云安全技术与应用

- 日照职业技术学院
- 电子信息工程系
- 赵娜

项目三

安全实验环境搭建

目录

CONTENTS

01.

安装配置 CentOS7、Kali 系统

Linux系统

- CentOS
  - 属于RedHat派系，服务器主流操作系统。
  - 用作Web服务器
- Kali
  - 属于Debian派系，网络安全必备操作系统。
  - 用作攻击机

CentOS基本配置

- 配置远程连接
  - ifconfig查看IP，利用Xshell远程连接。
- 设置yum源
  - 清空原有yum源：rm -f /etc/yum.repos.d/*
  - 从阿里云下载yum源：

wget -O /etc/yum.repos.d/CentOS-Base.repo

https://mirrors.aliyun.com/repo/Centos-7.repo

CentOS基本配置

- 关闭防火墙
  - 停止运行服务：systemctl stop firewalld
  - 禁止开机自动运行：systemctl disable firewalld
- 关闭SElinux
  - 临时关闭：setenforce 0
  - 永久关闭：vim /etc/selinux/config，修改

    SELINUX=disabled

Kali基本配置

- 切换到root用户
  - 默认账号和密码：kali/kali
  - 为root设置密码：sudo passwd root
  - 切换到root：su – root

Kali基本配置

- 设置安装源
  - 修改配置文件：vim /etc/apt/sources.list
  - 添加阿里云为安装源：

    deb https://mirrors.aliyun.com/kali kali-rolling main non-free contrib

    deb-src https://mirrors.aliyun.com/kali kali-rolling main non-free contrib
  - 更新软件索引列表：apt-get update

Kali基本配置

- 设置中文界面
  - 安装中文字体： apt-get install xfonts-intl-chinese ttf-wqy-microhei
  - 设置系统语言：

    dpkg-reconfigure locales

    选择语言zh_CN.UTF-8
  - 重启系统： reboot

Kali基本配置

- 设置远程登录
  - 修改SSH配置文件：vim /etc/ssh/sshd_config

    将PermitRootLogin prohibit-password修改为

    PermitRootLogin yes
  - 启动服务：systemctl start ssh
  - 将SSH服务设为开机自动运行：systemctl enable ssh
  - 利用Xshell远程登录

云服务器

- 建议购买自己的云服务器
  - 阿里云
  - 腾讯云
  - 百度云
  - ……

02.

搭建LAMP（Web服务器套件）

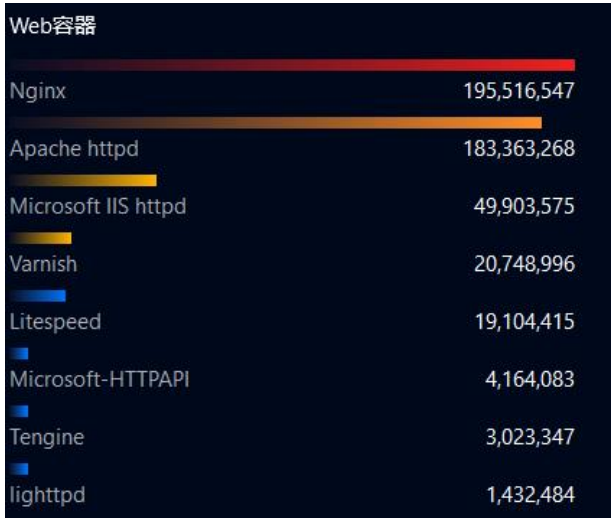
Web服务器

- Web服务器主要由以下四部分组成：
  - 操作系统、Web容器、脚本程序、数据库

- 操作系统
  - 主要是Linux和Windows Server
  - 目前绝大多数服务器都是采用的Linux系统，尤其是CentOS。

Web容器

- Web容器是用于提供WWW服务的服务程序
  - Apache和Nginx是目前应用最为广泛的Web容器，也是著名的开源软件。
  - IIS是Windows系统中默认的Web服务程序。



脚本语言

- Web容器只能接收客户端的请求，并将相应的HTML文档发送给客户端，本身并不具备执行脚本程序的能力。
- 在Web服务器上，还应安装脚本语言程序。
  - PHP、JSP、.NET。

数据库

- 常见组合
  - LAMP：Linux+Apache+PHP+MySQL
  - LNMP：Linux+Nginx+PHP+MySQL

- 软件安装的一般顺序
  - Linux→Apache→PHP→MySQL

安装LAMP

- 安装Apache：
  - # yum install httpd -y
  - # systemctl start httpd
  - # systemctl enable httpd
- 安装PHP：
  - # yum install php php-mysql -y
  - # systemctl restart httpd
- 安装MariaDB：
  - # yum install mariadb-server -y
  - # systemctl start mariadb
  - # systemctl enable mariadb
- 设置密码，登录MariaDB：
  - # mysqladmin -u root password "123"
  - # mysql -uroot –p123

装好Apache之后，就可以浏览器测试IP了

进入网站主目录 /var/www/html
创建一个文件index.php，写入代码：

```
<?php
        phpinfo();
?>
```

访问IP，测试php是否装成功。

测试PHP能否连接MariaDB

- 测试代码：

```
<?php
    $conn=mysqli_connect("127.0.0.1","root","123");
    if ($conn) {
            echo "success";
    }else{
            echo "fail";
    }
    mysqli_close($conn);
?>
```

03.

搭建网站：DVWA、WordPress

安装DVWA

- DVWA（Damn Vulnerable Web App）是用PHP+MySQL编写的Web安全实验平台。
  - 下载：（参考：https://blog.csdn.net/MRS_jianai/article/details/128112761
  - https://blog.csdn.net/qq_42620328/article/details/127313806）
  - 下载地址：https://github.com/digininja/DVWA/archive/master.zip
  - 解压： unzip DVWA-1.0.8.zip -d /var/www/html
  - 改名：mv /var/www/html/DVWA-1.0.8 /var/www/html/dvwa
- 修改配置文件：
  - # vim /var/www/html/dvwa/config/config.inc.php

```
$_DVWA = array();
$_DVWA[ 'db_server' ] = 'localhost';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = '123';
```

安装DVWA

- 默认账号
  - admin/password

安装WordPress

- WordPress是一款著名的用于搭建个人网站或博客的开源CMS
  - 下载：wget https://cn.wordpress.org/wordpress-5.1.13-zh_CN.zip
  - 解压：unzip wordpress-5.1.13-zh_CN.zip -d /var/www/html

- 创建数据库
  - 登录MySQL：mysql –uroot –p123
  - 创建数据库：create database wordpress;
  - 退出MySQL：exit

黑客攻击的目的

- 攻击网站
  - 获取网站里的敏感数据
  - 获取网站管理权限

- 攻击服务器
  - 获取Shell，获得普通用户权限，能够对服务器进行基本操作。
  - 提权，获得root权限，完全控制服务器。

黑客攻击的目的

- 攻击网站
  - 获取网站里的敏感数据
  - 获取网站管理权限

- 攻击服务器
  - 获取Shell，获得普通用户权限，能够对服务器进行基本操作。
  - 提权，获得root权限，完全控制服务器。

04.

Web基本概念

什么是Web?

- WWW（World Wide Web，万维网）服务，又称为Web服务
  - 互联网上使用最为广泛的服务，它的出现是互联网发展过程中的一个里程碑。
  - WWW服务的核心技术是超文本标记语言HTML和超文本传输协议HTTP。

前后端代码——Html

- HTML(Hyper Text Markup Language，超文本标记语言)是互联网的核心语言
  - HTML是网站中最常见到的代码。查看网页源码，所看到的主要是HTML代码。
  - 浏览器的主要功能就是对HTML页面中的标签进行解析，显示出我们所看到的内容。
  - HTML网页文件大都以“.htm”或“.html”作为文件名后缀。

前后端代码——Html

- HTML特点
  - 并非编程语言，而是标记语言。
  - 标记也称为标签，HTML标签通常成对出现，如 和 。
  - 每组标签都有相对应的功能，学习HTML，主要就是学习各种标签的用法。

```
<!DOCTYPE HTML>
<html>
    <head>
        <meta charset="utf-8">
        <title>这是一个HTML网页</title>
    </head>
    <body>
        <h1>这是一级标题</h1>
        <!-- 这是注释 -->
        <p>这是一个段落</p>
    </body>
</html>
```

前后端代码——Html常用标签

-
标签用于换行

```
<p>
To break<br />lines<br />in a<br />paragraph,<br />use the br tag.
</p>
```

To break
lines
in a
paragraph,
use the br tag.

前后端代码——Html常用标签

- <pre>标签用于原样输出指定的信息

```
<pre>
床前明月光，
疑是地上霜。
举头望明月，
低头思故乡。
</pre>
```

床前明月光，
疑是地上霜。
举头望明月，
低头思故乡。

前后端代码——Html常用标签

- <img>标签用于在网页中插入图片
- <img src="图片位置" alt="图片描述信息">
- src属性用于指定图片位置，
- alt属性用于指定图片描述信息

```
<p><img src="/images/1.jpg" alt="本地图片"></p>
```

前后端代码——Html常用标签

- <a>标签用于设置超链接

  文字描述

```
<a href="/test.html">test</a>
```

```
<a href="/test.html"><img src="/images/1.jpg"></a>
```

前后端代码——form表单

- form表单主要用于接收客户端输入的数据，并发送给服务器。
  - 用户登录页面就是典型的form表单
- 表单是一个整体，在表单中还包括很多元素。
  - 用户登录页面中用于输入用户名和密码的两个文本框以及login按钮都属于是表单元素

前后端代码——form表单典型代码

- 典型代码

```
<form action="UserLogin.php" method="post">
    <p>用户名：<input type="text" name="username"></p>
    <p>密  &nbsp码：<input type="password" name="password"></p>
    <p><input type="submit" name="submit" value="确定">   <input type="reset" value="重置"></p>
</form>
```

前后端代码——JavaScript简介

- JavaScript特点
  - JavaScript是对HTML功能上的扩展，JavaScript代码嵌入在HTML里。
  - 通过JavaScript可以将部分功能在客户端实现，从而减轻服务器端的压力。
  - JavaScript代码的开始标记是<script>，结束标记是</script>。

```
<!doctype html>
<html lang="zh-CN">
<head>
    <meta charset="UTF-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <link rel="profile" href="https://gmpg.org/xfn/11" />
    <title>我的测试站点 &#8211; 又一个WordPress站点</title>
<link rel='dns-prefetch' href='//s.w.org' />
<link rel="alternate" type="application/rss+xml" title="我的测试站点 &raquo; Feed" href="http://192.168.80.50/wordpress/?feed=rss2" />
<link rel="alternate" type="application/rss+xml" title="我的测试站点 &raquo; 评论Feed" href="http://192.168.80.50/wordpress/?feed=comments-rss2" />
        <script type="text/javascript">
            window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/11.2.0\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/ima
            !function(e,a,t){var n,r,o,i=a.createElement("canvas"),p=i.getContext&&i.getContext("2d");function s(e,t){var a=String.fromCharCode;p.clearR
        </script>
```

前后端代码——查看网页源码

- 查看网页源码主要是查看HTML和JavaScript代码。
  - 查看源码通常是解Web题的第一步。有的flag直接就藏在源码中，有些题目则是在源码中给出提示和线索。
  - 推荐使用Firefox浏览器。

- CTF例题
  - BugKu-Web-滑稽
  - 攻防世界-Web-view_source

前后端代码——前端代码

- HTML和JavaScript都是在客户端浏览器上执行，因而称之为前端代码。
  - 前端代码可以修改，并影响执行效果。
  - 修改前端代码需要借助于浏览器中的开发者工具。
  - 大多数浏览器都支持通过F12按键或是“查看元素”功能调出开发者工具。

- CTF例题
  - BugKu-Web-计算器
  - 攻防世界-Web- disabled_button

前后端代码——后端代码

- 后端代码在服务器上执行，并将执行结果以HTML形式发给客户端。
  - 在客户端只能看到后端代码的执行结果，无法看到源码。
  - 后端代码包含了网站的运行逻辑，属于敏感信息，不能泄露。
  - 典型的后端代码：PHP、JSP、.NET。

```php
<?php
        phpinfo();
?>
```

前后端代码——PHP代码规范

- PHP代码规范
  - 开始标记<?php，结束标记?>，每行PHP代码必须以分号表示结束。
  - PHP中的变量必须以“$”符号开头，变量名称对大小写敏感。
  - echo语句用于输出，双引号中的变量会被解析执行，点号“.”用于连接字符串。
  - 在PHP中可以输出HTML标签，在客户端浏览器以HTML代码的形式执行。

```php
<?php
    $a=2;
    $b=3;
    $c=$a+$b;
    echo "$a+$b=".$c";
?>
```

```php
echo "<h1>$a+$b=".$c</h1>";
```

前后端代码——PHP注释

- 单行注释：//和#
- 多行注释：/*……*/

```
// 这是单行注释

# 这也是单行注释

/*
这是多行注释块
它横跨了
多行
*/
```

前后端代码——PHP语句

- 选择语句
- for循环
- while循环

前后端代码——Web资源

- Web资源
  - 在HTTP请求和响应的过程中，客户端所请求的以及服务端所返回的内容称为Web资源。
  - Web资源总体上分为静态资源和动态资源两类。

前后端代码——静态资源

- 客户端访问静态资源时，服务器可直接将这些资源发送给客户端。
  - 文件名后缀为“.htm”或“.html”的各类静态网页文件
  - 文件名后缀为“.jpg”、“jpeg”、“.gif”、“.png”的各类图片文件
  - 各类文本文件和压缩文件
  - 文件名后缀为“.mp3”、“.avi”的各类音频和视频文件
  - 文件名后缀为“.css”、“.js”的各类前端脚本文件
  - 所有的静态资源都可以直接下载

前后端代码——动态资源

- 动态资源通常是指用编程语言开发的脚本程序文件。
  - 脚本程序先在服务器端运行，然后再将得到的结果以静态页面的形式发给客户端。
  - 在客户端无法看到脚本程序的源码，也无法下载脚本程序。
  - 动态资源可以根据客户端请求的不同而向客户端发送动态变化的内容，从而实现客户端与服务端的交互。