Teemo：域名信息收集及爆破工具

bit4 / 2017-02-20 06:25:00 / 浏览数 3495 安全工具 工具 顶(0) 踩(0)

项目主页

https://github.com/bit4woo/Teemo

简介

域名收集及枚举工具

提莫(teemo)是个侦察兵，域名的收集如同渗透和漏洞挖掘的侦察，故命名为提莫（Teemo）！

该工具主要有三大模块：

利用搜索引擎

- Baidu
- Google（需要代理，可能被Block）
- bing（使用 cn.bing.com）
- Yahoo
- Yandex（可能被Block，替代方案 xml.yandex.com）
- Dogpile
- Exaland（可能被Block）
- Ask（需要代理）
- GoogleCSE（需要API）

利用第三方站点

- Alex
- Chaxunla（图形验证码）
- Netcraft
- DNSDumpster
- Virustotal
- ThreatCrowd
- CrtSearch
- PassiveDNS
- GooglCT
- ILink
- Sitedossier
- Threatminer
- Pgpsearch

利用枚举

- Subbrute：https://github.com/TheRook/subbrute

基本使用

运行环境：python 2.7.*

- 查看帮助：

```
python teemo.py -h
```

- 枚举指定域名（会使用搜索引擎和第三方站点模块）：

```
python teemo.py -d example.com
```

- 使用代理地址（默认会使用config.py中的设置）：

```
python teemo.py -d example.com -x "http://127.0.0.1:9999"
```

- 启用枚举模式：

```
python teemo.py -b -d example.com
```

- 将结果保存到指定文件(默认会根据config.py中的设置保存到以域名命名的文件中)：

```
python teemo.py -d example.com -o result.txt
```

- 收集域名并扫描指定端口：

```
python teemo.py -d example.com -p 80,443
```

参考

参考以下优秀的工具修改而来

- https://github.com/ring04h/wydomain
- https://github.com/aboul3la/Sublist3r
- https://github.com/laramies/theHarvester

Thanks for their sharing.

优缺点

为什么要修改，相对以上优秀工具有什么优缺点？

优点：

1. 使用的搜索引擎和第三方站点更全面，经过实际测试，发现收集的域名会更多。
2. 添加了代理的支持，像google，ask等可以通过指定代理地址去访问，个人使用google较多，所以这个对我很重要。
3. 使用搜索引擎的模块，会收集邮箱地址。

缺点：

1. 初始版本，单线程，速度慢，bug很多。但后续会持续更新改进。

To Do

- 随机请求参数，减小被block几率
- 接入打码平台
- 域名有效性判断，端口扫描并记录–json格式（■domain:{ip■127.0.0.1■ports:{80,443},cdn:{yes or no,具体是谁}}■domain）
- 泛解析，dns轮询相关
- 优化config.py
- 模糊匹配，例如包含"qq"的所有域名，比如qqimg.com
- 搜索引擎模块，使用google hacking 搜索
- 优化正则表达式，去除以"-"开头的非法域名

change log

v0.1

- 添加多线程支持。
- 添加www.so.com 360搜索引擎
- 修复ask页面参数不正确问题
- 优化代理参数设置

相关思维导图

上一篇：WebCruiserWVS354特别版 下一篇：保护内网安全之提高Windows ...

1. 0 条回复
   - 动动手指，沙发就是你的了！

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板