信息收集

问题：
你接到了一个任务，需要对某个公司做测试，
你会如何对他来进行测试呢？

学院介绍

学院宗旨：专注网安人才实战技能培养

学院官网：https://edu.hetianlab.com/

合天网安实验室：https://www.hetianlab.com/

主打课程：

《web安全》：OWASP TOP 10漏洞原理及测试

《渗透测试》：渗透测试流程及工具的使用

《安全开发》：用python写一个综合的扫描器

《CTF-PWN》：CTF中的PWN相关

《CTF-WEB》：CTF中WEB相关

目录
CONTENTS

/01 信息收集简介

1.1 信息收集介绍

信息收集是指通过各种方式获取所需要的信息，以便我们在后续的渗透过程更好的进行。比如目标站点IP、中间件、脚本语言、端口、邮箱等等。信息收集包含资产收集但不限于资产收集。

1.2 信息收集的意义

信息收集是渗透测试成功的保障

更多的暴露面

更大的可能性

1.3 信息收集的分类

主动信息收集

通过直接访问网站在网站上进行操作、对网站进行扫描等，这种是有网络流量经过目标服务器的信息收集方式。

被动信息收集

基于公开的渠道，比如搜索引擎等，在不与目标系统直接交互的情况下获取信息，并且尽量避免留下痕迹。

1.4 收集哪些信息

服务器信息（端口、服务、真实IP）

网站信息（网站架构[操作系统、中间件、数据库、编程语言]、指纹信息、WAF、敏感目录、敏感文件、源码泄露、旁站、C段）

域名信息（whois、备案信息、子域名）

管理员信息（姓名、职务、生日、联系电话、邮件地址）

/02 域名信息收集

2.1 域名介绍

域名（Domain Name），简称域名、网域，是由一串用点分隔的名字组成的Internet上某一台计算机或计算机组的名称，用于在数据传输时标识计算机的电子方位（有时也指地理位置）。

DNS（域名系统，Domain Name System）是互联网的一项服务。它作为将域名和IP地址相互映射的一个分布式数据库，能够使人更方便地访问互联网。

2.2 域名分类

顶级域名	二级域名	三级域名
.com	baidu.com	www.baidu.com

政府域名	商业域名	教育域名
.gov	.com	.edu

2.3 备案信息查询

可以通过备案查询查到其它的域名，再根据这些域名收集其它子域名

https://beian.miit.gov.cn/#/Integrated/recordQuery

域名 hetianlab.com 的信息 以下信息更新时间：2020-08-09 22:56:08 立即更新

主办单位名称	湖南合天智汇信息技术有限公司
主办单位性质	企业
网站备案/许可证号	湘ICP备14001562号-4 查看截图
网站名称	合天网安实验室
网站负责人	[VIP可见]
网站首页网址	www.hetianlab.com
安全认证	未认证 / 可信百科 未认证 / 未认证 / 未认证 / 不安全https
审核时间	2019-08-20
快捷查询	Whois查询 | SEO综合查询 | Alexa排名查询 | PR查询 | 网站测速 | 中文网站排名

该单位还备案了以下网站

网站网址	网站名称	负责人	网站备案/许可证号
hetianlab.com	合天网安实验室	[VIP可见]	湘ICP备14001562号-4
hetianlab.cn	合天网安实验室	[VIP可见]	湘ICP备14001562号-4
hetianlab.org	合天网安实验室	[VIP可见]	湘ICP备14001562号-4
hetianlab.com.cn	合天网安实验室	[VIP可见]	湘ICP备14001562号-4
erangelab.com.cn	合天网安竞赛系统	[VIP可见]	湘ICP备14001562号-5

2.4 子域名介绍

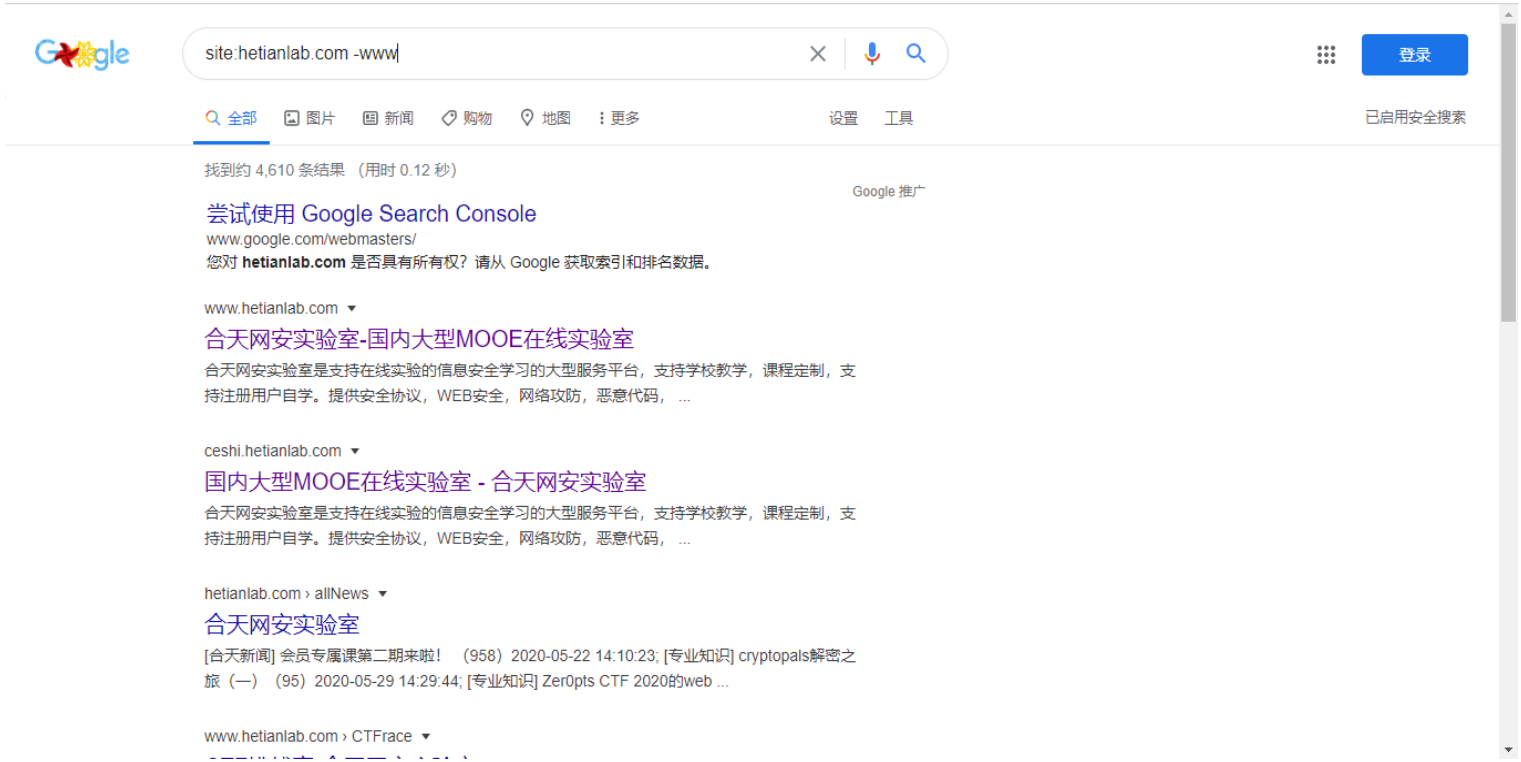
子域名指二级域名,二级域名是顶级域名(一级域名)的下一级。

比如mail.heetian.com和bbs.heetian.com是heetian.com的子域，而heetian.com则是顶级域名.com的子域。

2.4.1 子域名收集渠道一

搜索引擎-google hacking

site:hetianlab.com



2.4.2 子域名收集渠道二

https://fofa.so/

domain=“baidu.com”

https://www.zoomeye.org/

site:”baidu.com”

https://www.shodan.io/

hostname:baidu.com

2.4.3 子域名收集渠道三

js文件发现子域名

https://github.com/Threezh1/JSFinder

```
root@kali:~/JSFinder# python3 JSFinder.py -u http://www.mi.com
url:http://www.mi.com
Find 64 URL:
http://s02.pre.mi.com/assets/
http://time.hd.mi.com/gettimestamp
http://hd.mi.com/x/03021d/img/loading.gif
http://order.mi.com
http://api.order.mi.com
http://cn.orderapi.mi.com
http://www.mi.com
http://cart.mi.com
http://item.mi.com
http://list.mi.com
http://search.mi.com
http://my.mi.com
http://tp.hd.mi.com/
```

2.4.4 子域名收集渠道四

OneForAll

https://github.com/shmilylty/OneForAll

```
root@kali:~/OneForAll# python3 oneforall.py
NAME
    oneforall.py - OneForAll help summary page

SYNOPSIS
    oneforall.py - GROUP | COMMAND | VALUE

DESCRIPTION
    OneForAll is a powerful subdomain integration tool

    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 --format 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
```

/03 IP、端口信息搜集

3.1 域名查询IP

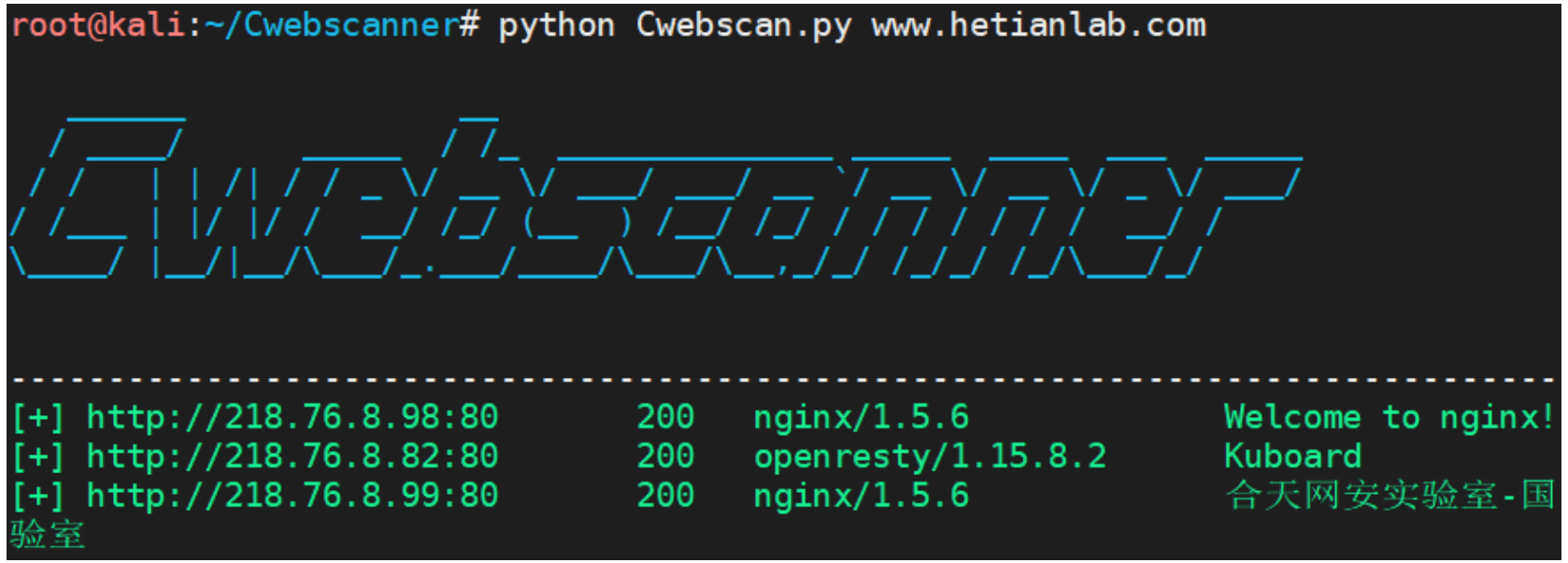
http://ip.tool.chinaz.com/

知道一个站点的域名需要得到它的IP以便之后获取端口信息或扫描等后续工作。

3.2 同C段查询

nmap -sP 192.168.1.*

https://github.com/se55i0n/Cwebscanner



3.3 端口扫描

端口	服务	入侵方式
21	ftp/tftp/vsftpd文件传输协议	爆破/嗅探/溢出/后门
22	ssh远程连接	爆破/openssh漏洞
23	Telnet远程连接	爆破/嗅探/弱口令
25	SMTP邮件服务	邮件伪造
53	DNS域名解析系统	域传送/劫持/缓存投毒/欺骗
67/68	dhcp服务	劫持/欺骗
110	pop3	爆破/嗅探
139	Samba服务	爆破/未授权访问/远程命令执行
143	Imap协议	爆破
161	SNMP协议	爆破/搜集目标内网信息
389	Ldap目录访问协议	注入/未授权访问/弱口令
445	smb	ms17-010/端口溢出
512/513/514	Linux Rexec服务	爆破/Rlogin登陆
873	Rsync服务	文件上传/未授权访问
1080	socket	爆破
1352	Lotus domino邮件服务	爆破/信息泄漏
1433	mssql	爆破/注入/SA弱口令
1521	oracle	爆破/注入/TNS爆破/反弹shell
2049	Nfs服务	配置不当
2181	zookeeper服务	未授权访问

端口	服务	入侵方式
2375	docker remote api	未授权访问
3306	mysql	爆破/注入
3389	Rdp远程桌面链接	爆破/shift后门
4848	GlassFish控制台	爆破/认证绕过
5000	sybase/DB2数据库	爆破/注入/提权
5432	postgresql	爆破/注入/缓冲区溢出
5632	pcanywhere服务	抓密码/代码执行
5900	vnc	爆破/认证绕过
6379	Redis数据库	未授权访问/爆破
7001/7002	weblogic	java反序列化/控制台弱口令
8069	zabbix服务	远程命令执行/注入
8161	activemq	弱口令/写文件
8080/8089	Jboss/Tomcat/Resin	爆破/PUT文件上传/反序列化
8083/8086	influxDB	未授权访问
9000	fastcgi	远程命令执行
9090	Websphere控制台	爆破/java反序列化/弱口令
9200/9300	elasticsearch	远程代码执行
11211	memcached	未授权访问
27017/27018	mongodb	未授权访问/爆破

3.3.1 Nmap端口状态

Open	端口开启，数据有到达主机，有程序在端口上监控
Closed	端口关闭，数据有到达主机，没有程序在端口上监控
Filtered	数据没有到达主机，返回的结果为空，数据被防火墙或IDS过滤
UnFiltered	数据有到达主机，但是不能识别端口的当前状态
Open|Filtered	端口没有返回值，主要发生在UDP、IP、FIN、NULL和Xmas扫描中
Closed|Filtered	只发生在IP ID idle扫描

3.3.2 基础用法

单一主机扫描：nmap 192.168.1.2

子网扫描：nmap 192.168.1.1/24

多主机扫描：nmap 192.168.1.1 192.168.1.10

主机范围扫描：nmap 192.168.1.1-100

IP地址列表扫描：nmap –iL target.txt

3.3.3 Nmap存活主机探测

nmap –sP 192.168.1.1/24

3.3.4 扫描全部端口

nmap -sS -v -T4 -Pn -p 0-65535 -iL liveHosts.txt

• -sS：SYN扫描,又称为半开放扫描，它不打开一个完全的TCP连接，执行得很快，效率高（一个完整的tcp连接需要3次握手，而-sS选项不需要3次握手）

优点：Nmap发送SYN包到远程主机，但是它不会产生任何会话，目标主机几乎不会把连接记入系统日志。（防止对方判断为扫描攻击），扫描速度快，效率高，在工作中使用频率最高

缺点：它需要root/administrator权限执行

• -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

• -iL：导入需要扫描的列表

3.3.5 扫描常用端口及服务信息

nmap -sS -T4 -Pn -oG 1.txt -iL LiveHosts.txt

系统扫描

nmap -O -T4 -Pn -oG 1.txt -iL LiveHosts.txt

版本检测

nmap -sV -T4 -Pn -oG 1.txt -iL LiveHosts.txt

感谢您的聆听

学习工具、资料及课程回放

扫码免费领取