Secure Coding.
Practical steps to defend your web apps.

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?
Check out the list of upcoming events offering  
"Defending Web Applications Security Essentials (DEV522)"
 at http://software-security.sans.orghttp://software-security.sans.org/events/
How to Avoid Information Disclosure when Managing Windows with WMI

GSEC Gold Certification

Author: Alex M. Timkov, atimkov@gmail.com

Adviser: John C. A. Bambenek

Accepted: April 2007
How to Avoid Information Disclosure when Managing Windows with WMI

Table of Content

1. Introduction ................................................................................................................. 6

2. Brief Introduction to Windows Management Interface Access ............................. 7

   2.1. Using the Object Method to Access WMI .......................................................... 7

   2.2. Alternative WMI Access with Monkier String ................................................. 12

3. WMI Default Security on the Wire ........................................................................... 15

4. WMI Scripting Security Options ............................................................................... 19

5. Avoiding the Trap with Packet Privacy ..................................................................... 23

6. Improved WMI Connection Security on the Wire .................................................. 28

7. Advanced WMI Scripting Security Options ............................................................. 32

   7.1. Keep Administrative Passwords out of Scripts ............................................... 32

   7.2. Using Specific Permissions in WMI Scripts ...................................................... 35

   7.3. WMI Authority ................................................................................................. 38

   7.4. Summary of WMI Scripting Security Options ................................................ 40

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

7.5. WMI Default Impersonation and Legacy Platforms ........................................... 41

8. Securing the Server for WMI Management .......................................................... 41

8.1. Scripting Account and Administrative Rights .................................................. 42

8.2. WMI Namespace Security Auditing ................................................................. 44

8.3. Request Encrypted WMI Connections to the Server ........................................ 47

8.4. Configure DCOM for Remote WMI Access ..................................................... 49


10. References ......................................................................................................... 52

11. Appendixes ....................................................................................................... 55

 Appendix 1: Capture of Default WMI Request and Response .............................. 55

 Appendix 2: Secure WMI Information Exchange on the Wire .............................. 62

 Appendix 3: Enforcing Encrypted Access at the Server ....................................... 70

 Appendix 4: Cross Platform WMI Connection Limitations ................................. 72

 Appendix 5: Setting DCOM Remote Access Security .......................................... 72

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

Appendix 6: Vista Specific Security Descriptor Access ...........................................74

Appendix 7: Sample WMI Service Management Script ...........................................78
List of Figures

Figure 1: WMI Service Start Script ................................................................. 9

Figure 2: WMI Data Exchange on the Wire .................................................... 16

Figure 3: WMI Impersonation Levels ............................................................... 21

Figure 4: WMI Authentication Levels ............................................................. 23

Figure 5: Updated WMI Service Start Script ............................................... 28

Figure 6: Secure WMI Data Exchange on the Wire ....................................... 30

Figure 7: Specific Permissions for WMI Scripting ......................................... 37
1. **Introduction**

Windows Management Instrumentation (WMI) is a widespread mechanism of managing Windows infrastructure. WMI is convenient. It gives Windows administrators and developers easy access to a wealth of system objects and object properties, allowing for relatively easy automation of administrative tasks and monitoring of the operating system, and in many cases applications and hardware. The convenience of WMI is a compelling reason for adopting WMI as a way of monitoring and managing Windows infrastructure. Many vendors have implemented their Windows monitoring and management solutions by using WMI. Before you do, it is worth taking a quick look at some of the security aspects of the WMI scripting mechanism. It is all too often that Windows provides the security features that can be used effectively, but fails to supply the default configuration that would benefit from own security features that are available and are waiting to be of service. WMI is no exception.

This paper provides an introduction to accessing Windows via WMI in a secure manner. After introducing the subject of WMI security, we will demonstrate how the default WMI access level leads to unnecessary exposure of rather sensitive information, as management data travels between the management station and the Windows hosts that are being managed via WMI. We will make recommendations on using WMI to manage remote Windows hosts securely, without exposing the sensitive management session.
How to Avoid Information Disclosure when Managing Windows with WMI

information. We will demonstrate how very simple and effective measures can stop unnecessary information leaks and boost management access security.

2. **Brief Introduction to Windows Management Interface Access**

2.1. **Using the Object Method to Access WMI**

WMI is most frequently accessed with VBScript due to the simplicity of VBScript code. Other scripting languages may be used to access WMI, however in most cases more lines of code may be required to achieve the same purpose. Another reason for the widespread use of VBScript for scripting WMI connectivity is the large number of classes and objects immediately accessible for retrieval. Last and not least, VBScript is included with any modern Windows operating system. Provided you do not mind using Notepad to edit text, a simple development environment and interpretation is taken care of, without the requirement for additional software. All of the examples in this paper are written in VBScript.

The goal of this paper is to focus on the security issues associated with WMI, and to suggest workarounds to these issues. This paper is not a WMI scripting guide. However, initial understanding of WMI access techniques is required to follow further sections of the paper. This section provides such basic introduction to accessing WMI with VBScript.

Here is the sample script that was used to perform some of the testing during the...
How to Avoid Information Disclosure when Managing Windows with WMI

research phase. This script can be used to start a service on a remote system:

```vbscript
'---------- Service Start Script - WMI Based -------------
'
' Test the state of the service of user choice on the remote host
' Start the service on the remote host if the service is not running
'
' Written by Alex Timkov to facilitate SANS GSEC research paper
'-------------------------------------------------------------------

Option Explicit

Dim strComputer, strPassword, strService, strUser
Dim objLocator, objService, objWMIService
Dim colServices
Dim intTimeout

intTimeout = 10000

Do
  strComputer = inputbox
    ("Please enter host name or IP address", "Input")
Loop until strComputer <> ""

Do
  strUser = inputbox("Please enter username", "Input")
Loop until strUser <> ""

Do
  strPassword = inputbox("Please enter password", "Input")
Loop until strPassword <> ""

strService = inputbox
  ("Please enter the name of service to start, " & 
   "or hit Enter to exit", "Input")

If strService <> ""
  Then

    Set objLocator = CreateObject("WbemScripting.SWbemLocator")

    Set objWMIService = objLocator.ConnectServer
      (strComputer, "root\CIMV2", strUser, strPassword)

    Set colServices = objWMIService.ExecQuery
      ("Select * from Win32_Service Where Name = " & 
       strService & "")

    If Not(colServices Is Nothing)
      Then
        For Each objService in colServices
          If Not(objService Is Nothing)
            Then
              If objService.State = "Stopped" Then
                Wscript.Echo vbCrlf & "Starting " & strService _
                  & " service..."
            End If
          End If
        Next
    End If

```

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

```vbscript
objService.StartService()
WSCript.Sleep intTimeout
Else
    WScript.Echo vbCrLf & "Service is not stopped."
End If
End If
Next
End If

Set objService = Nothing
Set colServices = Nothing
Set objWMIService = Nothing
Set objLocator = Nothing

End If

WScript.Echo vbCrLf & "Script execution completed. Exiting."
WScript.Quit

' ........................................
' End of WMI Based Service Start Script
' ........................................
```

**Figure 1: WMI Service Start Script**

The WMI connection establishment and object retrieval starts mid-way through the sample script. The script is of 73 lines, and the first WMI specific line is line 37:

```vbscript
Set objLocator = CreateObject("WbemScripting.SWbemLocator")
```

Prior to this line, the code is non WMI specific VB Script: declarations and dialogs to accept user input of the remote system name or IP address, the name of the user authorised to carry out the remote operation, the user password, and the name of the service to be tested for current state and started if it is found to be in a stopped state.

The line referenced above does nothing else but accessing the standard object named SWbemLocator. The next line makes use of the method called ConnectServer to connect to the standard WMI namespace root\CIMV2 on the remote host specified by

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

strComputer, using the user account strUser with the account password strPassword:

```vbscript
Set objWMIService = objLocator.ConnectServer(strComputer, "root\CIMV2", strUser, strPassword)

objWMIService.Security_ property can then be used to set specific security parameters for the WMI namespace connection. We will cover WMI security parameters in more detail in the following sections. We will stick with the default WMI security values for the moment. It is one of our targets to see what is happening across a WMI management connection when the default WMI security settings are used.

Once the WMI namespace connection has been established, we can retrieve the objects that belong to the namespace. We also get a powerful capability to read and modify object properties that will control the behaviour of the operating system on the remote host. There are several ways to achieve this purpose. We will use the ExecQuery method. The ExecQuery method allows for the selective retrieval of objects, thus minimising the size of data retrieved and transported across the network. Other methods of WMI object retrieval typically extract more information than is necessary to perform the system management or monitoring task of choice. The line below retrieves only the collection of service(s) that match the string specified by strService:

```vbscript
Set colServices = objWMIService.ExecQuery("Select * from Win32_Service Where Name=" & strService & ")
```

The next section of code is iterative. It steps through the returned object collection, performs error tests, checks the state of the requested service, and starts the requested

Alex M. Timkov
service if it is in a stopped state. Otherwise, the script reports that the service is not found to be in a stopped state:

```vbscript
If Not(colServices Is Nothing) Then
    For Each objService in colServices
        If Not(objService Is Nothing) Then
            If objService.State = "Stopped" Then
                Wscript.Echo vbCrLf & "Starting " & strService & " service..."
                objService.StartService()
                WScript.Sleep intTimeout
            Else
                Wscript.Echo vbCrLf & "Service is not stopped."
            End If
        End If
    Next
End If
```

There are more service state tests that can be and should be carried out, but for the simplicity sake, we will limit ourselves with a single service state test per iteration.

The last section of the script performs the cleanup:

```vbscript
Set objService = Nothing
Set colServices = Nothing
Set objWMIService = Nothing
Set objLocator = Nothing
```

Our brief introduction to WMI scripting by stepping through our sample script should be sufficient for the purpose of basic understanding of how to construct WMI access to a remote system. Hope this section helps appreciation of the simplicity and power of WMI.
How to Avoid Information Disclosure when Managing Windows with WMI

access, and more importantly, appreciation of the security responsibility associated with the easy and powerful system management mechanism such as WMI.

If you would like a text introducing basic WMI architecture and scripting technique, you could pay a visit to Microsoft's Scripting Clinic and retrieve the set of three articles written by Greg Stemp, Dean Tsaltas, Bob Wells of Microsoft, and Ethan Wilansky of Network Design Group. These texts were written in 2002 - 2003, however this set of introductory articles remains a good point to get familiar with WMI. Here are the links:


After developing the understanding of WMI architecture and technique, use your favourite search engine to find plenty of WMI script resources available on the Internet. One of my favourites is Cwashington WMI script library that contains plenty of simple, useful, and easy to start with scripts. Here is where to find it:

http://cwashington.netreach.net/depo/default.asp?topic=wmifaq

2.2. **Alternative WMI Access with Monkier String**

Monkier string is another way to script WMI access. This method allows to skip a
How to Avoid Information Disclosure when Managing Windows with WMI

line when coding, at the expense of clarity and flexibility that is partially lost if you choose to use the monkier. The monkier string method is used frequently nonetheless. We will cover the basics by comparing with the object access method described in previous section.

Here is the code fragment used to return the collection of WMI objects as an example in previous section:

```vbscript
Set objLocator = CreateObject("WbemScripting.SWbemLocator")
Set objWMIService = objLocator.ConnectServer (strComputer, "root\CIMV2", strUser, strPassword)
Set colServices = objWMIService.ExecQuery ("Select * from Win32_Service Where Name = " & strService & "")
```

The monkier string equivalent would look as shown below. As promised, it is one line shorter:

```vbscript
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\CIMV2")
Set colServices = objWMIService.ExecQuery ("Select * from Win32_Service Where Name = " & strService & "")
```

Monkier may be Ok for testing purpose. The downside of the moniker way of scripting a WMI connection is that the monkier way employs standard COM access. WMI namespace connection will use the credentials of the currently logged on user. This is
How to Avoid Information Disclosure when Managing Windows with WMI

probably not what our security policy would like us to do most of the time, when administering remote Windows hosts.

Considering performance, moniker may provide a quicker once off access to a collection of WMI objects. On the other side, if we were to access the objects repeatedly as with most real life administrative tasks, the moniker way may be a less efficient way of connecting to WMI. If performance is important, the overall recommendation would be to use the object way of connecting to WMI, as described in previous section.

The object way of WMI scripting not only performs better, but also more importantly provides better authentication. Moniker immediately retrieves an object instance, while the object method first creates an object, and then allows logging on to the object name space with the explicitly specified credentials. The capability to specify user credentials is a significant advantage of the object way of WMI connection scripting. In addition, the object way provides better error reporting, when comparing with the moniker mechanism.

Despite our justified preference for the object way of WMI scripting, we provide a number of examples of using moniker throughout this paper, due to the fact that the moniker string technique is often used in Microsoft scripting examples, as well as in non-vendor specific script archives on the Internet.

At this point, it is time to move on and see what happens when the sample script

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
presented in section 2.1 is run against a remote Windows host.

3. **WMI Default Security on the Wire**

The purpose of this section is to demonstrate how system management information is transported along the wire, when the default WMI security settings are in use. We run the sample script from Section 2.1 on the local host (scripting host) against the remote host. Both systems are running Windows XP Professional, Service Pack 2.

Packets are captured on the wire during the running of the sample script, as WMI authentication and name space connection is taking place. Then a WMI query is sent from the local host to the remote hosts. Finally, WMI management information is returned by the remote host to the local host.

Below is the part of the network dialog between the two systems from the moment when the initial management query is sent, and to the moment when the management data of interest is returned. The full network conversation between the two hosts is shown in Appendix 1.

<table>
<thead>
<tr>
<th>Packet</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol and Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Request: call_id: 5 opnum: 20 ctx_id: 3 IWbemServices V0</td>
</tr>
<tr>
<td>53</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERPC Response: call_id: 5 ctx_id: 3 IWbemServices V0</td>
</tr>
<tr>
<td>54</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IRemUnknown2 RemQueryInterface request IID[1]=IWbemFetchSmartEnum</td>
</tr>
<tr>
<td>56</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Alter_context: call_id: 7 IWbemFetchSmartEnum V0.0</td>
</tr>
<tr>
<td>58</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Request: call_id: 7 opnum: 3 ctx_id: 4 IWbemFetchSmartEnum V0</td>
</tr>
</tbody>
</table>
How to Avoid Information Disclosure when Managing Windows with WMI

Figure 2: WMI Data Exchange on the Wire

Please note packets 52 and 73. Packet 52 contains the WMI query sent from the host with IP address 10.252.253.8 (our scripting host) to the host with IP address 10.252.253.44 (our remote host). Packet 73 contains the WMI management data returned by the remote host 10.252.253.44 to the scripting host 10.252.253.8.

The partial payload of packet 52 is shown below. We are not reproducing the entire packet here. The entire packet and its payload are included in Appendix 1.

Conversion from hexadecimal to ASCII is a straightforward matter. I have written a
short VBScript to do such conversions, and to deal with the capture file format.

Alternatively, here are tools available on the Internet that would suit the same purpose.

After running the selected partial packet payload through the converter script, we get the following data:

```
Select * from Win32_Service Where Name = 'TlntSvr'
```

This corresponds to the ExecQuery, lines 42 - 44 of the sample script, where TlntSvr is the value assigned to the strService string variable. This value was indeed assigned during the interactive part of the script, as the Telnet service was selected on the remote host for the purpose of this experiment.

We observe that the WMI management query is transmitted over the network in clear. It is trivial to find out the exact query information by snooping on the network.

The next interesting packet is packet 73. This packet contains partial WMI data sent from the remote host 10.252.253.44 to the scripting host 10.252.253.8, in response to the previously shown WMI query. Once again, please refer to Appendix 1 to see the full packet payload content. The partial packet payload is shown below:

```
45 3a 5c 57 49 4e 44 4f 57 53 5c 79 73 74 65 6d 33 32 5c 74 6c 6e 74 73 76 72 2e 65 78 65 00 00 4c 6f 61 6c 53 79 73 74 65 6d 00 00 57 69 6e 33 32 5f 53 65 72 76 69 63 65 00 00 57 69 6e 33 32 5f 43 6f 6d 70 74 65 72 53 79 73 74 65 6d 00 00 50 49 47 41 00 00 54 6c 6e 74 53 76 72
```

Alex M. Timkov

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
How to Avoid Information Disclosure when Managing Windows with WMI

As with previous payload fragment, we run this through our converter script, and find the data transmitted by the remote host to the scripting host:

```
E:\WINDOWS\System32\tlntsvr.exeLocalSystemWin32_ServiceWin32_ComputerSystemP|GATlntSvr
```

The WMI management data is returned in clear, just as the WMI query was sent. It is easy to see that the information available in clear includes system name, service name, path, access authority, and more. We have referenced only the small fragment of the returned management data. Captured data also included service state, description, and other information. Such system data is more often than not considered confidential information. It should not travel across the network without protection.

In this section, we have shown that it is trivial to snoop on the sensitive WMI management data, as long as the default WMI security settings are in use. We have accessed system service information in this particular example. While system service information is often unique and sensitive, it is easy to imagine the cases where data that is even more sensitive is exchanged across the network via Windows Management Interface. Clear text is not the best way to transmit such data. Next section will focus on the basic security options available for configuring WMI access security. WMI security options must be set explicitly in order to avoid unnecessary exposure of the sensitive management data.
4. **WMI Scripting Security Options**

"We have all some experience of a feeling, that comes over us occasionally, of what we are saying and doing having been said and done before, in a remote time – of our having been surrounded, dim ages ago, by the same faces, objects, and circumstances – of our knowing perfectly what will be said next, as if we suddenly remember it!"

*Dickens, Charles (1991)*

*The Personal History of David Copperfield*

WMI is unquestionably a deja vu experience, as far as Windows reputation of providing rich functionality coupled with not so secure default settings is concerned.

Windows Management Interface does not provide its own security mechanism. Instead, WMI makes use of the DCOM security functionality offered by Windows. WMI supports a number of security levels. The WMI security levels are best documented in the Microsoft TechNet article called WMI Security Settings (Microsoft TechNet, 2007). There is a good supplement article that provides updates to the above-mentioned reference, along with useful examples. This second Microsoft MSDN Library article is called Setting the Default Process Security Level Using VBScript (Microsoft MSDN Library, 2007). The links to both articles are included in the References section.

At this point, we will discuss basic WMI security options. This should start us on the road to securing WMI remote management connections. Basic WMI security settings may
How to Avoid Information Disclosure when Managing Windows with WMI

be set according to so-called impersonation and authentication levels.

In simple terms, impersonation setting is what WMI service will use on the remote host to carry out the tasks requested by the WMI script. Authentication setting allows WMI scripts to request the desired level of DCOM authentication for the WMI connection. There is more to the authentication setting. The WMI authentication setting allows specifying the use of encryption across the WMI connection. This is exactly the option that will help us dealing with the clear data transport problem identified in previous section.

First, let us take a look at the impersonation levels available. The table containing the description of the impersonation levels is below. We provide the value of WbemImpersonationLevelEnum for each of the impersonation levels, along with a description, a summary of useability, and a general scripting use recommendation. We reference both numeric and constant values. More on the values and their implementation in WMI scripts in the next section.

<table>
<thead>
<tr>
<th>Level: Anonymous Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value: 1 or wbemImpersonationLevelAnonymous</td>
</tr>
<tr>
<td>Description: Caller credentials are hidden when the Anonymous level of impersonation is chosen. From the security standpoint, this should not be allowed, and in fact, this is not allowed. WMI will automatically upgrade the requested impersonation level to Identify. Such upgrade is of questionable useability. Identify is likely to not work in the WMI script against a remote host, and the WMI script is likely to fail.</td>
</tr>
<tr>
<td>General recommendation: Do not use Anonymous impersonation level.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level: Identify Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value: 2 or wbemImpersonationLevelIdentify</td>
</tr>
<tr>
<td>Description: Objects will query the caller credentials. As this would fail a script, this is not a recommended impersonation setting for scripting WMI connections. Microsoft specified the Identify level for performing</td>
</tr>
</tbody>
</table>
How to Avoid Information Disclosure when Managing Windows with WMI

access control list checks, not so much for WMI scripting.

General recommendation: Do not use Identify impersonation level.

<table>
<thead>
<tr>
<th>Level: Impersonate Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value: 3 or wbemImpersonationLevelImpersonate</td>
</tr>
<tr>
<td>Description: Objects will use the caller credentials. In simple terms, such impersonated WMI script will use current user credentials or better yet, explicitly specified user credentials. Remote host should have no problem with such authentication mechanism, and the script should run against the remote host once the authentication is successful.</td>
</tr>
<tr>
<td>General recommendation: Do use Impersonate impersonation level, as this is the best impersonation option available for most WMI scripting tasks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level: Delegate Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value: 4 or wbemImpersonationLevelDelegate</td>
</tr>
<tr>
<td>Description: Caller credentials are trusted for delegation to other objects. If you run your WMI script against a remote host specifying Delegate impersonation level, not only remote host object access is granted, but also the remote host is then able to use the same credentials for other hosts. While such scenario will work, it will allow excessive access, not required for the majority of scripting tasks.</td>
</tr>
<tr>
<td>There is a possibility of Delegate impersonation level being required in a situation when remotely managed system needs to manage other systems. An example of this may be a central patch distribution system. If this is not your case, the Delegate impersonation level should not be required.</td>
</tr>
<tr>
<td>General recommendation: Do not use Delegate impersonation level, unless it is required. Delegate impersonation level should be considered a security risk.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level: Default Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value: 0 or WbemAuthenticationLevelDefault</td>
</tr>
<tr>
<td>Description: This setting allows WMI to negotiate the authentication level with the remote host. The authentication level specified by the remote host will be used. Microsoft recommends using this setting.</td>
</tr>
<tr>
<td>General recommendation: Do not use Default authentication level in WMI. Do not rely on the default security as it allows WMI exchange management data in clear. Do use Level 6, PktPrivacy instead.</td>
</tr>
<tr>
<td>Please note that our recommendation contradicts the practice suggested by Microsoft. As we have seen in previous section, the default authentication level allows clear data exchange over the network. We recommend that the default authentication is only used if the use of encryption is not allowed. Normally there should not be an issue with encrypting WMI connections.</td>
</tr>
</tbody>
</table>

Figure 3: WMI Impersonation Levels

There are six authentication levels that can be used with WMI:

Alex M. Timkov
# How to Avoid Information Disclosure when Managing Windows with WMI

<table>
<thead>
<tr>
<th>Level: None Level</th>
<th>Value: 1 or WbemAuthenticationLevelNone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Connection without authentication is attempted. Security settings are ignored.</td>
</tr>
<tr>
<td>General recommendation:</td>
<td>Needless to say, we recommend against using this authentication level.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level: Connect Level</th>
<th>Value: 2 or WbemAuthenticationLevelConnect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Perform credentials authentication only when the WMI script attempts to connect to the remote host. No additional authentication is performed after this moment.</td>
</tr>
<tr>
<td>General recommendation:</td>
<td>Do not use Connect authentication level. While Connect is better than None, there are better options available.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level: Call Level</th>
<th>Value: 3 or WbemAuthenticationLevelCall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Call authentication level does a little better. Authentication of credentials is performed at the beginning of each call/ request to the remote host. The initial packets have their headers signed and checked. However, data packets that are subsequently exchanges between the scripting host and the remote host are neither signed nor encrypted.</td>
</tr>
<tr>
<td>General recommendation:</td>
<td>Do not use Call authentication level. While some session authentication is performed, neither data integrity nor confidentiality is implemented with the Call authentication level.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level: Pkt Level</th>
<th>Value: 4 or WbemAuthenticationLevelPkt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Authentication is performed on all of the data received from the scripting host. In a way, Pkt authentication level is not far away from Call level. All the headers are signed and checked. We may be better assured about the source, but as with the Call level, data packet payload is neither signed nor encrypted.</td>
</tr>
<tr>
<td>General recommendation:</td>
<td>Do not use Pkt level of WMI authentication. Do use Level 6, PktPrivacy instead.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level: PktIntegrity Level</th>
<th>Value: 5 or WbemAuthenticationLevelPktIntegrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Authenticates and verifies that none of the data transferred between the scripting host and the remote host has been modified.</td>
</tr>
<tr>
<td>PktIntegrity authentication level provides integrity. Every WMI data packet travelling between the script host and the remote host is signed and checked. We have the assurance that the management data traversing the network has not been modified in transit.</td>
<td></td>
</tr>
<tr>
<td>There is no protection from data traffic snooping, as the data packet payload is not encrypted.</td>
<td></td>
</tr>
<tr>
<td>General recommendation:</td>
<td>PktIntegrity WMI authentication level can be used when data confidentiality is not an issue, or if the use of encryption is not allowed. Generally, it is better to use PktPrivacy authentication level that provides the data encryption service.</td>
</tr>
</tbody>
</table>
How to Avoid Information Disclosure when Managing Windows with WMI

**Figure 4: WMI Authentication Levels**

This brings us to the end of this section. We have introduced the basic WMI security settings: impersonation and authentication. Our recommendation is to never rely on the default security settings, but instead set the WMI impersonation level to 3 (Impersonate), and set the WMI authentication level to 6 (PktPrivacy) for general WMI scripting tasks. We will look at how to implement the basic WMI security options in VBScript based WMI scripts in the next section.

5. **Avoiding the Trap with Packet Privacy**

We have referred to the Microsoft MSDN Library article called Setting the Default Process Security Level Using VBScript (Microsoft MSDN Library, 2007) in previous section. The Web link to the article is available in the References section. This article contains useful examples of implementing basic WMI security with VBScript.

For the purpose of our discussion, we will return to the sample script used for the illustrations through this paper. The script is found in Section 2.1. We first discussed the

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

sample script when providing an introduction to WMI scripting. The script implemented a WMI call with the default WMI security settings. As we pointed out, this was done deliberately, for the purpose of our subsequent investigation of whether the default WMI security is sufficient to provide secure management data exchange.

The part of the script that makes use of the object method to retrieve a service collection using the default WMI security levels is reproduced below for your convenience:

```
Set objLocator = CreateObject("WbemScripting.SWbemLocator")
Set objWMIService = objLocator.ConnectServer(strComputer, "root\CIMV2", strUser, strPassword)
Set colServices = objWMIService.ExecQuery("Select * from Win32_Service Where Name = " & strService & "")
```

The same scripted with monkier instead of the object method would look as:

```
Set objWMIService = GetObject("winmgmts:\\" & strComputer & " root\CIMV2")
Set colServices = objWMIService.ExecQuery("Select * from Win32_Service Where Name = " & strService & "")
```

We have discussed that we generally recommend the object method for the reasons of better security and better performance.

In Section 3, we have shown that using the default WMI security settings is not the
How to Avoid Information Disclosure when Managing Windows with WMI

best approach to WMI scripting security. The default WMI connection does not encrypt data payload. Instead, sensitive WMI management information is transmitted over the network in clear text.

Here is how to modify the sample script to set the basic WMI security options explicitly, for the object access method. Please note the two extra lines:

```vbscript
Set objLocator = CreateObject("WbemScripting.SWbemLocator")
Set objWMIService = objLocator.ConnectServer(_, strComputer, "root\CIMV2", strUser, strPassword)
objWMIService.Security_.impersonationlevel = 3
objWMIService.Security_.authenticationlevel = 6
Set colServices = objWMIService.ExecQuery(_
"Select * from Win32_Service Where Name = " _
& strService & "")
```

Monkier example with the explicitly set security options is also two lines longer:

```vbscript
Set objWMIService = GetObject("winmgmts:" _
& "/impersonationLevel = impersonate," _
& "authenticationLevel = pktPrivacy)!\" _
& strComputer & "/root\CIMV2")
Set colServices = objWMIService.ExecQuery(_
"Select * from Win32_Service Where Name = " _
& strService & "")
```

The two extra lines used to set the explicit WMI security for the object access are:

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

objWMIService.Security_.impersonationlevel = 3
objWMIService.Security_.authenticationlevel = 6

The corresponding extension of the monkier string with the security parameters is:

{impersonationLevel = impersonate, authenticationLevel = pktPrivacy}!

The newly added lines set the impersonation and authentication levels to the levels that we have generally recommend for optimal security, performance, and interoperability:

WbemImpersonationLevelImpersonate or 3 best used as impersonation level
WbemAuthenticationLevelPktPrivacy or 6 best used as authentication level

There is a unique case of distributed WMI management, whereby the scripting host connects to the remote management host that should in turn perform operations on other hosts. While it may not be ideal from the WMI security standpoint, such scenario may require the use of the Delegate impersonation level. In such case, the two lines setting the explicit WMI security parameters would become, for the object method:

objWMIService.Security_.impersonationlevel = 4
objWMIService.Security_.authenticationlevel = 6

The same lines for the monkier string are below:

& "{impersonationLevel=delegate," _
& "authenticationLevel=pktPrivacy}!" _

Once again, only use the Delegate impersonation level if your design cannot use the preferred Impersonate impersonation level.

Alex M. Timkov

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
How to Avoid Information Disclosure when Managing Windows with WMI

Now let us take a look at the updated service start script. We have added the line explicitly setting WMI authentication level to PktPrivacy. We should now have the WMI connection that encrypts data packet payload protecting the sensitive management data.

```
'--------------- Service Start Script - WMI Based ---------------
' Test the state of service of user choice on the remote host
' Start service on the remote host if the service is not running
' Written by Alex Timkov to facilitate SANS GSEC research paper
'-------------------------------------------------------------------

Option Explicit

Dim strComputer, strPassword, strService, strUser
Dim objLocator, objService, objWSIService
Dim colServices
Dim intTimeout

intTimeout = 10000

Do
    strComputer = inputbox
dostrComputer = inputbox
dostrComputer = inputbox
Do
    strUser = inputbox
dostrUser = inputbox
Do
    strPassword = inputbox
dostrPassword = inputbox

strService = inputbox
dostrService = inputbox
If strService <> "" Then

Set objLocator = CreateObject("WbemScripting.SWbemLocator")
Set objWSIService = objLocator.ConnectServer
dostrComputer, "root\CIMV2", strUser, strPassword)
objWSIService.Security_.impersonationlevel = 3
objWSIService.Security_.authenticationlevel = 6
Set colServices = objWSIService.ExecQuery

Alex M. Timkov

© SANS Institute 2007,  As part of the Information Security Reading Room  Author retains full rights.
How to Avoid Information Disclosure when Managing Windows with WMI

(`Select ` from Win32_Service Where Name = ` & strService & ` & `)

If Not(colServices Is Nothing) Then
    For Each objService in colServices
        If Not(objService Is Nothing) Then
            If objService.State = "Stopped" Then
                WScript.Echo vbCrLf & "Starting " & strService & " service..."
                objService.StartService()
                WScript.Sleep intTimeout
            Else
                WScript.Echo vbCrLf & "Service is not stopped."
            End If
        End If
    Next
End If

Set objService = Nothing
Set colServices = Nothing
Set objWMIService = Nothing
End If

WScript.Echo vbCrLf & "Script execution completed. Exiting."
WScript.Quit

'--------------------------------------
' End of WMI Based Service Start Script
'--------------------------------------

**Figure 5: Updated WMI Service Start Script**

6. **Improved WMI Connection Security on the Wire**

We are going to execute the updated service start script against the remote host, and make sure that when the correct WMI security options are set explicitly, we are no longer able to snoop on the WMI management data traversing the network.

We run the updated sample script from Section 5 on the scripting host against the remote host. Both systems are running Windows XP Professional, Service Pack 2.

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

Packets are captured on the wire during the running of the updated sample script, as WMI authentication and name space connection is taking place, the WMI query is sent from the local host to the remote hosts, and the WMI management information is returned by the remote host to the local host.

Below is the part of the network dialog between the two systems from the moment when the initial management query is sent, and to the moment when the management data of interest is returned. The full network conversation between the two hosts is shown in Appendix 2.

<table>
<thead>
<tr>
<th>Packet</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol and Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERP Request: call_id: 5 opnum: 20 ctx_id: 3 IWbemServices V0</td>
</tr>
<tr>
<td>53</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP 1032 &gt; 1842 [ACK] Seq=185 Ack=667 Win=64869 Len=0</td>
</tr>
<tr>
<td>54</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERP Response: call_id: 5 ctx_id: 3 IWbemServices V0</td>
</tr>
<tr>
<td>55</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERP Alter_context: call_id: 6 IRemUnknown2 V0.0</td>
</tr>
<tr>
<td>57</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IRemUnknown2 RemQueryInterface request[Malformed Packet]</td>
</tr>
<tr>
<td>59</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERP Alter_context: call_id: 7 IWbemFetchSmartEnum V0.0</td>
</tr>
<tr>
<td>61</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERP Request: call_id: 7 opnum: 3 ctx_id: 4 IWbemFetchSmartEnum V0</td>
</tr>
<tr>
<td>62</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1838 &gt; epmap [ACK] Seq=97 Ack=193 Win=65343 Len=0</td>
</tr>
<tr>
<td>63</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1839 &gt; epmap [ACK] Seq=1147 Ack=1241 Win=64295 Len=0</td>
</tr>
<tr>
<td>64</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERP Response: call_id: 7 ctx_id: 4 IWbemFetchSmartEnum V0</td>
</tr>
<tr>
<td>65</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERP Alter_context: call_id: 8 IWbemWCOSmartEnum V0.0</td>
</tr>
<tr>
<td>67</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERP Request: call_id: 8 opnum: 3 ctx_id: 5 IWbemWCOSmartEnum V0</td>
</tr>
<tr>
<td>68</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP 1032 &gt; 1842 [ACK] Seq=929 Ack=1491 Win=65535 Len=0</td>
</tr>
<tr>
<td>69</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1840 &gt; 1032 [ACK] Seq=899 Ack=497 Win=65039 Len=0</td>
</tr>
<tr>
<td>70</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1841 &gt; 1032 [ACK] Seq=507 Ack=409 Win=65127 Len=0</td>
</tr>
<tr>
<td>71</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP [TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>72</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP [TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>73</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1842 &gt; 1032 [ACK] Seq=1491 Ack=3449 Win=65535 Len=0</td>
</tr>
</tbody>
</table>
When investigating the default WMI security in section 3, we analysed the packet payload containing the WMI query, and the response packet of interest. The interesting packets selected were packet 52 and packet 73. Packet numbers are different this time. This does not come as a surprise, since if encryption is used indeed, the packet sequence and size may vary from our prior experiment.

We notice that the packet with the payload of the query is still packet 52, however the data of interest is returned not in packet 73, but in packet 79.

As previously, we take a look at the partial payload of packet 52, as shown below.

The entire packet and its payload are shown in Appendix 2.

```
Figure 6: Secure WMI Data Exchange on the Wire

Upon a superficial look, this time around the payload seems harder to snoop at, more than simple encoded text. Running our ASCII converter would not do any good to
```

<table>
<thead>
<tr>
<th>Packet</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Sequence</th>
<th>Acknowledgment</th>
<th>Window Size</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>74</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>1024</td>
<td>1024</td>
<td>65535</td>
<td>0</td>
</tr>
<tr>
<td>75</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842</td>
<td>1491</td>
<td>65535</td>
<td>0</td>
</tr>
<tr>
<td>76</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>1024</td>
<td>1024</td>
<td>65535</td>
<td>0</td>
</tr>
<tr>
<td>77</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERPC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>78</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842</td>
<td>1491</td>
<td>65535</td>
<td>0</td>
</tr>
<tr>
<td>79</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERPC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Sequence</th>
<th>Acknowledgment</th>
<th>Window Size</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>1024</td>
<td>1024</td>
<td>65535</td>
<td>0</td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842</td>
<td>1491</td>
<td>65535</td>
<td>0</td>
</tr>
<tr>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>1024</td>
<td>1024</td>
<td>65535</td>
<td>0</td>
</tr>
<tr>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERPC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842</td>
<td>1491</td>
<td>65535</td>
<td>0</td>
</tr>
<tr>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERPC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

f8 e6 c0 f9 81 14 b5 eb 6f 14 ad 1a a3 9a a1 1c a1 c7
0f e0 0c fb b5 1d 82 e8 01 c2 68 73 7c 8a ff 57 74 b7
24 87 7f 57 53 55 65 6a 8b 64 7c 31 48 cc ae 05 74 ae
30 b3 75 cc 09 16 9a c0 7f d4 bd 3d 47 6d 50 df 46 f1
8a a5 2a b2 ca 83 04 f7 d0 b0 26 42 59 49 93 46 88 e3
ce 34 4c 04 2b 0e 13 77 27 50

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

help reading this payload fragment. Indeed, after performing a more thorough analysis of
the packet, the payload appears to be encrypted. Such analysis goes beyond the scope of
this paper, and we will leave the detailed analysis out of this text.

Let us take a look at the second packet of interest, packet 79. This packet is the
response packet, containing some of the WMI management data. Once again, please refer
to Appendix 2 for the full packet payload content. Below is the partial payload:

```
56 9b a8 57 dd af 2c a7 af 86 ab 65 f5 4b 2c bf dd db
d5 d8 37 e4 9b dd 28 b6 f3 52 36 bf 3a 89 3b cc 52 be
c4 56 23 62 ca af ce e0 44 2b ea 50 6f ef f4 dd c5 8b
49 32 2e 5a 66 8c 60 c3 f5 86 3e b4 67 6a 94 4b 43 b4
6f 40 49 3c bb a2 14 44 6a 0a 2e 3c d4 7f c1 ba 79 ba
1a 99 02 8d 02 22
```

As with the query packet payload, the data packet payload does not look like giving
much hope of reading its content easily. Same as the WMI query packet, the payload of
the packet carrying WMI management data appears to be encrypted. A detailed analysis
of the entire packet content confirms this to be the case.

Adding the recommended explicit WMI authentication setting to our sample WMI
script did the trick. The WMI management data exchange is now considerably more
secure. We have eliminated the data exposure caused by the weak default WMI
authentication setting.

Alex M. Timkov
7. Advanced WMI Scripting Security Options

It is time to move on from the analysis of the basic WMI security options to discuss advanced WMI security topics, and to offer tips that should aid our WMI management security policy and practice.

7.1. Keep Administrative Passwords out of Scripts

In this section, we would like to step back for a moment, and to bring to your attention an example illustrating the obvious fact that no amount of advanced technology will compensate for the lack of security policy and the lack of complete approach to security.

Not long ago I was checking Microsoft Web pages for the new developments and updates in the field of WMI security. I came across new secure WMI access examples. If I were to re-write the sample script used through this paper, using the new recommendations from the new Microsoft site articles, the WMI object access lines from the sample script would change to look as this:

```vbscript
Set objLocator = CreateObject("WbemScripting.SWbemLocator")
Set objWMIService = objLocator.ConnectServer (_
    "computername", "root\CIMV2", "useraccount", "userpassword")
objWMIService.Security_.impersonationlevel = 3
objWMIService.Security_.authenticationlevel = 6
```

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

Set colServices = objWMIService.ExecQuery(_
   "Select * from Win32_Service Where Name = " & strService & ""
& strService & "")

There is a new good intention. Microsoft scripting examples are now showing explicitly set WMI security levels. However, is there a problem with this code? The ConnectServer method shows the user password in clear. If we were to guard our scripts, could we get away with such approach? This does not seem likely. In practice, scripts reside on the servers, CDs, USB disks and the like. Not many administrators keep scripts inside safes.

In other WMI scripting examples that I have seen, the script account was in fact called "administrator", and the administrative password was typed in clear text as the next parameter. Is it worth worrying about the authentication and the encryption of the WMI data exchange, if scripts leave administrative account password in clear?

May this be only an example, and nothing to do with the real life? No one would force administrators to write their real scripts in such a way. The problem is that the examples are often taken from vendor sites, and re-used without due analysis of implications. The other week I was shown a management script used to administer a critical and very sensitive real life system. The script contained administrative account and password, both in clear text. Would this be as bad as it gets? It got worse. The script resided on the server file system with world read access, and there were multiple users on

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

that system. We may never know where the scripts end up.

One way around exposing passwords through scripts is to use interactive scripts, just as part of the sample we have been using throughout this paper shows:

```vbscript
Do
    strComputer = inputbox _
        ("Please enter host name or IP address", "Input")
Loop until strComputer <> ""

Do
    strUser = inputbox("Please enter username", "Input")
Loop until strUser <> ""

Do
    strPassword = inputbox("Please enter password", "Input")
Loop until strPassword <> ""

strService = inputbox _
    ("Please enter the name of service to start, " _
    & "or hit Enter to exit", "Input")

If strService <> "" Then
    Set objLocator = CreateObject("WbemScripting.SWbemLocator")
    Set objWMIService = objLocator.ConnectServer _
        (strComputer, "root\CIMV2", strUser, strPassword)
    objWMIService.Security_.impersonationlevel = 3
    objWMIService.Security_.authenticationlevel = 6
    Set colServices = objWMIService.ExecQuery _
        ("Select * from Win32_Service Where Name = " _
        & strService & ")

The ConnectServer is using the string variables that are filled with user input during an interactive session.

There may be a situation where we may prefer not to use an interactive session. In such situation, we would recommend the use of the monkey account authentication. This

Alex M. Timkov

© SANS Institute 2007, As part of the Information Security Reading Room

Author retains full rights.
is not ideal because we lose the flexibility to specify credentials of the user other than the
user currently logged on, but it is better still than storing administrative password in clear
text. It is most dangerous to lose track of where privileged passwords end up.

Here is the example of the monkier account authentication:

```vbscript
Set objWMIService = GetObject("winmgmts:" _
& "{impersonationLevel = impersonate," _
& "authenticationLevel = pktPrivacy}!\" _
& strComputer & \\
Set colServices = objWMIService.ExecQuery _
("Select * from Win32_Service Where Name = " _
& strService & \\
	We have deviated from discussing the pure specifics of WMI security. This was a
quick detour, a reminder that the security approach should be complete, and that all
effects must be taken into account when security is considered. Now we will return to the
specifics of WMI and discuss the advanced subject of using specific permissions in WMI
scripts.

### 7.2. Using Specific Permissions in WMI Scripts

Aside from correctly setting the impersonation and authentication for WMI
connections, and along with following sound security practices, there are several
advanced security options that can help us secure WMI connections.
How to Avoid Information Disclosure when Managing Windows with WMI

WMI allows controls that are more granular and go beyond the general security levels. One of the available options is to override the default privileges. A specific access privilege can be added or revoked as part of a WMI script. Below is the full list of privileges that can be granted and revoked, as specified in the Microsoft TechNet article WMI Security Settings (Microsoft TechNet, 2007):

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateToken</td>
<td>Required to create a primary token.</td>
</tr>
<tr>
<td>AssignPrimaryToken</td>
<td>Required to assign the primary token of a process.</td>
</tr>
<tr>
<td>LockMemory</td>
<td>Required to lock physical pages in memory.</td>
</tr>
<tr>
<td>IncreaseQuota</td>
<td>Required to increase the quota assigned to a process.</td>
</tr>
<tr>
<td>MachineAccount</td>
<td>Required to create a computer account.</td>
</tr>
<tr>
<td>Tcb</td>
<td>Identifies its holder as part of the trusted computer base. Some trusted, protected subsystems are granted this privilege.</td>
</tr>
<tr>
<td>Security</td>
<td>Required to perform a number of security-related functions, such as controlling and viewing audit messages. This privilege identifies its holder as a security operator.</td>
</tr>
<tr>
<td>TakeOwnership</td>
<td>Required to take ownership of an object without being granted discretionary access. This privilege allows the owner value to be set only to those values that the holder might legitimately assign as the owner of an object.</td>
</tr>
<tr>
<td>LoadDriver</td>
<td>Required to load or unload a device driver.</td>
</tr>
<tr>
<td>SystemProfile</td>
<td>Required to gather profiling information for the entire system.</td>
</tr>
<tr>
<td>SystemTime</td>
<td>Required to modify the system time.</td>
</tr>
<tr>
<td>ProfileSingleProcess</td>
<td>Required to gather profiling information for a single process.</td>
</tr>
<tr>
<td>IncreaseBasePriority</td>
<td>Required to increase the base priority of a process.</td>
</tr>
<tr>
<td>CreatePagefile</td>
<td>Required to create a paging file.</td>
</tr>
<tr>
<td>CreatePermanent</td>
<td>Required to create a permanent object.</td>
</tr>
<tr>
<td>Backup</td>
<td>Required to perform backup operations.</td>
</tr>
<tr>
<td>Restore</td>
<td>Required to perform restore operations. This privilege lets you set any valid user or group SID as the owner of an object.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Required to shut down a local computer.</td>
</tr>
<tr>
<td>Debug</td>
<td>Required to debug a process.</td>
</tr>
<tr>
<td>Audit</td>
<td>Required to generate audit-log entries.</td>
</tr>
<tr>
<td>SystemEnvironment</td>
<td>Required to modify the non-volatile RAM of systems that use this type of memory to store configuration information.</td>
</tr>
</tbody>
</table>

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChangeNotify</td>
<td>Required to receive notifications of changes to files or directories. This privilege also causes the system to skip all traversal access checks. It is enabled by default for all users.</td>
</tr>
<tr>
<td>RemoteShutdown</td>
<td>Required to shut down a computer using a network request.</td>
</tr>
<tr>
<td>Undock</td>
<td>Required to remove a computer from its docking station.</td>
</tr>
<tr>
<td>SyncAgent</td>
<td>Required to synchronize directory service data.</td>
</tr>
<tr>
<td>EnableDelegation</td>
<td>Required to enable computer and user accounts to be trusted for delegation.</td>
</tr>
</tbody>
</table>

*Figure 7: Specific Permissions for WMI Scripting*

We will modify our monkier example from Section 7.1 to add the explicit privileges to lock memory and debug, and to remove the privilege to remotely shut down the system.

Please note the exclamation mark preceding the privilege that is being revoked:

```
Set objWMIService = GetObject("winmgmts:" _
& "{impersonationLevel = impersonate," _
& "authenticationLevel = pktPrivacy," _
& "(LockMemory, Debug, !RemoteShutdown)}!" _
& strComputer & "root\CIMV2")

Set colServices = objWMIService.ExecQuery _
("Select * from Win32_Service Where Name = " _
& strService & "")
```

Please do not assume that WMI will allow the scripting account to gain the privileges that the scripting account does not hold. WMI mechanism is not designed to circumvent Windows user account security. The user executing the script can only enable those privileges for which his account is authorised by the remote host, as part of that user account authorisation on the target system. If the user running the WMI script specifies a privilege for which his account is not authorised by the remote host, access will fail.

Alex M. Timkov
7.3. **WMI Authority**

WMI Authenticating Authority is another security parameter that can be used with the WMI object connection. Examples of this are rather rare. The authority can be set to use either Kerberos or NTLM authentication. Usually the parameter is not used, and the effect is that the authentication mechanism is negotiated between the scripting host and the remote host. Microsoft article Connecting to WMI Objects (Microsoft TechNet, 2007) contains a couple of relevant examples.

We will build on the previous monkey example, and you can port this to the object method as a practical exercise if you wish. We will re-use our most recent example from Section 7.2, adding one line to it:

```vbscript
Set objWMIService = GetObject("winmgmts:" & 
    "[impersonationLevel = impersonate,"
    & "authenticationLevel = pktPrivacy," & 
    "authority = ntlmdomain:DomainName," & 
    "(LockMemory ,Debug, !RemoteShutdown)]!\" & strComputer & 
    "root\CIMV2")
Set colServices = objWMIService.ExecQuery _
    ("Select * from Win32_Service Where Name = " & strService & 
    ")"
```

Please note the added line:

```vbscript
& "authority = ntlmdomain:DomainName," _
```

This line requests that NTLM authentication is used. If we prefer to use Kerberos...
How to Avoid Information Disclosure when Managing Windows with WMI

instead of NTLM, we should write instead:

```
Set objWMIService = GetObject("winmgmts:" _
& "\{impersonationLevel = impersonate," _
& "authenticationLevel = pktPrivacy," _
& "authority = kerberos:DomainName\ServerName," _
& "\{LockMemory, Debug, !RemoteShutdown})!\" _
& strComputer & "\" root\CIMV2")
```

where the added line is:

```
& "authority = kerberos:DomainName\ServerName," _
```

The DomainName is the name of our domain, and the ServerName is the name of the remote host.

A word of caution, authenticating authority parameter can only be used against a remote system. If we attempted a WMI connection to the local system with authenticating authority parameter set, the connection would fail. Omit the authentication authority parameter in the WMI scripts running against the local host.

Another word of caution, if the Delegate impersonation level is used, Kerberos authentication may be required by the remote system.
7.4. **Summary of WMI Scripting Security Options**

The purpose of this short section is to provide a reference summary of the WMI security options specified in WMI scripts, with a one-liner example for each option. For brevity sake, we use monkey string based examples.

Set Impersonation level to Impersonate:

```
winmgmts:{impersonationLevel = 3}
```

Set Authentication level to PktPrivacy:

```
winmgmts:{authenticationLevel =6 }
```

Set Authenticating Authority instead of leaving it to negotiation between systems:

```
winmgmts:{authority = ntlmdomain:DomainName}
```

for NTLM authentication, or

```
winmgmts:{authority = kerberos:DomainName\ServerName}
```

for Kerberos authentication.

Grant or revoke specific privileges, preceding removals with the exclamation mark:

```
winmgmts:{(Debug, !RemoteShutdown)}
```

To add the Debug privilege and to revoke the Remote Shutdown privilege.

---

Alex M. Timkov
7.5. **WMI Default Impersonation and Legacy Platforms**

This is another very short section. It contains the notes that may be needed when managing older Windows platforms, prior to Windows 2000.

Starting with Windows 2000, the default impersonation level is set to Impersonate. If we somehow forgot to specify impersonation level explicitly, the impersonation level is set to Impersonate automatically. This is a nice safety net.

We could encounter a problem with this if managing mixed environments. If the environment contained hosts with the operating system prior to Windows 2000, any scripts not explicitly stating Impersonation level would fail against such legacy hosts.

If we needed to change this default setting for some odd reason, the default DCOM impersonation level setting can be managed with the help of a registry entry:

```plaintext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Scripting\Default Impersonation Level
```

Windows 2000 and later set this entry to 3, Impersonate level.

8. **Securing the Server for WMI Management**

So far, we have looked at the options applicable to the script code and the scripting host in order to secure WMI connectivity. This section will look at the options available at the remote host to make sure incoming WMI connections are as secure as possible.

Alex M. Timkov
8.1. Scripting Account and Administrative Rights

As we all know, good security practice always applies the principle of the least privilege. In other terms, if the right is not required to perform the function, do not grant the right. Good security practice suggests against using administrative accounts, unless necessary. However, if you consider the default Windows permissions, the scripting account would need to be a member of the administrative group, in order to access WMI namespace objects, retrieve object properties, and modify object properties.

In order to follow good security practice, we should adopt the view of creating specific accounts and account groups for specific purpose. We recommend creating a user account, and granting that account specific access to specific namespaces, as the remote system management tasks require.

Setting WMI Namespace Permissions

Microsoft MSDN Library article Setting Namespace Security with the WMI Control (Microsoft MSDN Library, 2007) describes how to set security on WMI namespaces. The instructions below closely follow the instructions from the above-mentioned article. Setting up WMI namespace permissions is a very simple three-step process:

1. Run the WMI Control. On the Start menu, click Run and type wmic.msc.
2. In the WMI Control pane, right-click WMI Control, choose Properties, and then select the Security tab.
3. Navigate to the new namespace of choice, click Security, and configure groups and permissions.
How to Avoid Information Disclosure when Managing Windows with WMI

What exactly permissions can be granted to user accounts? Open the Security tab of the WMI Control Properties, and click the Security button to find the following available permission options:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Security</td>
<td>Grant read and write access to WMI security information</td>
</tr>
<tr>
<td>Enable Account</td>
<td>Grant read access to objects within the namespace</td>
</tr>
<tr>
<td>Execute Methods</td>
<td>Allow object methods from the CIM Object Manager to be run</td>
</tr>
<tr>
<td>Full Write</td>
<td>Grant full read, write, and delete access to all CIM objects, classes, and instances</td>
</tr>
<tr>
<td>Partial Write</td>
<td>Grant write access to static objects in the repository</td>
</tr>
<tr>
<td>Provider Write</td>
<td>Grant write access to objects that are provided by the provider</td>
</tr>
<tr>
<td>Read Security</td>
<td>Grant read-only access to WMI security information</td>
</tr>
<tr>
<td>Remote Enable</td>
<td>Grant remote access with the same rights as if connecting from the local host</td>
</tr>
</tbody>
</table>

There is an advanced option that allows editing the ACL, and to set the inheritance on child objects. To get there click the Advanced button from the Security Property screen, and follow the three simple steps outlined below.

1. Add an account, or select existing account and click Edit.
2. Use the Apply Onto dialog box to set inheritance in one of the following ways:
   - On the current namespace
   - On the current namespace and subnamespaces
   - Only on the subnamespaces
3. Save for the settings to take effect.

Changing the Default WMI Namespace

Sometimes programmers may not state explicitly to which WMI namespace their
How to Avoid Information Disclosure when Managing Windows with WMI script should be connecting. In such scenario, the script will be directed to the default WMI namespace. The default WMI name space is Root\CIMV2.

If we would like to change the default namespace that is hit by the scripts that are not explicit about their namespace access requirement, we could change this setting. The default WMI namespace setting can be accessed through the following registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Scripting\Default Namespace
```

There is another way of changing the default WMI namespace. The default can be changed from the WMI control interface:

1. Run the WMI Control. On the Start menu, click Run and type wmiimgmt.msc.
2. In the WMI Control pane, right-click WMI Control, choose Properties, and then select the Advanced tab.
3. Click the Change button and select the namespace and save the setting to make it the default.

8.2. **WMI Namespace Security Auditing**

In the last section, we focused on implementing the security principle of the least privilege for WMI. The next important security principle is the audit trail. Administrators should implement a way to verify the day to day functioning of the security policy.

WMI namespace security auditing is best described in the Microsoft MSDN Library article named Access to WMI Namespaces (Microsoft MSDN Library, 2007).

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

Windows versions prior to Vista, including Windows XP and Windows Server 2003, provide only limited logging function. In Windows versions prior to Vista, there is a Logging tab available through the WMI Control Properties page. The Logging tab allows setting the logs location, size, and level. The WMI logs are located in the following Windows subdirectory:

```
System32\WBEM\Logs\n```

There are only three options available for the WMI logging:

- The default logging level is Error. It will log errors only.
- Second available level is Verbose. Set this to enable additional WMI logging.
- The third available option is Disabled, that will disable WMI logging.

WMI logging is one of the areas where Windows Vista improves WMI security, comparing with previous Windows versions. Windows Vista WMI makes use of the system ACLs that can be set along the WMI namespace tree, providing improved and more flexible auditing of WMI events.

There is no Logging tab in the WMI Control Properties interface in Windows Vista. Instead, we should use previously mentioned Security tab. From the Security tab interface, select Advanced, and then Auditing, to find the option to select the audited accounts of users, groups, computers, and security principals. The audited privileges and the inheritance of the audited privileges can be specified.

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

By default, auditing is not enabled in Vista. We must configure auditing as described above. Please do not forget that Windows Group Policy for the local computer must be set to allow auditing. Once auditing is enabled, the Windows event log is used to log WMI audit events.

There is one more distinction as far as WMI access is concern that favours Vista over previous versions of Windows. Starting with Windows Vista, the following security groups are granted access to WMI:

<table>
<thead>
<tr>
<th>Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCAL SERVICE</td>
</tr>
<tr>
<td>NETWORK SERVICE</td>
</tr>
<tr>
<td>Authenticated Users</td>
</tr>
</tbody>
</table>

Previous Windows versions used to grant WMI access to the following security groups:

<table>
<thead>
<tr>
<th>Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCAL SERVICE</td>
</tr>
<tr>
<td>NETWORK SERVICE</td>
</tr>
<tr>
<td>Everyone</td>
</tr>
</tbody>
</table>

It is good to see Everyone is finally disallowed WMI access by default!

The default access rights are similar for both Windows Vista and previous Windows versions:

| Execute Methods |

Alex M. Timkov
8.3. **Request Encrypted WMI Connections to the Server**

With the permissions and the audit trail set correctly, the next important security consideration is securing server communications. We have talked a lot about securing the WMI information exchange, due to the sensitivity of some of the WMI data. We have discussed that the scripts should specify the most secure authentication option available, PktPrivacy. As it happens, some administrators may not be willing to spend the time required to make their scripts secure. Is there a way to force less diligent administrators to write their scripts to request encrypted connections?

Starting with Windows Server 2003 Service Pack 1, the answer is yes. Provider namespace security can be configured to require encryption, prior to sending WMI data back. This is a very good practice, as it allows enforcing encryption at the server end, to make sure the scripts requesting a connection to the server via WMI have to use the PktPrivacy authentication level, and to encrypt WMI data. Should the script attempt to use a lower WMI authentication level, the server will deny access.

The technical detail of setting up namespace encryption enforcement is documented in the Microsoft MSDN article Requiring an Encrypted Connection to a

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

Namespace (Microsoft MSDN, 2007). If you would like to see how this is done, please refer to Appendix 3.

When we specify the WMI security levels required by the server, and in the event incoming WMI connection requests have a lower (e.g. default) security setting, the setting is negotiated to the highest level required. If the WMI script has specified the explicit security level that is lower than the one required by the server system, access is denied. The WMI script is left no choice but to specify the security level high enough to be accepted by the remote system.

The default WMI security settings are best documented in the article Connecting Between Different Operating Systems (Microsoft MSDN Library, 2007, Win32 and COM Development). Below is the list of the default DCOM impersonation, authentication level, and authentication service settings for WMI access to the server (remote) system, starting with the most recent Windows Vista, and going back to WMI version 1 in Windows NT.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Impersonation level</th>
<th>Authentication Level</th>
<th>Authentication Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Vista</td>
<td>Impersonate</td>
<td>Pkt</td>
<td>Kerberos</td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>Impersonate</td>
<td>Pkt</td>
<td>Kerberos</td>
</tr>
<tr>
<td>Windows XP Professional</td>
<td>Impersonate</td>
<td>Pkt</td>
<td>Kerberos</td>
</tr>
<tr>
<td>Windows 2000 (WMI 1.5)</td>
<td>Impersonate</td>
<td>Connect</td>
<td>Kerberos</td>
</tr>
<tr>
<td>Windows NT Server 4.0 SP4 and later (WMI 1.5)</td>
<td>Impersonate</td>
<td>Connect</td>
<td>NTLMDomain</td>
</tr>
<tr>
<td>Windows NT Server 4.0 SP4 and later (WMI 1.01)</td>
<td>Identify</td>
<td>Connect</td>
<td>NTLMDomain</td>
</tr>
</tbody>
</table>

Alex M. Timkov
8.4. Configure DCOM for Remote WMI Access

DCOM configuration for WMI access is described in the Microsoft article Securing a Remote WMI Connection (Microsoft MSDN Library, 2007, Win32 and COM Development). As we have mentioned previously, WMI security relies on the underlying DCOM security model. Windows allows administrative access to DCOM by default. When administrators perform the hardening task, and add specific scripting accounts for WMI access to specific WMI namespaces, the underlying DCOM access must be allowed.

To set this up, go to Start, and Run. Run Dcomcnfg.exe. Alternatively, navigate to Control Panel, Administrative Tools, and Component Services. This should bring up the Component Services interface. After expanding Component Services, and then Computers, check the Properties of My Computer, and the DCOM Security tab. This is where the user access is set. Select Edit Limits, and add the accounts that require access.

The article extract containing step-by-step instructions is provided in Appendix 5.


In this section, we discuss the configuration of the security mechanisms new to Windows Vista that affect WMI management access. The major Windows Vista security features that affect WMI security and operation include Windows Firewall configuration, User Account Control (UAC) filtering, DCOM settings, and the specific WMI security features...
controls implemented in Vista for the first time. Microsoft article Connecting to WMI Remotely Starting with Vista (Microsoft MSDN Library, 2007) provides an overview of Vista security features, as the new features affect the security of the WMI interface.

**Windows Firewall Configuration**

When the firewall is enabled on the remote host, a firewall rule (or exception) must be set on the firewall for WMI, in order to allow remote WMI access. The firewall exception rule will also work if the WMI service was configured for a fixes port, using the `winmgmt /standalonehost` command.

Here is the extract from the above referenced Microsoft article containing step-by-step instructions for enabling or disabling WMI across Windows firewall:

1. In the Control Panel, click Security then Windows Firewall.
2. Click Change Settings and click the Exceptions tab.
3. In the Exceptions window, select the check box for Windows Management Instrumentation (WMI) to enable WMI traffic through the firewall. To disable WMI traffic, clear the check box.

A service port lockdown always makes life easier in firewalled environments. Prior to Windows Vista, WMI was not known to be firewall friendly. This is because WMI runs using the service ports assigned through DCOM. Windows Vista allows WMI service to run as a separate host, using a specific fixed port. Clearly, this is an advantage to WMI management, particularly for firewalled environments.

**WMI Port Lockdown in Vista**

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

The procedure for configuring a fixed WMI service port is described in the Microsoft article Setting Up a Fixed Port for WMI (Microsoft MSDN Library, 2007). Here are the three simple steps to set up the fixed WMI service port, based on the Microsoft article content:

1. At the command prompt, type `winmgmt -standalonehost`.
2. Restart the WMI service
3. Establish a new port number for the WMI service:

   ```
   netsh firewall add portopening port=24158 name=WMIFixedPort
   ```

**User Account Control Filter**

With the introduction of User Account Control (UAC) in Vista, access token filter controls the operations allowed for the WMI namespaces. Quoting the above mentioned Microsoft article Connecting to WMI Remotely Starting with Vista (Microsoft MSDN Library, 2007),

"Under UAC, all accounts in the local Administrators group, run with a standard user access token, also known as UAC access token filtering. An administrator account can run a script with elevated privilege — 'Run as Administrator'. When you are not connecting to the built-in Administrator account, UAC affects connections to a remote computer differently depending on whether the two computers are in a domain or a workgroup."

**DCOM Settings**
How to Avoid Information Disclosure when Managing Windows with WMI

DCOM settings have not changed in Windows Vista. The situation may look different in the above-mentioned case of connecting to the remote host from the local scripting host while the systems are not domain members, because of the effect of the UAC. The best approach is to grant explicit remote DCOM access, activation rights, and launch rights for your scripting account, as discussed in previous sections.

**Specific WMI Security Controls New to Vista**

Windows Vista added the flexibility to ease WMI management and improve WMI security by allowing granular access to many new security properties of WMI objects. WMI security properties can be set specifically on printers, services, registry keys, DCOM applications, and WMI namespaces, under the guard of the UAC. Specific permissions can be set on these security properties for the users and user groups designated for WMI management tasks, providing for flexible security architecture.

Please refer to Microsoft MSDN Library article Changing Access Security on Securable Objects (Microsoft MSDN Library, 2007) for more detail. If you are planning to implement access to the specific security descriptors, please look up Appendix 6.

10. **References**


Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI


Alex M. Timkov

© SANS Institute 2007, Author retains full rights.
How to Avoid Information Disclosure when Managing Windows with WMI


Alternative URL http://support.microsoft.com/default.aspx?scid=kb;en-us;295292


Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI


11. **Appendixes**

**Appendix 1: Capture of Default WMI Request and Response**

WMI query packet with the default WMI security options in use:

<table>
<thead>
<tr>
<th>Packet</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol and Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCE RPC Request: call_id: 5 opnum: 20 ct_x_id: 3 IWbemServices</td>
</tr>
</tbody>
</table>

Frame 52 (342 bytes on wire, 342 bytes captured)


DCE RPC Request, Fragment: Single, FragLen: 288, Call: 5 Ctx: 3:

00 80 c7 ea 03 27 00 17 31 2e 1f 0 a 08 00 45 00
01 48 2c 6a 40 00 80 06 bd 18 0 a fc fd 08 0 a fc
fd 2c 06 b4 04 08 9c 14 fe 4a 69 29 90 ab 50 18
fe 2f 40 50 00 00 05 00 00 83 10 00 00 00 20 01
10 00 05 00 00 00 d8 00 00 00 03 00 14 00 1e 20
00 00 00 00 00 af ee 6b 09 24 c2 3d 43 05 00
07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 a 91 c f 93 90 e 3
How to Avoid Information Disclosure when Managing Windows with WMI

Initial WMI response packet with the default WMI security options in use (not including the reassembly):

<table>
<thead>
<tr>
<th>Packet</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol and Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>73</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERPC Response: call_id: 8 ctx_id: 5 IWbemWCOSmartEnum V0</td>
</tr>
</tbody>
</table>

Frame 73 (854 bytes on wire, 854 bytes captured)
Transmission Control Protocol, Src Port: 1032 (1032), Dst Port: 1716 (1716), Seq: 6865, Ack: 1299, Len: 800

DCE RPC Response, Fragment: Last, FragLen: 800, Call: 8 Ctx: 5:

00 17 31 2e 1f 0a 00 80 c7 ea 03 27 08 00 45 00
03 48 02 46 40 00 80 06 e5 3c 0a fc fd 2c 0a fc
fd 08 04 08 06 b4 69 29 a9 ab 9c 15 01 1a 50 18
ff ff 0e 9a 00 00 05 00 02 02 10 00 00 00 20 03
10 00 08 00 00 00 ec 02 00 00 05 00 00 00 73 65
72 76 69 63 65 20 69 73 20 73 74 6f 70 70 65 64

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

Alex M. Timkov

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
How to Avoid Information Disclosure when Managing Windows with WMI

<table>
<thead>
<tr>
<th>Packet</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol and Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>NBNS Name query NBSTAT</td>
</tr>
<tr>
<td>4</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>NBNS Name query response NBSTAT</td>
</tr>
<tr>
<td>5</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP epmap -&gt; 1713 [SYN] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460</td>
</tr>
<tr>
<td>6</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP epmap &gt; 1713 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1260</td>
</tr>
<tr>
<td>7</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP epmap &gt; 1713 [ACK] Seq=1 Ack=1 Win=65535 Len=0</td>
</tr>
<tr>
<td>8</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Bind: call_id: 1 IOXIDResolver V0.0</td>
</tr>
<tr>
<td>10</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IOXIDResolver ServerAlive2 request</td>
</tr>
<tr>
<td>11</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IOXIDResolver ServerAlive2 response[Long frame (2 bytes)]</td>
</tr>
<tr>
<td>12</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP epmap &gt; 1714 [SYN] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460</td>
</tr>
<tr>
<td>13</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP epmap &gt; 1714 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1260</td>
</tr>
<tr>
<td>14</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Bind: call_id: 2 ISystemActivator V0.0, NTLMSSP_NEGOTIATE</td>
</tr>
<tr>
<td>15</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Bind_ack: call_id: 2 NTLMSSP_CHALLENGE accept max_xmit: 5840</td>
</tr>
<tr>
<td>16</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC AUTH3: call_id: 2, NTLMSSP_AUTH, User: PIGO\manager</td>
</tr>
<tr>
<td>17</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>ISystemActivator RemoteCreateInstance request</td>
</tr>
<tr>
<td>18</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP epmap &gt; 1714 [ACK] Seq=185 Ack=1147 Win=64389 Len=0</td>
</tr>
<tr>
<td>19</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP epmap &gt; 1714 [ACK] Seq=185 Ack=1147 Win=64389 Len=0</td>
</tr>
<tr>
<td>20</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP epmap &gt; 1714 [ACK] Seq=97 Ack=193 Win=65343 Len=0</td>
</tr>
<tr>
<td>21</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>ISystemActivator RemoteCreateInstance response</td>
</tr>
<tr>
<td>22</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1715 &gt; 1032 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460</td>
</tr>
<tr>
<td>23</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1032 &gt; 1715 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1260</td>
</tr>
</tbody>
</table>

WMI management session with the default WMI security options in use:
How to Avoid Information Disclosure when Managing Windows with WMI

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Sequence</th>
<th>Acknowledgment</th>
<th>Window Size</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1032</td>
<td>1715</td>
<td>1032</td>
<td>1</td>
<td>65535</td>
<td>0</td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCE RPC</td>
<td>Bind</td>
<td>1 RemUnknown2 V0.0</td>
<td>call_id: 1</td>
<td>IRemUnknown2 RemQueryInterface request IID[1]=IWbemLoginClientID</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How to Avoid Information Disclosure when Managing Windows with WMI

Alex M. Timkov

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
How to Avoid Information Disclosure when Managing Windows with WMI

| 108 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 109 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 110 | 10.252.253.8 | 10.252.253.44 | TCP | 1716 > 1032 [ACK] Seq=1491 Ack=36065 Win=65535 Len=0 |
| 112 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 113 | 10.252.253.8 | 10.252.253.44 | TCP | 1716 > 1032 [ACK] Seq=1491 Ack=38125 Win=65535 Len=0 |
| 114 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 115 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 116 | 10.252.253.8 | 10.252.253.44 | TCP | 1716 > 1032 [ACK] Seq=1491 Ack=40645 Win=65535 Len=0 |
| 117 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 119 | 10.252.253.8 | 10.252.253.44 | TCP | 1716 > 1032 [ACK] Seq=1491 Ack=42705 Win=65535 Len=0 |
| 120 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 121 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 122 | 10.252.253.8 | 10.252.253.44 | TCP | 1716 > 1032 [ACK] Seq=1491 Ack=45225 Win=65535 Len=0 |
| 123 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 124 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 125 | 10.252.253.8 | 10.252.253.44 | TCP | 1716 > 1032 [ACK] Seq=1491 Ack=47745 Win=65535 Len=0 |
| 127 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 128 | 10.252.253.8 | 10.252.253.44 | TCP | 1716 > 1032 [ACK] Seq=1491 Ack=49805 Win=65535 Len=0 |
| 129 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 130 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 131 | 10.252.253.8 | 10.252.253.44 | TCP | 1716 > 1032 [ACK] Seq=1491 Ack=52325 Win=65535 Len=0 |
| 132 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 134 | 10.252.253.8 | 10.252.253.44 | TCP | 1716 > 1032 [ACK] Seq=1491 Ack=54385 Win=65535 Len=0 |
| 135 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 136 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 137 | 10.252.253.8 | 10.252.253.44 | TCP | 1716 > 1032 [ACK] Seq=1491 Ack=56905 Win=65535 Len=0 |
| 138 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 139 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 140 | 10.252.253.8 | 10.252.253.44 | TCP | 1716 > 1032 [ACK] Seq=1491 Ack=59425 Win=65535 Len=0 |
| 142 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 143 | 10.252.253.8 | 10.252.253.44 | TCP | 1716 > 1032 [ACK] Seq=1491 Ack=61485 Win=65535 Len=0 |
| 144 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 145 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
| 146 | 10.252.253.8 | 10.252.253.44 | TCP | 1716 > 1032 [ACK] Seq=1491 Ack=64005 Win=65535 Len=0 |
| 147 | 10.252.253.44 | 10.252.253.8 | TCP | [TCP segment of a reassembled PDU] |
# How to Avoid Information Disclosure when Managing Windows with WMI

## Appendix 2: Secure WMI Information Exchange on the Wire

WMI query packet with the recommended base WMI security options set explicitly:

<table>
<thead>
<tr>
<th>Packet</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>149</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1716 &gt; 1032 [ACK] Seq=1491 Ack=66065 Win=65535 Len=0</td>
</tr>
<tr>
<td>150</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP [TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>151</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP [TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>152</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1716 &gt; 1032 [ACK] Seq=1491 Ack=68585 Win=65535 Len=0</td>
</tr>
<tr>
<td>153</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERPC Response: call_id: 9 cxt_id: 3 IWbemServices V0</td>
</tr>
<tr>
<td>154</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Request: call_id: 10 opnum: 24 cxt_id: 3 IWbemServices V0</td>
</tr>
<tr>
<td>155</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1032 &gt; 1716 [ACK] Seq=69473 Ack=1763 Win=65071 Len=0</td>
</tr>
<tr>
<td>156</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERPC Response: call_id: 10 cxt_id: 3 IWbemServices V0</td>
</tr>
<tr>
<td>157</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1716 &gt; 1032 [ACK] Seq=1763 Ack=69953 Win=65535 Len=0</td>
</tr>
<tr>
<td>158</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Request: call_id: 11 opnum: 3 cxt_id: 5 IWbemWCOSmartEnum V0</td>
</tr>
<tr>
<td>159</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Response: call_id: 11 cxt_id: 5 IWbemWCOSmartEnum V0</td>
</tr>
<tr>
<td>160</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IRemUnknown2 RemRelease request Cnt=2 Refs=5-0 [Long frame (4 bytes)]</td>
</tr>
<tr>
<td>161</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1032 &gt; 1715 [ACK] Seq=625 Ack=1267 Win=65535 Len=0</td>
</tr>
<tr>
<td>162</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IRemUnknown2 RemRelease response -&gt; S_OK</td>
</tr>
<tr>
<td>163</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IRemUnknown2 RemRelease request Cnt=1 Refs=5-0 [Long frame (4 bytes)]</td>
</tr>
<tr>
<td>164</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IRemUnknown2 RemRelease response -&gt; S_OK</td>
</tr>
<tr>
<td>165</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IRemUnknown2 RemRelease request Cnt=1 Refs=5-0 [Long frame (4 bytes)]</td>
</tr>
<tr>
<td>166</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IRemUnknown2 RemRelease response -&gt; S_OK</td>
</tr>
<tr>
<td>167</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1715 &gt; 1032 [FIN, ACK] Seq=1555 Ack=817 Win=64719 Len=0</td>
</tr>
<tr>
<td>168</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1716 &gt; 1032 [FIN, ACK] Seq=1955 Ack=70033 Win=65455 Len=0</td>
</tr>
<tr>
<td>169</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1032 &gt; 1715 [ACK] Seq=817 Ack=1556 Win=65247 Len=0</td>
</tr>
<tr>
<td>170</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1032 &gt; 1716 [ACK] Seq=70033 Ack=1956 Win=64879 Len=0</td>
</tr>
<tr>
<td>171</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1032 &gt; 1715 [FIN, ACK] Seq=817 Ack=1556 Win=65247 Len=0</td>
</tr>
<tr>
<td>172</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1715 &gt; 1032 [ACK] Seq=1556 Ack=818 Win=64719 Len=0</td>
</tr>
<tr>
<td>173</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1032 &gt; 1716 [FIN, ACK] Seq=70033 Ack=1956 Win=64879 Len=0</td>
</tr>
<tr>
<td>174</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1716 &gt; 1032 [ACK] Seq=1956 Ack=70034 Win=65455 Len=0</td>
</tr>
<tr>
<td>175</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1714 &gt; epmap [FIN, ACK] Seq=1147 Ack=1241 Win=64295 Len=0</td>
</tr>
<tr>
<td>176</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1713 &gt; epmap [RST, ACK] Seq=97 Ack=193 Win=0 Len=0</td>
</tr>
<tr>
<td>177</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP epmap &gt; 1714 [ACK] Seq=1241 Ack=1148 Win=64389 Len=0</td>
</tr>
<tr>
<td>178</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP epmap &gt; 1714 [FIN, ACK] Seq=1241 Ack=1148 Win=64389 Len=0</td>
</tr>
<tr>
<td>179</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1714 &gt; epmap [ACK] Seq=1148 Ack=1242 Win=64295 Len=0</td>
</tr>
</tbody>
</table>

---

Alex M. Timkov 62

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
How to Avoid Information Disclosure when Managing Windows with WMI

<table>
<thead>
<tr>
<th>Frame 52 (406 bytes on wire, 406 bytes captured)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCE RPC Request, Fragment: Single, FragLen: 352, Call: 5 Ctx: 3:</td>
</tr>
<tr>
<td>Frame (406 bytes):</td>
</tr>
<tr>
<td>00 80 c7 ea 03 27 00 17 31 2e 1f 0a 08 00 45 00</td>
</tr>
<tr>
<td>01 88 34 ad 40 00 80 06 b4 95 0a fc fd 08 0a fc</td>
</tr>
<tr>
<td>fd 2c 07 32 04 08 9a ed 4f 00 3f c0 4a 8b 50 18</td>
</tr>
<tr>
<td>ff 47 c3 5a 00 00 05 00 00 83 10 00 00 00 60 01</td>
</tr>
<tr>
<td>10 00 05 00 00 14 01 00 00 03 00 14 00 12 5c</td>
</tr>
<tr>
<td>00 00 01 03 00 00 bf 4f 10 82 9e 42 46 2f b7 84</td>
</tr>
<tr>
<td>ac 9d 85 f7 20 62 34 da b2 77 f8 fa da 21 2f 9a</td>
</tr>
<tr>
<td>57 16 48 9e 66 db b2 37 8e ae c7 50 b6 9b 6e e8</td>
</tr>
<tr>
<td>72 e4 2b 17 09 f1 0e 14 8d f2 a0 a9 7e bd f7 42</td>
</tr>
<tr>
<td>a0 e2 a3 b6 2b d3 dd 43 af 06 c7 ce d3 03 91 5e</td>
</tr>
<tr>
<td>72 97 03 09 92 1d f8 e6 c0 f9 81 14 b5 eb 6f 14</td>
</tr>
<tr>
<td>ad 1a a3 9a a1 1c a1 c7 0f e0 0c fb b5 1d 82 e8</td>
</tr>
<tr>
<td>01 c2 68 73 7c 8a ff 57 74 b7 24 87 7f 57 53 55</td>
</tr>
<tr>
<td>65 6a 8b 64 7c 31 48 cc ae 05 74 ae 30 b3 75 cc</td>
</tr>
<tr>
<td>09 16 9a c0 7d f4 bd 3d 47 6d 50 df 46 f1 8a a5</td>
</tr>
<tr>
<td>2a b2 ca 83 04 17 d0 b0 26 42 59 49 93 46 88 e3</td>
</tr>
<tr>
<td>ce 34 4c 04 2b 0e 13 77 27 50 24 58 dc ec 78 31</td>
</tr>
<tr>
<td>75 9d 80 7a fd 59 0f 2b b6 8d 82 89 b9 99 7e 80</td>
</tr>
<tr>
<td>a5 96 6e db e7 1d 66 01 97 74 24 6c 92 91 13 b3</td>
</tr>
<tr>
<td>31 bb 70 95 a9 22 d0 4b cd c5 e7 85 19 da 92 92</td>
</tr>
<tr>
<td>e0 e5 6e 34 e7 d6 2f 08 9b fb f9 c7 a5 42 27 1e</td>
</tr>
<tr>
<td>6c 08 d6 ec 06 84 e1 de 22 f9 ee d3 41 e0 b3 a9</td>
</tr>
<tr>
<td>cd ba 2e 8f d4 20 a5 2f 42 cc 53 57 aa e6 55 17</td>
</tr>
<tr>
<td>2c fc 10 c8 f8 6d 73 bb 44 27 8f 38 91 f9 0a 06</td>
</tr>
</tbody>
</table>

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
How to Avoid Information Disclosure when Managing Windows with WMI

Initial WMI response packet with the recommended base WMI security options set explicitly (not including the reassembly):

<table>
<thead>
<tr>
<th>Packet</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>79</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERPC Response: call_id: 8 ctx_id: 5 IWbemWCOSmartEnum V0</td>
</tr>
</tbody>
</table>

Frame 79 (854 bytes on wire, 854 bytes captured)


DCE RPC Response, Fragment: Last, FragLen: 800, Call: 8 Ctx: 5:

Frame (854 bytes):

```
00 17 31 2e 1f 0a 00 80 c7 ea 03 27 08 00 45 00
03 48 03 0c 40 00 80 06 e4 76 0a fc fd 2c 0a fc
fd 08 04 08 07 32 3f c0 64 43 9a ed 53 98 50 18
ff ff cb 14 00 00 05 00 02 02 10 00 00 00 20 03
10 00 08 00 00 00 ec 02 00 00 05 00 00 00 94 29
54 95 77 f0 bc 9f 7b ab 7d 84 3f 0a af ab d7 98
dd 66 6f 2a a0 9e a0 67 23 65 05 e6 31 ac 63 70
d3 ca 3e 44 15 d7 8a 7a b9 3b 54 77 2f 90 6c 6d
ad b7 80 d1 8d f8 61 57 a1 c9 61 25 ea 7c 84
d8 51 6d 07 58 23 ca 88 c9 6d 5b 54 17 24 93 b6
bd 41 fa 5f 89 ad 2e 2c 8c 88 b3 d7 b3 d7 eb
49 23 ad fe 48 d8 3a b2 cd 4e 47 73 a1 5f d7 3d
30 c4 e5 73 28 eb a6 dc 85 00 e4 d5 85 6a d3 02
45 9f e4 7e 9c 7f a6 2d d6 c6 00 b3 d5 9c 5f d8
cb a7 61 00 6d 18 6e 1b 70 21 6d 6b b0 cd a5 8d
73 2c 14 9f 3d 26 25 08 b1 6b a7 35 cb 72 09 94
e8 94 68 1f f6 03 c2 70 5e 70 a3 04 2a 69 79 75
```
How to Avoid Information Disclosure when Managing Windows with WMI

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

Alex M. Timkov

WMI management session with the recommended base WMI security options set explicitly:

<table>
<thead>
<tr>
<th>Packet</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol and Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>NBNS Name query NBSTAT</td>
</tr>
<tr>
<td>4</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>NBNS Name query response NBSTAT</td>
</tr>
<tr>
<td>5</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1838 &gt; epmap [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
<tr>
<td>6</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP epmap &gt; 1838 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1260</td>
</tr>
<tr>
<td>7</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1838 &gt; epmap [ACK] Seq=1 Ack=1 Win=65535 Len=0</td>
</tr>
<tr>
<td>8</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Bind call_id: 1 IOXIDResolver V0.0</td>
</tr>
<tr>
<td>9</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERPC Bind_ack call_id: 1 accept max_xmit: 5840 max_recv: 5840</td>
</tr>
<tr>
<td>10</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IOXIDResolver ServerAlive2 request</td>
</tr>
<tr>
<td>11</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>IOXIDResolver ServerAlive2 response[Long frame (2 bytes)]</td>
</tr>
<tr>
<td>12</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1839 &gt; epmap [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
<tr>
<td>13</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP epmap &gt; 1839 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1260</td>
</tr>
<tr>
<td>14</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP 1839 &gt; epmap [ACK] Seq=1 Ack=1 Win=65535 Len=0</td>
</tr>
<tr>
<td>15</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Bind call_id: 2 ISystemActivator V0.0, NTLMSSP_NEGOTIATE</td>
</tr>
<tr>
<td>17</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC AUTH3 call_id: 2, NTLMSSP_AUTH, User: PIGO\manager</td>
</tr>
<tr>
<td>18</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>ISystemActivator RemoteCreateInstance request</td>
</tr>
<tr>
<td>19</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP epmap &gt; 1839 [ACK] Seq=185 Ack=1147 Win=64389 Len=0</td>
</tr>
<tr>
<td>20</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP epmap &gt; 1839 [ACK] Seq=185 Ack=1147 Win=64389 Len=0</td>
</tr>
<tr>
<td>21</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP 1840 &gt; 1032 [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
<tr>
<td>22</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP 1032 &gt; 1840 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1260</td>
</tr>
<tr>
<td>23</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP 1840 &gt; 1032 [ACK] Seq=1 Ack=1 Win=65535 Len=0</td>
</tr>
<tr>
<td>24</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERPC Alter_context call_id: 2 IWbemLoginClientID V0.0</td>
</tr>
<tr>
<td>26</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Request call_id: 2 opnum: 3 ctx_id: 1 IWbemLoginClientID V0</td>
</tr>
<tr>
<td>27</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Response call_id: 2 ctx_id: 1 IWbemLoginClientID V0</td>
</tr>
<tr>
<td>28</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Request call_id: 2 opnum: 3 ctx_id: 1 IWbemLoginClientID V0</td>
</tr>
<tr>
<td>29</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Response call_id: 2 cxt_id: 1 IWbemLoginClientID V0</td>
</tr>
<tr>
<td>30</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Request call_id: 2 opnum: 3 cxt_id: 1 IWbemLoginClientID V0</td>
</tr>
<tr>
<td>31</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC Response call_id: 2 cxt_id: 1 IWbemLoginClientID V0</td>
</tr>
</tbody>
</table>
### How to Avoid Information Disclosure when Managing Windows with WMI

<table>
<thead>
<tr>
<th>Time</th>
<th>Source/IP</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.252.253.8</td>
<td>TCP 1841 &gt; 1032 [ACK] Seq=1 Ack=1 Win=65535 Len=0</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC Bind: call_id: 3 IWbemLevel1Login V0.0</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC Bind_ack: call_id: 3 accept max_xmit: 5840 max_recv: 5840</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC AUTH3: call_id: 3</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC Request: call_id: 3 opnum: 20 ctx_id: 4 IWbemServices V0.0</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC AUTH3: call_id: 3 accept max_xmit: 5840</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC Bind: call_id: 5 IWbemServices V0.0, NTLMSSP_NEGOTIATE</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC Bind_ack: call_id: 5, NTLMSSP_CHALLENGE accept max_xmit: 5840</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC BIND: call_id: 6 IWbemLevel1Login V0</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC Alter_context: call_id: 6 accept max_xmit: 5840</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC Alter_context Resp: call_id: 6 accept max_xmit: 5840 max_recv: 5840</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC RemQueryInterface request [Malformed Packet]</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC RemQueryInterface response [Malformed Packet]</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC Alter_context: call_id: 7 IWbemServices V0.0</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC Alter_context Resp: call_id: 7 accept max_xmit: 5840 max_recv: 5840</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC Request: call_id: 7 opnum: 19 ctx_id: 4 IWbemFetchSmartEnum V0.0</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC RemRelease request Cnt=1 Refs=5-0-5 [Long frame (4 bytes)]</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC RemRelease response -&gt; S_OK</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC RemQueryInterface request [Malformed Packet]</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC RemQueryInterface response [Malformed Packet]</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC Alter_context: call_id: 8 IWbemLevel1Login V0</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC Alter_context Resp: call_id: 8 accept max_xmit: 5840</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC RemRelease request Cnt=1 Refs=5-0-5 [Long frame (4 bytes)]</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC RemRelease response -&gt; S_OK</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC RemQueryInterface request [Malformed Packet]</td>
<td></td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>DCERPC RemQueryInterface response [Malformed Packet]</td>
<td></td>
</tr>
</tbody>
</table>

**Example Packet Details**

- **TCP**: 10.252.253.8 > 10.252.253.44 (ACK) Seq=1 Ack=1 Win=65535 Len=0
- **DCERPC**: Bind: call_id: 3 IWbemLevel1Login V0.0
- **DCERPC**: Bind_ack: call_id: 3 accept max_xmit: 5840 max_recv: 5840
- **DCERPC**: AUTH3: call_id: 3
- **DCERPC**: Request: call_id: 3 opnum: 20 ctx_id: 4 IWbemServices V0.0
- **DCERPC**: BIND: call_id: 6 IWbemLevel1Login V0
- **DCERPC**: Alter_context: call_id: 6 accept max_xmit: 5840
- **DCERPC**: Alter_context Resp: call_id: 6 accept max_xmit: 5840 max_recv: 5840
- **DCERPC**: RemQueryInterface request [Malformed Packet]
- **DCERPC**: RemQueryInterface response [Malformed Packet]
- **DCERPC**: Alter_context: call_id: 7 IWbemServices V0.0
- **DCERPC**: Alter_context Resp: call_id: 7 accept max_xmit: 5840 max_recv: 5840
- **DCERPC**: Request: call_id: 7 opnum: 19 ctx_id: 4 IWbemFetchSmartEnum V0.0
- **DCERPC**: RemRelease request Cnt=1 Refs=5-0-5 [Long frame (4 bytes)]
- **DCERPC**: RemRelease response -> S_OK
- **DCERPC**: RemQueryInterface request [Malformed Packet]
- **DCERPC**: RemQueryInterface response [Malformed Packet]
- **DCERPC**: Alter_context: call_id: 8 IWbemLevel1Login V0
- **DCERPC**: Alter_context Resp: call_id: 8 accept max_xmit: 5840

**Additional Notes**

- Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
- Alex M. Timkov

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
### How to Avoid Information Disclosure when Managing Windows with WMI

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Seq</th>
<th>Ack</th>
<th>Win</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842</td>
<td>1032</td>
<td>1683</td>
<td>35969</td>
<td>65535</td>
<td>0</td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC</td>
<td>Call id: 8</td>
<td>Context id: 5</td>
<td>1683</td>
<td>10089</td>
<td>65535</td>
<td>0</td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERPC</td>
<td>Call id: 9</td>
<td>Context id: 3</td>
<td>1683</td>
<td>12609</td>
<td>65535</td>
<td>0</td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>TCP segment of a reassembled PDU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Key Fingerprint

```
AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
```

---

Alex M. Timkov

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
How to Avoid Information Disclosure when Managing Windows with WMI

<table>
<thead>
<tr>
<th></th>
<th>10.252.253.8</th>
<th>10.252.253.44</th>
<th>TCP</th>
<th>1842 &gt; 1032 [ACK] Seq=1683 Ack=38029 Win=65535 Len=0</th>
</tr>
</thead>
<tbody>
<tr>
<td>120</td>
<td>10.252.253.8</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>121</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>122</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=40549 Win=65535 Len=0</td>
</tr>
<tr>
<td>123</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>124</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>125</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=43039 Win=65535 Len=0</td>
</tr>
<tr>
<td>126</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>127</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>128</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=44519 Win=65535 Len=0</td>
</tr>
<tr>
<td>129</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>130</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>131</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=47649 Win=65535 Len=0</td>
</tr>
<tr>
<td>132</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>133</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>134</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=49709 Win=65535 Len=0</td>
</tr>
<tr>
<td>135</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>136</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>137</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=52229 Win=65535 Len=0</td>
</tr>
<tr>
<td>138</td>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>139</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=54289 Win=65535 Len=0</td>
</tr>
<tr>
<td>140</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>141</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=56809 Win=65535 Len=0</td>
</tr>
<tr>
<td>142</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>143</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=59329 Win=65535 Len=0</td>
</tr>
<tr>
<td>144</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>145</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>146</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=61389 Win=65535 Len=0</td>
</tr>
<tr>
<td>147</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>148</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=63909 Win=65535 Len=0</td>
</tr>
<tr>
<td>149</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>150</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=65599 Win=65535 Len=0</td>
</tr>
<tr>
<td>151</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>152</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=68489 Win=65535 Len=0</td>
</tr>
<tr>
<td>153</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>154</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=69569 Win=65535 Len=0</td>
</tr>
<tr>
<td>155</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>156</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=69569 Win=65535 Len=0</td>
</tr>
<tr>
<td>157</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>158</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>1842 &gt; 1032 [ACK] Seq=1683 Ack=69569 Win=65535 Len=0</td>
</tr>
<tr>
<td>159</td>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
</tbody>
</table>

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

Appendix 3: Enforcing Encrypted Access at the Server

The instructions are documented in the Microsoft article Requiring an Encrypted Connection to a Namespace (Microsoft MSDN, 2007). The article extract is provided below for your convenience. To set required encryption:

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Dest Address</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Dest Port</th>
<th>Command</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERP</td>
<td>1025</td>
<td>2596</td>
<td>Request</td>
<td>call_id: 10 opnum: 24 ctx_id: 3 IWbemServices V0</td>
</tr>
<tr>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>1032</td>
<td>1842</td>
<td>Request</td>
<td>call_id: 10 ctx_id: 3 IWbemServices V0</td>
</tr>
<tr>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>DCERP</td>
<td>1025</td>
<td>2596</td>
<td>Response</td>
<td>call_id: 10 ctx_id: 3 IWbemServices V0</td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>DCERP</td>
<td>1025</td>
<td>2596</td>
<td>Request</td>
<td>call_id: 11 opnum: 3 ctx_id: 5 IWbemWCOSmartEnum V0</td>
</tr>
<tr>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>1032</td>
<td>1842</td>
<td>Response</td>
<td>call_id: 11 ctx_id: 5 IWbemWCOSmartEnum V0</td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IRemUnknown2</td>
<td>RemRelease</td>
<td>Request</td>
<td>Malformed Packet</td>
<td></td>
</tr>
<tr>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>1032</td>
<td>1842</td>
<td>Response</td>
<td>Malformed Packet</td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IRemUnknown2</td>
<td>RemRelease</td>
<td>Request</td>
<td>Malformed Packet</td>
<td></td>
</tr>
<tr>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>1032</td>
<td>1842</td>
<td>Response</td>
<td>Malformed Packet</td>
</tr>
<tr>
<td>10.252.253.8</td>
<td>10.252.253.44</td>
<td>IRemUnknown2</td>
<td>RemRelease</td>
<td>Request</td>
<td>Malformed Packet</td>
<td></td>
</tr>
<tr>
<td>10.252.253.44</td>
<td>10.252.253.8</td>
<td>TCP</td>
<td>1032</td>
<td>1842</td>
<td>Response</td>
<td>Malformed Packet</td>
</tr>
</tbody>
</table>

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
How to Avoid Information Disclosure when Managing Windows with WMI

1. Create a Managed Object Format (MOF) file or modify your existing MOF file that defines the namespace. In the following example, the namespace to be modified is root\MyNamespace and the file is named MyNamespace_security.mof.

RequiresEncryption has a Boolean data type so it must be set to TRUE or FALSE.

```
#pragma namespace("\\\\Root\MyNamespace")
[RequiresEncryption(TRUE)]
instance of __systemSecurity { }; 
```

2. Run mofcomp.exe to compile the MOF file.

   `c:\mofcomp MyNamespae_security.mof`

When returning data on an asynchronous callback connection, WMI returns an access denied message to the requesting computer. WMI also makes a log entry in the NT Event Log of the computer with the encrypted namespace stating that a secure connection cannot be established to the client.

Starting with Windows Vista, the Wbemcore.log file no longer exists. You can check the NT Event Log for entries indicating rejected inbound data requests to namespaces that require encryption.

Windows Server 2003, Windows XP, Windows 2000, and Windows NT 4.0: Entries for rejected inbound data requests can be found in both the NT Event Log and Wbemcore.log.
How to Avoid Information Disclosure when Managing Windows with WMI

Appendix 4: Cross Platform WMI Connection Limitations

The article Connecting Between Different Operating Systems (Microsoft MSDN Library, 2007, Win32 and COM Development) documents the limitations that are occurring in mixed Windows environments using WMI management. The article extract is provided in this appendix for your convenience:

Some connections between operating system versions are not supported:

- You cannot connect to a computer that is running Windows XP Home Edition.
- A computer running Windows NT cannot connect to an operating system later than Windows 2000, such as Windows XP or Windows Server 2003.
- Accessing a Windows Server 2003 computer from Windows 98 or Windows 95 is not supported.

Some connections between operating system versions have special requirements:

- To connect to a Windows 2000 Server SP4 and later running WMI version 1.01, you must explicitly set the impersonation level to Impersonate.
- Windows 2000 computers must have Service Pack 2 installed to be able to connect to Windows XP and later operation systems.
- To connect from Windows Server 2003 to computers running Windows 98, Windows Me, and Windows NT Server 4.0 SP3 and later, the credentials must be specified. If you try to use the default current user by not supplying a username and password, then the connection does not work.

Appendix 5: Setting DCOM Remote Access Security

Configuring DCOM for WMI access is described in the Microsoft article Securing a Remote WMI Connection (Microsoft MSDN Library, 2007, Win32 and COM Development).

This Appendix provides the article extract for your convenience:

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

The following procedure describes how to grant DCOM remote launch and activation permissions for certain users and groups. If Computer A is connecting remotely to Computer B, you can set these permissions on Computer B to allow a user or group that is not part of the administrators group on Computer B to execute DCOM launch and activation calls on Computer B. To grant DCOM remote launch and activation permissions for a user or group:

1. Click Start, click Run, type DCOMCNFG, and then click OK.
2. In the Component Services dialog box, expand Component Services, expand Computers, and then right-click My Computer and click Properties.
3. In the My Computer Properties dialog box, click the COM Security tab.
4. Under Launch and Activation Permissions, click Edit Limits.
5. In the Launch Permission dialog box, follow these steps if your name or your group does not appear in the Groups or user names list:
   1. In the Launch Permission dialog box, click Add.
   2. In the Select Users, Computers, or Groups dialog box, add your name and the group in the Enter the object names to select box, and then click OK.
6. In the Launch Permission dialog box, select your user and group in the Group or user names box. In the Allow column under Permissions for User, select Remote Launch and select Remote Activation, and then click OK.

The following procedure describes how to grant DCOM remote access permissions for certain users and groups. If Computer A is connecting remotely to Computer B, you can set these permissions on Computer B to allow a user or group that is not part of the administrators group on Computer B to connect to Computer B. To grant DCOM remote access permissions:

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

1. Click Start, click Run, type DCOMCNFG, and then click OK.
2. In the Component Services dialog box, expand Component Services, expand Computers, and then right-click My Computer and click Properties.
3. In the My Computer Properties dialog box, click the COM Security tab.
5. In the Access Permission dialog box, select ANONYMOUS LOGON name in the Group or user names box. In the Allow column under Permissions for User, select Remote Access, and then click OK.

Appendix 6: Vista Specific Security Descriptor Access

Here is the extract from the Microsoft MSDN library article Changing Access Security on Securable Objects (Microsoft MSDN Library, 2007), detailing Windows Vista specific access to some of the security descriptors. Please refer to the article for full detail: http://msdn2.microsoft.com/en-us/library/aa384905.aspx.

WMI Namespaces

A provider can establish security that only allows certain groups to have access to the data in a WMI namespace. Namespace security is controlled by methods on the __SystemSecurity class. Starting with Windows Vista, the GetSecurityDescriptor and SetSecurityDescriptor methods return and write __SecurityDescriptor objects. For more information, see Setting Namespace Security Descriptors.


Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

class allow you to change the namespace security. However, these methods only use the
binary byte array form of the security descriptor, which is difficult to manipulate. You can
call methods in the BinarySDToWin32SD or BinarySDToSDDL methods in the
Win32_SecurityDescriptorHelper class to convert the binary descriptor to an instance of
Win32_SecurityDescriptor or to Security Descriptor Definition Language (SDDL).

Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0, and
Windows Me/98/95: In a script or Visual Basic, you can use the procedure described in
Securing WMI Namespaces to change the security of a namespace.

Registry keys

Starting with Windows Vista, you can secure registry keys so that they cannot be
changed by unauthorized users. The StdRegProv class has the GetSecurityDescriptor and
SetSecurityDescriptor methods. These methods return and write
Win32_SecurityDescriptor objects.

Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0, and
Windows Me/98/95: The GetSecurityDescriptor and SetSecurityDescriptor methods in the
StdRegProv class are not available. You can call the CheckAccess method in StdRegProv
to determine if a user has access to a registry key.

Printers

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

Starting with Windows Vista, you can secure access to instances of the Win32_Printer class using the GetSecurityDescriptor and SetSecurityDescriptor methods. These methods return and write Win32_SecurityDescriptor objects.


Services

Starting with Windows Vista, you can secure access to instances of the Win32_Service class using the GetSecurityDescriptor and SetSecurityDescriptor methods. These methods return and write Win32_SecurityDescriptor objects.


DCOM applications

DCOM applications instances have several security descriptors. Starting with Windows Vista, you can use methods of the Win32_DCOMApplicationSetting class to get or change the various security descriptors. Security descriptors are returned as instances.
How to Avoid Information Disclosure when Managing Windows with WMI

of the Win32_SecurityDescriptor class. To get or change the configuration permissions, call the GetConfigurationSecurityDescriptor or SetConfigurationSecurityDescriptor methods. To get or change the access permissions, call the GetAccessSecurityDescriptor or SetAccessSecurityDescriptor methods. To get or change the startup and activation permissions, call the GetLaunchSecurityDescriptor or SetLaunchSecurityDescriptor methods.


Files

The GetSecurityDescriptor and SetSecurityDescriptor methods are in the Win32_LogicalFileSecuritySetting class, rather than in the CIM_DataFile class.

Shares

The GetSecurityDescriptor and SetSecurityDescriptor methods are in the Win32_LogicalShareSecuritySetting class, rather than in the Win32_Share class.

Security Issues

It is recommended that changes to security descriptors be done with great caution.

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

so that the security of the object is not compromised. Be aware that the order of ACEs in a DACL can affect access security. For more information, see Order of ACEs in a DACL.

Windows Server 2003, Windows XP, Windows 2000, and Windows NT 4.0: If the SE_DACL_PRESENT bit is set, but a DACL parameter is not set, a null DACL is written to the new security descriptor. A null DACL creates security vulnerability because it grants the Everyone account full access to the object. For more information, see Creating a DACL.

Appendix 7: Sample WMI Service Management Script

You may recall our very short sample script used for illustrations through this paper. Here is a slightly more robust service manipulation script. This is the version that was used to perform most of the testing tasks for this paper. If you would like to re-use parts of this script, please implement your own error checks. Please keep in mind this only a basic test script. All it does is accepting remote system name/IP, user name, user password, and a local file path. The script then retrieves the full service list from the remote system, to both the shell and the log file specified by the local file path. The script then prompts to select the service from the service list for manipulation, performs the service state test, and allows for the service state change:

`1 Retrieve service information from remote system to file
1 Display service information
1 Search service list for specific service`

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

Alex M. Timkov

© SANS Institute 2007, As part of the Information Security Reading Room
Author retains full rights.
How to Avoid Information Disclosure when Managing Windows with WMI

Alex M. Timkov

ServiceSearch strFileName, strService, intSearchResult

' ----- Debug -----
' Wscript.Echo vbCrLf & "Search result = " & intSearchResult
' -- End Debug --

If intSearchResult Then
    WScript.Echo strService & " service found."
    ServiceTest strComputer, strService, strUser, strPassword

    strManage = inputbox _
        ("Type Stop or Start to manage service. " _
        & "Hit Enter to exit.", "Input")

    If strManage = "Stop" Then
        ServiceStop strComputer, strService, strUser, strPassword
        End If

    If strManage = "Start" Then
        ServiceStart strComputer, strService, strUser, strPassword
        End If

    ServiceTest strComputer, strService, strUser, strPassword
Else
    WScript.Echo vbCrLf & strService _
        & " service not installed. Nothing to do."
End If

End If

WScript.Echo vbCrLf & "Script execution completed. Exiting."
WScript.Quit

'-------------------------------------------------------------
' List services running on remote host and output to local file
'-------------------------------------------------------------

Sub ServiceList(strComputer, strFileName, strUser, strPassword)

    Dim colServices
    Dim objFSO, objLocator, objService, objTextFile, objWMIService

    Const constWrite = 2

    Set objFSO = CreateObject("Scripting.FileSystemObject")
    Set objTextFile = objFSO.OpenTextFile _
        (strFileName, constWrite, True)
    Set objLocator = CreateObject("WbemScripting.SWbemLocator")
    Set objWMIService = objLocator.ConnectServer _
        (strComputer, "root\CIMV2", strUser, strPassword)

    colServices = GetServices(objWMIService)

    For Each objService In colServices
        objTextFile.WriteLine objService.Name
    Next

    objTextFile.Close

End Sub
How to Avoid Information Disclosure when Managing Windows with WMI

```vbs
objWMIService.Security_.impersonationlevel = 3

Set colServices = objWMIService.ExecQuery _
("Select * from Win32_Service")

If Not(colServices Is Nothing) Then
    For Each objService in colServices
        If Not(objService Is Nothing) Then
            objTextFile.WriteLine(objService.DisplayName & vbTab & objService.Name & vbTab & objService.State)
        End If
    Next
End If

objTextFile.Close
Set objService = Nothing
Set colServices = Nothing
Set objWMIService = Nothing

End Sub

End Sub
```

```vbs
Sub ServiceDisplay(strFileName)
    Dim objFSO, objTextFile
    Dim strLine
    Const constRead = 1

    Set objFSO = CreateObject("Scripting.FileSystemObject")
    Set objTextFile = objFSO.OpenTextFile (strFileName, constRead, True)

    Do Until objTextFile.AtEndOfStream
        strLine = objTextFile.ReadLine
        Wscript.Echo strLine
    Loop

    objTextFile.Close

End Sub
```

```vbs
Sub ServiceSearch(strFileName, strService, intSearchResult)
    Dim objFSO, objTextFile

    Set objFSO = CreateObject("Scripting.FileSystemObject")
    Set objTextFile = objFSO.OpenTextFile (strFileName, constRead, True)

    Do Until objTextFile.AtEndOfStream
        strLine = objTextFile.ReadLine
        Wscript.Echo strLine
    Loop

    objTextFile.Close

End Sub
```

Alex M. Timkov

© SANS Institute 2007, As part of the Information Security Reading Room

Author retains full rights.
How to Avoid Information Disclosure when Managing Windows with WMI

```vba
Dim strFile
Const constRead = 1
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objTextFile = objFSO.OpenTextFile(_
    strFileName, constRead, True)
strFile = objTextFile.ReadAll
objTextFile.close
If InStr(1, strFile, strService, 1) Then
    intSearchResult = 1
Else
    intSearchResult = 0
End If
End Sub

Sub ServiceStop(strComputer, strService, strUser, strPassword)
    Dim colServices
    Dim objLocator, objService, objWMIService
    Dim intTimeout
    intTimeout = 10000
    Set objLocator = CreateObject("WbemScripting.SWbemLocator")
    Set objWMIService = objLocator.ConnectServer(_
        strComputer, "root\CIMV2", strUser, strPassword)
    objWMIService.Security_.impersonationlevel = 3
    Set colServices = objWMIService.ExecQuery(_
        "Select * from Win32_Service Where Name = " & _
        strService & "")
    If Not(colServices Is Nothing) Then
        For Each objService in colServices
            If Not(objService Is Nothing) Then
                If objService.State = "Running" Then
                    WScript.Echo vbCrLf & "Stopping " & strService _
                        & " service..."
                    objService.StopService()
                    WScript.Sleep intTimeout
                End If
            End If
        Next
    End If
End Sub
```

Alex M. Timkov
End If

Set objService = Nothing
Set colServices = Nothing
Set objWMIService = Nothing
Set objLocator = Nothing

End Sub

'--------------------------------------------------
' Start service of user choice not running on remote host
'--------------------------------------------------

Sub ServiceStart(strComputer, strService, strUser, strPassword)
    Dim colServices
    Dim objLocator, objService, objWMIService
    Dim intTimeout

    intTimeout = 10000

    Set objLocator = CreateObject("WbemScripting.SWbemLocator")

    Set objWMIService = objLocator.ConnectServer(strComputer, "root\CIMV2", strUser, strPassword)

    objWMIService.Security_.impersonationlevel = 3

    Set colServices = objWMIService.ExecQuery("Select * from Win32_Service Where Name = " & strService & """)

    If Not(colServices Is Nothing) Then
        For Each objService in colServices
            If Not(objService Is Nothing) Then
                If objService.State <> "Running" Then
                    Wscript.Echo vbCrLf & "Starting " & strService & " service..."
                    objService.StartService()
                    Wscript.Sleep intTimeout
                End If
            End If
        Next
    End If

    Set objService = Nothing
    Set colServices = Nothing
    Set objWMIService = Nothing
    Set objLocator = Nothing

End Sub

'-----------------------------------------------------
'Test state of service chosen by user
'-----------------------------------------------------

Alex M. Timkov
How to Avoid Information Disclosure when Managing Windows with WMI

Sub ServiceTest(strComputer, strService, strUser, strPassword)
    Dim colServices
    Dim objLocator, objService, objWMIService
    Set objLocator = CreateObject("WbemScripting.SWbemLocator")
    Set objWMIService = objLocator.ConnectServer(strComputer, "root\CIMV2", strUser, strPassword)
    objWMIService.Security_.impersonationlevel = 3
    Set colServices = objWMIService.ExecQuery("Select * from Win32_Service Where Name = " & strService & ")
    If Not(colServices Is Nothing) Then
        For Each objService in colServices
            If Not(objService Is Nothing) Then
                If objService.State = "Stopped" Then
                    Wscript.Echo vbCrlf & strService & " service is not running."
                Else If objService.State = "Running" Then
                    Wscript.Echo vbCrlf & strService & " service is running."
                Else
                    Wscript.Echo vbCrlf & strService & " service state is unknown."
                End If
            End If
        Next
    End If
    Set objService = Nothing
    Set colServices = Nothing
    Set objWMIService = Nothing
    Set objLocator = Nothing
End Sub

'---------------------------------------------
' End of WMI Based Service Manipulation Script
'---------------------------------------------

Alex M. Timkov
# Upcoming SANS App Sec Training

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS San Francisco Spring 2020</td>
<td>San Francisco, CA</td>
<td>Mar 16, 2020 - Mar 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2020</td>
<td>Orlando, FL</td>
<td>Apr 03, 2020 - Apr 10, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Mentor Session - DEV522</td>
<td>Novi, MI</td>
<td>Apr 21, 2020 - May 21, 2020</td>
<td>Mentor</td>
</tr>
<tr>
<td>SANS Amsterdam May 2020</td>
<td>Amsterdam, Netherlands</td>
<td>May 11, 2020 - May 18, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Silicon Valley - Cupertino 2020</td>
<td>Cupertino, CA</td>
<td>Jun 22, 2020 - Jun 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Copenhagen August 2020</td>
<td>Copenhagen, Denmark</td>
<td>Aug 24, 2020 - Aug 29, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Network Security 2020</td>
<td>Las Vegas, NV</td>
<td>Sep 20, 2020 - Sep 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>