域名信息

1.对应IP收集

ping 域名、nslookup 回车后输入域名

2.子域名收集

layer子域名挖掘机、site:域名、subDomainsBrute-master（先安装dnspython插件）

3.whois(注册人)查询

查询注册人，注册邮箱及电话等关键信息。适用于、社工查询、邮箱反查该邮箱其他网站，通过其他网站的漏洞获取密码以用

站长工具、爱站网、微步在线(x.threatbook.cn/)、site.ip138.com、searchdns.netcraft.com

4.kali 查询dns

dnswalk qq.com. 域名后面加个 `.`
dnsenum baidu.com 查看服务器
dns 后按两下tab键就能查看所有dns工具
whois baidu.com

敏感目录

收集方向

robots.txt、后台目录、安装包、上传目录、mysql管理接口、安装页面、phpinfo、编辑器、iis短文件

安装包：网站备份打包www.***.rar/zip、beifen.rar/zip、tar.gz等打包

上传目录：fckeditor、ewebedit、ckfinder

mysql管理接口：phpmyadmin、pmd、pma、phadmin)

安装页面：可能会爆出指纹

常用工具

字典爆破>>burp、御剑、dirbuster、wwwscan、IIS_shortname_Scanner、owasp DirBuser

蜘蛛爬行>>爬行菜刀、webrobot、burp、awvs、appscan

端口扫描

> 21>>FTP
> 22>>SSH
> 23>>Telnet
> 110>>POP3
> 1433 >>Sqlserver
> 3306>> Mysql
> 3389>>Mstsc 远程桌面

> 8080>>(Tomcat/jboss)
> 9090>>WebSphere

常用工具：nmap、portscan、ntscan、telnet（telnet 域名 端口）、scanport

旁站C段

旁站:同服务器上的其他站点

C段：同一网段其他服务器

常用工具：

web：K8旁站、御剑、在线工具（www.5kik.com/c）

端口：portscan

整站分析

操作系统：

windows/linux

判断方法：将网页后缀修改大小写看网页状态，windows下不区分大小写，因此不会报错

脚本格式：

asp/aspx/php/jsp

判断方法：输入index.asp/index.php >> 就能判断出什么脚本

数据库类型：

access/sqlserver/mysql/oracle/db2/postgresql/sqlite

若为PHP脚本，则mysql较多一些

CMS类型：

dedecms/diguocms/meterinfocms等等

判断方法：readme.txt、使用说明.txt、指纹识别系统www.yunsee.cn

防护情况：

软硬waf(web application firewall)

服务器类型：服务器平台、版本

网站容器：

搭建网站的服务组件，如iis、Apache、nginx、tomcat等

判断方法：抓包看响应包、随便输入一个东西查看报错特征

指纹识别：

谷歌hacker

> intext：查看网页中含有XX关键字的网站　如: intext: 管理员登录
> intitle：查找某个标题　如：intitle:后台登录
> Filetype：查找某个文件类型的文件　如：　数据挖掘 filetype: doc
> inurl: 查找url中带有某字段的网站 如：　inurl: php?id=
> site: 在某域名中查找信息

URL采集

采集相关url的同类网站

如：php?id=

漏洞网站

相同某种指纹网站

常用工具

谷歌hacker

url采集器

后台查找

•1 弱口令默认后台：admin，admin/login.asp，manage，login.asp等等常见后台

•2 查看网页的链接：一般来说，网站的主页有管理登陆类似的东西，有些可能被管理员删掉

•3 查看网站图片的属性

•4 查看网站使用的管理系统，从而确定后台

•5 用工具查找：wwwscan，intellitamper，御剑

•6 robots.txt的帮助：robots.txt文件告诉蜘蛛程序在服务器上什么样的文件可以被查看

•7 GoogleHacker

•8 查看网站使用的编辑器是否有默认后台

•9 短文件利用

a~！.asp 访问a开头的文件

•10 sqlmap --sql-shell load_file('d:/wwroot/index.php'); 读源文件

CDN绕过方法

什么是CDN

内容分发网络，主要用于对网络加速的

如何判断网站有没有使用CDN（超级ping）

超级ping：http://ping.chinaz.com/域名

查看每个地区的IP地址，如果都一样说明没有CDN；

很多厂商可能让www使用cdn，空域名不使用CDN缓存。

所以直接ping sysorem.xyz可能就能得到真实IP

绕过CDN查找真是IP（验证IP和域名是否真实对应最简单的办法）

•1.查找二级域名

查看子域名或c段的IP与主域名是否相同

•2.让服务器主动给你发包（邮件）

查看邮件的源文件

•3.敏感文件泄露

扫描phpinfo,test等，得到真实Ip

•4.查询历史解析ip

CND的ip地址之前所用的IP就是真实IP

在ip138、toolbar.netcraft.com/中查询，如果有app的话，下载app抓包，也能得到ip

•5.通过 znmap 全网爆破查询真实 ip

•6.国外访问

国内的CDN往往只会针对国内用户访问加速

所以国外就不一定了。因此通过国外代理访问就能查看真实IP了

或者通过国外的DNS解析，可能就能得到真实的IP，社工也可以。

nslookup [目标ip] [国外CND]

•7.绕过CloudFlare

如何访问绕过cdn

•修改本地hosts文件，强行将域名与IP解析对应

然后访问域名查看页面是否变化

app

如果目标又app，就下载进行抓包分析流量，获取真实服务器IP，找到之后修改本地hosts.txt文件

常见工具使用

avws/IBM Security APPscan/nessus（openvs扫描漏洞）/metasploit（利用漏洞）/nmap/sqlmap/metsta/appscan/Netsparker/jsky/safe3wvs/椰树/M7Lrv

建议burp 手工挖取，工具只是辅助作用

Nmap （nmap使用手册）

*主机探测

扫描单个主机：nmap 192.168.1.2

扫描整个子网：nmap 192.168.1.1/24

扫描多个目标：nmap 192.168.1.2 192.168.1.5

扫描一个范围内的目标：nmap 192.168.1.1-100

扫描文件ip列表（和nmap在同一目录下）：nmap -iL ip.txt

扫描所有存活主机的列表：nmap -sL 192.168.1.1/24

扫描除某个ip之外的所有主机命令：nmap 192.168.1.1/24-exclude 192.168.1.1

扫描除某个文件内ip列表外的子网主机：nmap 192.168.1.1/24-excludefilex.txt

*端口扫描

> nmap -F -sT -v nmap.org
>
> -F:扫描100个最有可能开放的端口，
>
> -v:获取扫描的信息
>
> -sT：默认采用的是TCP扫描，不写也可以
>
> -p：指定要扫描的端口 nmap -p80,23,24 192.168.1.1
>
> 扫描端口的状态
>
> open（打开，有程序在端口上监控）
>
> closed（关闭）
>
> Filtered（数据没有到达主机，可能被防火墙或IDS（入侵检测系统）过滤）
>
> UnFiltered（数据到达主机，但不能识别端口的状态）
>
> 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（只发在IP ID idle扫描）

TCP扫描（-sT）

> 速度快，准确度高，无权限要求，但容易被防火墙和IDS发现
>
> 运行原理：通过建立TCP的三次握手连接进行信息1的传递
>
> 1、Client端发送SYN；
>
> 2、server端发送SYN/ACK，表明端口开放；
>
> 3、client端返回ACK，表明连接已建立（这里服务器会有一个等待的时间，如果大量的ACK不返回，将造成DDOS）
>
> 4、client端主动断开连接

SYN扫描（-sS）

比TCP扫描快一些，因为没有建立一个正常的TCP链接，不会再目标主机上留下任何痕迹，但需要ROOT权限

UDP ping检测主机

nmap -PU 192.168.1.0/24

*服务版本扫描

nmap -sV 192.168.1.1

精准确认端口上运行的服务

nmap -sV --script unusual-port 192.168.1.1

syn扫描器/扫描外网主机网段/对应的端口爆破工具/提供访问木马服务器下载的工具/ftp、http、hfs（有个代码执行漏洞）/一个远控

设个蜜罐 抓黑客服务器

03 1433 netstat -an 找到黑客ip

主机系统指纹识别

探测主机操作系统

nmap -O 192.168.1.19

nmap -A 192.168.1.19 -oX c:\123.xml

-oN 导出扫描结果

-oX 导出扫描结果XML格式

密码破解

•暴力破解VNC

•nmap --script vnc-brute --script-args brute.guesses=6,brute.emptypass=true,userdb=/root/dictionary/user.txt,brute.useraspass=true,passdb=/root/dictionary/pass.txt,brute.retries=3,brute.threads=2,brute.delay=3 42.96.170.128

•破解telnet

•nmap -p 23 --script telnet-brute --script-args userdb=myusers.lst,passdb=mypwds.lst --script-args telnet-brute.timeout=8s 192.168.1.1

•ftp弱口令暴力破解

•nmap --script ftp-brute --script-args brute.emptypass=true,ftp-brute.timeout=30,userdb=/root/dirtionary/usernames.txt,brute.useraspass=true,passdb=/root/dirtionary/passwords.txt,brute.threads=3,brute.delay=6 192.168.1.1

漏洞探测

•HTTP.sys 远程代码执行

•nmap -sV --script http-vuln-cve2015-1635 192.168.1.1

•IIS 短文件泄露

•nmap -p 8080 --script http-iis-short-name-brute 192.168.1.1

•拒绝服务

•nmap --max-parallelism 800--script http-slowloris www.cracer.com

•验证http 中开启了put 方法

•nmap --script http-put --script-args http-put.url=/uploads/testput.txt,http-put.file=/root/put.txt 218.19.141.16

•验证MySQL 匿名访问

•nmap --script mysql-empty-password 203.195.139.153

创建扫描脚本

防火墙躲避绕过

-f 分片绕过

-D 使用诱饵隐蔽扫描

NMAP -D 1.1.1.1,222.222.222.222 www.baidu.com

--source-port 源端口欺骗

AWVS

web Scanner：漏洞扫描

•Bind sql Injection sql注入

•Cross site scripting（verifiled） XSS（可能会误报，手工测试）

•Directory listing 目录遍历

•Host header attack 主机头攻击

•HTML form without CSRF prodition

Tools

site Crawler 网站爬行

•在扫描j结束的时候开启http sniffer，目的是让用户手动的去浏览，以免crawler没有爬行到。

•仅爬行网站首页的所有链接。

•不抓取上级目录 www.。

•抓取子目录。

•尝试抓取其他链接（不全是从首页爬行到的）。

•处理的文件robots.txt和sitemap.xml 。

•是否忽略文件中的大小写。

•从每个文件夹中先爬取类似index.php，default.asp的文件。

•防止无线递归目录。

•如果探测到URL重写的话，警告用户。

•忽略文件格式（例如.js .css等）。

•防止自定义404界面的探测。

•讲www.domain.com和domain.com视为同一个站。

•启用这项目，如果在一个文件夹中存在超过20中写入模式的话，爬虫只会爬行钱20个。

•优化输入已知的应用

Target Finder 目标发现

subdomain scanner 子域名扫描

sql 注入利用

http 编辑

http嗅探（推荐使用burp site）

http模糊测试（相当于暴力破解）

认证测试

网络服务扫描器

Netsparker

整站目录结构

网站一般是由html代码+动态脚本语言+数据库+css样式+js代码组成

1.asp+access

admin：后台管理目录

Database：数据库目录　　Inc也可能是数据库目录

-xydata：数据库目录（存在data的关键词肯能是数据库目录）

ewebEditor：编辑器目录 editor关键词

Guestbook：留言板目录

Include_files：包含文件目录

Upload_files：上传文件目录

setup：安装目录

2.论坛网站

manage（管理）：管理目录

editor：编辑器目录

install.php：安装

config.php：数据库目录

conn.php：是告诉数据库的位置

inc ：数据库目录

3.常见的数据库

access、mssql、mysql、oracle、db2、sql server

4.利用0day拿站

简介：所谓“0Day漏洞”，是指那些没有公开过，因而也没有补丁的漏洞，也就是通常所说的“未公开漏洞”。

注：多收集0day，对于拿站更方便

5.利用啊D批量拿站

6.利用椰树批量拿站