网络安全 – 漏洞攻击

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

OS漏洞及攻防

Web漏洞及攻防

OS漏洞及攻防

Web漏洞及攻防

Win漏洞

XP的热键漏洞

Windows Redirector

资源管理器内存破坏漏洞

帮助支持中心接口欺骗

不安全的脚本

。。。

Win的防护

Windows的防护

- **系统补丁**
- **Internet连接防火墙**
- **支持多用户的加密文件系统**
- **改进的访问控制**
- **对智能卡的支持**
- **。。。**

Unix漏洞

处理畸形ELF二进制文件

- 拒绝服务攻击

Samba共享应用系统

- 获得Root用户权限

惠普的Tru64Unix (Ipsec,SSH)

- 迫使服务器离线

Win系统攻击实例 - 1

攻击web server+mysql

```
F:\cmd>mysql -u root -h www.target.net
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 3038 to server version:
3.23.21-beta
Type 'help;' or '\h' for help. Type '\c' to clear the
buffer
mysql〉
```

网关没有给MySQL账号root设置一个账号，可利用该漏洞，读取服务器文件

ASP (Active Server Page)

ASP就是Active Server Page的缩写。

当浏览器浏览ASP网页时，Web服务器就会根据请求生成相应的HTML代码然后再返回给浏览器,这样浏览器端看到的 就是动态生成的网页。

通过ASP，可能可以很方便地入侵web server、窃取服务器上的文件、捕获 web 数据库等系统的用户口令，甚至恶意删除服务器上的的文件。

Win系统攻击实例 - 2

```
Mysql> use test;create table cmd（str TEXT）;
Database changed
Query OK, 0 rows affected （0.05 sec）
```

获取IIS主目录的物理路径

```
Mysql> insert into cmd values（"asp代码"）;
```

插入ASP

入侵总结

黑客的攻击按如下六个步骤进行：

- **收集资料**
- **取得普通用户的权限**
- **远程登录**
- **取得超级用户的权限**
- **留下后门**
- **清除日志**

OS漏洞及攻防

Web漏洞及攻防

Web入侵

Web入侵就是利用Web的安全漏洞进行攻击，使Web服务器无法正常工作，甚至瘫痪，影响网站正常地为网络用户提供服务

以Web入侵作为跳板来进行其他形式的攻击，对网络系统造成更严重的破坏

网络管理员通常为了防止网络遭受入侵，就将可能导致攻击的端口全部关闭，但Web服务器的80端口必须打开，这样就给了黑客以可乘之机

Web的三种安全问题

Web的三种安全问题

- **服务器向公众提供了不应该提供的服务**
- **服务器把本应私有的数据放到了公开访问的区域**
- **服务器信赖了来自不可信赖数据源的数据**

Web安全问题的来源

Web安全问题的来源

- **管理员为了管理方便而设立远程管理功能**
- **为了方便用户使用而设立上传/下载机制**
- **由于疏忽而缺乏应有的安全检查**
- **为了省钱而使用不足够安全的软件和硬件**

常见Web安全问题

常见Web安全问题

- 物理路径泄露
- CGI源代码泄露
- 目录遍历
- 执行任意命令
- 缓冲区溢出
- 拒绝服务
- 。。。

CGI

CGI (Common Gateway Interface)

- **公共网关接口**
- **它在Web服务器上定义了Web客户请求与应答的一种方式**
- **是外部扩展应用程序与WWW服务器交互的一个标准接口**

CGI安全性

- **Web服务器的安全**
- **CGI语言的安全**

CGI的安全问题

- 暴露敏感或不敏感信息
- 缺省提供的某些正常服务未关闭
- 利用某些服务的漏洞执行命令
- 应用程序存在远程溢出
- 非通用CGI程序的编程漏洞

CGI的漏洞 1

配置错误

- **安装完CGI程序后没有删除安装脚本，这样攻击者就可能远程重置数据**

边界条件错误

- **C语言编写的CGI （缓冲区溢出）**

访问验证错误

- **安全的验证：账号和密码，Session认证**
- **不安全的验证：Userid ，Cookie**

CGI的漏洞 2

来源验证错误

- 利用CGI程序没有对文章的来源进行验证，从而不间断的发文章，最后导致服务器硬盘充满而挂起

输入验证错误

- 没有过滤“%20”造成的畸形注册
- 没有过滤“../”经常造成泄露系统文件
- 没有过滤“$”经常导致泄露网页中的敏感信息
- 没有过滤“;”经常导致执行任意系统指令
- 没有过滤“|”或“\t”经常导致文本文件攻击
- 没有过滤“’ ”和“#”经常导致SQL数据库攻击
- 没有过滤“<”和“>”导致的Cross-Site Scripting攻击

CGI的漏洞 3

异常情况处理失败

- 没有检查文件是否存在就直接打开设备文件导致拒绝服务，
- 没有检查文件是否存在就打开文件提取内容进行比较而绕过验证

策略错误

- 原始密码生成机制脆弱导致穷举密码导致在Cookie中明文存放账号密码导致敏感信息泄露
- 使用与CGI程序不同的扩展名存储敏感信息导致该文件被直接下载
- 丢失密码模块在确认用户身份之后直接让用户修改密码而不是把密码发到用户的注册信箱
- 登录时采用账号和加密后的密码进行认证导致攻击者不需要知道用户的原始密码就能够登录

CGI的漏洞 4

习惯问题

- 使用某些文本编辑器修改CGI程序时，经常会生成“.bak”文件，如果程序员编辑完后没有删除这些备份文件，则可能导致CGI源代码泄露
- 如果程序员总喜欢把一些敏感信息（如账号密码）放在CGI文件中的话，只要攻击者对该CGI文件有读权限（或者利用前面介绍的一些攻击方法）就可能导致敏感信息泄露

课后习题

1. 跳板的作用是什么?

2. 如何避免多个服务系统之间的连带关系?

3. 简述用ASP编写的网站的常见攻击方式有哪些?

4. 假如你现在要攻陷一个Windows server + IIS + ASP的网站，请描述一下你的初步想法、攻击步骤和策略

谢谢!