# 使用Nikto漏洞扫描工具检测网站安全

一、扫面主机IP端口（举例192.168.0.1）

1.默认扫描端口为80

-h（host）

nikto -h 192.168.0.1

2.自定义扫描端口（443）

-p（port）

nikto -h 192.168.0.1 -p 443

3.同时扫描多端口（范围、多个）（80、88、443）

nikto -h 192.168.0.1 -p 80,88,443

4.如果运行nikto的二主机通过HTTP proxy来访问互联网的，可以使用代理扫描

-u（useproxy）

nikto -h 192.168.0.1 -p80 -u

#### 二、其他命令

-Cgidirs+扫描CGI目录

-config+使用指定的config文件代替安装在本地的config.txt文件

-Display+控制nikto输出的显示

1直接显示信息

2显示的cookies信息

3显示所有200/OK的反应

4显示认证请求的URLs

D Debug输出

E显示所有的HTTP错误

P显示STDOUT的进度

S清除IP地址和主机名输出

V冗长的输出

-dbcheck选择语法错误的扫描数据库

-evasion使用LibWhisker中对IDS的躲避技术，可使用一下几种类型：

1随机URL编码（非UTF-8方式）

2自选择路径（/./）

3虚假的请求结束

4长的URL请求

5参数隐藏

6使用TAB作为命令的分隔符

7更改URL情况

8使用Windows路径分隔符\替换/

A使用回车（0x0d）作为请求间隔

B使用二进制（0x0b）作为请求间隔

-Format+指定检测报告输出文件的格式，默认是txt文件格式

csv/htm/nbe/sql/txt/xml

-help功能说明

-host+目标主机，主机名、IP地址、主机列表文件

-404code忽略这些HTTP代码作为负面响应（一直）。格式“302,301”

404string忽略这个字符串在响应体中作为负响应（一直）。可以是正则表达式

-id+密码和ID对于授权的HTTP认证。格式：-id：password

-key+客户端认证密钥文件

-list-plugins列出所有有效的插件，执行任何测试

-maxtime最大测试时长

-mutate+变化猜测技术

1使用所有的root目录测试所有文件

2猜测密码文件名字

3列举Apache的用户名字（/~user）

4列举cgiwrap的用户名字（/cgi-bin/cgiwrap/~user）

5暴力尝试子域名（假设主机名是父域）

6尝试猜测提供目录文件的目录名

-output+输出文件

-findonly仅用来发现HTTP和HTTPS端口，而不执行检测规则

-nolookup不执行主机名查找

-output报告输出指定地点

-Pause每次操作的延迟时间

-port扫描端口指定。格式：-p 端口

-Plugins+客户端证书文件

-ssl强制在端口上使用SSL模式

-Single执行单个对目标服务的请求操作。

-timeout每个请求的超时时间，默认为10秒

-Tuning+选项控制Nikto使用不同的方式来扫描目标。

0文件上传

1日志文件

2默认的文件

3信息泄漏

4注射（XSS/Script/HTML）

5远程文件检索（Web 目录中）

6拒绝服务

7远程文件检索（服务器）

8代码执行－远程shell

9 SQL注入

0文件上传

a认证绕过

b软件关联

c远程数据关联

d web服务

e管理主控台

x反向连接选项

-useproxy使用指定代理扫描

-update更新插件和数据库

例子：使用Nikto扫描目标主机10.0.0.12的phpwind论坛网站。

Perl nikto.pl –h 10.0.0.12 –o test.txt

查看test.txt文件，如下图所示：

<img class="fit-image" big(this)"="" alt="" src="http://netsecurity.51cto.com/files/uploadimg/20071212/1103040.jpg" border="0" style="padding: 0px; margin: 0px; vertical-align: top; border: none;">

通过上面的扫描结果，我们可以发现这个Phpwind论坛网站，是在windows操作系统上，使用Apache/2.2.4版本，Php/5.2.0版本，以及系统默认的配置文件和路径等。

综上所述，Nikto工具可以帮助我们对Web的安全进行审计，及时发现网站存在的安全漏洞，对网站的安全做进一步的扫描评估。