Day01　基础入门–概念名词

1.1 域名

1.1.1什么是域名?

- 域名：是由一串用点分割的名字组成的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）

1.1.2域名发现对于安全测试的意义?

- 可以给安全测试提供更多的测试点，方便获取更多相关信息

1.2 DNS

1.2.1什么是DNS?

- 域名系统（Domain Name System）。它是一个域名和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UDP端口53。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。

1.2.2本地HOSTS与DNS的关系?

- Hosts在本地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”，当我们访问域名时，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。
- Hosts地址：C:\Windows\System32\drivers\etc\hosts

1.2.3常见的DNS安全攻击有哪些?

- 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。
- DNS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。（针对面较广）
- 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。（针对面窄一点）
- DNS 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。

1.3 脚本语言

1.3.1常见的脚本语言类型有哪些?

- ASP PHP ASPX JSP JavaWeb PL PY CGI等

1.3.2不同脚本类型与安全漏洞的关系?

- 不同脚本可能爆发漏洞的可能性有所不同
- 不同脚本漏洞的存在点可能不同，因为不同语言的适用范围不同

1.4 后门

1.4.1什么是后门?

- 通常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。
- 在软件的开发阶段，程序员常常会在软件内创建后门程序以便可以修改程序设计中的缺陷。

1.4.2后门在安全测试中的实际意义?

- 可以更方便的链接到主机
- 在获取到玩主机权限的时候，后门可以充当命令控制台的角色

1.5 WEB

1.5.1WEB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 MssSQL Oracle SyBase DB2 PostSQL等

1.5.2为什么要从WEB层面为主为首?

- web使用的比较广
- web网站了漏洞相对较多
- web 作为跳板深入到其他资源相对容易

1.6 WEB相关安全漏洞

1. 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
2. WEB 中间件对应漏洞：未授权访问，变量覆盖...
3. WEB 数据库对应漏洞：弱口令，权限提升...
4. WEB 系统层对应漏洞：提权，远程代码执行
5. 其他第三方对应漏洞
6. APP 或 PC 应用结合类

资源

```
http://www.xyaz.cn
http://www.downcc.com/soft/11196.html
https://github.com/quasar/QuasarRAT/releases
```