西普实验吧密码学题目--一个img文件

原创

Neil-Yale ● 于 2017-03-18 21:45:10 发布 ● 4455 ◆ 收藏 2 文章标签: <u>密码学 数据 CTF 软件 硬盘</u> 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/yalecaltech/article/details/63291031</u> 版权 本来是准备把同种类型的题目只发一篇博客的,但是有些题目确实有些复杂,所以单独拿出来写Write Up. 题目连接: <u>http://www.shiyanbar.com/ctf/60</u> 下载来是一个.img格式的文件,img格式是镜像的一种。可以通过制作数据光盘或者使用虚拟光驱(如 WinMount)安装IMG数据文件。 题目的hint为恢复数据,故想到使用diskgenius。 打开软件后-》硬盘-》打开虚拟硬盘文件-》选择data.img 选择data.img(383M)这个虚拟硬盘文件-》恢复文件 效果如图

🕞 DiskGenius V4.9.2.371

文件(F) 硬盘(D) 分区(P) 工具(T) 查看(V) 帮助(H)

保存更改 搜索分区 恢复文件 快速分区	○ A A A A A A A A A A A A A A A A A A A														
× 《 》 硬盘 1	空闲 383.6MB														
接口:File 型号:Disk Image 容里:38 ●●● 主分区(0) ●●● 主分区(2) ●●● 主分区(2) ●●● 大分区(2) ●●● 大分区(次夏文件) ●●● 大分区(恢夏文件) ●●● 大分区(次夏文件) ●●●● 大分区(次夏文件) ●●●● 大台(大会) ●●●● 大台(大会) ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	6010 柱面数:48 磁头数:255 每道扇区数:63 总扇区数:785626 ●00(23 ★ A**: ● (*.jpg:*.bmp) ● 名称 大小 文件类型 ● 200000.zip 226 B 好压 ZIP ●00077F04	ch													

通过winhex等十六进制软件查看或者直接在.zip文件上或者其他任何方式都可以发现两个文件内容完全一样。随机右击保存一个 到桌面上待会儿会用到。 使用linux(我这里使用kali) apt-get install aeskeyfind 命令安装aeskeyfind. 将下载的data.img拖入kali中,输入aeskeyfind '/root/桌面/data.img'(路径按照自己的实际情况写) 即可得出结果(还没完呢) 如图所示

root@kali: # aeskeyfind data.img image open failed: No such file or directory root@kali: # aeskeyfind '/root/桌面/data.img' 3ae383e2163dd44270284f1554d9be8d 3ae383e2163dd44270284f1554d9be8d cda2bdc8f20c46db216c0a616cd11e11 Keyfind progress: 100%

有三个结果,分别尝试,此处需要用到在线AES解密网站,我推荐http://aes.online-domain-tools.com/ 各选项注意按照下图所示进行选择,即可得到flag

AES – Symmetric Ciphers Online

Check all your site's rankings in 640+ search engines																													
Rank	Rank Tracker WWW.your-site.com															Check													
Input type:	File																												
File:	data_encrypted																			В	row	se							
Function:	4	AES																											
Mode:	E	ECB (electronic codebook)																											
Key: (hex)	3	3ae383e2163dd44270284f1554d9be8d																											
○ Plaintext																													
	> Encrypt! > Decrypt!																				I		S						
																													_
File was uploaded.																													
Decrypted text:																													
00000000	66	6c	61	67	7b	32	34	35	64	37	33	34	62	35	35	39		f	1	a	g {	2	4	5 (17	3	4 b	5	59
00000010	63	36	62	30	38	34	62	37	65	63	62	34	30	35	39	36		с	6	b	0 8	4	Ь	7	e c	Ь	4 0	5	96
00000020 [Download as	30 a bir	35 nary	35 file] [32 ?]	34	33	65	38	61	66	64	64	32	7d ht	00 tp:	00	b1	og.	5 C 3	sd	24 n.	3 ne	et/	8 i ya	a f	d ec:	d 2 al	} tec	b active

忘记说了,最后一张图File:选择的是之前我们保存在桌面的.zip文件解压后的文件即data_encrypted.而input type默认是Text,注意 需要选择File