\_

\_\_\_ \_\_\_| |\_\_\_ \_\_\_ \_\_ \_ \_ \_\_

/ \_\_/ \_\_| / \_\_|/ \_\_/ \_` | '\_ \

\\_\_ \\_\_ \ \\_\_ \ (\_| (\_| | | | |

|\_\_\_/\_\_\_/\_|\_\_\_/\\_\_\_\\_\_,\_|\_| |\_|

主要探测基于ssl的服务，如https。Sslscan是一款探测目标服务器所支持的SSL加密算法工具。

1.11.7-static

OpenSSL 1.0.2i-dev xx XXX xxxx

命令:

sslscan [Options] [host:port | host]

选项:

--targets=<file> 一个包含主机列表检查的文件。

主机可以提供与端口（主机：端口）

--ipv4 只使用IPv4

--ipv6 只使用IPv6

--show-certificate 显示完整的证书信息

--no-check-certificate 不要警告弱证书算法或密钥

--show-client-cas 显示受信任的CA TLS客户端认证

--show-ciphers 显示支持的客户端密码

--show-cipher-ids Show cipher ids

--show-times 以毫秒为单位显示handhake倍

--ssl2 只检查SSL版本2密码

--ssl3 只检查以及密码

--tls10 只检查tlsv1.0密码

--tls11 只检查TLSv1.1密码

--tls12 只检查TLSv1.2密码

--tlsall 只检查TLS密码（所有版本）

--ocsp OCSP响应从服务器请求

--pk=<file> 一个包含私钥或PKCS 12文件#包含密钥/证书对文件 --pkpass=<password> 私钥的#或PKCS 12文件的密码

--certs=<file> A file containing PEM/ASN1 formatted client certificates

--no-ciphersuites 不检查支持密码套件

--no-fallback 不检查scsv TLS回退

--no-renegotiation 不检查TLS协商

--no-compression 不检查TLS压缩（犯罪）

--no-heartbleed 不检查的OpenSSLHeartbleed (CVE-2014-0160)

--starttls-ftp 将设置FTP

--starttls-imap 将设置IMAP

--starttls-irc 将安装IRC

--starttls-pop3 将安装POP3

--starttls-smtp 设置SMTP STARTTLS

--starttls-xmpp 将设置XMPP

--starttls-psql 将安装PostgreSQL

--xmpp-server 使用服务器到服务器的通信握手

--http 测试一个HTTP连接

--rdp 在开始扫描发送RDP序言

--bugs 启用SSL实现错误处理方法

--timeout=<sec> 设置套接字超时。默认是3S

--sleep=<msec> 连接请求之间的暂停。默认是禁用的

--xml=<file> 结果输出到一个XML文件<文件>可以，这意味着它

--version 显示程序版本

--verbose 显示详细的输出

--no-cipher-details 禁用EC曲线名称和EDH / RSA密钥长度的输出

--no-colour 禁用彩色输出

--help 显示您现在正在阅读的帮助文本

实例:

sslscan 127.0.0.1

sslscan [::1]