魔方安全
CUBESEC TECH

信息收集&主机侦察

讲师：陈晟

CONTENTS

目录

信息收集作用

- 了解组织安全架构
- 缩小攻击范围
- 描绘网络拓扑
- 建立脆弱点数据库

CONTENTS

目录

信息收集要求

- **全面**：做到对目标所有的业务面和非业务面的存在点进行全面的信息收集。
- **准确**：对于收集到的信息尤其是重要信息要再三确认其信息的准确性。
- **时效性**：对于收集到的信息要注意信息产生的时间和收集到的时间，是否具有时间差，时间差能否接受，如果存在失效的信息要及时清除。
- **清晰**：对于收集到的信息要做到逻辑清晰，能清楚地分辨出各个收集到的信息之间的逻辑关系和资产之间的相对位置，对于总体目标要有清晰的资产逻辑和业务逻辑认识。
- **拓扑**：对于收集到的信息要以这些信息为起点做拓扑的信息收集。

CONTENTS

目录

信息收集分类
（基于ATT&CK侦察战术框架）

- MITRE是一个由美国政府资助的研究机构，它在1958年脱离MIT，并且参与了许多商业和最高机密项目，甚至一些美国军方的威胁建模项目。

- 2013年，MITRE推出了ATT&CK模型，该模型根据实际观测数据对对抗行为进行描述和分类。ATT&CK将已知的攻击行为转化为结构化列表，将这些已知行为归纳为战术和技术，并通过若干矩阵和结构化威胁信息表达(STIX)、指标信息的可信自动化交换（TAXII）来表述。

- ATT&CK将已知的攻击行为转化为结构化列表，将这些已知行为归纳为战术和技术，并通过若干矩阵和结构化威胁信息表达(STIX)、指标信息的可信自动化交换（TAXII）来表述。

- ATT&CK模型共包括14个模块，依次为：侦察、资源开发、初始访问、执行、持久化、权限提升、防御绕过、凭证访问、发现、横向移动、收集、命令与控制（C2）、数据窃取、影响

信息收集分类（基于ATT&CK侦察战术框架）

https://attack.mitre.org/

信息收集分类（基于ATT&CK侦察战术框架）

Active Scanning
主动扫描

主动扫描是攻击者通过网络流量探测受害者基础设施的扫描，而不是其他不涉及直接交互的侦察形式。

Gather Victim Host Information
收集受害主机信息

有关主机的信息可能包括各种详细信息，包括管理数据（例如：名称、分配的 IP、功能等）以及有关其配置的细节（例如：操作系统、语言等）。

Gather Victim Identity Information
收集受害者身份信息

有关身份的信息可能包括各种详细信息，包括个人数据（例如：员工姓名、电子邮件地址等）以及凭证等敏感详细信息。

信息收集分类（基于ATT&CK侦察战术框架）

Gather Victim Network Information 收集受害者网络信息

有关网络的信息可能包括各种细节，包括管理数据（例如：IP 范围、域名等）以及有关其拓扑和操作的细节。

Gather Victim Org Information 收集受害者组织信息

有关组织的信息可能包括各种详细信息，包括分部/部门的名称、业务运营的细节以及关键员工的角色和职责。

Phishing for Information 信息网络钓鱼

信息网络钓鱼是企图诱骗目标泄露信息，通常是凭据或其他可操作的信息。信息网络钓鱼不同于网络钓鱼，因为其目的是从受害者那里收集数据，而不是执行恶意代码。

网络钓鱼可以有针对性，称为鱼叉式网络钓鱼。在鱼叉式网络钓鱼中，特定的个人、公司或行业将成为对手的目标。更一般地说，对手可以进行无针对性的网络钓鱼，例如大规模凭证收集活动。

信息收集分类（基于ATT&CK侦察战术框架）

Search Closed Sources 搜索封闭源

可以从信誉良好的私人来源和数据库购买有关受害者的信息，例如付费订阅技术/威胁情报数据。 也可能从信誉较差的来源购买信息，例如暗网或网络犯罪黑市。

Search Open Websites/Domains 搜索开放的网站/域

有关受害者的信息可以在各种在线网站上找到，例如社交媒体、新网站，或托管有关业务运营信息（例如雇用或请求/奖励合同）的网站

Search Open Technical Databases 搜索开放技术数据库

有关受害者的信息可能在在线数据库和存储库中可用，例如域/证书的注册以及从流量和/或扫描中收集的网络数据/工件的公共集合。

CONTENTS

目录

信息收集工具&方法—子域名

- Amass: https://github.com/OWASP/Amass
- Subfinder: https://github.com/projectdis
- OneForAll: https://github.com/shmilylty/OneForAll
- ksubdomain: https://github.com/knownsec/ksubdomain
- subDomainsBrute: https://github.com/lijiejie/subDomainsBrute
- Sonar: https://omnisint.io/
- 查子域(在线) : https://chaziyu.com/
- 在线：https://phpinfo.me/domain

信息收集工具&方法—子域名：OneForAll

- Example:
- python3 oneforall.py version
- python3 oneforall.py check
- python3 oneforall.py --target example.com run
- python3 oneforall.py --targets ./domains.txt run
- python3 oneforall.py --target example.com --alive False run
- python3 oneforall.py --target example.com --brute False run
- python3 oneforall.py --target example.com --port medium run
- python3 oneforall.py --target example.com --fmt csv run
- python3 oneforall.py --target example.com --dns False run
- python3 oneforall.py --target example.com --req False run
- python3 oneforall.py --target example.com --takeover False run
- python3 oneforall.py --target example.com --show True run

- Note:
- --port small/medium/large See details in ./config/setting.py(default small)
- --fmt csv/json (result format)
- --path Result path (default None, automatically generated)

```
PS D:\魔方\方班讲课\信息收集工具\子域名\OneForAll> python3 .\oneforall.py --target gzhu.edu.cn run

OneForAll is a powerful subdomain integration tool

                ___                 _ _
 ___ ___ ___ ___|  _|___ ___ ___ ___| | | {v0.4.5 #dev}
| . |   | -_|  _|  _| . |  _| -_| .'| | |
|___|_|_|___|_| |_| |___|_| |___|__,|_|_| git.io/fjHT1

OneForAll is under development, please update before each use!

[*] Starting OneForAll @ 2023-01-01 17:37:57

17:37:57,184 [INFOR] utils:532 - Checking dependent environment
17:37:57,184 [INFOR] utils:544 - Checking network environment
17:37:58,789 [INFOR] utils:555 - Checking for the latest version
17:37:59,362 [INFOR] utils:579 - The current version v0.4.5 is already the latest version
17:37:59,365 [INFOR] oneforall:241 - Start running OneForAll
17:37:59,367 [INFOR] oneforall:246 - Got 1 domains
17:37:59,406 [INFOR] wildcard:108 - Detecting gzhu.edu.cn use wildcard dns record or not
17:37:59,658 [ALERT] wildcard:123 - The domain gzhu.edu.cn disables wildcard
17:37:59,659 [INFOR] collect:44 - Start collecting subdomains of gzhu.edu.cn
17:37:59,882 [INFOR] module:63 - NSECCheck module took 0.1 seconds found 0 subdomains
17:37:59,889 [INFOR] module:63 - QueryMX module took 0.0 seconds found 0 subdomains
17:37:59,898 [INFOR] module:63 - AXFRCheck module took 0.1 seconds found 0 subdomains
17:37:59,918 [INFOR] module:63 - QuerySOA module took 0.1 seconds found 1 subdomains
17:37:59,920 [INFOR] module:63 - QueryNS module took 0.1 seconds found 2 subdomains
17:37:59,924 [INFOR] module:63 - QuerySPF module took 0.1 seconds found 0 subdomains
17:37:59,928 [INFOR] module:63 - QueryTXT module took 0.1 seconds found 0 subdomains
17:38:00,163 [INFOR] module:63 - CSPCheck module took 0.3 seconds found 0 subdomains
17:38:00,168 [INFOR] module:63 - CertInfo module took 0.4 seconds found 1 subdomains
```

信息收集工具&方法—子域名：ksubdomain

- 使用内置字典爆破
- ksubdomain -d seebug.org

- 使用字典爆破域名
- ksubdomain -d seebug.org -f subdomains.dict

- 字典里都是域名，可使用验证模式
- ksubdomain -f dns.txt -verify

- 爆破三级域名
- ksubdomain -d seebug.org -l 2

- 通过管道爆破
- echo "seebug.org"|ksubdomain

- 通过管道验证域名
- echo "paper.seebug.org"|ksubdomain -verify

- 仅使用网络API接口获取域名
- ksubdomain -d seebug.org -api

- 完整模式,先使用网络API，在此基础使用内置字典进行爆破
- ksubdomain -d seebug.org -full

```
PS D:\魔方\方班讲课\信息收集工具\子域名\ksubdomain> .\ksubdomain.exe -d gzhu.edu.cn

 _  __   _____        _          _                      _
| |/ /  / ____|      | |        | |                    (_)
| ' /  | (___   _   _| |__   __| | ___  _ __ ___   __ _ _ _ __
|  <    \___ \| | | | '_ \ / _| |/ _ \| '_   _ \ / _  | | '_ \
| . \   ____) | |_| | |_) | (_| | (_) | | | | | | (_| | | | | |
|_|\_\ |_____/ \__,_|_.__/ \__,_|\___/|_| |_| |_|\__,_|_|_| |_|

[INFO] Current Version: 0.7
[INFO] Npcap version 1.10, based on libpcap version 1.9.1
..
[INFO] Use Device: \Device\NPF_{11B2595E-883C-40CD-83AB-94703DA69C4B}
[INFO] Use IP:192.168.0.107
[INFO] Local Mac:60:f2:62:17:d2:16
[INFO] GateWay Mac:c8:5b:a0:ed:7a:ad
[INFO] 加载内置字典
[INFO] 检测域名:[gzhu.edu.cn]
[INFO] 设置rate:10000pps
[INFO] DNS:[223.5.5.5 223.6.6.6 180.76.76.76 119.29.29.29 182.254.116.116 114.114.114.115]
zsjy.gzhu.edu.cn => CNAME zsjy-gzhu-edu-cn.cname.saaswaf.com => CNAME gzhu.cache.saaswaf.com => CNAME gdedu-ipv6.cache.saaswaf.com => 58.205.213.52
lib.gzhu.edu.cn => 202.192.41.6
gz.gzhu.edu.cn => 59.41.252.239
zbb.gzhu.edu.cn => CNAME zbb-gzhu-edu-cn.cname.saaswaf.com => CNAME gzhu.cache.saaswaf.com => CNAME gdedu-ipv6.cache.saaswaf.com => 58.205.213.52
Success:4 Sent:2545 Recved:2005 Faild:0
```

信息收集工具&方法—旁站

- 在线: http://stool.chinaz.com/same
- 在线: https://site.ip138.com
- 在线：https://chapangzhan.com/
- 在线：https://c.webscan.cc/

信息收集工具&方法—真实ip

- 全球ping: https://www.wepcc.com
- dns检测: https://tools.ipip.net/dns.php
- Xcdn: https://github.com/3xp10it/xcdn
- 在线: https://ipchaxun.com
- 站长之家：https://ping.chinaz.com/

信息收集工具&方法—Whois信息

- 站长之家: http://whois.chinaz.com
- Bugscaner: http://whois.bugscaner.com
- 国外在线: https://bgp.he.net
- whois：https://www.whois.com/whois/

信息收集工具&方法—端口+C段

- Nmap: https://nmap.org
- Fscan: https://github.com/shadow1ng/fscan
- Txportmap: https://github.com/4dogs-cn/TXPortMap
- Masscan: https://github.com/robertdav

信息收集工具&方法—Nmap主要基本参数

参　数	说　明
-sT	TCP connect()扫描，这种方式会在目标主机的日志中记录大批连接请求和错误信息。
-sS	半开扫描，很少有系统能把它记入系统日志。不过，需要Root权限。
-sF -sN	秘密FIN数据包扫描、Xmas Tree、Null扫描模式
-sP	ping扫描，Nmap在扫描端口时，默认都会使用ping扫描，只有主机存活，Nmap才会继续扫描。
-sU	UDP扫描，但UDP扫描是不可靠的
-sA	这项高级的扫描方法通常用来穿过防火墙的规则集
-sV	探测端口服务版本
-Pn	扫描之前不需要用ping命令，有些防火墙禁止ping命令。可以使用此选项进行扫描
-v	显示扫描过程，推荐使用
-h	帮助选项，是最清楚的帮助文档
-p	指定端口，如“1-65535、1433、135、22、80”等
-O	启用远程操作系统检测，存在误报
-A	全面系统检测、启用脚本检测、扫描等
-oN/-oX/-oG	将报告写入文件，分别是正常、XML、grepable 三种格式
-T4	针对TCP端口禁止动态扫描延迟超过10ms
-iL	读取主机列表，例如，“-iL C:\ip.txt”

信息收集工具&方法—Nmap NSE

NSE脚本功能详解：https://nmap.org/nsedoc/scripts/

模块	作用
auth	负责处理鉴权证书（绕开鉴权）的脚本
broadcast	在局域网内探查更多服务开启状况，如dhcp/dns/sqlserver等服务
brute	提供暴力破解方式，针对常见的应用如http/snmp等
default	使用-sC或-A选项扫描时候默认的脚本，提供基本脚本扫描能力
discovery	对网络进行更多的信息，如SMB枚举、SNMP查询等
dos	用于进行拒绝服务攻击
exploit	利用已知的漏洞入侵系统
external	利用第三方的数据库或资源，例如进行whois解析
fuzzer	模糊测试的脚本，发送异常的包到目标机，探测出潜在漏洞 intrusive
malware	探测目标机是否感染了病毒、开启了后门等信息
safe	此类与intrusive相反，属于安全性脚本
version	负责增强服务与版本扫描（Version Detection）功能的脚本
vuln	负责检查目标机是否有常见的漏洞（Vulnerability），如是否有MS08_067

- 使用模块进行扫描：
  - nmap --script=brute 127.0.0.1
- 使用模块中的子模块扫描：
  - nmap --script=telnet-brute 127.0.0.1
  - nmap --script telnet-brute, http-slowloris 127.0.0.1

信息收集工具&方法—APP

- 小蓝本: https://www.xiaolanben.com/pc
- 七麦: https://www.qimai.cn
- AppStore: https://www.apple.com/app-store
- 禅大师： https://app.chandashi.com/

信息收集工具&方法—公众号

- 微信直接搜索
- 搜狗: https://weixin.sogou.com
- 小蓝本: https://www.xiaolanben.com/pc

信息收集工具&方法—小程序

- 微信直接搜索
- 小蓝本: https://www.xiaolanben.com/pc

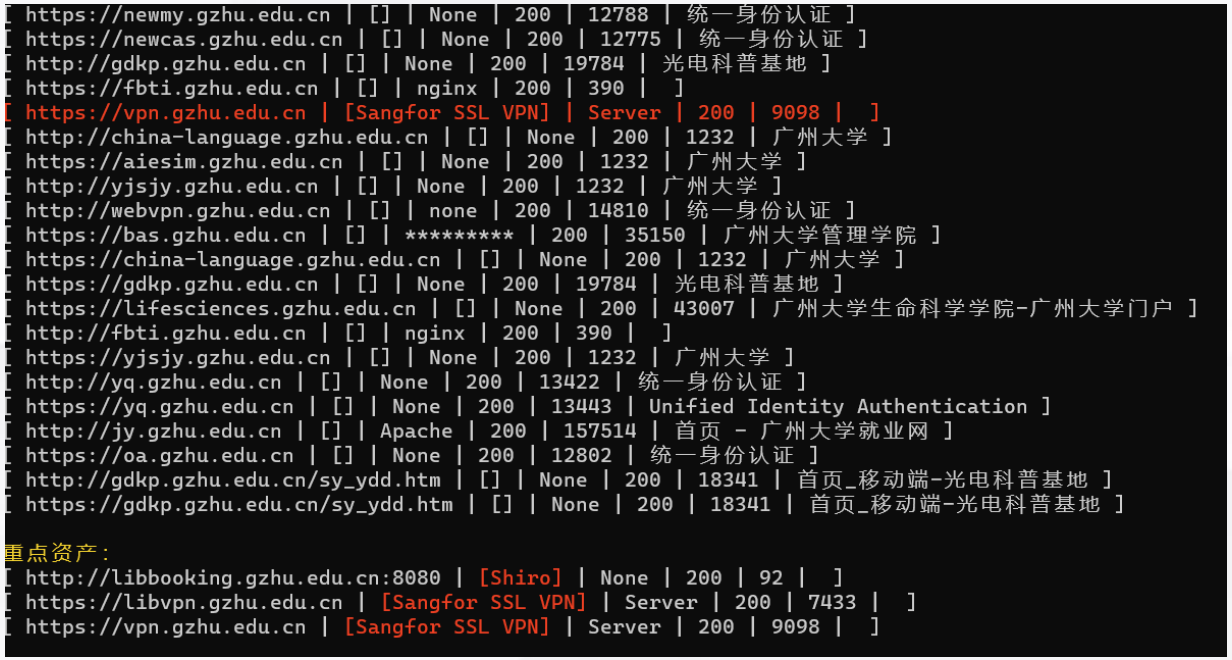
信息收集工具&方法—指纹识别

- 火狐插件: Wappalyzer
- 云悉: http://www.yunsee.cn
- EHole: https://github.com/EdgeSecurityTeam/EHole
- TideFinger: https://github.com/TideSec/TideFinger
- ObserverWard:https://github.com/0x727/ObserverWard_0x727

信息收集工具&方法—EHole

Usage: Ehole [-f|-l] [parameter]

Options:
  -f string
        Fofa searches for assets , supports IP and IP segments。(192.168.1.1 | 192.168.1.0/24)
  -fall string
        fofa batch search IP
  -fofa string
        Fofa searches for assets ,All fofa search syntax is supported.
        Ps：“”must be preceded by"\".(ip=\"192.168.1.0/24\" | domain=\"test.com\")
  -ftime string
        fofa timeout (default "10")
  -h   this help
  -json string
        out json
  -l string
        Probe based on local file
  -log string
        Log file name (default "server.log")
  -t string
        thread (default "100")
  -u string
        Target URL



信息收集工具&方法—Title识别

- HTTPX: https://github.com/projectdiscovery/httpx
- WebBatchRequest: https://github.com/ScriptKid-Beta/WebBatchRequest
- Bscan: https://github.com/broken5/bscan

信息收集工具&方法—HTTPX

Probes	Default check	Probes	Default check
URL	true	IP	true
Title	true	CNAME	true
Status Code	true	Raw HTTP	false
Content Length	true	HTTP2	false
TLS Certificate	true	HTTP Pipeline	false
CSP Header	true	Virtual host	false
Line Count	true	Word Count	true
Location Header	true	CDN	false
Web Server	true	Paths	false
Web Socket	true	Ports	false
Response Time	true	Request Method	true
Favicon Hash	false	Probe Status	false
Body Hash	true	Header Hash	true
Redirect chain	false	URL Scheme	true
JARM Hash	false	ASN	false

```
PS D:\魔方\方班讲课\信息收集工具\title识别\httpx> .\httpx.exe -l .\target.txt -sc -title

    __    __  __       _  __
   / /_  / /_/ /_____ | |/ /
  / __ \/ __/ __/ __ \|   /
 / / / / /_/ /_/ /_/ /   |
/_/ /_/\__/\__/ .___/_/|_|
             /_/              v1.2.5

                projectdiscovery.io

Use with caution. You are responsible for your actions.
Developers assume no liability and are not responsible for any misuse or damage.
https://lib.gzhu.edu.cn [200] [正在打开网页......]
https://yq.gzhu.edu.cn [302] [302 Found]
https://libbooking.gzhu.edu.cn [200] [Information Commons]
http://fbti.gzhu.edu.cn [301] [301 Moved Permanently]
http://yjsyxt.gzhu.edu.cn [302] [302 Found]
http://pay.gzhu.edu.cn [200] [缴费大厅]
http://dservice.gzhu.edu.cn [301] [301 Moved Permanently]
http://ffs.gzhu.edu.cn [301] [301 Moved Permanently]
http://newmy.gzhu.edu.cn [301] []
http://messagewx.gzhu.edu.cn [301] [301 Moved Permanently]
https://bas.gzhu.edu.cn [200] [广州大学管理学院]
https://rcep.gzhu.edu.cn [200] [广州大学教育政策研究中心]
https://health.gzhu.edu.cn [200] [广州大学健康管理交叉科学研究中心]
http://libmobile.gzhu.edu.cn:8080 [200] []
https://gpsjxcgsb.gzhu.edu.cn [200] [认证驱动产教协同:给排水科学与工程卓越人才培养的改革与实践]
http://ky.gzhu.edu.cn [302] []
http://wxtb.gzhu.edu.cn [200] [Welcome to nginx!]
```

信息收集工具&方法—JS接口

- URLFinder: https://github.com/pingc0y/URLFinder
- JSFinder: https://github.com/Threezh1/JSFinder
- LinkFinder: https://github.com/GerbenJavado/LinkFinder
- Packer-Fuzzer: https://github.com/rtcatc/Packer-Fuzzer (webpack)

信息收集工具&方法—JSFinder

- optional arguments:
- -h, --help show this help message and exit
- -u URL, --url URL The website
- -c COOKIE, --cookie COOKIE
- The website cookie
- -f FILE, --file FILE The file contains url or js
- -ou OUTPUTURL, --outputurl OUTPUTURL
- Output file name.
- -os OUTPUTSUBDOMAIN, --outputsubdomain OUTPUTSUBDOMAIN
- Output file name.
- -j, --js Find in js file
- -d, --deep Deep find

```
PS D:\魔方\方班讲课\信息收集工具\JS接口\JSFinder> python3 .\JSFinder.py -u http://www.gzhu.edu.cn/ -d
ALL Find 117 links
url:http://www.gzhu.edu.cn/gzdxxnhc.htm
Remaining 117 | Find 2 URL in http://www.gzhu.edu.cn/gzdxxnhc.htm
url:http://www.gzhu.edu.cn/javascript:showimagecloseu1();
Remaining 116 | Find 0 URL in http://www.gzhu.edu.cn/javascript:showimagecloseu1();
url:http://www.gzhu.edu.cn/index.htm
Remaining 115 | Find 19 URL in http://www.gzhu.edu.cn/index.htm
url:http://english.gzhu.edu.cn/
Remaining 114 | Find 19 URL in http://english.gzhu.edu.cn/
url:http://news.gzhu.edu.cn/index.htm
Remaining 113 | Find 6 URL in http://news.gzhu.edu.cn/index.htm
url:http://www.gzhu.edu.cn/xxgk/xxjj.htm
Remaining 112 | Find 18 URL in http://www.gzhu.edu.cn/xxgk/xxjj.htm
url:http://www.gzhu.edu.cn/xxgk/xrld.htm
Remaining 111 | Find 15 URL in http://www.gzhu.edu.cn/xxgk/xrld.htm
url:http://www.gzhu.edu.cn/xxgk/xxxhxg.htm
Remaining 110 | Find 15 URL in http://www.gzhu.edu.cn/xxgk/xxxhxg.htm
url:http://www.gzhu.edu.cn/xxgk/xyfj.htm
Remaining 109 | Find 15 URL in http://www.gzhu.edu.cn/xxgk/xyfj.htm
url:http://www.gzhu.edu.cn/zzjg/glfwjg.htm
Remaining 108 | Find 15 URL in http://www.gzhu.edu.cn/zzjg/glfwjg.htm
url:http://www.gzhu.edu.cn/zzjg/xy_b_.htm
Remaining 107 | Find 15 URL in http://www.gzhu.edu.cn/zzjg/xy_b_.htm
url:http://www.gzhu.edu.cn/zzjg/kydw.htm
Remaining 106 | Find 15 URL in http://www.gzhu.edu.cn/zzjg/kydw.htm
```

信息收集工具&方法—WAF识别

- WhatWaf: https://github.com/Ekultek/WhatWaf
- wafw00f: https://github.com/EnableSecurity/wafw00f

信息收集工具&方法—wafw00f

Usage: main.py url1 [url2 [url3 ...]]

Options:

-h, --help show this help message and exit

-v, --verbose Enable verbosity, multiple -v options increase verbosity

-a, --findall Find all WAFs which match the signatures, do not stop testing on the first one

-r, --noredirect Do not follow redirections given by 3xx responses

-t TEST, --test=TEST Test for one specific WAF

-o OUTPUT, --output=OUTPUT
Write output to csv, json or text file depending on file extension. For stdout, specify - as filename.

-f FORMAT, --format=FORMAT
Force output format to csv, json or text.

-i INPUT, --input-file=INPUT
Read targets from a file. Input format can be csv, json or text. For csv and json, a `url` column name or element is required.

-l, --list List all WAFs that WAFW00F is able to detect

-p PROXY, --proxy=PROXY
Use an HTTP proxy to perform requests, examples: http://hostname:8080, socks5://hostname:1080, http://user:pass@hostname:8080

-V, --version Print out the current version of WafW00f and exit.

-H HEADERS, --headers=HEADERS
Pass custom headers via a text file to overwrite the default header set.

--no-colors Disable ANSI colors in output.

```
PS D:\魔方\方班讲课\信息收集工具\WAF识别\wafw00f\wafw00f> python3 .\main.py -i .\target.txt

                    ______
                   /      \
                  (  Woof! )
                   \  ____/                    )
                   ,,                        ) (_
              .-. -'        _______           ( |__|
             ()``; |==|_______)               .)|__|
             / ('            /|\             (  |__|
           (  /  )          / | \             . |__|
            \(_)_))        /  |  \              |__|

                      ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://5ystudy.gzhu.edu.cn
ERROR:wafw00f:Something went wrong HTTPConnectionPool(host='5ystudy.gzhu.edu.cn', port=80): Read timed out. (read timeou
t=7)
[+] Generic Detection results:
ERROR:wafw00f:Something went wrong ('Connection aborted.', RemoteDisconnected('Remote end closed connection without resp
onse'))
[*] The site http://5ystudy.gzhu.edu.cn seems to be behind a WAF or some sort of security solution
[~] Reason: Blocking is being done at connection/packet level.
[~] Number of requests: 3
[*] Checking https://webvpn.gzhu.edu.cn
[+] Generic Detection results:
[-] No WAF detected by the generic detection
```

信息收集工具&方法—企业信息收集

- 爱企查: https://aiqicha.baidu.com
- 天眼查: https://www.tianyancha.com
- 企查查: https://www.qichacha.com
- 小蓝本: https://www.xiaolanben.com/pc
- ICP备案查询：http://www.miitbeian.gov.cn/icp/publish/query/icpMemoInfo_showPage.action#
  ICP查询脚本：https://github.com/wongzeon/ICP-Checker
- 公安部备案查询：http://www.beian.gov.cn/portal/recordQuery

信息收集工具&方法—敏感信息（google hack语法）

- 后台地址

  site:xxx.com intitle:管理|后台|登陆|管理员|系统|内部

  site:xxx.com inurl:login|admin|system|guanli|denglu|manage|admin_login|auth|dev

- 敏感文件

  site:xxx.com (filetype:doc OR filetype:ppt OR filetype:pps OR filetype:xls OR filetype:docx OR filetype:pptx OR filetype:ppsx OR filetype:xlsx OR filetype:odt OR filetype:ods OR filetype:odg OR filetype:odp OR filetype:pdf OR filetype:wpd OR filetype:svg OR filetype:svgz OR filetype:indd OR filetype:rdp OR filetype:sql OR filetype:xml OR filetype:db OR filetype:mdb OR filetype:sqlite OR filetype:log OR filetype:conf)

- 测试环境

  site:xxx.com inurl:test|ceshi

  site:xxx.com intitle:测试

- 邮箱

  site:xxx.com (intitle:”Outlook Web App” OR intitle:”邮件” OR inurl:”email” OR inurl:”webmail”)

- 其他

  site:xxx.com inurl:api|uid=|id=|userid=|token|session

  site:xxx.com intitle:index.of "server at"

信息收集工具&方法—敏感信息（github）

- @xxx.com password/secret/credentials/token/config/pass/login/ftp/ssh/pwd
- @xxx.com security_credentials/connetionstring/JDBC/ssh2_auth_password/send_keys

信息收集工具&方法—敏感信息（网盘）

- 超能搜: https://www.chaonengsou.com
- 凌风云：https://www.lingfengyun.com/
- http://www.panduoduo.net/
- http://www.zhuzhupan.com/
- https://www.quzhuanpan.com/

信息收集工具&方法—历史漏洞

- 乌云镜像: https://wooyun.x10sec.org
- Seebug: https://www.seebug.org
- Exploit Database: https://www.exploit-db.com
- Vulners: https://vulners.com
- Sploitus: https://sploitus.com
- http://www.anquan.us/

信息收集工具&方法—信息收集集成平台

- ARL: https://github.com/TophantTechnology/ARL
- ARL-plus: https://github.com/ki9mu/ARL-plus-docker
- ShuiZe: https://github.com/0x727/ShuiZe_0x727
- BBOT: https://github.com/blacklanternsecurity/bbot

信息收集工具&方法—空间引擎搜索（网络空间资产测绘）

- FOFA: https://fofa.so
- Quake: https://quake.360.cn/quake/#/index
- Hunter: https://hunter.qianxin.com
- Shadon: https://www.shodan.io
- ZoomEye: https://www.zoomeye.org
- 坤舆：https://github.com/knownsec/Kunyu/blob/main/

信息收集工具&方法—社会工程学的信息收集

- 领英、猎聘、boss直聘
- 贴吧
- 微博
- 图片中的地理位置信息收集
  https://www.163.com/dy/article/GJHR3DVB05522ZEC.html
- telegram上的社工库
- 注册过的网站：https://www.reg007.com/

CONTENTS

目录

信息收集工具&方法—信息收集后的处理

- 信息的归类：
  将收集到的信息以资产的类别分类
- 信息的关联：
  将收集到的信息之间的关系大致标识出来
- 信息的筛查：
  将收集到的信息检查是否存在失效或不准确的进行排除
- 信息的拓扑：
  将重点内容作为信息收集的起点再做一次信息收集
- 整合

THANKS

协助企业随时洞察和有效缓解数字化时代的网络空间风险

深圳市魔方安全科技有限公司
www.cubesec.cn| 0755-23612251