攻防世界-Misc-新手练习记录



rectural: 下文件系统, strings查看一下 rectural: # strings linux | grep flag .flag.txt.swp flag.txtt.swx ~root/Desktop/file/07avZhikg flag.txtt.swp flag.txtt.swp flag.txtt.swp flag.txtt.swp flag.txtt.swx

flag应该就在这个flag.txt中了,把这个文件系统挂载到Linux上:

mount linux /mnt

挂上去之后看一下/mnt/下的文件,用命令ls -al /mnt/,可以看到上面strings查找到的O7avZhikgKgbF,flag.txt 就在这个目录里,得到文件内容为:ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=,base64 解码即可。

give_you_flag



这个二维码少了三个角的定位符,没有定位符肯定是扫不出来东西的,手动画上定位符:



扫描得flag。

```
是一个pdf文件,里面有一个图片,用pdf编辑器把图片挪开,flag在图片后面。
```

stegano

pdf文件,打开许多文字,linux中查看pdf信息:使用命令pdfinfo

<pre>root@kali:~# pdi</pre>	finfo stegano50.pdf
Title:	polar bear during a snow storm
Subject:	< tr AB >
Keywords:	<pre>Could this be the flag? : Tm9wZSAsIG5vdCBoZXJlIDspCg==</pre>
Author:	KeiDii
Creator:	LaTeX /o/
Producer:	find mr.morse text
CreationDate:	Fri Mar 14 05:33:50 2014 CST
ModDate:	Fri Mar 14 05:33:50 2014 CST
Tagged:	no
UserProperties:	no
Suspects:	no
Form:	none
JavaScript:	no
Pages:	
Encrypted:	no
Page size:	595.276 x 841.89 pts (A4)
Page rot:	
File size:	38742 bytes
Optimized:	no https://blog.codp.pot/cz. Colob
PDF version:	1.5 https://biog.csdn.hei/22_Caleb

有个base64码,然而解码是:Nope,nothere;) 用pdftotext命令提取一下文件内容:

```
e!
ler
οF
la
gН
e!
Ν
Close - but still not here !
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id
laoreet magna
volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus
rutrum. Nunc diam
orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum
sit amet at orci.
Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis
adipiscing dui. Duis eget
ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum,
leo nisi porttitor
massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit
porta ipsum. Donec sed nibh
egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet
vulputate. Aenean quis tempor
orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet,
consectetur adipiscing
elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu
porttitor egestas.
Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctoreizz Calab
vehicula. interdum ut mi.
```

同样也是没什么线索,火狐的开发者工具pdf.js排上用场了,用火狐打开之后,控制台输入: document.documentElement.textContent,然后得到:

这一串AB字符串,把AB分别转成.-,得到摩斯密码,解码得flag。

SimpleRAR

参考https://blog.csdn.net/zz Caleb/article/details/88891524

坚持60s

一个java做的游戏,游戏大师可以试试玩着过,既然是程序会给出flag,那么flag就在阿代码中了,用java反编译 工具反编译,在文件中可以找到PlaneGameFrame.class中找到flag(大括号中base64需要解码)。

```
switch (period / 10)
1
case 0:
 printInfo(g, "真.头顶一片青青草原", 50, 150, 300);
 break;
case 1:
 printInfo(g, "这东西你也要抢着带? ", 50, 150, 300);
 break:
case 2:
 printInfo(g, "如果梦想有颜色,那一定是原谅色", 40, 30, 300);
 break;
case 3:
 printInfo(g, "哟, 炊事班长呀兄弟", 50, 150, 300);
 break;
case 4:
 printInfo(g, "加油你就是下一个老王", 50, 150, 300);
 break;
case 5:
 printInfo(g, "如果撑过一分钟我岂不是很没面子", 40, 30, 300);
 break;
case 6:
             "flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}", 50, 150, 300);
 printInfo(g,
}
```

gif

掀桌子

一串密文:

c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e

解密方法,两个一位,16进制转10进制,然后减去128再转成字符即可:

```
string = "c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e
flag = ''
for i in range(0,len(string), 2):
    s = "0x" + string[i] + string[i+1]
    flag += chr(int(s, 16) - 128)
print(flag)
```

如来十三掌

真是要念经啊:

夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數著奢集遠俱老竟 寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙罰娑是怯遠得呐數罰輸 哆遠薩得槃漫夢盧皤亦醯呐娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙 楞缽三死怯摩大蘇者數一遮

与佛论禅: http://www.keyfc.net/bbs/tools/tudoucode.aspx

得到base64码: MzkuM3gvMUAwnzuvn3cgozMIMTuvqzAenJchMUAeqzWenzEmLJW9

但是要先进行ROT13然后再base64解码:

flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

base64stego

参考: https://blog.csdn.net/zz Caleb/article/details/89298335

功夫再高也怕菜刀

foremost分解出来一个加密的压缩包,里面是flag.txt文件,不是伪加密。

wireshark打开文件,分组字节流查找flag.txt:

	应用显示过漂器 … <ct< th=""><th>r1-/></th><th></th><th></th><th></th><th></th><th></th><th>表达式…</th><th>+</th></ct<>	r1-/>						表达式…	+
	分组字节流 ∨	宽窄 ~	□ 区分大小写	字符串 ~	flag. txt		查找	取消	
N,	o. Time	Source	Destin	nation	Protocol	Length Info			^
	1 0.0000000	00 219.216.128.	25 192.1	168.25.128	TCP	2814 80 → 58418 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=2760			
	2 0.0000536	37 192.168.25.1	28 219.2	216.128.25	TCP	54 58418 → 80 [ACK] Seq=1 Ack=2761 Win=64240 Len=0			

查找到第1150个包时,追踪流看到:

🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 7) · 6666.pcapng Х ~ POST /upload/1.php HTTP/1.1 User-Agent: Java/1.8.0_151 Host: 192.168.43.83 Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2 Connection: keep-alive Content-type: application/x-www-form-urlencoded Content-Length: 204999 aa=@eval. (base64_decode(\$_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3 F1b3Rlc19ydW50aW1lKDAp02VjaG8oIi0%2BfCIp0zskZj1iYXNlNjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JGM9JF9QT1NUWyJ6MiJd0yRjPXN0cl9yZXBsYW NlKCJcciIsIiIsJGMpOyRjPXN0cl9yZXBsYWNlKCJcbiIsIiIsJGMpOyRidWY9IiI7Zm9yKCRpPTA7JGk8c3RybGVuKCRjKTskaSs9MikkYnVmLj11cmxkZWNv ZGUOIIUILNN1YnN0cigkYywkaSwyKSk7ZWNobyhAZndyaXRlKGZvcGVuKCRmLCJ3IiksJGJ1Zik%2FIjEiOIIwIik7O2VjaG8oInw8LSIpO2RpZSgpOw%3D%3D 03020403050504040000017D01020300041105122131410613516107227114328191A1082342B1C11552D1F02433627282090A161718191A2526272829 2A3435363738393A43445464748494A535455565758595A636465666768696A737475767778797A838485868788898A92939495969798999AA2A3A4A5 A6A7A8A9AAB2B3B4B5B6B7B8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE1E2E3E4E5E6E7E8E9EAF1F2F3F4F5F6F7F8F9FAFFC4001F0100030101 1322328108144291A1B1C109233352F0156272D10A162434F125F11718191A262728292A35363738393A434445464748494A535455565758595A636465 666768696A737475767778797A82838485868788898A92939495969798999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B7B8B9BAC2C3C4C5C6C7C8C9CAD2D3D4 0056C4310192E7D0CC40EFFC30478E3B0DFF00FD8F352DA3DBB0AF0769F2C1FF00964839699CF3866C9C11CF719E33AD6F1B7C840EB930AB71C672D732 7B0C1D99EC0632179FF49A8C75F376FF002FB9DFAD9BE65D66EDFE56D79EFADBB3D9AB5BE4AC95FB69D5455EDC28724C9C703CD238D89FC30A1F523AE3 D4F6539D88632E4EE013080CA57FE58C5FC31A7FD34933F377E7DCD54B78F714DA0B00711038F9DC7DF9DFFD95E703FA6EAD98101D8A83702FF20FF9ED 3779187FCF34391CF5F539AF568C36EFDF7BAD36F5BBDBBE9F146DE3D79F4DDAFBAFA2F93D1EFA2B35B4657B90A6428036314F7C5BC1F967CC7DDCF739 1D0B1C6CDBA6D0BB70A4292B9FF963177918FF00CF47E3033B88C6324A8AAB020551D24F9B1EF7336781D4131A13C738C7BB606BDBC4064B82FF0030DF 8EB34BD5635C7F021C671DBA0C9435EA528EDE56FF0087D3F357B745A42FE4566B5F3EFADB656B3F5B5B4ECDABD465BB78CFC85540620B421B811A1FBD 7327FB47036F4F5F47DD4AD7B78F732141F2AFFA856FF73FBCB993B0C6D2573C63D81354F14C96DDF32FF5F39971FBC906365B45D72A300311C71F8A2B 6A353921B19E3CE65FE151F72DA3C74E061B6F4C73F74E7D6A11DB4ED7B697DBEE4ADD3E1B69750478D5A5ABD6FA7E76F4BEEBD6FAD9CED1B70A9F9047 F30DC7C956E3CD9070F3B8FEEA9FBBBBD30790D5A70C61400079997C2E7ADCCFD0B9C9E638B2703EEFA9059B15E24DBB830D8DB479C47FCB284E36C080 E7E77380D9FA1CE18D694319272C446760DDD48B780F0101EF2CB9C63A9CF62C71D96D52D36DBB256F5B7CF6B59E91A89F0DDEBAE8DAEFEF6D6775BEFB ADEE74RDE476R31464796CR487191D4DCDC765E689339E43D74304D2452C4863R81606661EE2D45EE18131D634E99E871C7E05578D1890061095C8E9EE 19 套户端 分组,0 服务器 分组,0 turn(s)

整个对话(206 kB)	\sim	显示和保存数据为 ASCII 🛛 🗸					流 7 🌻
查找:							查找下一个(N)
		滤掉	此流 打日	D Save as…	返回	Close	Help _{aleb}

📕 Wireshark · 追踪 TCP 流 (tcp.stream eq 7) · 6666.pcapng				-		×	
Keep-Alive: timeout=5, max=100						^	
Content-Type: text/html; charset=UTF-8							
-> 1 <-POST /upload/1.php HTTP/1.1							
Host: 192.168.43.83							
Accept: text/html, image/gif, image/jpeg, *;	=.2, */*; q=.2						
Connection: keep-alive							
Content-Length: 723	u						
22-00421							
<pre>(base64 decode(\$ POST[action]));&action=QGlua</pre>	9zZXQoImRpc3BsYXlfZX	Jyb3JzIiwiMCIpO0Bz	ZXRfdGltZV9saW1pdCgwKTtA	c2V0X2	1hZ2ljX	(3	
F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskR	1iYXNlNjRfZGVjb2RlKC	RfUE9TVFsiejEiXSk7	JEY9QG9wZW5kaXIoJEQpO2lm	KCRGPT:	10VUxMK	<mark>cx</mark>	
tlY2hvKCJFUlJPUjovLyBQYXRoIE5vdCBGb3VuZCBPciBu	byBQZXJtaXNzaW9uISIp	031lbHNleyRNPU5VTE	W7JEW9TlVMTDt3aGlsZSgkTj	1AcmVh2	ZGRpcig	<u>zk</u>	
ROKSwxMCw4KSwtNCk7JFI9Ilx0Ii4kVC4iXHOiLkBmaWx	c2l6ZSgkUCkuIlx0Ii4k	RS4iCiI7aWYoOGlzX2	2RpcigkUCkpJE0uPSROLiIvIi	4kUitl	OHNLICF	RM	
LjØkTi4kUjt9ZWNobyAkTS4kTDtAY2xvc2VkaXIoJEYPO	07ZWNobygifDwtIik7ZG	llKCk7&z1=RDpcd2Ft	cDY0XHd3d1x1cGxvYWRcHTTP	/1.1 20	30 OK		
Date: Fri, 08 Dec 2017 11:42:11 GMT							
Server: Apache/2.4.23 (Win64) PHP/5.6.25							
Content-Length: 221							
Keep-Alive: timeout=5, max=99							
Connection: Keep-Alive							
Content-Type: text/html; charset=UTF-8							
-> ./ 2017-12-08 11:42:11 0 0777							
/ 2017-12 08 11:39:10 4096 0777							
1.php 201-12-08 11:33:16 33 0666							
6666.jpg 2017-12-08 11:42:11 10222	0666						
hello.zin 2017-12-08 09:32:36 224	0666						
<pre></pre>	0000						
						~	
が出 1150-53 条/1% が出,2 減み線 が出,3 turn(s). 点面透痒。 整个对话 (206 kB)	显示和保存数据为 ASCII	~			法	7	
查找·	TENNEDKITXXIX/9 HOOTI				がし	· ▼	
		油指山法 打印		 			
		4651年1467元 1111	bave as… 巡回	CTO26	niner/#el	Baleb	

再回过头来看看16进制码的头和尾,发现就是一个图片,把这个图片搞出来:



