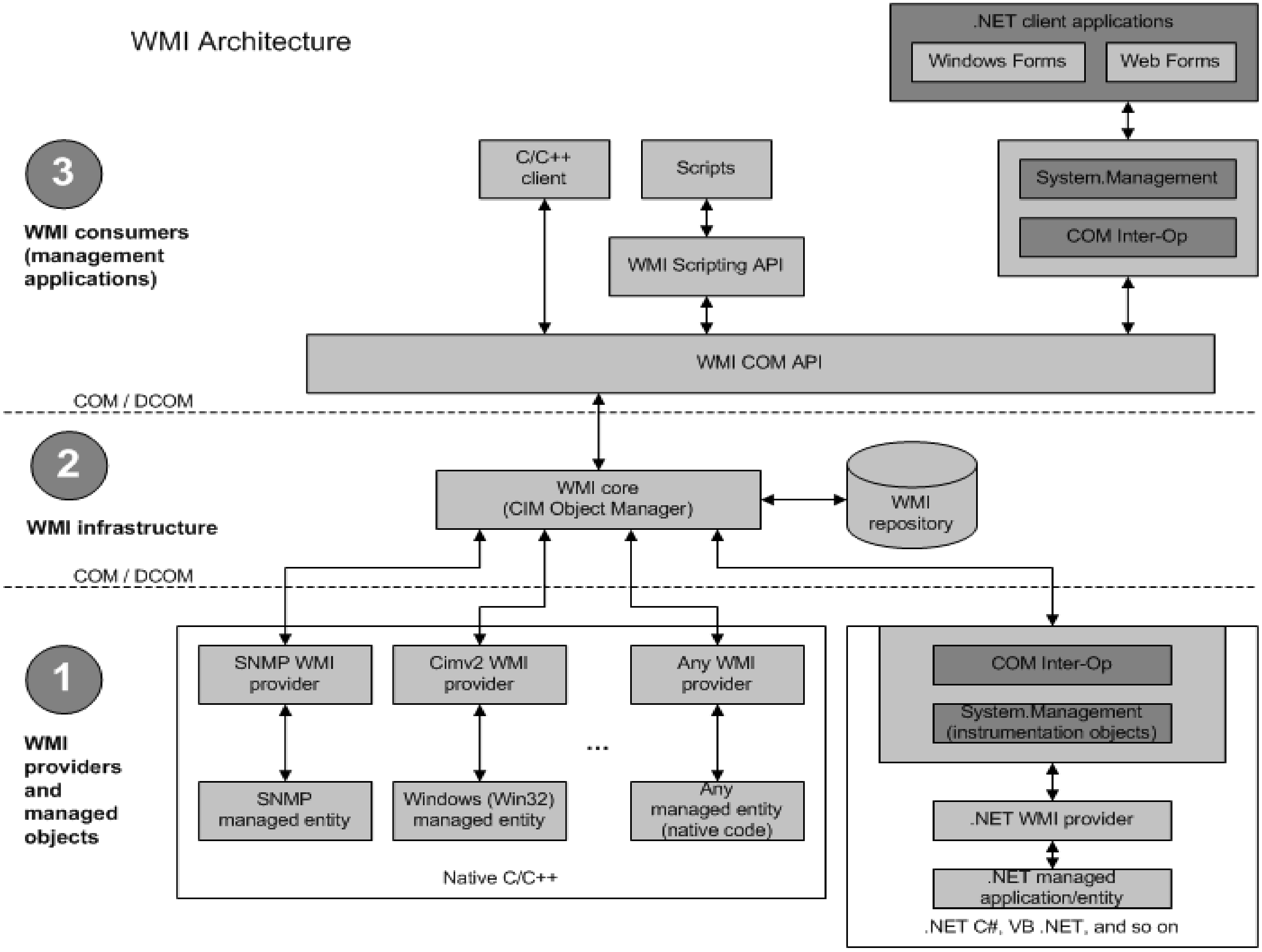
- Create/kill processes, shutdown machine, ping

WMI service can be reached on port 135. Available only for admins

WMI BASICS

- Data source:
  - WMI Providers
  - MOF Files and DLLs: %windir%\system32\wbem
- Data organization: WMI repository
- Data access:
  - WMI Query Language (WQL) – read-only
  - Scripts & applications that use WQL

WMI BASICS


WMI Architecture
.NET client applications
Windows Forms
Web Forms
3
WMI consumers (management applications)
C/C++ client
Scripts
WMI Scripting API
System.Management
COM Inter-Op
WMI COM API
COM / DCOM
2
WMI infrastructure
WMI core (CIM Object Manager)
WMI repository
COM / DCOM
1
WMI providers and managed objects
SNMP WMI provider
Cimv2 WMI provider
Any WMI provider
SNMP managed entity
Windows (Win32) managed entity
...
Any managed entity (native code)
Native C/C++
COM Inter-Op
System.Management (instrumentation objects)
.NET WMI provider
.NET managed application/entity
.NET C#, VB .NET, and so on

WMI BASICS: EXISTING TOOLS

- **wmic**:
  - default tool on Windows
  - executes WQL query : “select * from Win32_Process”
  - or it executes an alias: “process list”

- **wmis**:
  - wrapper on Linux for “wmic process call create”
  - available on Kali Linux
  - also available as **pth-wmis** on Kali Linux

PLAN

- Introduction
- Authenticated RCE methods on Windows
- WMI basics & existing tools
- **WMI Shell tool: research & implementation**
- Demo
- Conclusion
- Questions ?

WMI SHELL TOOL: RESEARCH

- Demo: wmic, wmis
- WQL is **read-only**: no INSERT or UPDATE statements
- How do you get the command output out???

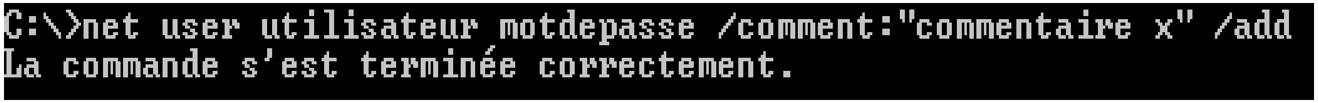
WMI SHELL TOOL: RESEARCH

WMI SHELL TOOL: RESEARCH

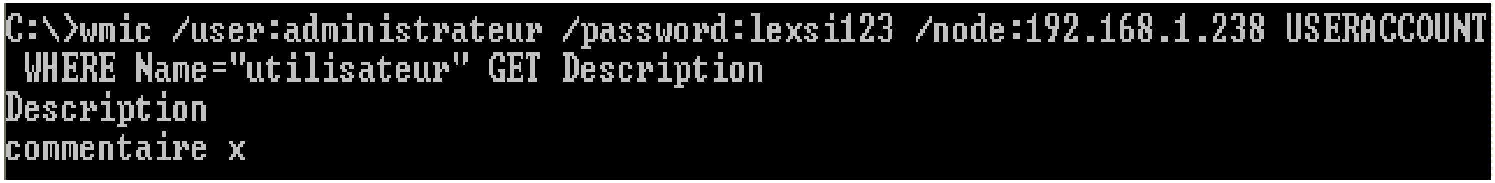
- Standard way: remote file access
- **The new way**: create and store data with WMI
- Possible methods and their limitations

WMI SHELL TOOL: RESEARCH

1. Create Windows user accounts:



```
C:\>net user utilisateur motdepasse /comment:"commentaire x" /add
La commande s'est terminée correctement.
```

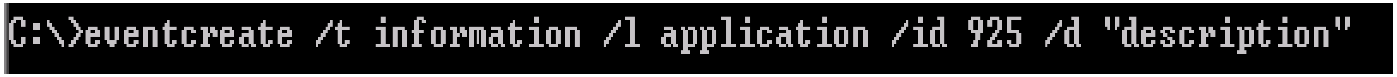


```
C:\>wmic /user:administrateur /password:lexsi123 /node:192.168.1.238 USERACCOUNT
 WHERE Name="utilisateur" GET Description
Description
commentaire x
```

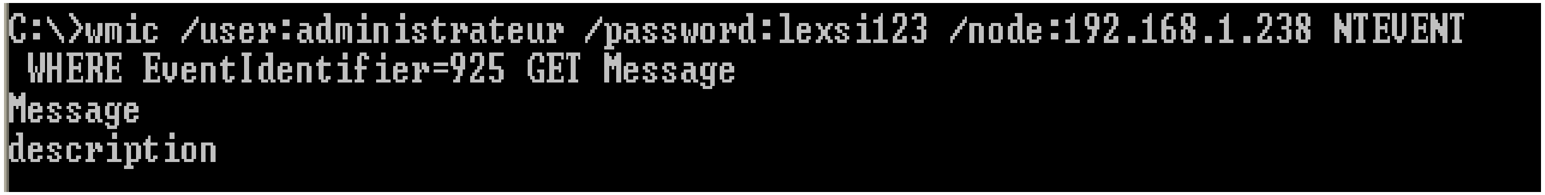
- Limits: maximum 48 characters

WMI SHELL TOOL: RESEARCH

2. Create events in log files:



```
C:\>eventcreate /t information /l application /id 925 /d "description"
```

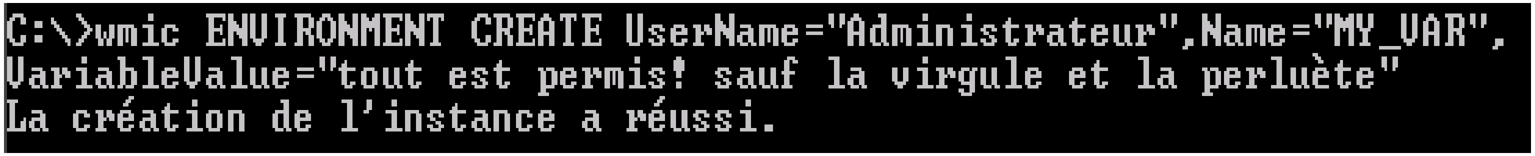


```
C:\>wmic /user:administrateur /password:lexsi123 /node:192.168.1.238 NTEVENT
 WHERE EventIdentifier=925 GET Message
Message
description
```

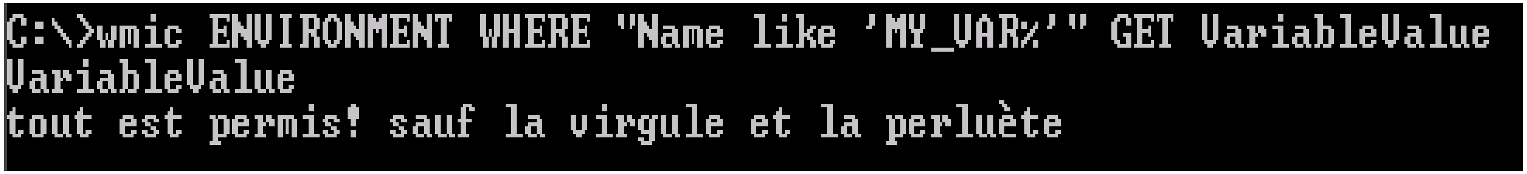
- Limits: maximum 255 characters

WMI Shell tool: research

3. Create environment variables:



```
C:\>wmic ENVIRONMENT CREATE UserName="Administrateur",Name="MY_VAR",
VariableValue="tout est permis! sauf la virgule et la perluète"
La création de l'instance a réussi.
```



```
C:\>wmic ENVIRONMENT WHERE "Name like 'MY_VAR%'" GET VariableValue
VariableValue
tout est permis! sauf la virgule et la perluète
```

- Limits: maximum 32767 characters, but…

WMI SHELL TOOL: RESEARCH

- **Finally**: WMI Namespaces
  - Only [A-z_0-9] characters (it seemed…)
  - Limited at ~8000 characters
  - Inside WMI repository
  - As many as you want
- Limits: Base64 characters [a-Z0-9+/] are “difficult” to store
- Default namespaces:
  - root\default, root\cimv2, root\subscription

WMI SHELL TOOL: IMPLEMENTATION

- Written in Python & VBScript (for obvious reasons)
- Proof-of-concept
- Emulates an interactive shell
- Execute commands / display output
- File upload using a **command stager** (inspired by Metasploit's VBScript Command stager)
- VBScript file does all the work, executed by **wmis**

WMI SHELL TOOL: IMPLEMENTATION

Execution stages:

1

Execute **wmis** , send the VBScript file via **echo** commands:

```
echo ‘VBScript commands’ > r4nd0mN4m3.vbs
```

2

The command entered is executed by the VBScript file and the output is uploaded piece by piece inside WMI:

```
cscript %TEMP%\r4nd0mN4m3.vbs "dir %Temp%"
```

3

When upload to WMI is complete, we download the command output with **wmic:**

```
wmic [..] "select Name from __Namespace where Name
like 'EVILTAG%‘
```

WMI Shell tool: implementation

- File upload: VBScript is not an efficient base64 decoder
- Send an efficient decoder first (a base64.exe, written in C)
- The actual file we want is uploaded and decoded with the efficient decoder

PLAN

- Introduction
- Authenticated RCE methods on Windows
- WMI basics & existing tools
- WMI Shell tool: research & implementation
- **Demo**
- Conclusion
- Questions ?

PLAN

Introduction

Authenticated RCE methods on Windows

WMI basics & existing tools

WMI Shell tool: research & implementation

Demo

Conclusion

Questions ?

LEXSI

CONCLUSION

- Advantages:
  - The WMI technology is built into all Windows versions since Windows Millenium
  - No need for remote file access !
  - It’s stealthy ☺
- Limitations:
  - Local Firewall, if active, must be configured to allow remote WMI access
  - On Windows Vista+, UAC can be a problem:

User Account Control and WMI

LEXSI

CONCLUSION

- Possible improvements:
  - Build an efficient tool (non-interactive mode, deploy and execute on multiple targets).
  - Compress files before upload
  - Powershell
  - Add “change dir” feature
  - Metasploit module or **wmis** patch
  - Multi-threading
  - …
- Download here: https://www.lexsi.fr/conference/wmi-shell.zip

WMI BASICS

References:

1. http://i.msdn.microsoft.com/dynimg/IC108955.png
2. http://www.dmtf.org/sites/default/files/standards/documents/DSP0004V2.3_final.pdf
3. http://msdn.microsoft.com/en-us/library/aa826699%28v=vs.85%29.aspx
4. http://passing-the-hash.blogspot.fr/2013/04/missing-pth-tools-writeup-wmic-wmis-curl.html
5. http://passing-the-hash.blogspot.fr/2013/07/WMIS-PowerSploit-Shells.html
6. http://www.blackhat.com/presentations/bh-dc-10/Bannedit/BlackHat-DC-2010-Bannedit-Advanced-Command-Injection-Exploitation-1-wp.pdf
7. http://www.scriptjunkie.us/2013/02/authenticated-remote-code-execution-methods-in-windows/

PLAN

- Introduction
- Authenticated RCE methods on Windows
- WMI basics & existing tools
- WMI Shell tool: research & implementation
- Demo
- Conclusion
- **Questions ?**

LEXSI