PowerShell Remoting：从Linux到Windows

大闸蟹清蒸最好吃 / 2018-11-11 08:55:00 / 浏览数 3350 技术文章 技术文章 顶(0) 踩(0)

PowerShell Remoting：从Linux到Windows

原文链接：https://blog.quickbreach.io/ps-remote-from-linux-to-windows/

0x00 前言

声明：我个人努力确保本文提供信息的准确度，但我是其实是一个菜鸟。

如果能做到以下几点，我们就能从Linux系统远程PS到Windows：

1、在后渗透测试中对某个目标发起NTLM身份认证；

2、重启WinRM服务；

3、使用支持NTLM的PowerShell Docker镜像从Linux远程PS到Window。

0x01 背景

我有次偶然发现，在渗透测试中我可以将PowerShell远程执行作为远程代码执行的主要方法。PowerShell是Windows的一个内置功能，由于客户端检测功能越来越强，因此
不幸的是，由于PowerShell Core的Linux分支支持的身份验证机制有限，因此想从我的Kali Linux系统远程连接到目标并不是一件容易的事。

PowerShell远程操作需要使用Kerberos相互身份验证过程，这意味着客户端计算机和目标计算机必须都连接到域环境中。
如果我们还没有搞定某个域节点用来执行远程命令，那么这种情况可能会给我们的测试人员带来各种问题。
幸运的是，我们可以选择将自己添加为目标配置中的`TrustedHost`，这样我们就能执行NTLM身份验证，而不用去处理Kerberos，因此无需通过域环境中的系统进行连接。

现在唯一的问题在于，适用于Linux的PowerShell核心（撰写本文时为PowerShell 6.1.0）并未支持NTLM身份验证。
这个问题并非无法解决，因为我们总是可以从Windows VM执行PowerShell远程操作。
幸运的是，一些研究人员找到了在Centos上使用PowerShell进行NTLM身份验证的一种方法，因此我将他们的发现整合到一个简单的PowerShell
Docker镜像中：quickbreach/powershell-ntlm。

0x02 如何使用PowerShell从Linux远程处理Windows

本节将逐步介绍如何从Linux客户端建立到Windows系统的远程PowerShell会话。 假设我们对目标PC具有管理员级别的访问权限（通过RDP、载荷等）。

1、在目标上启用PowerShell远程功能。

```
Enable-PSRemoting –Force
```

2、获取目标系统上当前的`TrustedHosts`列表，以供后续参考。

```
Get-Item WSMan:\localhost\Client\TrustedHosts
```

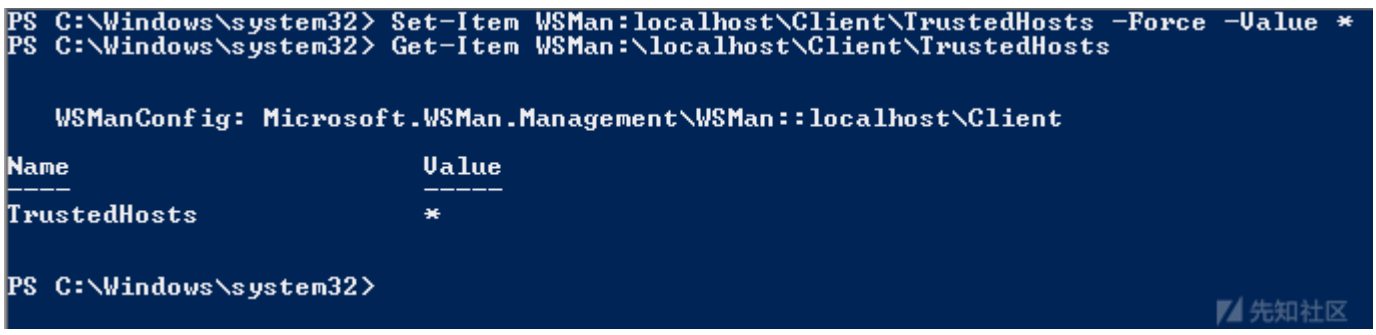
3、将自己添加为目标上的`TrustedHost`。为了在`Enter-PSSession`配置阶段使用NTLM身份验证，我们需要执行这个步骤，NTLM是从Linux通过PowerShell远程连接到
要完成此任务，请运行以下任意一条命令：

使用通配符，允许所有计算机在对此主机进行身份验证时使用NTLM协议：

```
Set-Item WSMan:\localhost\Client\TrustedHosts -Force -Value *
```

或者更加具体，只将我们的IP添加到NTLM身份验证的允许列表中。

```
Set-Item WSMan:\localhost\Client\TrustedHosts -Force -Concatenate -Value 192.168.10.100
```



4、设置并重新启动WinRM服务，以应用我们所做的更改。

```
Set-Service WinRM -StartMode Automatic

Restart-Service -Force WinRM
```

5、进入PowerShell-NTLM Docker镜像实例。 如下示例命令还会将本地某个目录加载到docker镜像内的/mnt路径中（该目录中包含一些PowerShell脚本）。

```
docker run -it -v /pathTo/PowerShellModules:/mnt quickbreach/powershell-ntlm
```

6、现在就是我们一直在期待的时刻：使用以下命令进入远程PowerShell会话。请注意，我们必须指定-Authentication类型：

```
# Grab the creds we will be logging in with
$creds = Get-Credential

# Launch the session
# Important: you MUST state the  authentication type as Negotiate
Enter-PSSession -ComputerName (Target-IP) -Authentication Negotiate -Credential $creds

# i.e.

Enter-PSSession -ComputerName 10.20.30.190 -Authentication Negotiate -Credential $creds
```

我们也可以以类似的方式使用Invoke-Command功能：

```
Invoke-Command -ComputerName 10.20.30.190 -Authentication Negotiate -Credential $creds -ScriptBlock {Get-HotFix}
```

```
quickbreach@kali:$ docker run -it quickbreach/powershell-ntlm
PowerShell 6.1.0
Copyright (c) Microsoft Corporation. All rights reserved.

https://aka.ms/pscore6-docs
Type 'help' to get help.

PS /> $creds = Get-Credential -UserName quickbreach

PowerShell credential request
Enter your credentials.
Password for user quickbreach: ***********

PS /> Enter-PSSession -Credential $creds -ComputerName 10.20.30.190 -Authentication Negotiate
[10.20.30.190]: PS C:\Users\quickbreach\Documents> [System.Environment]::OSVersion.Version

Major  Minor  Build  Revision
-----  -----  -----  --------
6      1      7601   65536


[10.20.30.190]: PS C:\Users\quickbreach\Documents>
```


0x03 清理现场

如果将我们的节点添加为TrustedHost之前，已经有其他人占了坑，那么我们需要更换IP，然后运行以下命令：

```
$newvalue = ((Get-ChildItem WSMan:\localhost\Client\TrustedHosts).Value).Replace(",192.168.10.100","")
Set-Item WSMan:\localhost\Client\TrustedHosts -Force -Value $newvalue
```

或者，我们可以移除所有的TrustedHost，使我们成为唯一的一个成员：

```
Clear-Item WSMan:\localhost\Client\TrustedHosts
```

重新启动WinRM服务以应用更改（请注意，这将使我们断开与Enter-PSSession的连接）。

```
Restart-Service WinRM
```

0x04 参考资料

This Reddit Thread
PowerShell Remoting Cheatsheet

点击收藏 | 1 关注 | 1

上一篇：http代理攻击威胁分析 下一篇：如何在math.js中进行远程代码...

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板