

Nmap 和图片报告

2012-06-18 08:18:55 By admin

前言

讨厌命令行，web安全性分析/漏洞利用一直是风险评估/渗透测试过程中一个重要的环节。甚至有时是外网渗透测试过程中唯一的突破口

随着互联网的发展，金融网上交易、政府电子政务、企业门户网站、社区论坛、电子商务等各类基于HTML文件格式的信息共享平台(WEB应用系统)越发完善，深入到人们生活中的点点滴滴。然而WEB应用共享平台为我们的生活带来便利的同时，也面临着前所未有的挑战：WEB应用系统直接面向Internet，以WEB应用系统为跳板入侵服务器甚至控制整个内网系统的攻击行为已成为最普遍的攻击手段。据Gartner的最新调查，目前75%以上的攻击行为都基于WEB应用层面而非网络层面;同时数据显示，三分之二的WEB站点都相当脆弱，易受攻击。

渗透测试对于我等小菜几乎是用WEB安全漏洞进行，每次进行渗透测试几乎是用一推扫描工具狂草泥马，但是这些扫描工具都不能给HTTP服务来个快照，我们只能看到 80 Open 8080 Open,不用浏览器访问很难知道这个开放的HTTP服务器到底是什么，我们能让他的扫描报告生成图形模式吗？能的

Nmap的脚本引擎（NSE），他几乎可以帮你干任何事，NSE是基于Lua，他可以帮你破解WORDPRESS，帮你扫描漏洞，帮你扫描开放的服务，甚至能进行一些简单的溢出攻击

什么是wkhtmltoimage？能将网页转换为图片

，某位大牛写了一个wkhtmltoimage的插件，当这两者结合，碰撞出了爱情的火花

安装wkhtmltoimage

```
root@Dis9Team:~# wget http://wkhtmltopdf.googlecode.com/files/wkhtmltoimage-0.11.0_rc1-static-i386.tar.bz2
```

```
--2012-06-18 00:52:06-- http://wkhtmltopdf.googlecode.com/files/wkhtmltoimage-0.11.0_rc1-static-i386.tar.bz2
```

```
Resolving wkhtmltopdf.googlecode.com... 74.125.31.82, 2404:6800:4008:c01::52
```

```
Connecting to wkhtmltopdf.googlecode.com|74.125.31.82|:80... connected.
```

```
HTTP request sent, awaiting response... 200 OK
```

```
Length: 11393207 (11M) [application/octet-stream]
```

```
Saving to: `wkhtmltoimage-0.11.0_rc1-static-i386.tar.bz2'
```

```
100%[=====>] 11,393,207 486K/s in 26s
```

```
2012-06-18 00:52:32 (433 KB/s) - `wkhtmltoimage-0.11.0_rc1-static-i386.tar.bz2' saved [11393207/11393207]
```

```
root@Dis9Team:~# tar -jxvf wkhtmltoimage-0.11.0_rc1-static-i386.tar.bz2
```

```
wkhtmltoimage-i386
```

```
root@Dis9Team:~# cp wkhtmltoimage-i386 /usr/local/bin/
```

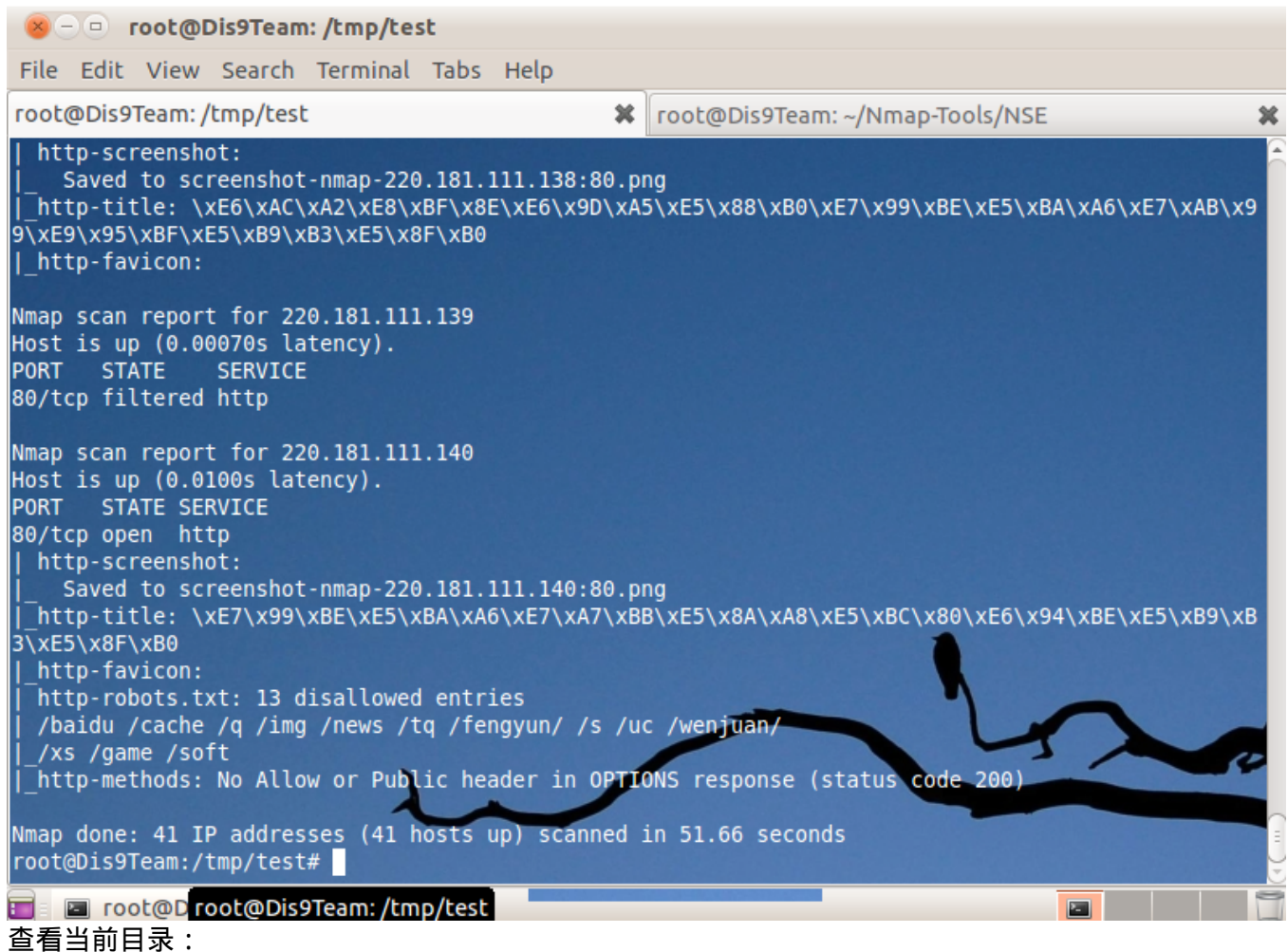
Nmap模块

```
root@Dis9Team:~# git clone git://github.com/SpiderLabs/Nmap-Tools.git
Cloning into Nmap-Tools...
remote: Counting objects: 15, done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 15 (delta 3), reused 15 (delta 3)
Receiving objects: 100% (15/15), done.
Resolving deltas: 100% (3/3), done.
root@Dis9Team:~# cd Nmap-Tools/NSE/
root@Dis9Team:~/Nmap-Tools/NSE# ls
http-screenshot.nse  README.SpiderLabs
root@Dis9Team:~/Nmap-Tools/NSE# cp http-screenshot.nse /pen/nmap/share/nmap/scripts/
root@Dis9Team:~/Nmap-Tools/NSE# nmap --script-updatedb
```

```
Starting Nmap 5.51 ( http://nmap.org ) at 2012-06-18 01:06 PDT
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.41 seconds
root@Dis9Team:~/Nmap-Tools/NSE#
```

进行测试

```
root@Dis9Team:~/Nmap-Tools/NSE# mkdir /tmp/test
root@Dis9Team:~/Nmap-Tools/NSE# cd /tmp/test/
root@Dis9Team:/tmp/test# nmap -sS --script=default,http-screenshot 220.181.111.100-140 -p 80
```



```
root@Dis9Team: /tmp/test
File Edit View Search Terminal Tabs Help

root@Dis9Team: /tmp/test x root@Dis9Team: ~/Nmap-Tools/NSE x

| http-screenshot:
|   Saved to screenshot-nmap-220.181.111.138:80.png
|_ http-title: \xE6\xAC\xA2\xE8\xBF\x8E\xE6\x9D\xA5\xE5\x88\xB0\xE7\x99\xBE\xE5\xBA\xA6\xE7\xAB\x9
9\xE9\x95\xBF\xE5\xB9\xB3\xE5\x8F\xB0
|_ http-favicon:

Nmap scan report for 220.181.111.139
Host is up (0.00070s latency).
PORT      STATE      SERVICE
80/tcp    filtered  http

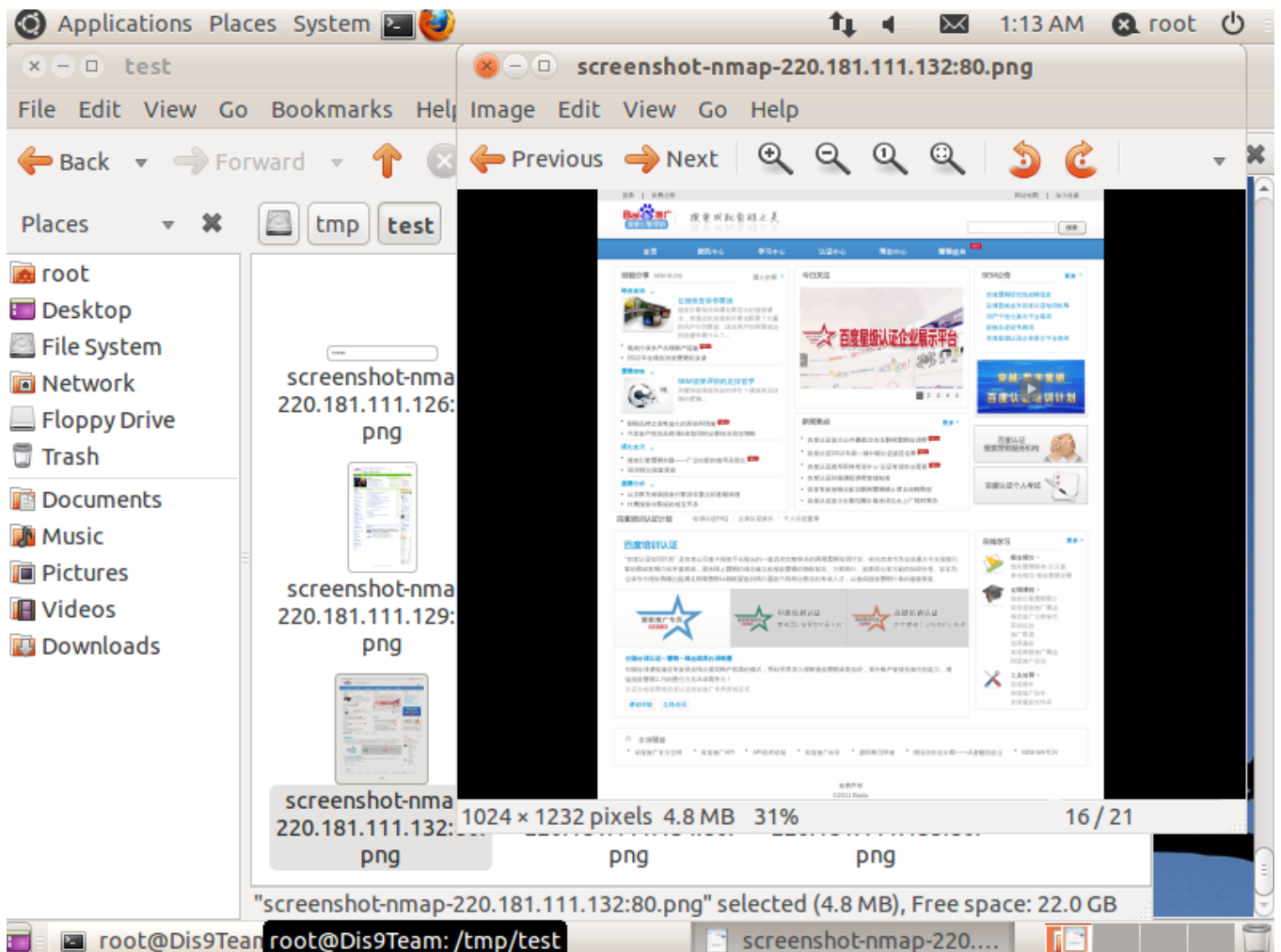
Nmap scan report for 220.181.111.140
Host is up (0.0100s latency).
PORT      STATE      SERVICE
80/tcp    open       http
| http-screenshot:
|   Saved to screenshot-nmap-220.181.111.140:80.png
|_ http-title: \xE7\x99\xBE\xE5\xBA\xA6\xE7\xA7\xBB\xE5\x8A\xA8\xE5\xBC\x80\xE6\x94\xBE\xE5\xB9\xB
3\xE5\x8F\xB0
|_ http-favicon:
| http-robots.txt: 13 disallowed entries
| /baidu /cache /q /img /news /tq /fengyun/ /s /uc /wenjuan/
| /xs /game /soft
|_ http-methods: No Allow or Public header in OPTIONS response (status code 200)

Nmap done: 41 IP addresses (41 hosts up) scanned in 51.66 seconds
root@Dis9Team: /tmp/test#
```

查看当前目录：

```
root@Dis9Team: /tmp/test# ls
screenshot-nmap-220.181.111.108:80.png screenshot-nmap-220.181.111.128:80.png
screenshot-nmap-220.181.111.111:80.png screenshot-nmap-220.181.111.129:80.png
screenshot-nmap-220.181.111.112:80.png screenshot-nmap-220.181.111.130:80.png
screenshot-nmap-220.181.111.115:80.png screenshot-nmap-220.181.111.131:80.png
screenshot-nmap-220.181.111.117:80.png screenshot-nmap-220.181.111.132:80.png
screenshot-nmap-220.181.111.120:80.png screenshot-nmap-220.181.111.134:80.png
screenshot-nmap-220.181.111.121:80.png screenshot-nmap-220.181.111.135:80.png
screenshot-nmap-220.181.111.122:80.png screenshot-nmap-220.181.111.137:80.png
screenshot-nmap-220.181.111.124:80.png screenshot-nmap-220.181.111.138:80.png
screenshot-nmap-220.181.111.126:80.png screenshot-nmap-220.181.111.140:80.png
screenshot-nmap-220.181.111.127:80.png
root@Dis9Team: /tmp/test#
```

是的 多了很多图片 围观下：



这些都是扫描截取的网站截图

合并脚本

当然这么浏览不方便 所以又了一个脚本

```
#!/bin/bash
printf "
" > preview.html
ls -l *.png | awk -F ':' '{ print $1":"$2"\n
"}' >> preview.html
printf "" >> preview.html
```

当运行他后 多了一个HTML文档 打开

```
root@Dis9Team:/tmp/test# firefox preview.html
```

方便阅读的结果出来鸟



screenshot-nmap-220.181.111.134:80.png



screenshot-nmap-220.181.111.135:80.png



screenshot-nmap-220.181.111.137:80.png

screenshot-nmap-220.181.111.138:80.png



参考

[123](#)

版权声明：

本站遵循 [署名-非商业性使用-相同方式共享 2.5](#) 共享协议.

转载请注明转自Penattack.org并标明URL.

本文链接：<http://penattack.org/?p=3798>