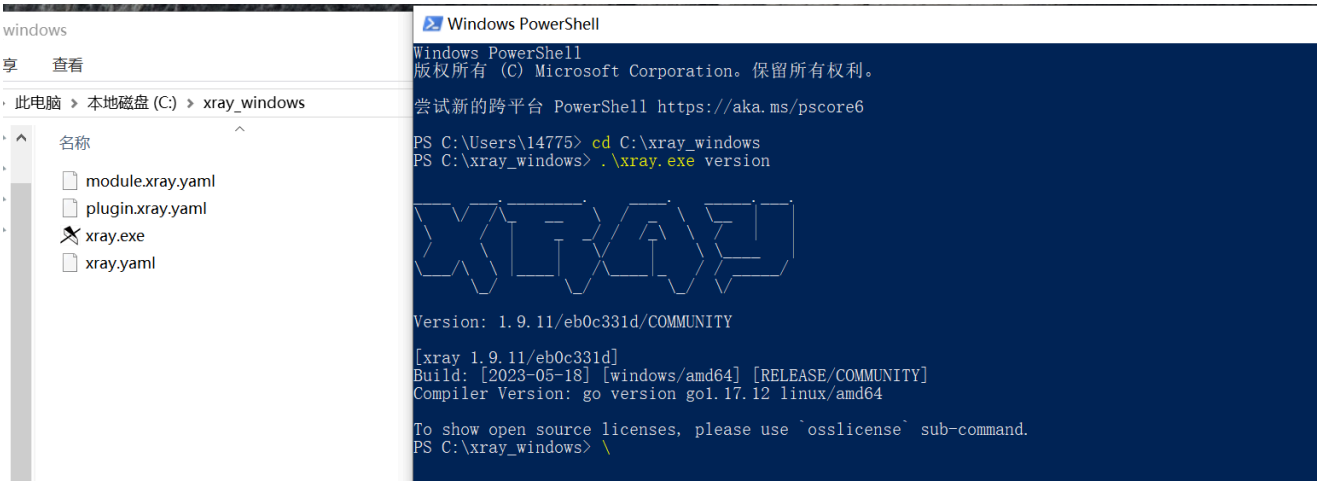
xray扫描器

1.快速开始

打开powershell，进入xray.exe 所在的文件夹，运行

```
.\xray.exe version
```

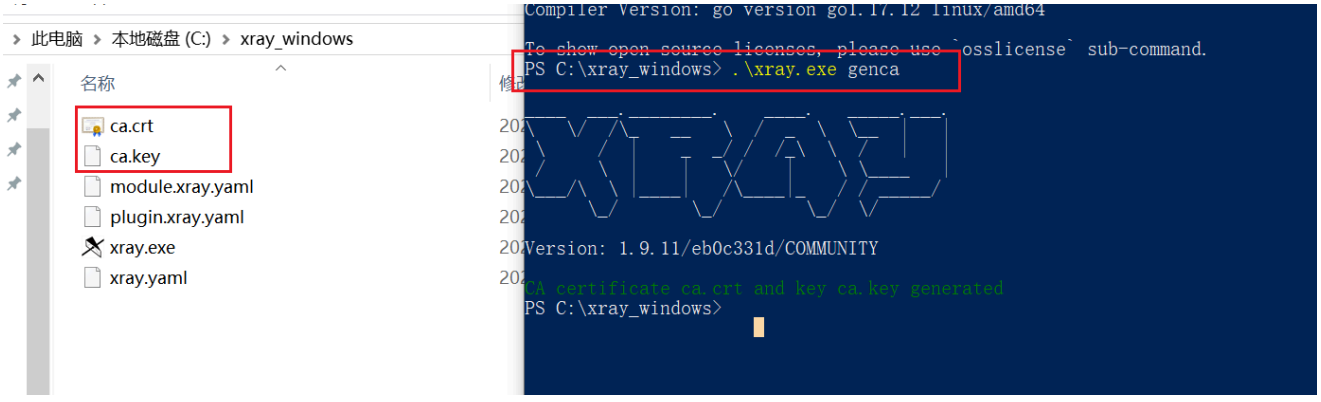


2.安装ca证书

运行

```
.\xray.exe genca
```

在xray_windows文件夹下生成，ca.crt和ca.key两个文件



将ca.crt文件安装进入火狐浏览器中的ca证书

3.被动扫描

a.新建火狐代理127.0.0.1：7777

b.运行命令使用被动扫描

```
.\xray.exe webscan --listen 127.0.0.1:7777 --html-output xray-testphp.html
```

4.主动扫描

```
.\xray.exe webscan --basic-crawler http://192.168.219.136 --html-output
xray-crawler-pikachu.html
```

5.对目标进行扫描

```
./xray servicescan --target 127.0.0.1:8009 --html-output xxx.html //对单一目
标进行扫描


./xray servicescan --target-file 1.file --html-output xxx.html//批量进行扫描

/*1.file格式为
ip1:端口1
ip2:端口2
...
每一行一个目标*/
```

6.配置文件的使用

详见xray文件夹下的config.yaml

hydra爆破

常用命令

-l LOGIN 指定破解的用户名称，对特定用户破解。

-L FILE 从文件中加载用户名进行破解。

-p PASS小写p指定密码破解，少用，一般是采用密码字典。

-P FILE 大写字母P，指定密码字典。

-e nsr 可选选项，n：空密码试探，s：使用指定用户和密码试探，r：指定密码与用户名相反。

-C FILE 使用冒号分割格式，例如“登录名:密码”来代替-L/-P参数。

-t TASKS 同时运行的连接的线程数，每一台主机默认为16。

-M FILE 指定服务器目标列表文件一行一条

-w TIME 设置最大超时的时间，单位秒，默认是30s。

-o FILE 指定结果输出文件。

-f 在使用-M参数以后，找到第一对登录名或者密码的时候中止破解。

-v / -V 显示详细过程。

-R 继续从上一次进度接着破解。

-S 采用SSL链接。

-s PORT 可通过这个参数指定非默认端口。

-U　服务模块使用细节

-h　更多的命令行选项（完整的帮助）

server 目标服务器名称或者IP（使用这个或-M选项）

service 指定服务名，支持的服务和协议：telnet ftp pop3[-ntlm] imap[-ntlm] smb smbnt http[s]-{head|get} http-{get|post}-form http-proxy cisco cisco-enable vnc ldap2 ldap3 mssql mysql oracle-listener postgres nntp socks5 rexec rlogin pcnfs snmp rsh cvs svn icq sapr3 ssh2 smtp-auth[-ntlm] pcanywhere teamspeak sip vmauthd firebird ncp afp等等

OPT　一些服务模块支持额外的输入（-U用于模块的帮助）

实例演示

（1）windows密码破解

SMB服务很稳定，跑得快，不容易ban掉ip

hydra -l 用户名 -p 密码 smb://ip –v

或者hydra -l 用户名 -p 密码 smb ip –v //-v 显示爆破详细信息

（2）MySQL密码破解

数据库一般会提供一个默认的帐户，SQL Server的sa用户，MySQL的root用户，Oracle的System用户等。

假如我们现在破解mysql数据库

hydra -L user.txt -P pass.txt ip mysql

hydra -L user.txt -P pass.txt mysql://目标IP:mysql端口号

（3）ssh密码破解

hydra -l 用户名 -P 密码字典 -t 线程 -vV -e nsr ip ssh

hydra -l 用户名 -P 密码字典 -t 线程 -o save.log -vV ip ssh

（4）破解ftp

hydra ip ftp -l 用户名 -P 密码字典 -t 线程数(默认16) –vV

如果你发现目标ftp并不是在21端口，而是在其他端口上，可以使用-s参数指定正确的端口，其他服务同样如此。

（5）破解rdp

如果不支持rdp模块，尝试升级一下 apt install hydra

hydra ip rdp -l administrator -P pass.txt –V

（6）post方式提交 破解web登录

hydra -l admin -P small.txt 域名/ip -s 端口 http-post-form "/Pass-09/index.php:username=^USER^&password=^PASS^&Login=Login:F=密码错误" -v

F表示错误信息，根据实际情况填写