WinRM远程管理工具的使用

WinRM概述

WinRM是Windows Remote Managementd（Windows远程管理）的简称。它基于Web服务管理(WebService-Management)标准，WinRM2.0默认端口5985（HTTP端口）或5986（HTTPS端口）。

如果所有的机器都是在域环境下，则可以使用默认的5985端口，否则的话需要使用HTTPS传输(5986端口)。使用WinRM我们可以在对方有设置防火墙的情况下远程管理这台服务器，因为启动WinRM服务后，防火墙默认会放行5985端口。WinRM服务在Windows Server 2012以上服务器自动启动。

在WindowsVista上，服务必须手动启动。WinRM的好处在于，这种远程连接不容易被察觉到，也不会占用远程连接数!

```
PORT     STATE SERVICE VERSION
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

WinRM官方文档

https://docs.microsoft.com/en-us/windows/win32/winrm/portal

WinRM的配置

```
#查看WinRM状态
winrm enumerate winrm/config/listener

#开启WinRM远程管理
Enable-PSRemoting -force

#设置WinRM自启动
Set-Service WinRM -StartMode Automatic

#对WinRM服务进行快速配置，包括开启WinRM和开启防火墙异常检测,默认的5985端口
winrm quickconfig -q
#对WinRM服务进行快速配置，包括开启WinRM和开启防火墙异常检测，HTTPS传输，5986端口
winrm quickconfig -transport:https

#查看WinRM的配置
winrm get winrm/config

#查看WinRM的监听器
winrm e winrm/config/listener

#为WinRM服务配置认证
winrm set winrm/config/service/auth '@{Basic="true"}'

#修改WinRM默认端口
winrm set winrm/config/client/DefaultPorts '@{HTTPS="8888"}'

#为WinRM服务配置加密方式为允许非加密:
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
```

```
#设置只允许指定IP远程连接WinRM
winrm set winrm/config/Client '@{TrustedHosts="192.168.10.*"}'

#执行命令
winrm invoke create wmicimv2/win32_process -SkipCAcheck -skipCNcheck
'@{commandline="calc.exe"}'

#执行指定命令程序
winrm invoke create wmicimv2/win32_process -SkipCAcheck -skipCNcheck
'@{commandline="c:\users\administrator\desktop\test.exe"}'
```

```
                    r> winrm enumerate winrm/config/listener
PS C:\Users\Administrator> enable-psremoting -force
在此计算机上，WinRM 已设置为接收请求。
WinRM 已经进行了更新，以用于远程管理。
在 HTTP://* 上创建 WinRM 侦听程序接受 WS-Man 对此机器上任意 IP 的请求。
WinRM 防火墙异常已启用。

PS C:\Users\Administrator> winrm enumerate winrm/config/listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 127.0.0.1, 192.168.10.131, ::1, fe80::100:7f:fffe%13, fe80::5efe:192.168.10.131%12, fe80
```

开启WinRM的过程，做了如下几件事：

```
其中包括:
    1. 启动或重新启动(如果已启动) WinRM 服务
    2. 将 WinRM 服务类型设置为自动启动
    3. 创建一个侦听器以接受任意 IP 地址上的请求
    4. 对 WS-Management 流量启用防火墙例外(仅适用于 http)。
```

快速配置WinRM

```
PS C:\Windows\system32> winrm quickconfig
在此计算机上，WinRM 未设置为接收请求。
必须进行以下更改:

将 WinRM 服务类型设置为延迟的自动启动。
启动 WinRM 服务。

进行这些更改吗[y/n]? y

WinRM 已更新为接收请求。

成功更改 WinRM 服务类型。
已启动 WinRM 服务。
WinRM 没有设置成为了管理此计算机而允许对其进行远程访问。
必须进行以下更改:

在 HTTP://* 上创建 WinRM 侦听程序接受 WS-Man 对此机器上任意 IP 的请求。
启用 WinRM 防火墙异常。

进行这些更改吗[y/n]? y

WinRM 已经进行了更新，以用于远程管理。

在 HTTP://* 上创建 WinRM 侦听程序接受 WS-Man 对此机器上任意 IP 的请求。
WinRM 防火墙异常已启用。
PS C:\Windows\system32> winrm enumerate winrm/config/listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 127.0.0.1, 169.254.194.11, 192.168.10.130, ::1, fe80::5efe:192.168.10.130%15, fe80::b8:65cd:3841:c20b%
14, fe80::5087:1354:d6c1:2cf7%11
```

```
PS C:\Windows\system32> winrm e winrm/config/listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 127.0.0.1, 169.254.194.11, 192.168.10.130, ::1, fe80::5efe:192.168.10.130%15, fe80::b8:65cd:3841:c20b%
14, fe80::5087:1354:d6c1:2cf7%11

PS C:\Windows\system32> winrm set winrm/config/service/auth @{Basic="true"}
错误: Invalid use of command line. Type "winrm -?" for help.
PS C:\Windows\system32> winrm set winrm/config/service/auth '@{Basic="true"}'
Auth
    Basic = true
    Kerberos = true
    Negotiate = true
    Certificate = false
    CredSSP = false
    CbtHardeningLevel = Relaxed

PS C:\Windows\system32> winrm set winrm/config/service '@{AllowUnencrypted="true"}'
Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 15
    EnumerationTimeoutms = 60000
    MaxConnections = 25
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = true
    Auth
        Basic = true
        Kerberos = true
        Negotiate = true
        Certificate = false
        CredSSP = false
        CbtHardeningLevel = Relaxed
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    IPv4Filter = *
    IPv6Filter = *
    EnableCompatibilityHttpListener = false
    EnableCompatibilityHttpsListener = false
```

设置只允许指定IP远程连接WinRM

```
PS C:\Users\Administrator> winrm s winrm/config/Client '@{TrustedHosts="192.168.10.*"}'
Client
    NetworkDelayms = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
    Auth
        Basic = true
        Digest = true
        Kerberos = true
        Negotiate = true
        Certificate = true
        CredSSP = false
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    TrustedHosts = 192.168.10.*
```

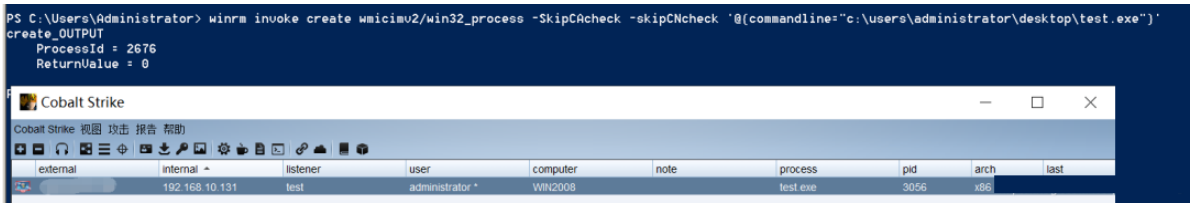
通过WinRM执行程序

执行calc.exe程序

```
PS C:\Users\Administrator> winrm invoke create wmicimv2/win32_process -SkipCAcheck -skipCNcheck '@{commandline="calc.exe"}'
create_OUTPUT
    ProcessId = 236
    ReturnValue = 0

PS C:\Users\Administrator> tasklist | findstr 236
calc.exe                     236 Services                   0      9,100 K
```

执行指定命令程序，我们这里执行木马



利用WinRM远程连接主机

客户端连接

客户端连接的话，也需要启动WinRM，然后再执行以下命令进行连接。

方法一：使用winrs连接

在cmd窗口执行以下命令

```
winrs -r:http://192.168.10.20:5985 -u:administrator -p:root cmd
```

方法二：使用Enter-PSSession连接

```
Enter-PSSession -computer win2008.xie.com -Credential xie\administrator -Port
5985
或
New-PSSession -Name test -ComputerName win7.xie.com -Credential
xie\administrator
Enter-PSSession -Name test
```

```
PS C:\Users\hack> hostname;whoami
WIN7
xie\hack
PS C:\Users\hack> Enter-PSSession -computer win2008.xie.com -Credential xie\administrator
[win2008.xie.com]: PS C:\Users\Administrator\Documents> hostname;whoami
WIN2008
xie\administrator
[win2008.xie.com]: PS C:\Users\Administrator\Documents> exit
PS C:\Users\hack>
PS C:\Users\hack> New-PSSession -Name test -ComputerName win7.xie.com -Credential xie\administrator

 Id Name            ComputerName    State    ConfigurationName     Availability
 -- ----            ------------    -----    -----------------     ------------
  1 test            win7.xie.com    Opened   Microsoft.PowerShell     Available


PS C:\Users\hack> Enter-PSSession -Name test
[win7.xie.com]: PS C:\Users\administrator\Documents> hostname;whoami
WIN7
xie\administrator
[win7.xie.com]: PS C:\Users\administrator\Documents>
```

查看WinRM远程会话

```
Get-PSSession
```

进入ID为2的WinRM会话中

```
Enter-PSSession -id 2
```

退出WinRM会话

```
Exit-PSSession
```

```
PS C:\Users\Administrator> Get-PSSession

 Id Name            ComputerName    State    ConfigurationName     Availability
 -- ----            ------------    -----    -----------------     ------------
  1 Priv            win7.xie.com    Opened   Microsoft.PowerShell     Available
  2 test            win7.xie.com    Opened   Microsoft.PowerShell     Available


PS C:\Users\Administrator> Enter-PSSession -id 2
[win7.xie.com]: PS C:\Users\administrator\Documents> hostname;whoami
WIN7
xie\administrator
[win7.xie.com]: PS C:\Users\administrator\Documents>
[win7.xie.com]: PS C:\Users\administrator\Documents> Exit-PsSession
PS C:\Users\Administrator>
```

如果是工作组环境运行，或客户端未加入域，则需要在客户端执行此命令：

```
Set-Item wsman:\localhost\Client\TrustedHosts -value *
```

```
PS C:\Windows\system32> Enter-PSSession -computer win2008 -Credential administrator
Enter-PSSession : 连接到远程服务器失败，错误消息如下：WinRM 客户端无法处理该请求。如果身份验证方案与 Kerberos 不同，或
者客户端计算机未加入到域中，则必须使用 HTTPS 传输或者必须将目标计算机添加到 TrustedHosts 配置设置。 使用 winrm.cmd 配
置 TrustedHosts。请注意，TrustedHosts 列表中的计算机可能未经过身份验证。 通过运行以下命令可获得有关此内容的更多信息：wi
nrm help config。 有关详细信息，请参阅 about_Remote_Troubleshooting 帮助主题。
所在位置 行:1 字符: 16
+ Enter-PSSession <<<<  -computer win2008 -Credential administrator
    + CategoryInfo          : InvalidArgument: (win2008:String) [Enter-PSSession], PSRemotingTransportException
    + FullyQualifiedErrorId : CreateRemoteRunspaceFailed

PS C:\Windows\system32> Set-Item wsman:\localhost\Client\TrustedHosts -value *

WinRM 安全配置。
此命令修改 WinRM 客户端的 TrustedHosts 列表。TrustedHosts
列表中的计算机可能不会经过身份验证。该客户端可能会向这些计算机发送凭据信息。是否确实要修改此列表?
[Y] 是(Y)  [N] 否(N)  [S] 挂起(S)  [?] 帮助 (默认值为“Y”): y
PS C:\Windows\system32> Enter-PSSession -computer win2008 -Credential administrator
[win2008]: PS C:\Users\Administrator\Documents> whoami;hostname
win2008\administrator
WIN2008
```

使用Python远程连接WinRM

首先，需要服务端WinRM配置如下，在cmd窗口执行以下命令：

```
#为winrm service 配置auth:
winrm set winrm/config/service/auth @{Basic="true"}
#为winrm service 配置加密方式为允许非加密:
winrm set winrm/config/service @{AllowUnencrypted="true"}
```

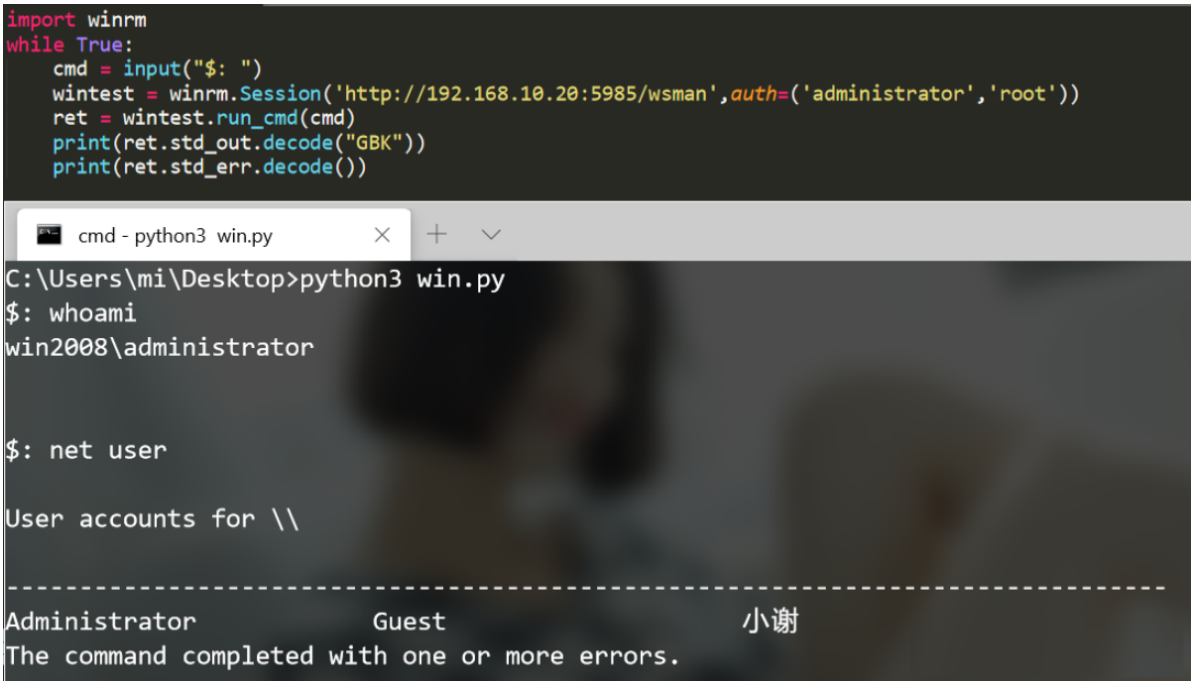
```
C:\Users\Administrator>winrm set winrm/config/service/auth @{Basic="true"}
Auth
    Basic = true
    Kerberos = true
    Negotiate = true
    Certificate = false
    CredSSP = false
    CbtHardeningLevel = Relaxed


C:\Users\Administrator>winrm set winrm/config/service @{AllowUnencrypted="true"}

Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 15
    EnumerationTimeoutms = 60000
    MaxConnections = 25
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = true
    Auth
        Basic = true
        Kerberos = true
        Negotiate = true
        Certificate = false
        CredSSP = false
        CbtHardeningLevel = Relaxed
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    IPv4Filter = *
    IPv6Filter = *
    EnableCompatibilityHttpListener = false
    EnableCompatibilityHttpsListener = false
    CertificateThumbprint
```

以下是python脚本(安装的包名：pywinrm)

```
import winrm
while True:
  cmd = input("$: ")
  wintest = winrm.Session('http://192.168.10.20:5985/wsman',auth=
('administrator','root'))
  ret = wintest.run_cmd(cmd)
  print(ret.std_out.decode("GBK"))
  print(ret.std_err.decode())
```



注意事项：如何支持其他用户远程连接

这里需要注意的是，通过WinRM远程连接也是受到LocalAccountTokenFilterPolicy的值影响的。

在 Windows Vista 以后的操作系统中，LocalAccountTokenFilterPolicy 的默认值为0，这种情况下内置账户 administrator 进行远程连接时会直接得到具有管理员凭证的令牌，而其他账号包括管理员组内账号远程连接时会提示权限不足。而在域环境中，只要是域管理员都可以建立具备管理员权限的远程连接。

如果要允许本地管理员组的其他用户登录WinRM，需要修改注册表设置。

命令修改 LocalAccountTokenFilterPolicy 的值=1即可

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

WinRM其他命令

```
winrm
winrm help auth
winrm help uris How to construct resource URIs.
winrm help aliases Abbreviations for URIs.
winrm help config Configuring WinRM client and service settings.
winrm help certmapping Configuring client certificate access.
winrm help remoting How to access remote machines.
winrm help auth Providing credentials for remote access.
winrm help input Providing input to create, set, and invoke.
winrm help switches Other switches such as formatting, options, etc.
winrm help proxy Providing proxy information.
```