如何优雅的穿透linux内网

四叶草@星光

lcx or nc

```
% nc
This is nc from the netcat-openbsd package. An alternative nc is available
in the netcat-traditional package.
usage: nc [-46bCDdhjklnrStUuvZz] [-I length] [-i interval] [-O length]
          [-P proxy_username] [-p source_port] [-q seconds] [-s source]
          [-T toskeyword] [-V rtable] [-w timeout] [-X proxy_protocol]
          [-x proxy_address[:port]] [destination] [port]
```

```
-v: version
-h1: host1
-h2: host2
-p1: port1
-p2: port2
-log: log the data
-m: the action method for this tool
1: listen on PORT1 and connect to HOST2:PORT2
2: listen on PORT1 and PORT2
3: connect to HOST1:PORT1 and HOST2:PORT2
Let me exit...all overd
```

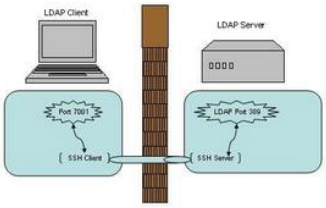
只能实现单个端口的穿透，
nmap无法使用

各种扫描器都无法使用

还能不能好好的渗透了?

ssh本地端口转发

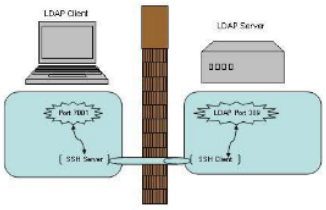
ssh -L <local port>:<remote host>:<remote port>
<SSH hostname>



ssh远程端口转发

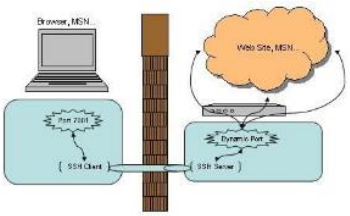
ssh -R <local port>:<remote host>:<remote port>
<SSH hostname>

传说中的反弹



SSH动态端口转发

ssh -D <local port> <SSH Server>



xsocks

git clone https://github.com/5loyd/xsocks

```
xsocks -l 8085 -u root -p 123456
xsocks -t -p1 8085 -p2 8086
xsocks -r 192.168.1.10:8085 -u root -p 123456
xsocks -s 192.168.1.11:8085 -r 192.168.1.10:8086
```

reGeorg

git clone https://github.com/sensepost/reGeorg

支持php

支持aspx

支持jsp

本地创建socks5服务

$ python reGeorgSocksProxy.py -p 8080 -u http://upload.sensepost.net:8080/tunnel/tunnel.jsp

浏览器插件，连接socks5服务

proxychains-ng

git clone https://github.com/rofl0r/prox
ychains-ng