Usage: sslyze.py [options] target1.com target2.com:443 etc...

参数:

--version 显示程序的版本号和退出

-h, --help 显示此帮助消息并退出

--xml\_out=XML\_FILE 将扫描结果作为XML文档的文件xml\_file。如果xml\_file设置为“-”，XML输出将被打印到标准输出。

--targets\_in=TARGETS\_IN

从文件读取目标targets\_in扫描列表。它应该包含一个主机：每行端口。

--timeout=TIMEOUT 将用于每个套接字连接的超时值设置为目标服务器（S）。默认是5S。 --nb\_retries=NB\_RETRIES

设置在整个扫描启动的所有网络连接的重试次数。当扫描一个特定的服务器时，增加这个值，如果你得到了很多的超时/连接错误。12月增加这个值会增加扫描的速度；结果可能会返回连接错误。默认是4连接尝试。

--https\_tunnel=HTTPS\_TUNNEL

隧道的交通到目标服务器（S）通过HTTP连接代理。http\_tunnel应代理的网址：http：/ /用户：密码@主机：端口/”。代理需要认证，只有基本的认证阳离子支持。

--starttls=STARTTLS 执行STARTTLS握手连接到目标服务器时（S）。将应该是：[ 'smtp '、' XMPP，“xmpp\_server”、“POP3”，“FTP”、“IMAP”、“LDAP”、“RDP”、“Postgres '，'自动' ]。“自动”它们会导致sslyze推断协议（FTP，IMAP，等）从提供的端口数，为每个目标服务器。

--xmpp\_to=XMPP\_TO 用于STARTTLS XMPP可选设置。xmpp\_to应该主机放在“到”的XMPP流属性。默认的服务器的主机名。

--sni=SNI 使用服务器名称指示指定要连接的主机名。只会影响TLS 1 +连接。 --quiet 隐藏脚本标准输出。只会影响脚本的输出如果xml\_out设置。 --regular 定期的HTTPS扫描；快捷——SSL版本2——SSLv3

--tlsv1 --tlsv1\_1 --tlsv1\_2 --reneg --resum

--certinfo=basic --http\_get --hide\_rejected\_ciphers

--compression --heartbleed

客户端证书支持:

--cert=CERT 客户端证书链文件名。该证书必须是PEM格式，必须要从主体的客户端证书，其次是中间的CA证书，如适用。

--key=KEY 客户端私钥文件名。

--keyform=KEYFORM 客户端私钥格式。明镜或PEM（默认）。

--pass=KEYPASS 客户端的私钥密码。

PluginOpenSSLCipherSuites:

扫描服务器（S）支持OpenSSL密码套件。

--sslv2 列出 SSL 2.0 OpenSSL 服务器支持的密码套件（S）。

--sslv3 列出 SSL 3.0 OpenSSL服务器支持的密码套件（S）。

--tlsv1 列出 TLS 1.0 OpenSSL 服务器支持的密码套件（S）。

--tlsv1\_1 列出 TLS 1.1 OpenSSL服务器支持的密码套件（S）。

--tlsv1\_2 列出TLS 1.2 OpenSSL 服务器支持的密码套件（S）。

--http\_get 选项为每个密码套件，发送一个HTTP GET请求完成SSL握手后返回的HTTP状态码。

--hide\_rejected\_ciphers

选项-隐藏被服务器拒绝的（通常是长的）密码列表列表列表。

PluginHeartbleed:

--heartbleed 测试服务器（S）对OpenSSL的Heartbleed漏洞（实验）。

PluginCertInfo:

--certinfo=CERTINFO

验证服务器证书的有效性（S）（S）对各种信任存储区，用于支持OCSP装订检查，并打印相关领域的证书。certinfo应该是'基本'或'Full'。

--ca\_file=CA\_FILE 当地权威证书文件（PEM格式），验证服务器证书的有效性（S）（S）对。

PluginChromeSha1Deprecation:

--chrome\_sha1 确定服务器将由谷歌浏览器的SHA-1贬低计划受影响。看到http://googleonlinesecurity.blogspot.com/2014/09 / gradually-sunsetting-sha-1.html更多信息

PluginHSTS:

--hsts 检查支持HTTP严格传输安全（HSTS）通过收集任何严格的交通安全领域在HTTP响应的服务器发送回（S）。.

PluginCompression:

--compression 测试服务器（S）为zlib压缩支持。

PluginSessionRenegotiation:

--reneg 测试服务器（S）为客户端发起的谈判和重新谈判支持安全。

PluginSessionResumption:

通过对目标服务器的SSL会话恢复功能。

--resum 测试服务器（S）使用会话ID和TLS会话票会话恢复支持（RFC 5077）。

--resum\_rate 100届恢复执行与服务器（S），以便估计会话恢复率。