格式: golismero.py [-h] [--help] [-f FILE] [--config FILE] [--user-config FILE] [-p NAME]

[--ui-mode MODE] [-v] [-q] [--color] [--no-color] [--audit-name NAME]

[-db DATABASE] [-nd] [-i FILENAME] [-ni] [-o FILENAME] [-no] [--full]

[--brief] [--allow-subdomains] [--forbid-subdomains] [--parent] [-np]

[-r DEPTH] [--follow-redirects] [--no-follow-redirects] [--follow-first]

[--no-follow-first] [--max-connections MAX\_CONNECTIONS] [-l MAX\_LINKS]

[-pu USER] [-pp PASS] [-pa ADDRESS] [-pn PORT] [--cookie COOKIE]

[--user-agent USER\_AGENT] [--cookie-file FILE] [--persistent-cache]

[--volatile-cache] [-a PLUGIN:KEY=VALUE] [-e PLUGIN] [-d PLUGIN]

[--max-concurrent N] [--plugin-timeout N] [--plugins-folder PATH]

COMMAND [TARGET [TARGET ...]]

可用的命令:

扫描:

对给定的目标执行漏洞扫描。随意进出从其他工具的结果，并写一份报告。跟随的论点是域名，IP地址或网页。

RESCAN:

和扫描相同，但以前运行的测试重复。如果数据库是新的，这个命令是相同的扫描。

PROFILES:

显示可用配置配置文件的列表。此命令不需要参数。

PLUGINS:

显示可用插件列表。此命令不需要参数。

INFO:

在一个给定的插件上显示详细的信息。跟随的论点是插件入侵检测系统。你可以使用glob方式通配符。

REPORT:

从早期的扫描写一份报告。此命令不需要参数。要指定输出文件，使用“O”开关。

IMPORT:

从其他工具的导入结果和可选的写一个报告，但不扫描目标。此命令不需要参数。指定输入文件使用-我开关。

DUMP:

转储数据库从早期扫描sql格式。这个命令不需要争论。要指定输出文件，使用“O”开关。

LOAD:

负载从早期扫描sql格式的数据库。这个命令以没有争吵。要指定输入文件，使用“I”开关。

UPDATE:

Update GoLismero的最新版本。需要安装Git可在路径。此命令不需要参数。

实例:

扫描一个网站，并显示屏幕上的结果：

golismero.py scan http://www.example.com

nmap扫描抓取结果，所有主机发现写HTML报告：

golismero.py scan -i nmap\_output.xml -o report.html

抓住结果OpenVAS和它们显示在屏幕上，但不扫描任何东西：

golismero.py import -i openvas\_output.xml

显示所有可用的配置配置文件的列表：

golismero.py profiles

显示所有可用插件的列表：

golismero.py plugins

显示所有bruteforcer插件信息：

golismero.py info brute\_\*

从先前的扫描转储数据库：

golismero.py dump -db example.db -o dump.sql

位置参数：

COMMAND 要执行的操作

TARGET 零或更多的参数，意义取决于命令

可选参数:

-h 显示此帮助消息并退出

--help 显示此帮助消息并退出

主要选项:

-f FILE, --file FILE 从一个简单的文本文件加载目标列表

--config FILE 全局配置文件

--user-config FILE 每个用户配置文件

-p NAME, --profile NAME

简介使用

--ui-mode MODE 用户界面模式

-v, --verbose 增加输出冗长

-q, --quiet 抑制的文本输出

--color 在控制台输出中使用颜色

--no-color 抑制控制台输出中的颜色

审计选项:

--audit-name NAME 自定义审计名称

-db DATABASE, --audit-db DATABASE

指定一个数据库文件名

-nd, --no-db 不要将结果存储在数据库中

-i FILENAME, --input FILENAME

在审核前阅读外部工具的结果

-ni, --no-input 不要从外部工具读取结果

报告选项：

-o FILENAME, --output FILENAME

写的审计结果这个文件（使用为stdout）

-no, --no-output 不要输出结果

--full 产生全面的详细报告

--brief 报告只有亮点

网络选项:

--allow-subdomains 包括子域在目标范围内

--forbid-subdomains 不包括在目标范围的子域

--parent 包括目标范围中的父文件夹

-np, --no-parent 不包括目标范围中的父文件夹

-r DEPTH, --depth DEPTH

最大爬行的深度（使用“无限”不限）

--follow-redirects 跟随重定向

--no-follow-redirects

不要跟随重定向

--follow-first 始终遵循目标网址本身的重定向

--no-follow-first 不要把一个目标网址重定向作为一个特殊的情况

--max-connections MAX\_CONNECTIONS

每个主机的并发连接的最大数量

-l MAX\_LINKS, --max-links MAX\_LINKS

分析的最大链接数（0 =无穷大）

-pu USER, --proxy-user USER

HTTP代理服务器的用户名

-pp PASS, --proxy-pass PASS

HTTP代理密码

-pa ADDRESS, --proxy-addr ADDRESS

HTTP代理地址

-pn PORT, --proxy-port PORT

HTTP代理服务器的端口号

--cookie COOKIE 设置请求的饼干

--user-agent USER\_AGENT

设置一个自定义的用户代理或“随机”值

--cookie-file FILE 从文件中加载一个

--persistent-cache 使用一个持久的网络缓存[默认]

--volatile-cache 使用一个易用的网络缓存

插件选项:

-a PLUGIN:KEY=VALUE, --plugin-arg PLUGIN:KEY=VALUE

通过一个参数到一个插件

-e PLUGIN, --enable-plugin PLUGIN

使一个插件

-d PLUGIN, --disable-plugin PLUGIN

禁用插件

--max-concurrent N 同时运行的最大数量的插件

--plugin-timeout N 超时在秒为一个插件的执行

--plugins-folder PATH

自定义插件的位置