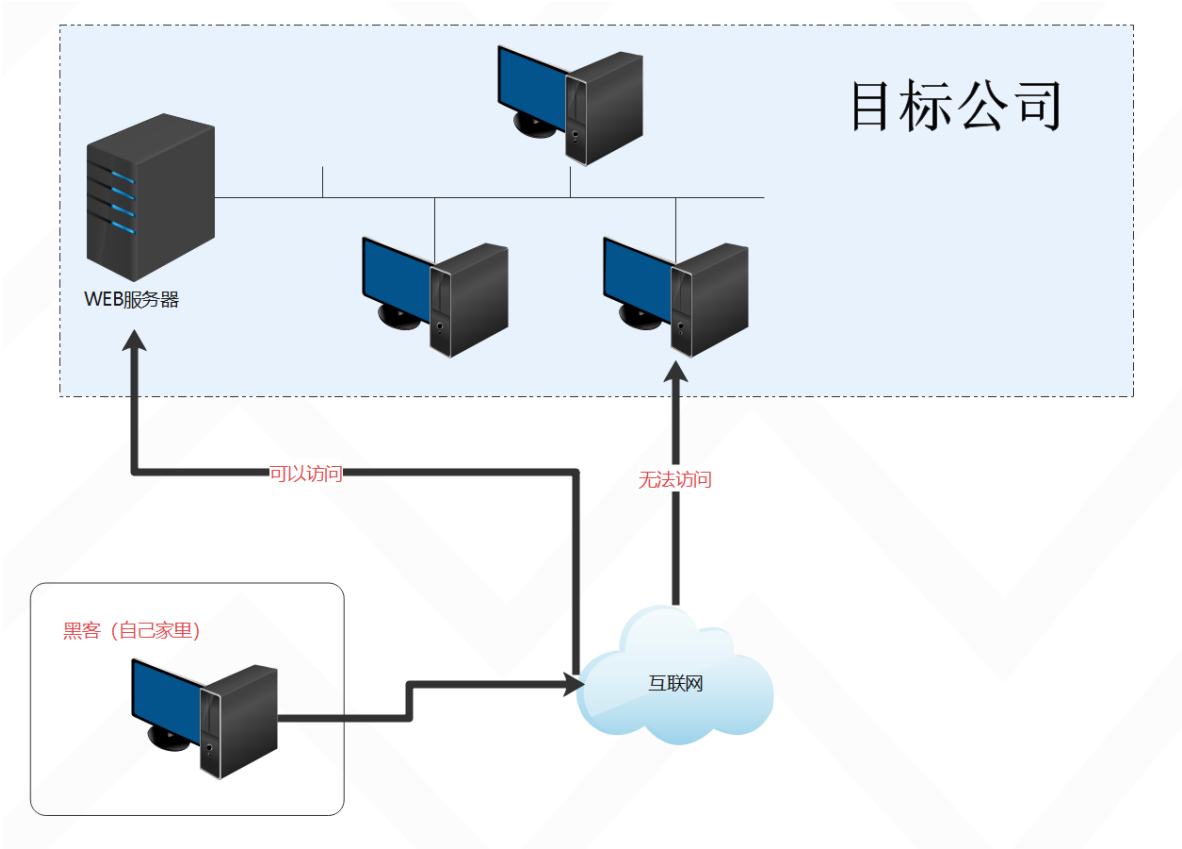
内网代理介绍

内网代理介绍

内网资产扫描这种场景一般是进行内网渗透才需要的代理技术，如果你不打内网一般是不需要这种技术的，内网代理技术一般也是采用http或者socks代理



针对以上的情况我们需要如何对内网进行扫描呢?

1、直接使用web服务进行扫描（这种方式请看内网渗透）

2、做代理让web服务成为代理机器

针对于内网的机器要考虑是用代理隧道还是使用端口转发

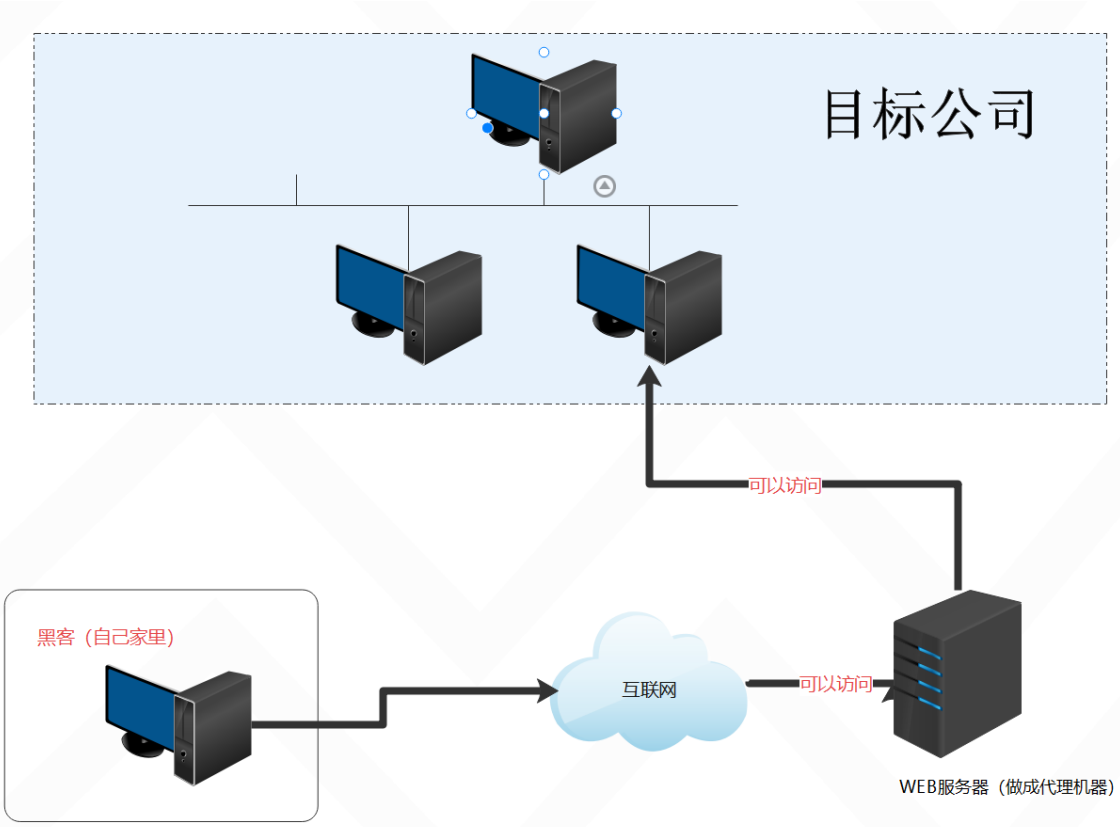
在这种情况需要用什么工具走代理呢?

1、扫描工具

2、浏览器

3、burp

使用代理一般是用http代理或者socks代理代理后的拓扑如下

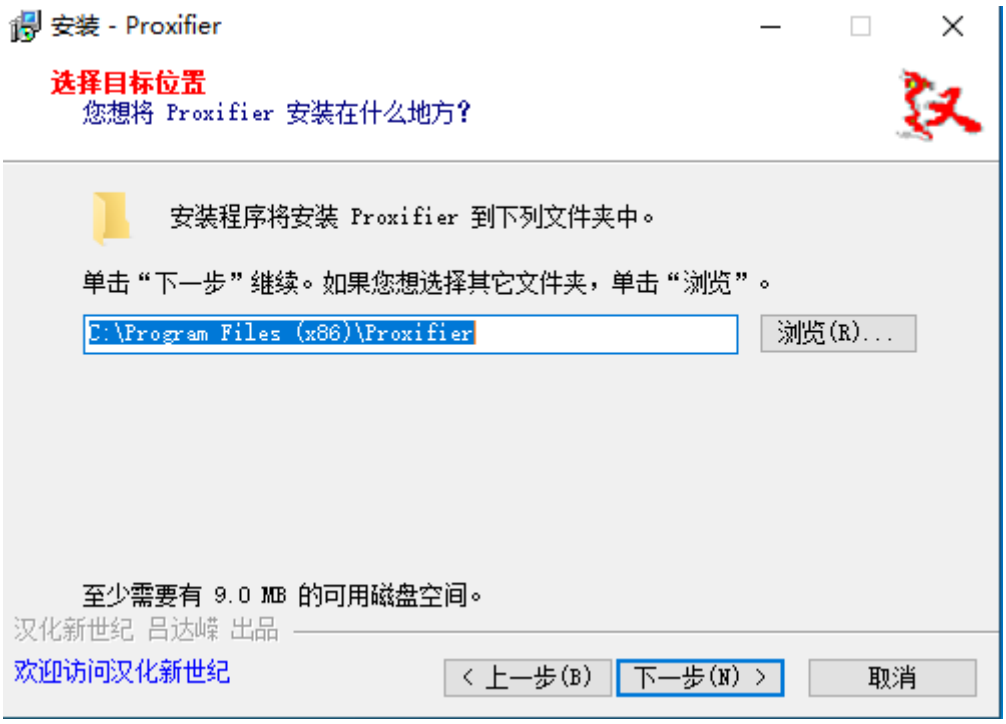


代理连接工具

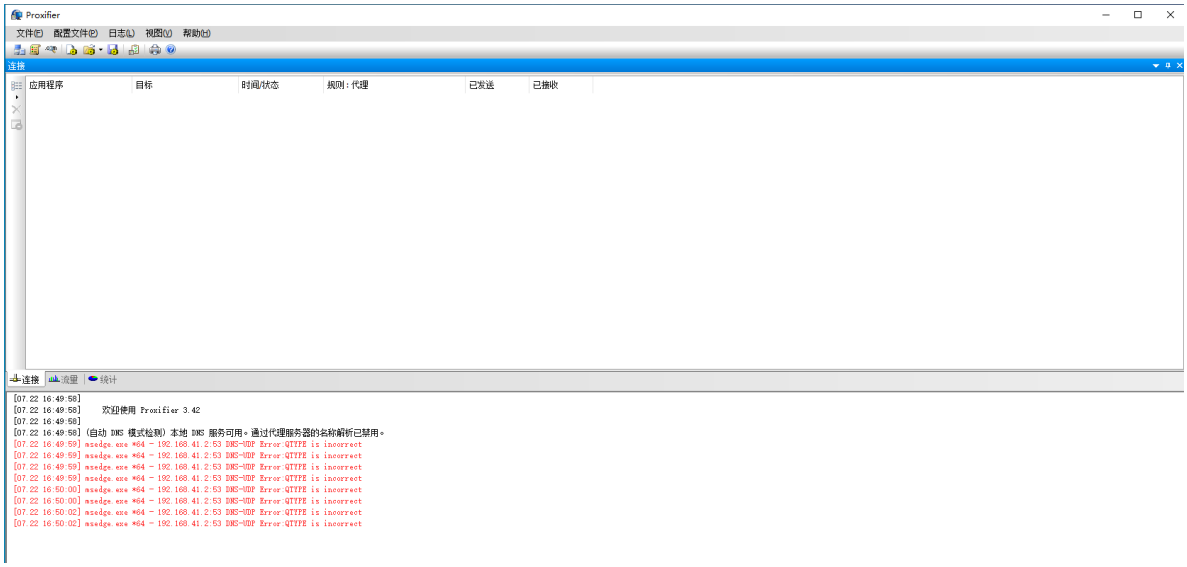
windows工具

如果是windows是proxyifile工具

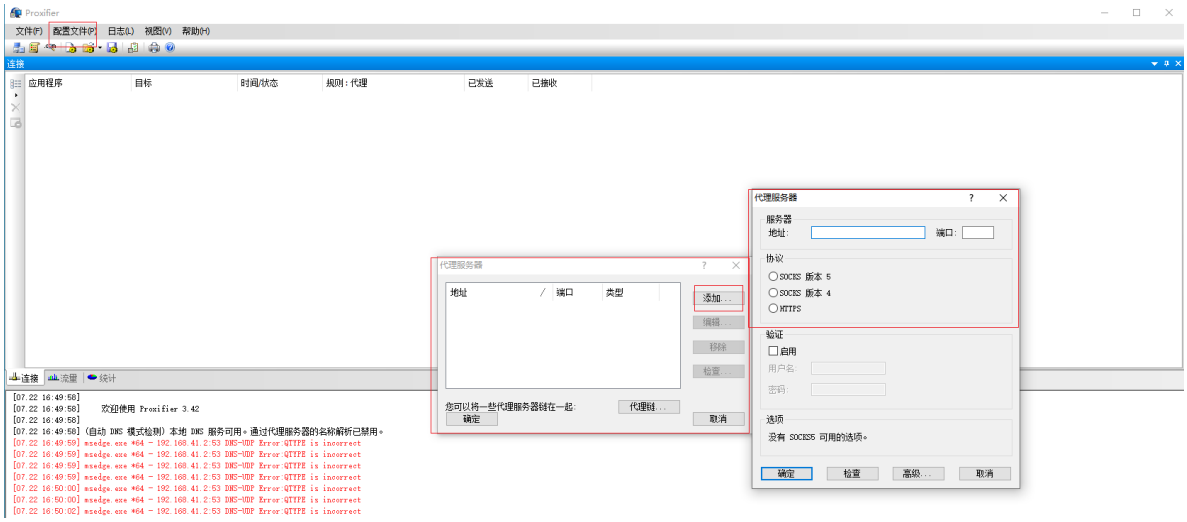
1、运行软件然后点进进行一步一步安装



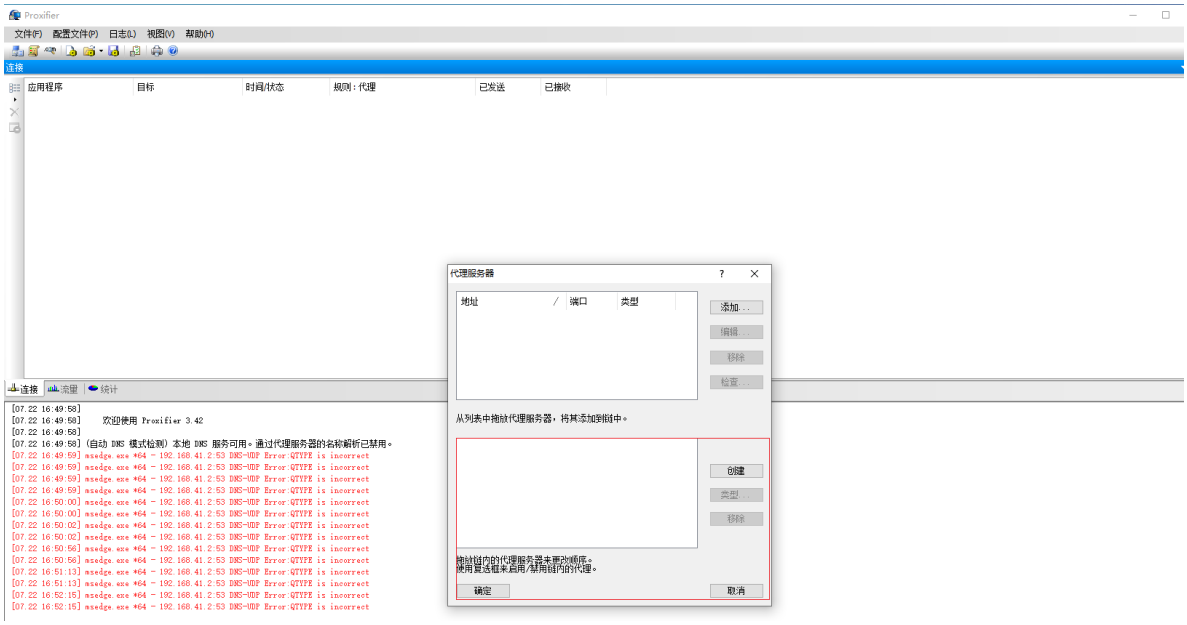
2、安装完成运行软件



3、打开代理服务器配置，可以看到支持http和socks代理



4、该工具支持代理链，代理链可以支持多级代理



linux工具

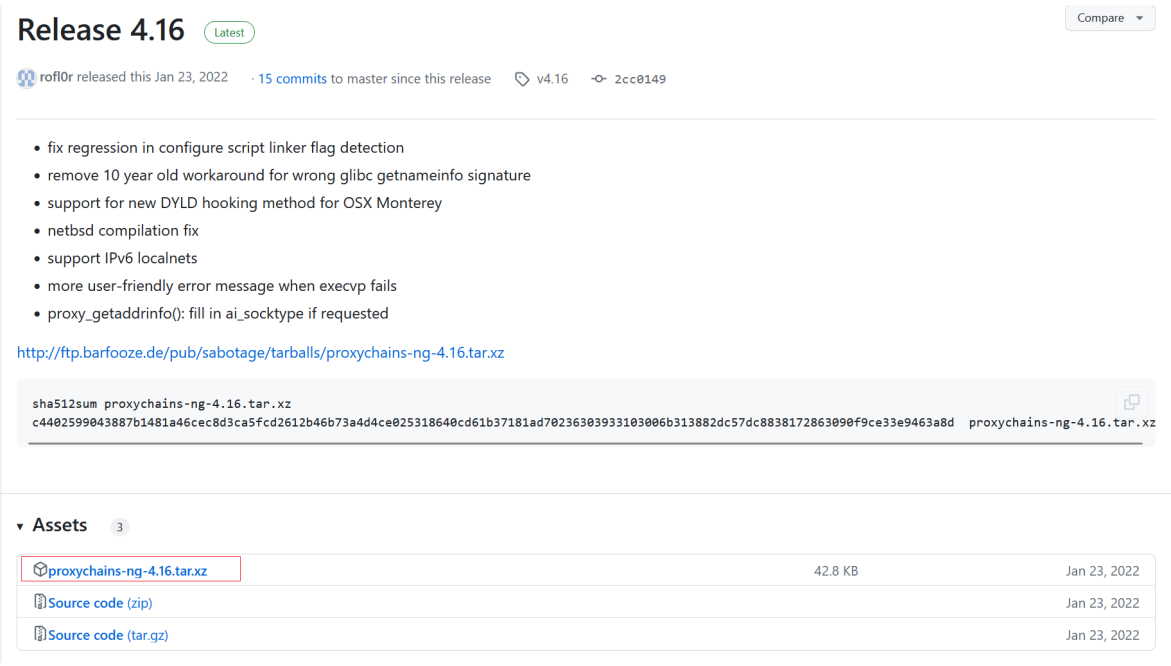
linux工具下一般使用命令行工具proxychains

```
┌──(root㉿kali)-[~/Desktop]
└─# proxychains

Usage:  proxychains -q -f config_file program_name [arguments]
        -q makes proxychains quiet - this overrides the config setting
        -f allows one to manually specify a configfile to use
        for example : proxychains telnet somehost.com
More help in README file
```

1、该工具在kali中自带我们看一下安装步骤

1、下载Proxychains源码，可以从GitHub上下载，或者直接从官网下载https://github.com/rofl0r/proxychains-ng，我已经下载好了



2、解压文件然后进行安装

```
tar zxvf proxychains-ng-4.16.tar.gz
cd proxychains-ng-4.16
./configure
make
make install
```

```
[root@localhost proxychains-ng-4.16]# proxychains4

Usage:  proxychains4 -q -f config_file program_name [arguments]
        -q makes proxychains quiet - this overrides the config setting
        -f allows one to manually specify a configfile to use
        for example : proxychains telnet somehost.com
More help in README file
```

3、安装完成之后，需要修改配置文件/usr/local/etc/proxychains.conf，将其中的代理服务器修改为你的代理服务器

```
1. socks4  127.0.0.1 9050
2. socks5  127.0.0.1 1080
```

4、修改完成之后，可以使用proxychains命令来使用代理服务器，示例

```
proxychains curl www.google.com
```