01 渗透基础入门-概念名词

一、域名

1. 什么是域名？

  域名（英语：Domain Name），又称网域，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，用于在数据传输时对计算机的定位标识（有时也指地理位置）。

  由于IP地址具有不方便记忆并且不能显示地址组织的名称和性质等缺点，人们设计出了域名，并通过网域名称系统（DNS，Domain Name System）来将域名和IP地址相互映射，使人更方便地访问互联网，而不用去记住能够被机器直接读取的IP地址数串。

比如www.baidu.com，这就是一个域名，简单来说就是ip不好记，所以有了域名来方便记忆。可以联想到地址和经纬度的关系（上海 ：经度 121.48 纬度 31.22）

2. 域名在哪里注册？

  找个域名注册商的网站（比如阿里、万网），搜索想要的域名（由于国内并非所有域名都支持备案，目前提供主流可备案域名有：

.com, .cn, .com.cn, .net, .top, .wang, .vip, .company, .org.cn,.ac.cn, .site, .online, .ren .store, .tech, .xyz, .club, .link, .pro, .red, .info, .biz, .ltd, .gov.cn, .mobi, .city 等。）

  填写域名资料。若你是以公司名义注册域名，则需要填写企业资料、联系人信息；若你是以个人名义注册，请切换到个人栏，填写个人信息。域名英文信息将会根据你填写的中文自动翻译，请核对是否有误，若有误请及时进行修改。

  确认域名账单。确认域名注册人信息、账单无误后，使用支付宝或微信扫码支付即可完成注册。

  域名实名验证。因国内法律法规要求，域名注册后需要进行实名认证，通过认证后即可正式生效。若审核有误，请及时进行修改，再次提交审核。

  域名备案及绑定网站。如果你需要在国内上线，则需要进行网站备案。

3. 什么是子域名、二级域名、多级域名？

  例如www.dns0755.net是dns0755.net的子域名，而dns0755.net又是net的子域名。国际顶级域名的子域名叫做二级域名。

  如A.com是一级域名，A.B.com则是二级域名。一级域名较二级域名级别更高，而二级域名则是依附于一级域名下的附属分区域名，即二级域名是一级域名的细分层级。

  通过网址上【.】数量来判断域名层级，有多少【.】就为几级域名，如A.com是一级域名，A.B.com则是二级域名。

   如：baidu.com 是百度的顶级域名，zhidao.baidu.com 是二级域名，zhidao.zhidao.baidu.com 是三（多）级域名，\*.baidu.com 是泛域名。

4. 域名发现对于安全测试意义？

  进行渗透测试时，其主域名找不到漏洞时，就可以尝试去测试收集到的子域名，有可能测试子域名网站时会有意向不到的效果，然后可以由此横向到主网站。

二、DNS与CDN

1. 什么是DNS？

  域名系统（英文：Domain Name System，缩写：DNS）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。DNS使用TCP和UDP端口53。当前，对于每一级域名长度的限制是63个字符，域名总长度则不能超过253个字符。

2. 本地HOSTS与DNS的关系？

   Hosts是一个没有扩展名的系统文件，可以用记事本等工具打开，其作用就是将一些常用的网址域名与其对应的IP地址建立一个关联“数据库”，当用户在浏览器中输入一个需要登录的网址时，系统会首先自动从Hosts文件中寻找对应的IP地址，一旦找到，系统会立即打开对应网页，如果没有找到，则系统会再将网址提交DNS域名解析服务器进行IP地址的解析。

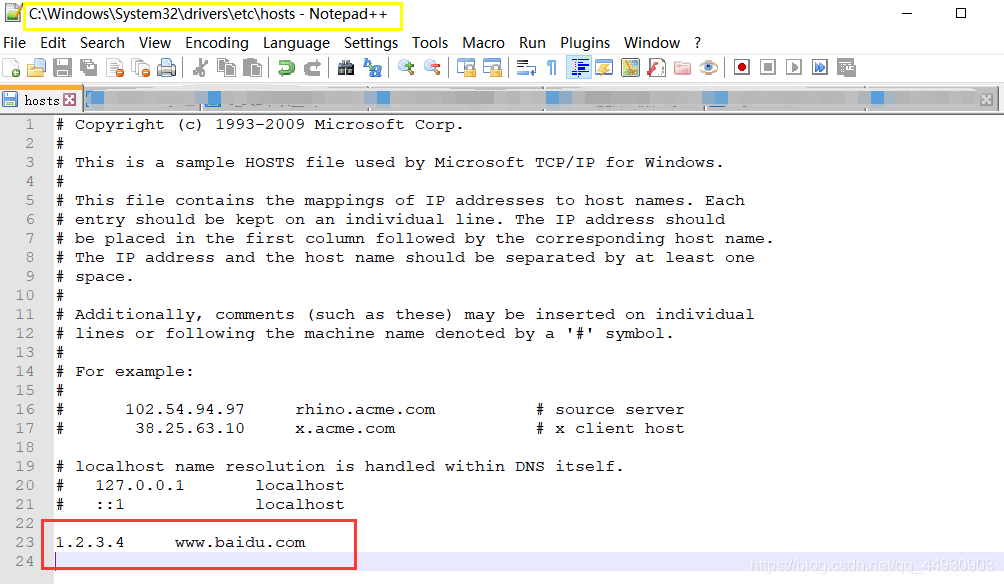
  需要注意的是，Hosts文件配置的映射是静态的，如果网络上的计算机更改了请及时更新IP地址，否则将不能访问。

   例：先打开cmd终端，输入命令 ping www.baidu.com，得到的结果如下图：



在这里插入图片描述

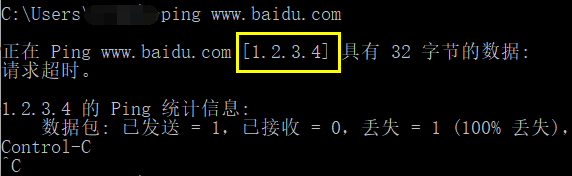
在hosts文件（图中黄色框内为hosts文件绝对路径）最后加上下图红色框内的内容，并ctrl+s保存



在这里插入图片描述

再次ping www.baidu.com 时会发现解析的ip变为你hosts文件中的了（当然了，访问不了）。

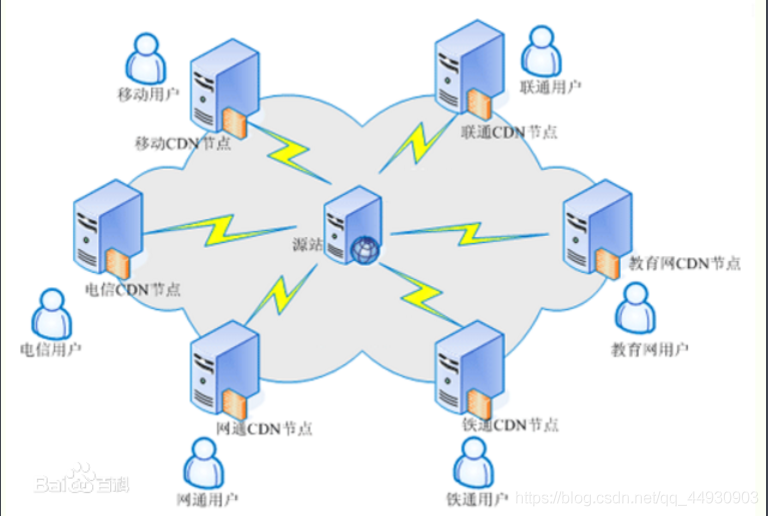
在这里插入图片描述



3. CDN是什么？与DNS的关系？

  CDN的全称是Content Delivery Network，即内容分发网络。CDN的基本思路是尽可能避开互联网上有可能影响数据传输速度和稳定性的瓶颈和环节，使内容传输的更快、更稳定。通过在网络各处放置节点服务器所构成的在现有的互联网基础之上的一层智能虚拟网络，CDN系统能够实时地根据网络流量和各节点的连接、负载状况以及到用户的距离和响应时间等综合信息将用户的请求重新导向离用户最近的服务节点上（单纯只使用DNS解析，直接PING就会显示出自己的真实IP,如果又使用CDN，PING出来的IP就不是用户的真实IP而是CDN服务器的IP节点。需要绕过CDN后去找真实IP地址：拓展：判断是否存在CDN并绕过，寻找真实IP）。其目的是使用户可就近取得所需内容，解决 Internet网络拥挤的状况，提高用户访问网站的响应速度。

在这里插入图片描述



扩展：DNS和CDN的区别与联系https://www.dns.com/supports/710.html

4. 常见的DNS安全攻击有哪些？

缓存投毒

  通常也称为域名系统投毒或DNS缓存投毒。它是利用虚假Internet地址替换掉域名系统表中的地址，进而制造破坏。当网络用户在带有该虚假地址的页面中进行搜寻，以访问某链接时，网页浏览器由于受到该虚假条目的影响而打开了不同的网页链接。在这种情况下，蠕虫、木马、浏览器劫持等恶意软件就可能会被下载到本地用户的电脑上。

DNS劫持

  DNS劫持又称域名劫持，是指在劫持的网络范围内拦截域名解析的请求，分析请求的域名，把审查范围以外的请求放行，否则返回假的IP地址或者什么都不做使请求失去响应，其效果就是对特定的网络不能访问或访问的是假网址。这类攻击一般通过恶意软件来更改终端用户TCP/IP设置，将用户指向恶意DNS服务器，该DNS服务器会对域名进行解析，并最终指向钓鱼网站等被攻击者操控的服务器。

域名劫持

  域名劫持就是在劫持的网络范围内拦截域名解析的请求，分析请求的域名，把审查范围以外的请求放行，否则直接返回假的IP地址或者什么也不做使得请求失去响应，其效果就是对特定的网址不能访问或访问的是假网址。一旦您的域名被劫持，用户被引到假冒的网站进而无法正常浏览网页，用户可能被诱骗到冒牌网站进行登录等操作导致泄露隐私数据。

DNS DDoS攻击

  针对DNS的DDoS攻击通过控制大批僵尸网络利用真实DNS协议栈发起大量域名查询请求，利用工具软件伪造源IP发送海量DNS查询，发送海量DNS查询报文导致网络带宽耗尽而无法传送正常DNS查询请求。发送大量非法域名查询报文引起DNS服务器持续进行迭代查询，从而达到较少的攻击流量消耗大量服务器资源的目的。

反射式DNS放大攻击

  所有放大攻击都利用了攻击者和目标Web资源之间的带宽消耗差异，由于每个机器人都要求使用欺骗性IP地址打开DNS解析器，该IP地址已更改为目标受害者的真实源IP地址，然后目标会从DNS解析器接收响应。为了创建大量流量，攻击者以尽可能从DNS解析器生成响应的方式构造请求。结果，目标接收到攻击者初始流量的放大，并且他们的网络被虚假流量阻塞，导致拒绝服务。

  当面对各种DNS攻击，墨者安全建议专业的高防DNS防劫持服务，保障服务器的稳定运行，从容应对各种DNS攻击，避免因DNS攻击造成在线业务中断，给企业带来重大损失。

三、脚本语言

1. 常见的脚本语言类型有哪些？

  asp php aspx jsp javaweb pl py cgi等

2. 不同脚本类型与安全漏洞的关系？

  不同的脚本语言的编写规则不一样，程序产生的漏洞自然也不一样（代码审计）。

3. 漏洞挖掘代码审计与脚本类型的关系？

  同上

四、后门

1. 什么是后门？有那些后门？

  后门程序一般是指那些绕过安全性控制而获取对程序或系统访问权的程序方法。类别：网页、线程插入、扩展、C/S后门。

2. 后门在安全测试中的实际意义？

  例如后门藏在网页上、软件内，悄无声息的进行攻击者想要的操作。

3. 关于后门需要了解那些？（玩法，免杀）

免杀，简单来讲就是绕过杀毒软件等。

五、WEB

1. WEB的组成架构模型？

网站源码：分脚本类型，分应用方向

操作系统：windows linux

中间件（搭建平台）：apache iis tomcat nginx等

数据库：access mysql mssql oracle sybase db2 postsql等

2.架构漏洞安全测试简要介绍？

3.为什么要从WEB层面为主为首？

  用户接触web层面最多，大部分都是从web页面入手慢慢渗透到服务器。直接从操作系统入手不太现实（大部分情况下接触不到）。

六、WEB相关安全漏洞

WEB源码类对应漏洞

  SQL注入，上传，XSS，代码执行，变量覆盖，逻辑漏洞，反序列化等

WEB中间件对应漏洞

WEB数据库对应漏洞

WEB系统层对应漏洞

其他第三方对应漏洞

APP或PC应用结合类

owasp top10

七、演示案例

1. 多级域名的枚举查找（原理，方式）

   layer子域名挖掘机、Maltego（kali自带）、各类挖掘子域名的网站：如 https://www.t1h2ua.cn/tools/

2. DNS解析修改后分析（本地或服务）

  把自己电脑的DNS服务的改成手动获取，并换dns（比如先8.8.8.8，再114.114.114.114），分别ping同一网站，看解析出来的ip是否不同。

3. EXE后门功能及危害及类似WEB后门

Quasar后门程序（.exe）生成并使用：https://blog.csdn.net/qq\_44930903/article/details/111600982

web后门：beef、WSExploer抓包、wireshark抓包等

4. APP类结合WEB协议，PC类结合WEB协议

Burp Suite抓app的包，然后改包发送等；

Apk数据提取（安卓逆向工具）：下载下方资源、解压，然后把一个apk文件放入到apps文件夹，运行exe文件，之后会生成results文件，apk的数据就在这里。

八、涉及资源

逍遥模拟器：http://www.xyaz.cn

WSExplorer抓包工具：http://www.downcc.com/soft/11196.html

Quasar后门程序生成：https://github.com/quasar/QuasarRAT/releases

Apk数据提取：https://pan.baidu.com/s/13\_i1ExwEaA59GfMt1Rp0Hg

提取码：0b7b

————————————————

版权声明：本文为CSDN博主「小言安全」的原创文章，遵循CC 4.0 BY-SA版权协议，转载请附上原文出处链接及本声明。

原文链接：https://blog.csdn.net/qq\_44930903/article/details/111517952