100 Forensics / Wi Will H4CK YOU!!

Description

Wifi Security Standards have been increased a lot in recent times.

But are they secure enough??? Get the password for our Wifi Network "encryptCTF"

Submit flag as encryptCTF{</password/>} captured.cap

Author:@mostwanted002

Files provided

• encryptCTFWPA.cap

Solution

This challenge is similar to <u>It's a WrEP</u> challenge. The only difference is that it is using the WPA protocol instead of the WEP protocol.

Using aircrack-ng again and waiting for a long time, give us the password.

\$ aircrack-ng -a 2 -w rockyou.txt encryptCTFWPA.cap

We pass in a wordlist (rockyou.txt in this case) and picking the network to crack and waiting for quite some time, it outputs the password ThanckYou.

encryptCTF{ThanckYou}

恶臭的数据包

题目

野兽前辈想玩游戏,但是hacker妨碍了他连上无线网,前辈发出了无奈的吼声。

题目存档: <u>恶臭的数据包.7z</u>

解决方案

解压得到一个cap流量包,Wireshark打开看看统计信息:

W V	the cu	油石公比	44	1ª		文节	比结质小	(# 击 스)40	佳市 文学	(書書 (合))
-	1977;		万 2日	15		70	1010/102	和米刀組	여자 구나	2027 10/1
Frame		100.0	4276		100.0	318387	92 k	0	0	0
VIEEE 802.11 wireless LAN		101.6	4346		22.5	/1491	20 k	3571	51775	14 k
 Logical-Link Control 		16.5	705		/0.5	224340	64 k	0	0	0
✓ Internet Protocol Version 4	н.	15.9	680	ŗ.	4.3	13660	3950	0	0	0
 User Datagram Protocol 		5.9	251	Ļ	0.6	2008	580	0	0	0
Simple Service Discovery Protocol		1.8	79	Į.	3.1	9982	2886	79	9982	2886
NetBIOS Name Service		0.7	30		0.6	1824	527	30	1824	527
Multicast Domain Name System		0.4	16		0.6	1851	535	16	1851	535
Link-local Multicast Name Resolution		0.4	19		0.2	594	171	19	594	171
Dynamic Host Configuration Protocol		0.0	2		0.2	644	186	2	644	186
Domain Name System		0.6	25		0.9	2965	857	25	2965	857
Data		1.9	80		11.5	36526	10 k	80	36526	10 k
 Transmission Control Protocol 		9.7	414		46.3	147257	42 k	325	99591	28 k
Transport Layer Security		1.6	69		15.0	47655	13 k	67	43967	12 k
 Hypertext Transfer Protocol 		0.4	19		15.8	50169	14 k	6	3085	892
 MIME Multipart Media Encapsulation 		0.1	3		12.6	40098	11 k	0	0	0
Malformed Packet		0.1	3		0.0	0	0	3	0	0
Line-based text data		0.2	10		0.6	1778	514	10	1778	514
Data		0.1	3		1.1	3404	984	3	3404	984
Internet Group Management Protocol		0.4	15		0.1	256	74	15	256	74
Address Resolution Protocol		0.5	20		0.2	560	161	20	560	161
802.1X Authentication		0.1	5		0.2	573	165	5	573	165

一个无线流量包, 信息都被加密了。来看看有没有握手包:

🚄 cacosmia.cap

```
文件(F) 編輯(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电活(Y) 无线(W) 工具(T) 帮助(H)

▲ ■ ② ③ - ▲ ③ 爻 ⑤ - ③ ◎ ◎ ◎ ◎ ◎ ③ ③ ■ ④ ④ ♀ ◎ ◎
```

eapol|

- N-										
1	No.	Time	Source	Destination	Protocol	Length	Info			
	509	4.557634	1a:d7:17:98:d0:51	HonHaiPr_c4:09:73	EAPOL	133	Key	(Message 1	of	4)
	510	4.560194	1a:d7:17:98:d0:51	HonHaiPr_c4:09:73	EAPOL	133	Key	(Message 1	of	4)
	512	4.561714	HonHaiPr_c4:09:73	1a:d7:17:98:d0:51	EAPOL	155	Key	(Message 2	of	4)
	514	4.567362	1a:d7:17:98:d0:51	HonHaiPr_c4:09:73	EAPOL	189	Key	(Message 3	of	4)
	516	4.568370	HonHaiPr_c4:09:73	1a:d7:17:98:d0:51	EAPOL	133	Key	(Message 4	of	4)

X

这个时候可以来尝试爆破了。Kali Linux, 启动:

```
aircrack-ng -w ./rockyou.txt ./cacosmia.cap
```

还是那个经典的字典。

```
Aircrack-ng 1.5.2

[00:00:07] 10680/7120712 keys tested (1538.79 k/s)

Time left: 1 hour, 17 minutes, 2 seconds 0.15%

KEY FOUND! [ 12345678 ]

Master Key : 7D 0E AF 7D EE 35 C0 75 74 65 AB 22 65 1A 42 6A

A9 29 FF 14 5A 44 E5 74 6B 52 92 CC F4 96 20 31

Transient Key : 78 E7 9C 0E 19 EF BF 53 86 F4 30 9A D4 94 56 72

EA 87 5C 14 18 97 96 45 84 E7 2A E1 08 F5 67 8C

93 53 28 28 F2 AD AF A2 83 68 10 B8 34 4D 76 75

BC A9 97 EE 8C DC 41 FF F0 3A 0D BD 92 26 B8 33

EAPOL HMAC : 87 89 61 A3 2A 63 BE B8 D3 50 AB F5 E6 74 FD F2
```

很快就爆出来了,无线密码是12345678。这个时候可以来解密了:

编辑	(E)	视图(V)	跳转(G)	捕获(C)	分析(A)	\$
	复制	J			,	•
9	查找	汸组(F)		Ctrl	+F	
	查找	ҟ 下一 个(N))	Ctrl	+N	
	查找	ἐ上一个(v)		Ctrl	+B	
	标记	3/取消标记	分组(M)	Ctrl	+M	
	标记	所有显示的	的分组	Ctrl	+Shift+M	
	取消	所有显示的	的标记(U)	Ctrl	+Alt+M	
	下	标记		Ctrl	+Shift+N	
	前一	-标记		Ctrl	+Shift+B	
	忽略	8/取消忽略	分组(I)	Ctrl	+D	
	忽略	新有显示的	的分组	Ctrl	+Shift+D	
	取消	認略所有的	显示的分组	Ctrl	+Alt+D	
	设置	計/取消设置	时间参考	Ctrl	+T	
	取消	设置所有明	时间参考	Ctrl	+Alt+T	
	下-	-时间参考		Ctrl	+Alt+N	
	前一	时间参考		Ctrl	+Alt+B	
	时间]平移		Ctrl	+Shift+T	
	分组	注释		Ctrl	+Alt+C	
	删除	新有分组法	主释			
	配置	記置文件(C)	Ctrl	+Shift+A	
	首选	硕(P)		Ctrl	+Shift+P	

Protocols -> IEEE 802.11 -> Decryption keys直达:

📕 Wireshark · 首选项		?	×
ICQ IEEE 802.11 IEEE 802.15.4 IEEE 802.14H iFCP ILP IMAP IMF INAP Infiniband SD Interlink IPDC IPDR/SP iPerf2 IPMI IPSICTL IPV4 IPV6 IPV5 IPX IRC ISAKMP	<pre>IFFE 802.11 vireless LAH</pre>	Help	

WEP and N	WPA Decryption Keys				?	×
Key type	Кеу					
wpa-pwd	12345678					
+ - Pa	~ ~ E	<u>C: Users dom</u>	ain AppData Ro	aming Wiresher	<u>-k 80211</u>	<u>keys</u>
		OK	复制自 🔻	Cancel	Hel	p

保存退出,此时应该能看到已经解密了。开始追踪流,先过滤一下再开始:

🚄 ca	cosmia.c	ар											
文件(E) 编辑(E) 视图(V)	跳转(<u>G</u>)	捕获(<u>C</u>)	分析	(<u>A</u>) \$\$	ն՝†(<u>S</u>)	电话	M F	无线(<u>W</u>)	I	具(<u>T</u>)	帮
	10	- 🔚 🔀	۹ 🖸	0 e e 5	<u> </u>	₽ .		Ð,	ର୍ ବ୍				
📕 top	.stream	eq O											
No.	Ti	ne	Sourc	e:			Desti	natio	n			Proto	ocol
	558 4.	703602	192.	168.43.	60		13.1	.07.4	.52			TCP	
	570 4	A) 统计(S)	电话(Y)	无线(<u>W</u>)	I	l(T) #	400 いい いし い い い し い し い い い い い い い い い い い い い	100	17 6	0		TCD	
		显示过滤器(F 显示过滤器宏) :(M)										
应用为歹 作为过:		应用为列 作为讨滤器应	用	Ctrl+Shift+I		Protoco TCP)l Ler	ngth 102	Info 2658	7 → 80	[5		
		准备过滤器 对话过滤器		,				102 90	80 → 2658: [TCP	26587 7 → 80	[S [A		
		启用的协议 解码为(<u>A</u>)		Ctrl+Shift+	E			602 90	TCP [TCP [TCP	ACKed	un un		
		重新载入 Lua SCTP	插件	Ctrl+Shift+	L			90 90 90	2658 [TCP	Previ 7 $\rightarrow 80$	ous [F		
		30FF				TCP	P流	00 Ct	trl+Alt	+Shift+	r un		
		显示分组字节 专家信息		Ctrl+Shift+	0	UI TL H	DP 流 .S 流 TTP 流	Ci	trl+Alt trl+Alt trl+Alt	+Shift+ +Shift+ +Shift+	H L		

🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 31) · cacosmia.cap

```
POST / HTTP/1.1
Host: 47.107.89.184
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win
20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,appli
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,z
US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Cookie:
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
LCBJIHN1dCBteSBwYXNzd29yZCBhcyBhIHd1YnNpdGUgd
WZvcmUifQ.P3x0ErNrUkYqdMBoo8WvU63kUVy0kZjiTK-
Content-Type: multipart/form-data;
boundary=-----191691572
Content-Length: 13366
Connection: close
Upgrade-Insecure-Requests: 1
-----191691572411478
Content-Disposition: form-data; name="face";
Content-Type: image/png
.PNG
. . .
IHDR...h...e.....1(...
                            pHYs.....
```

还有让人激动的PK文件头和flag.txt:

🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 31) · cacosmia.cap

{.a4v8"=.\$IK
0`0m,x+`E1.pz~iiiaa!)H"KU.L&T
]8:88V.=R.1Fl.bYv0,F
.ty.Se.l.DL*0D.X.^z= i.1W,\$zml&D%v.d&y.D".Ja6
%1rn.DD.}a.?:V./N[M89.,]oX8v:.UU777_yt
[m\$)Bv/J}.XWPNS81&.L\$>(.b .
%H%0F@.NuI.kU.`EnmsgoooUBji\$4.c6.14_T>R*.=\
nZ.u.HR#dD4py>.G 9Y11
<.cu.;qy\@?p`8r.`0U}b.7fIEND.B`.PK
d0;6*flag.txtr9Q1^.a.*.C,].0.N*f.Y)b.q. yvPK?.
d0;6*\$flag.txt
· · · · · · · · · · · · · · · · · · ·
191691572411478
HTTP/1.1 200 OK
Date: Mon, 04 Nov 2019 16:16:19 GMT
Server: Apache/2.4.18 (Ubuntu)

先	提	取出	宋は	再	说	:

显示和保存数据为 原始数据 🗸							
	滤掉此流	打印	Save as				

这样导出有HTTP头部信息,用010 Editor去掉即可得到一个图种,可以继续编辑把图和 种 压缩包拆 开。也可以用binwalk或者foremost之类的工具分离出来。图用Stegsolve看了看似乎没有什么信息,压 缩包被加密了:

名称	0% 正在复制		
📕 flag.txt	已用时间: 剩余时间: 文件:	00:00:05	总大小: 速度: 已处理:
	太日· 压缩率:	輸 入密码	X
	flag.txt	輸入密码: ┃ ☑ 显示密码(5)	
		确定	取消
ͳͶͺ	Debugger Libraries Intro	duction Ask Get a T-shirt!	Crafted by 😽
ncoded paste a token here		Decoded Edit THE PAYLOAD	AND SECRET
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpX VCJ9.eyJoaW50IjoiZm9yIHN1Y3VyaXR 5LCBJIHN1dCBteSBwYXNzd29yZCBhcyB hIHd1YnNpdGUgd2hpY2ggaSBqdXN0IHB		<pre>HEADER: ALGORITHM & TOKEN TYPE { "alg": "HS256", "typ": "JWT" }</pre>	
dMBoo8WvU63kUVyOkZji	TK-hwOIIS5A	PAYLOAD: DATA	
		{ "hint": "for security, a website which i just pi }	I set my password as Inged before"

提示密码是被ping过的一个站点。回到流量包中尝试过滤:



没有发现。不过ping一个站点通常会先进行DNS解析:

dns					▲
No.	Time	Source	Destination	Protocol	Length Info
1088	6.761984	192.168.43.1	192.168.43.60	DNS	296 Standard query response 0x4425 A geo.prod.do.dsp.mp.microsoft.com CNA
1191	7.058432	192.168.43.1	192.168.43.60	DNS	294 Standard query response 0xfa3d A kv701.prod.do.dsp.mp.microsoft.com C
1222	2 7.138292	192.168.43.60	192.168.43.1	DNS	112 Standard query 0x2481 A api.onedrive.com
1224	7.158272	192.168.43.1	192.168.43.60	DNS	323 Standard query response 0x2481 A api.onedrive.com CNAME odc-routekey-
1658	8.982130	192.168.43.60	192.168.43.1	DNS	130 Standard query 0x1931 A cp701.prod.do.dsp.mp.microsoft.com
1965	10.730750	192.168.43.1	192.168.43.60	DNS	300 Standard query response 0x2fe8 A disc701.prod.do.dsp.mp.microsoft.com
2159	11.677490	192.168.43.60	192.168.43.1	DNS	109 Standard query 0x6837 A mus.cisco.com
2162	11.678002	192.168.43.60	192.168.43.1	DNS	109 Standard query 0x6837 A mus.cisco.com
2167	11.682624	192.168.43.1	192.168.43.60	DNS	125 Standard query response 0x6837 A mus.cisco.com A 72.163.1.80
2726	15.991346	192.168.43.60	192.168.43.1	DNS	132 Standard query 0x74cf A disc701.prod.do.dsp.mp.microsoft.com
2726	5 15.995454	192.168.43.1	192.168.43.60	DNS	306 Standard query response 0x74cf A disc701.prod.do.dsp.mp.microsoft.com
3706	22.147008	192.168.43.1	192.168.43.60	DNS	128 Standard query response 0x1322 A 26rsfb.dnslog.cn A 127.0.0.1

发现最后一次解析有点可疑,返回了环回地址,如果ping环回的话,确实是会抓不到包的。尝试用 26rsfb.dnslog.cn 解压:

🥘 flag.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

flag{f14376d0-793e-4e20-9eab-af23f3fdc158}

flag{f14376d0-793e-4e20-9eab-af23f3fdc158}

wifi

vol内存取证,直接找zip,找到个奇怪的

b i
Dnl

导出,发现需要密码,

ē	👚 📃 📰 📑 mywifi.zip解包大小为 1 KB					
	名称	压缩前	压缩后	password is	s Network	Adapter
[1000]	<mark>▶</mark> (上级目录) ▶ 无线网络连接-My_Wifi.xml *	1 KB	1 KE			-

老考点了



花括号以内加花括号是密码, 解压后获得xml, xml获得密码



对加密的客户端流量进行解密,即可



随后进入流量分析环节。

首先分析服务器流量,直接看http

这是哥斯拉shell的初始化

我们解密得到加密函数和key

```
function encode($D,$K){
   for($i=0;$i<strlen($D);$i++) {
      $c = $K[$i+1&15];
      $D[$i] = $D[$i]^$c;
   }
   return $D;
}
$pass='key';
$payloadName='payload';
$key='3c6e0b8a9c15224a';</pre>
```

加密函数也是解密函数

分析客户端流量的回显

68	74	6d	6c	3b	20	63	68	61	72	73	65	74	3d	55	54	html; ch arset=UT
46	2d	38	0d	0a	0d	0a	37	32	61	39	63	36	39	31	63	F-8····7 2a9c691c
63	64	61	61	62	39	38	66	4c	31	74	4d	47	49	34	59	cdaab98f L1tMGI4Y
54	6c	6a	4d	6e	37	35	65	33	6a	4f	42	53	35	2f	56	TljMn75e 3j0BS5/V
33	31	51	64	31	4e	78	4b	51	4d	43	65	33	68	34	4b	31Qd1NxK QMCe3h4K
77	46	51	66	56	41	45	56	77	6f	72	43	69	30	46	66	wFQfVAEV worCi0Ff
67	42	2b	42	6c	57	5a	68	6a	52	6c	51	75	54	49	49	gB+B1WZh jR1QuTII
42	35	6a	4d	54	55	3d	62	34	63	34	65	31	66	36	64	B5jMTU=b 4c4e1f6d
64	64	32	61	34	38	38										dd2a488

去掉前面的16位和后面的16位得到

fL1tMGI4YTljMn75e3jOBS5/V31Qd1NxKQMCe3h4KwFQfVAEVworCi0FfgB+BlWZhjRlQuTIIB5jMTU=

```
$result=gzencode($result,6);
```

```
echo base64_encode(encode(@run($data),$key));
```

然后进行解密

```
function encode($D,$K){
    for($i=0;$i<strlen($D);$i++) {
        $c = $K[$i+1&15];
        $D[$i] = $D[$i]^$c;
    }
    return $D;
}
$a=
'fLltMGI4YT1jMn75e3j0BS5/V31Qd1NxKQMCe3h4KwFQfVAEVworCi0FfgB+B1WZhjR1QuTIIB5jMTU
=';
echo gzdecode(encode(base64_decode($a),'3c6e0b8a9c15224a'));</pre>
```

得到flag

flag{5db5b7b0bb74babb66e1522f3a6b1b12}