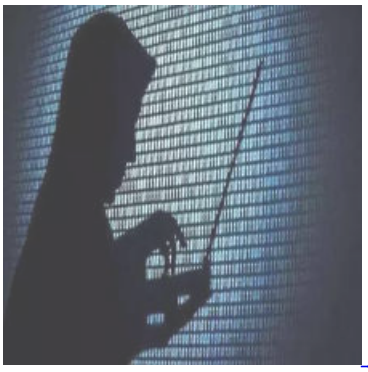
渗透测试第一步（信息收集）

原创

whoim_i 于 2020-04-04 20:33:30 发布

分类专栏： 渗透测试 文章标签： 安全

本文链接：https://blog.csdn.net/whoim_i/article/details/104406267



目录

> 因为想要面对一个新的开始，一个人必须有梦想、有希望、有对未来的憧憬。如果没有这些，就不叫新的开始，而叫逃亡。
>
> ————玛丽亚·杜埃尼亚斯

前言

信息收集对于渗透测试前期来说是非常重要的，因为我们只有掌握了目标网站或目标主机足够多的信息之后，我们才能更好地对其进行漏洞检测。最简单的比如说目标站点的ip、中间件、脚本语言、端口、邮箱等等。

信息收集方式区别

信息收集的方式可以分为两种：**主动和被动**

- 主动收集：相当于通过技术手段去侦察目标的情况，比如通过直接访问、扫描网站。这种流量将流经网站，目标可能会记录下我们的行为。
- 被动收集：相当于通过技术手段去收集目标遗留的信息，比如利用第三方的服务对目标进行访问了解，比例：Google搜索、Shodan搜索等

没有一种方式是完美的，每个方式都有自己的优势。主动可获取更多的信息，但目标机会有所察觉。被动收集信息相对较少，但不会被目标发现。那么在实际的应用中，通常都是两种方式相结合的方式，这样才能采集到目标更完整的信息。

域名信息收集

主域名信息

知道目标的域名之后，我们要做的第一件事就是获取域名的注册信息，包括该域名的DNS服务器信息和注册人的联系信息等。

whois查询

whois是一个标准的互联网协议，可以用于收集网络注册信息，注册的域名，ip地址等信息。

查询方法:

国外的who.is：https://who.is/

站长之家：http://whois.chinaz.com/

爱站：https://whois.aizhan.com/

微步：https://x.threatbook.cn/

备案信息查询

网站备案是根据国家法律法规规定，需要网站的所有者向国家相关部门申请的备案，这是国家信息产业部多网站的一种管理。主要针对国内的网站，如网站搭建在国外，则无需备案。

查询方法：

天眼查：https://www.tianyancha.com/

ICP备案查询网：http://www.beianbeian.com/

国家企业信用信息公示系统：http://www.gsxt.gov.cn/index.html

子域名信息

子域名是在顶级域名下的域名，收集的子域名越多，我们测试的目标就越多，渗透的成功率也越大。往往主站找不到突破口的时候，我们从子域名入手，有时候就会带来意想不到的惊喜。

在线查询

https://phpinfo.me/domain/

http://i.links.cn/subdomain/

http://dns.aizhan.com

https://www.dnsscan.cn/dns.html

子域名探测工具

工具比较多，常见的如下：

- layer子域名挖掘机
- subDomainsBrute
- K8
- orangescan
- DNSRecon

一般layaer和subdomainsbrute比较常用

搜索引擎枚举

我们可以利用google 搜索语法进行子域名搜索。

传送门在此——>黑客搜索大法（Google Hacking）

第三方聚合应用枚举

很多第三方服务汇聚了大量的DNS数据集，可以通过它们检索某个给定域名的子域名，只要往其搜索栏中输入域名就可以检索到相关的域名信息。

VirusTotal：https://www.virustotal.com/#/home/search

DNSdumpster：https://dnsdumpster.com/

证书透明度公开日志枚举

证书透明度(Certificate Transparency,CT)是证书授权机构(CA)的一个项目，证书授权机 构会为每一个 SSL/TLS 证书发布到公共日志中。一个 SSL/TLS 证书通常包含域名、子域名和邮 箱地址，这些也经常成为攻击者非常希望获得的有用信息。查找某个域名所属证书的最简单的 方法就是使用搜索引擎搜索一些公开的 CT 日志。

Crt.sh ：https://crt.sh/

censys：https://censys.io/

网络信息搜索

旁站、c段信息收集

旁站：是和目标网站在同一台服务器上的其它网站

c段：是和目标服务器ip处在同一个c段的其它服务器

查询方式

利用Bing.com：语法为：http://cn.bing.com/search?q=ip:111.111.111.111

站长之家：http://s.tool.chinaz.com/same

利用Google：语法：site:125.125.125.*

利用Nmap：语法：nmap -p 80,8080 –open ip/24

工具：K8、御剑、北极熊扫描器等

在线：http://www.webscan.cc/

绕过cdn获取真实ip

在渗透测试过程中，目标服务器可能只有一个域名，那么如何通过这个域名来确定目标服务器的真实ip呢。如果目标服务器不存在cdn可以直接通过ping域名或者nslookup解析域名信息。如果存在cdn就需要用到一些方法了。

传送门在此——>论网站CDN的绕过姿势

网站架构分析

服务器类型

服务器信息包括服务器用的操作系统：linux还是windows。知道服务器操作系统后还需要知道其具体版本，因为很多低版本的操作系统都存在一直的漏洞。

判断方法

- 可以通过ping来探测，windows的TTL值一般都是128，linux则为64.所以大于100的肯定就是windows系统，而几十的就是linux
- windows对大小写不敏感，linux则敏感。如www.xxx.com/index.php和www.xxx.com/index.Php打开的效果一样则说明是windows
- 用工具nmap进行探测

网站容器

知道操作系统后，我们就需要知道网站用的web服务器是什么类型的：apache、nginx、tomcat、iis。知道了类型后还要具体探测容器的具体版本，不同的web容器版本存在着不同的漏洞。我们可以使用whatweb进行探测。

判断方法

whatweb：https://whatweb.net/

或者命令行

传送门在此——>网站指纹扫描工具whatweb

常见的几种web容器（Apache、Nginx、Tomcat）

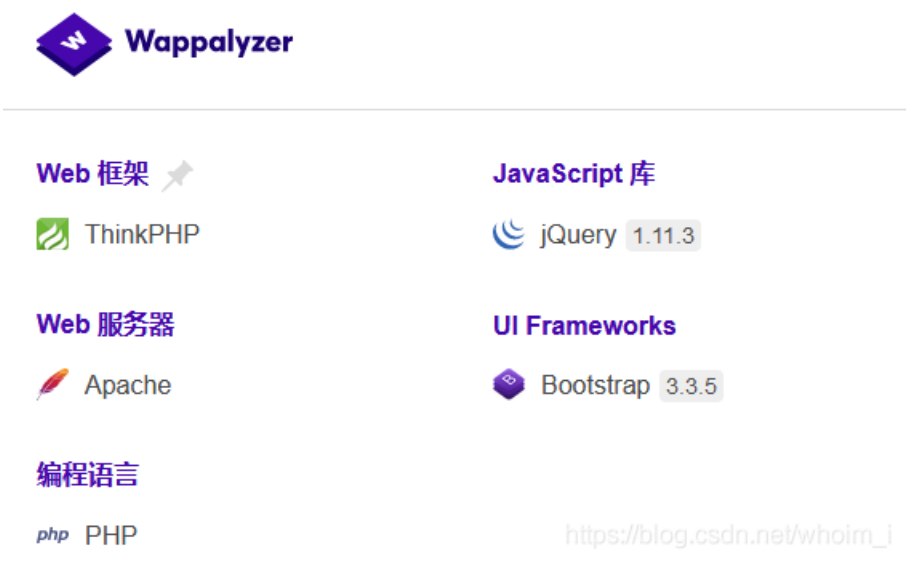
脚本类型

我们需要知道网站用的脚本类型：php、jsp、asp、aspx

了解它们之间的区别传送门在此——>各类后台脚本语言区别（PHP、JSP、ASP和ASPX）

判断方法

- 可以根据网站url来判断
- 谷歌语法判断，site:xxx filetype:php
- 根据firefox的插件判断比如wappalyzer



数据库类型

还需要知道网站用的是哪种类型的数据库：mysql、oracle、sqlserver、access。

几种数据库的区别

1.Access 全名是 Microsoft Office Access，是由微软发布的关联式数据库管理系统。小 型数据库，当数据库达到 100M 左右的时候性能就会下降。数据库后缀名： .mdb 一般是 asp 的网页文件用 access 数据库

2.SQL Server 是由 Microsoft 开发和推广的关系数据库管理系统（DBMS），是一个比较大 型的数据库。端口号为 1433。数据库后缀名 .mdf

3.MySQL 是一个关系型数据库管理系统，由瑞典 MySQL AB 公司开发，目前属于 Oracle 旗 下产品。MySQL 是最流行的关系型数据库管理系统，在 WEB 应用方面 MySQL 是最好的应用软件 之一，MySQL 数据库大部分是 php 的页面。默认端口是 3306

4.Oracle 又名 Oracle RDBMS，或简称 Oracle。是甲骨文公司的一款关系数据库管理系统。 常用于比较大的网站。默认端口是 1521

总结

成本上：access免费，mysql开源，sqlserver收费几千，oracle数万。

处理能力：access千以内访问量，sqlserver几千，mysql一万+，oracle海量。

规模：access小型数据库，sqlserver中型，mysql中小型，oracle大型

常见搭配

ASP 和 ASPX：ACCESS、SQL Server

PHP：MySQL、PostgreSQL

JSP：Oracle、MySQL

CMS类型

指纹识别是有必要的，只有识别出相应的web容器或者cms才能查找出与其相关的漏洞。cms又称为整站系统，常见的cms有：WordPress、Dedecms、Discuz、PhpWeb、PhpWind、Dvbbs、PhpCMS、ECShop、、SiteWeaver、AspCMS、帝国、Z-Blog等。

在线识别网站

BugScaner：http://whatweb.bugscaner.com/look/

云悉指纹：http://www.yunsee.cn/finger.html

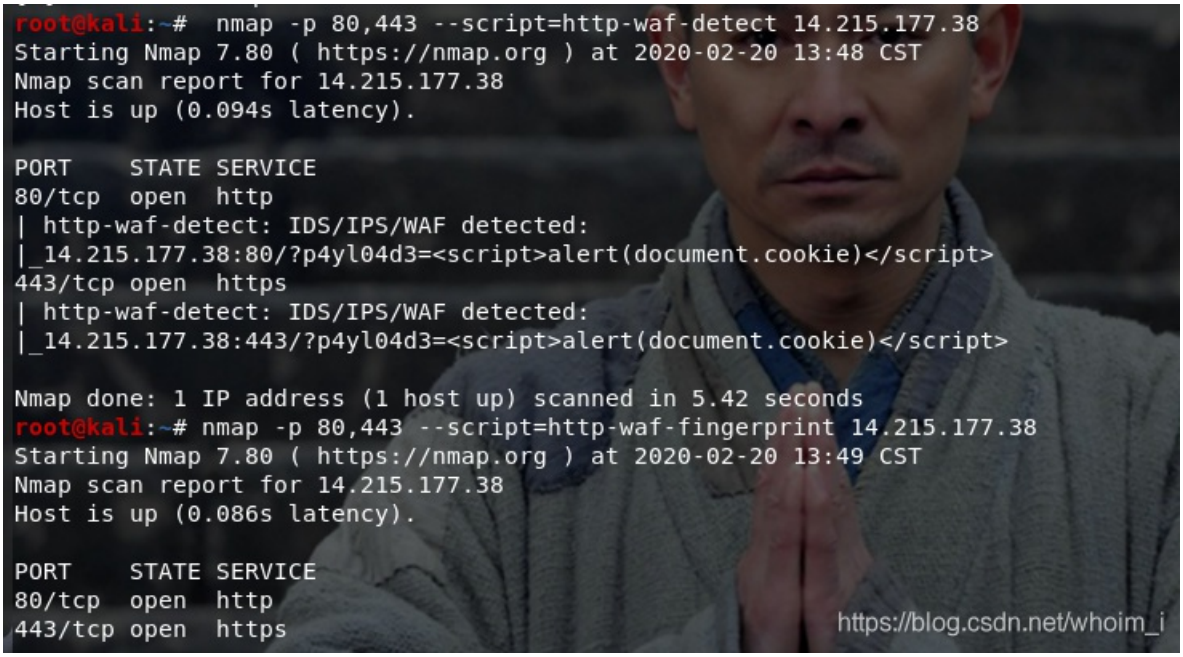
WhatWeb：https://whatweb.net/

WAF

waf也叫web应用防火墙，是通过一系列针对http/https的安全策略来专门为web应用提供保护的一款产品。waf的探测一般会被忽略，因为一般遇到waf的第一想法就是告辞告辞…。

判断方法

```
# nmap
root@kali:~# nmap -p 80,443 --script=http-waf-detect 14.215.177.38
root@kali:~# nmap -p 80,443 --script=http-waf-fingerprint 14.215.177.38
# waf00wf探测waf
root@kali:~# wafw00f -a www.baidu.com
```



主机及端口扫描

不仅仅要对目标网站进行扫描，还要对目标主机进行扫描，包括目标主机存在的漏洞，开放的端口，端口运行的服务等等。主机可以用nessus，端口扫描可以用nmap。

传送门在此——>Nmap相关介绍及使用、常见端口号

网站敏感目录和文件

在渗透测试中，探测web目录结构和隐藏的敏感文件是一个必不可少的环节，从中可以获取网站的后台管理页面，文件上传页面，甚至可以扫描出网站的源代码。

收集方向

后台目录：弱口令、万能密码、爆破

安装包：获取数据库信息，甚至是网站源码

上传目录：截断、上传图片马

mysql管理接口：弱口令、爆破、万能密码，甚至脱裤、拿到shell

安装页面：可以二次安装进行绕过

phpinfo：配置信息暴露

编辑器：fck、ke等

robots.txt文件：爬虫规范文件，侧面得知网站哪些目录重要

传送门——>robots协议相关

敏感文件、敏感目录的挖掘一般都是靠工具，常用的工具有：

字典爆破：dirb[kali 如：dirb http://192.168.200.113]对目标网站进行目录扫描]、DirBuster、 wwwscan 、御剑后台、Webdirscan 等

蜘蛛：Burp、OWASP ZAP、AWVS 等

在线工具：http://www.webscan.cc/

网络空间搜索引擎：zoomeye、shodan、fofa