WinRM远程执行命令横向移动

WinRM介绍

WinRM（Windows远程管理）是Microsoft 在Windows中对WS-Management的实现，它使系统可以跨通用网络访问或交换管理信息。利用脚本对象或内置的命令行工具，WinRM可以与可能具有基板管理控制器（BMC）的任何远程计算机一起使用，以获取数据。也可以获取基于Windows的计算机（包括WinRM）。 WinRM默认端口5985（HTTP端口）或5986（HTTPS端口），若配置了WINRM远程服务，当我们拿到一个管理员账户时，可以使用远程连接进行命令执行操作

winrm通过HTTP（5985）或HTTPS SOAP（5986）端口来进行通信

winrs.exe

Winrs.exe 是一个内置的命令行工具,它允许远程命令的执行在WinRm的适当的有资格的用户

```
winrs -r:http://127.0.0.1:5985 -u:administrator -p:Admin@123 "whoami"
winrs -r:http://127.0.0.1:5985 -u:机器名\用户名 -p:xxxxx "ipconfig"
winrs -r:https://127.0.0.1:5985 -u:机器名\用户名 -p:xxxxx "ipconfig"
winrs -r:http://127.0.0.1:5985 -u:机器名\用户名 -p:xxxxx cmd
winrs -r:https://127.0.0.1:5985 -u:机器名\用户名 -p:xxxxx cmd
Invoke-Command -ComputerName TARGET -ScriptBlock { dir c:\ }
Invoke-Command -ComputerName TARGET -Credential 域名\用户名 -command {Get-Culture}
Invoke-Command -ComputerName TARGET -Credential 域名\用户名 -ScriptBlock {Get-
Culture}
```

1、执行

```
winrs -r:http://192.168.41.147:5985 -u:administrator -p:Admin@123 "whoami"
```

提示:如果出现

```
Winrs error:WinRM 客户端无法处理该请求。 可以在下列条件下将默认身份验证与 IP 地址结合使用:
传输为 HTTPS 或目标位于 TrustedHosts 列表中，并且提供了显式凭据。 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。 有关如何设置
TrustedHosts 的详细信息，请运行以下命令
```

输入出现 请 输入 `winrm set winrm/config/Client @{TrustedHosts="*"}`