2019红帽杯(RedHat)【Broadcastc & 恶臭的数据包】writeup



<u>「已注销」</u> ● <u>1</u> <u>2019-11-11</u> <u>20:17:31</u> <u>发</u> 文章标签: <u>2019 红帽杯 CTF 数据分析 无线</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/chen574927274/article/details/103016539</u> 版权

首先请原谅我这么菜,只解了两道题还来发Blog;

[Broadcastc]

这题不多说,直接解压得到task.py打开获取flag

【恶臭的数据包】

首先下载压缩包解压得到数据包

Wireshark打开什么都看不懂,直接百度;

按照教程 把数据包丢到Kali

先看看ESSID



然后再破解WiFi密码



得到WiFi密码 12345678

打开Wireshark 编辑->首选项->Protocols->IEEE 802.11

| Sec. | Tise | Four ce | Destination | Protocol | Length Inf- | ~ |
|------|-----------------|----------------------|----------------------------|----------|---|---|
| | 3310 19.361522 | | HomHaiPr_c4:09:73 (- | 802.11 | 10 Clear-to-send, Flags | |
| | 3311 19.361522 | 192.168.43.60 | 47.107.89.184 | TCP | 90 20643 → 80 [ACK] Seq+1 Ack+1 Min+17408 Len+0 | |
| | 3312 19.362546 | 192.168.43.60 | 47,107,89,184 | TCP | 1470 26643 + 80 [ACK] Seq=1 Ack=1 win=17408 Len=1380 [TCP segment of a reassembled PDU] | |
| | 3313 19.362546 | 192.168.43.60 | 47.107.89.184 | TCP | 1470 26643 + 80 [ACK] Seq=1381 Ack=1 win=17408 Len=1380 [TCP segment of a reassembled PDU] | |
| | 3314 19.362546 | 192.168.43.60 | 47.107.89.184 | TCP | 1470 2054) + 80 [ACK] Seq-2761 Ack-1 win-17408 Len-1380 [TCP segment of a reassembled PDU] | |
| | 3315 19,362546 | 192.168.43.60 | 47,107,89,184 | TCP | 1470 20543 = 80 [ACK] Seq=4141 Ack=1 win=17408 Len=1380 [TCP segment of a reassembled PDU] | |
| | 3316 19, 362562 | la:d7:17:98:d0:51 (. | . HonHaiPr_c4:09:73 (. | 802.11 | 28 802.11 Block Ack, Flags | - |
| | 3317 19.362562 | 192.168.43.60 | 47.107.89.184 | TOP | 1470 2064) → 80 [ACK] Seq+5521 Ack+1_win+17408 Len+1180 [TCP segment of a reassembled POU] | |
| | 3318 19,363074 | 192.168.43.60 | 47,107,89,184 | TCP | 1470 26643 + 80 [ACK] Seq-6001 Ack-1 act = 4400 Len-1380 [TCP segment of a reassembled PCU] | |
| | 3319 19.363874 | 192.168.43.60 | 47,107,89,184 | TCP | 1470 20543 + 80 [ACK] Seq-8281 Ack-1 win-17408 Len-1740 [TCP segment of a reassembled POU] | |
| | 3320 19.363074 | 192.168.43.60 | 47.107.89.184 | TCP | 1470 2664) → 80 [ACK] Seq-9661 Ack-1 win+17408 Len-1180 [TCP treast of a reassembled POU] | |
| | 3321 19.363074 | 192.168.43.60 | 47,107,89,184 | TCP | 1470 2064) + 80 [ACK] Seq-11041 Ack-1 win-17408 Len-1380 [TCP segment of a negsembled PDU] | |
| | 3322 19,363058 | 192.168.43.60 | 47.107.89.184 | TCP | 1470 26643 + 80 [ACK] Seq-12421 Ack-1 win-17408 Len-1380 [TCP segment of a reassembled PDU] | |
| | 3333.14 363834 | 141071121001001001 | sensial Pr. r.A. 00-23. F. | 487 11 | balant ss alock Ark Flagss | ~ |

OK https:///制刷.csch.Cancelen574529274

设置wpa-pwd 值的格式(密码:WiFi名称/pass:essid)保存之后发现数据包被解密了

+ - 🗣 🔨 🕝 C: \Users\Administrat...\Uireshark\80211 keys

通过分析发现,有个可疑的HTTP请求

右击 追踪流->TCP



发现是个文件上传,末尾发现还有一个ZIP。



将 显示和保存数据为 改成原始数据



| THP T | | | | | | | | | | | | | | | | | |
|-----------|----|----|----|----|----|----|----|----|-----|-----------|----|----|----|----|----|----|------------------|
| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Α | В | С | D | Е | F | |
| 00000000 | 50 | 4F | 53 | 54 | 20 | 2F | 20 | 48 | 54 | 54 | 50 | 2F | 31 | 2E | 31 | OD | POST / HITP/1.1 |
| 00000010 | 0A | 48 | 6F | 73 | 74 | 3A | 20 | 34 | 37 | 2E | 31 | 30 | 37 | 2E | 38 | 39 | Host: 47.107.89 |
| 00000020 | 2E | 31 | 38 | 34 | OD | 0A | 55 | 73 | 65 | 72 | 2D | 41 | 67 | 65 | 6E | 74 | .184 User-Agent |
| 00000030 | ЗA | 20 | 4D | 6F | 7A | 69 | 6C | 6C | 61 | 2F | 35 | 2E | 30 | 20 | 28 | 57 | : Mozilla/5.0 (W |
| 00000040 | 69 | 6E | 64 | 6F | 77 | 73 | 20 | 4E | 54 | 20 | 31 | 30 | 2E | 30 | 3B | 20 | indows NT 10.0; |
| 00000050 | 57 | 69 | 6E | 36 | 34 | 3B | 20 | 78 | 36 | 34 | 3B | 20 | 72 | 76 | 3A | 37 | Win64; x64; rv:7 |
| 00000060 | 30 | 2E | 30 | 29 | 20 | 47 | 65 | 63 | 6B | 6F | 2F | 32 | 30 | 31 | 30 | 30 | 0.0) Gecko/20100 |
| 00000070 | 31 | 30 | 31 | 20 | 46 | 69 | 72 | 65 | 66 | 6F | 78 | 2F | 37 | 30 | 2E | 30 | 101 Firefox/70.0 |
| 00000080 | OD | 0A | 41 | 63 | 63 | 65 | 70 | 74 | 3A | 20 | 74 | 65 | 78 | 74 | 2F | 68 | Accept: text/h |
| 00000090 | 74 | 6D | 6C | 2C | 61 | 70 | 70 | 6C | 69 | 63 | 61 | 74 | 69 | 6F | 6E | 2F | tml.application/ |
| 000000A0 | 78 | 68 | 74 | 6D | 6C | 2B | 78 | 6D | 6C | 2C | 61 | 70 | 70 | 6C | 69 | 63 | xhtm +xml.applic |
| 00000080 | 61 | 74 | 69 | 6F | 6E | 2F | 78 | 6D | 60 | 38 | 71 | 3D | 30 | 2E | 39 | 20 | ation/xml:g=0.9. |
| 000000000 | 2A | 2F | 2A | 3B | 71 | 3D | 30 | 2E | 38 | OD | 0A | 41 | 63 | 63 | 65 | 70 | */:g=0.8 Accep |
| 000000000 | 74 | 2D | 4C | 61 | 6E | 67 | 75 | 61 | 67 | 65 | 3A | 20 | 7A | 68 | 2D | 43 | t Language: zh-C |
| 000000E0 | 4E | 2C | 7A | 68 | 38 | 71 | 3D | 30 | 2E | 38 | 2C | 7A | 68 | 2D | 54 | 57 | .zh:g=0.8.zh-TW |
| 000000F0 | 38 | 71 | 3D | 30 | 2E | 37 | 2C | 7A | 68 | 2D | 48 | 4B | 38 | 71 | 3D | 30 | :g=0.7.zh-HK:g=0 |
| 00000100 | 2E | 35 | 20 | 65 | 6E | 2D | 55 | 53 | 38 | 71 | 3D | 30 | 2E | 33 | 2C | 65 | .5.en-US:g=0.3.e |
| 00000110 | 6E | 3B | 71 | 3D | 30 | 2E | 32 | OD | 0A | 41 | 63 | 63 | 65 | 70 | 74 | 1 | n:g=0.2 Accept- |
| 00000120 | 45 | 6E | 63 | 6F | 64 | 69 | 6E | 67 | 3A | 20 | 67 | 7A | 69 | 70 | 20 | 20 | Encoding: gzip. |
| 00000130 | 64 | 65 | 66 | 6C | 61 | 74 | 65 | 0D | AD | 43 | 6F | 6F | 6B | 69 | 65 | 3A | deflate Cookie: |
| 00000140 | 20 | 73 | 65 | 73 | 73 | 69 | 6F | 6E | 3D | 65 | 79 | 4A | 68 | 62 | h | 63 | session=ev.JhbGc |
| 00000150 | 69 | 4F | 69 | 4A | 49 | 55 | 7A | 49 | 31 | 4E | 69 | 49 | 73 | 49 | 6E | 52 | i0iJIUzI1NiIsInR |
| 00000160 | 35 | 63 | 43 | 49 | 36 | 49 | 6B | 70 | 58 | 56 | 43 | 4A | 39 | 21 | 65 | 79 | ScCI6IkpXVCJ9.ev |
| 00000170 | 4A | 6F | 61 | 57 | 35 | 30 | 49 | 6A | 6F | 69 | SA | 6D | 39 | 4 | 49 | 48 | JoaW50LioiZm9vIH |
| 00000180 | 4E | 6C | 59 | 33 | 56 | 79 | 61 | 58 | 52 | 35 | 4C | 43 | 42 | 4A | 49 | 48 | N1Y3VvaXR5LCBJIH |
| 00000190 | 4E | 6C | 64 | 43 | 42 | 74 | 65 | 53 | 42 | 77 | 59 | 58 | 41 | 7A | 64 | 32 | N1dCBteSBwYXNzd2 |
| 000001A0 | 39 | 79 | 5A | 43 | 42 | 68 | 63 | 79 | 42 | 68 | 49 | 48 | 4 | 6C | 59 | 6E | 9vZCBhcvBhIHd1Yn |
| 00000180 | 4E | 70 | 64 | 47 | 55 | 67 | 64 | 32 | 68 | 70 | 59 | 32 | 67 | 67 | 61 | 53 | NpdGUgd2hpY2ggaS |
| 00000100 | 42 | 71 | 64 | 58 | 4E | 30 | 49 | 48 | 42 | 70 | 62 | 61 | 64 | 6C | 5A | 43 | BadXN0IHBpbmd1ZC |
| 00000100 | 42 | 69 | 5A | 57 | SA | 76 | 63 | 6D | 55 | 69 | 66 | 1 | 2E | 50 | 33 | 78 | BiZWZycmUif0.P3x |
| 000001E0 | 4F | 45 | 72 | 4E | 72 | 55 | 6B | 59 | 71 | 64 | 4D | 42 | 6F | 6F | 38 | 57 | 0ErNrUkYgdMBoo8W |
| 000001F0 | 76 | 55 | 36 | 33 | 6B | 55 | 56 | 79 | 4F | 6B | 54 | 6A | 69 | 54 | 4B | 2D | vU63kUVv0kZiiTK- |
| 00000200 | 68 | 77 | 4F | 49 | 49 | 53 | 35 | 41 | OD | 0A | 43 | 6F | 6E | 74 | 65 | 6E | hw0IIS5A Conten |
| 00000210 | 74 | 2D | 54 | 79 | 70 | 65 | 3A | 20 | 6D | 75 | 6C | 74 | 69 | 70 | 61 | 72 | t-Type: multipar |
| 00000220 | 74 | 2F | 66 | 6F | 72 | 6D | 2D | 64 | 61 | 74 | 61 | 38 | 20 | 62 | 6F | 75 | t/form-data: bou |
| 00000230 | 6E | 64 | 61 | 72 | 79 | 3D | 2D | 2D | 2D | D | 2D | 2D | 2D | 2D | 2D | 2D | ndarv= |
| 00000240 | 2D | 2D/ | 2D | 2D | 2D | 2D | 2D | 2D | 2D | |
| 00000250 | 2D | 31 | 39 | 31 | 36 | 39 | 31 | 35 | 3/ | 32 | 34 | 31 | 31 | 34 | 37 | 38 | -191691572411478 |
| 00000260 | OD | 0A | 43 | 6F | 6E | 74 | 65 | 6E | 74 | 2D | 4C | 65 | 6E | 67 | 74 | 68 | Content-Length |
| 00000270 | 3A | 20 | 31 | 33 | 33 | 36 | 36 | OD | 0A | 43 | 6F | 6E | 6E | 65 | 63 | 74 | : 13366 Connect |
| 00000280 | 69 | 6F | 6E | 3A | 20 | 63 | 6C | 6F | 73 | 65 | OD | 0A | 55 | 70 | 67 | 72 | ion: close Upgr |
| 00000290 | 61 | 64 | 65 | 2D | 49 | 6E | 73 | 65 | 63 | 75 | 72 | 65 | 2D | 52 | 65 | 71 | ade-Insecure-Reg |
| 00000280 | 75 | 65 | 73 | 74 | 73 | 34 | 20 | 31 | OD | NA | ND | 0A | 2D | 2D | 2D | 2D | uests: 1 |
| 000002B0 | 2D | 2D | 2D | 2D | 2D | 2D | 2D | 2D | |
| 00000200 | 2D | 31 | 39 | 31 | 36 | 39 | 31 | 35 | 1916915 |
| 00000200 | 37 | 32 | 34 | 31 | 31 | 34 | 37 | 38 | OD | AD | 43 | 6F | 6E | 74 | 65 | 6E | 72411478 Conten |
| 000002E0 | 74 | 2D | 44 | 69 | 73 | 70 | 6F | 73 | 69 | 74 | 69 | 6F | 6E | 34 | 20 | 66 | t-Disposition of |
| 000002F0 | 6F | 72 | 6D | 2D | 64 | 61 | 74 | 61 | 3B | 20 | 6E | 61 | 6D | 65 | 3D | 22 | orm-data: name=" |

将前面的HTTP头部信息去除,修复PNG图片,之后保存得到一张并没什么用的图片

襘.

将图片丢到Kali binwalk -e xx.png

将zip分解出来,可能是文件尾部清理不干净,导致binwalk卡住了,回车一下(也可以尝试修复一下)



得到以上文件夹,别以为看到flag就以为自己成功了

打开为空,哈哈哈哈

将zip拷贝到windows 放到archpr跑包,一直未果。

这就纳闷了。。。。。

后来分析发现请求头部的Cookie



后来得知是jwt

不懂可以看看 https://juejin.im/post/5a437441f265da43294e54c3

按照网上原理得知是base64加密,拷贝中间的payload

| 🚄 Wireshark - 追踪 TCP 揓 (tcp.stream eq 28) - cacosmia.cap | - | | × |
|--|---------------------|------------------|-----|
| POST / HTTP/1.1 Host: 47.107.89.184 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0 Accept: text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzip, deflate Cookie: session=ey1hbGci0iJlUzIINIISCCT6IkpXVC39.ayJoaH501j0iZ=09/HellV3Vy3XH5LCB)HelldCBtesBwySHzd2972CBhc Mgd2hy2Pg285dgXN0HTMBpbd1ZCB1ZAVzvewJIC_P3XOErNrUKSd_dMBocoBkvU63kUVy0KZjITX-hw0II55A | уBhIнd | 1¥nNpdG | ^ |
| Content-Type: multipart/form-data; boundary=191691572411478 Content-Length: 13366 Connection: close Upgrade-Insecure-Requests: 1 | | | |
| | | | |
| ImpRhe1(pHYS | } .{.%=. .f.y | aY | |
| [1],,,,,,,, . | y .}a. .x,5 | i. \N\$ MS | |
| .0(j6.4)Wi., | | | ~ |
| 整个对话(14 kB) > 显示和保存数据为 ASCII > | | 液 21 | |
| attehttps://biocreasimpet/shan5 | 740 | 前线下一个 | (%) |
| 清掉此液 打印 Save as ··· 近回 C | lose | Help | |

通过base64解密,得到如下



请原谅英语差的我

| 检测到英语 • | \neq | 中文 * | 1 1 17 | 人工程译 | 1 | ₩. |
|------------------------------------|--------------|---------------------|---------------|----------------|-----------------|----|
| for security, I set my p before | assword as a | website which i jus | t pinged X | 为了安全起见,我把我的密码设 | 重为一个我刚才ping过的网站 | |
| 이 습 | | | | () 🗈 📾 | HE OD REAL | |

Ping 无非就是ICMP协议; Wireshark过滤ICMP

发现没有任何东西

后来灵感一来,网站域名解析肯定就是DNS了;

| il de | | | | | 0 · +2.5- |
|-------|----------------|---------------|---------------|----------|--|
| \$r. | Time | Deserve | Destination | Protocol | Length Isla |
| | 886 5.839296 | 192.168.43.1 | 192.168.43.60 | DNS | 323 Standard query response 0x31e1 A bn1304.storage.live.com CMAVE odc-bn1304-meta-geo.onedrive.aka |
| | 1088 6.761984 | 192.168.43.1 | 192.168.43.60 | DNIS | 296 Standard query response @x6425 A geo.prod.do.dsp.mp.microsoft.com CNAME geo-prod.do.dsp.mp.micr |
| | 1191 7.058432 | 192.168.43.1 | 192.168.43.60 | DNS | 294 Standard query response 0xfa3d A kv701.prod.do.dsp.mp.mLcrosoft.com CMMME kv701.prod.dodsp.mp.m |
| | 1222 7.138292 | 192.168.43.60 | 192.168.43.1 | DHIS | 112 Standard query 0x2481 A api.onedrive.com |
| | 1224 7.158272 | 192.168.43.1 | 192.168.43.60 | DNIS | 323 Standard query response 0x2483 A api.onedrive.com CNAME odc-routekey-meta-geo.onedrive.akadns.n |
| | 1658 8.982130 | 192.168.43.60 | 192.168.43.1 | DNS | 138 Standard query 8x1931 A cg701_prod.do.dsp.mp.microsoft.com |
| | 1965 10.730750 | 192.168.43.1 | 192.168.43.60 | DHIS | 300 Standard query response 0x2fe8 A disc701.prod.do.dsp.mp.microsoft.com CNAME disc701.prod.dodsp. |
| | 2159 11.677490 | 192.168.43.60 | 192.168.43.1 | DNIS | 109 Standard query 0x6837 A mus.cisco.com |
| | 2162 11.678002 | 192.168.43.60 | 192.168.43.1 | DRES | 189 Standard query 0x6837 A mus.clisco.com |
| | 2167 11.682624 | 192.168.43.1 | 192.168.43.60 | DNS | 125 Standard query response 0x6837 A mus.cisco.com A 72.163.1.00 |
| | 2720 15.991346 | 192.168.43.60 | 192.168.43.1 | DNS | 132 Standard guery 0x74cf A disc701.prod.do.dsp.mp.microsoft.com |
| 1 | 2726 15.995454 | 192.168.43.1 | 192.168.43.60 | DNS | 306 Standard query response 0x74cf A disc701.prod.do.dsp.mp.microsoft.com CMAME disc701.prod.dodsp.i |
| | 3706 22.147008 | 192.168.43.1 | 192.168.43.60 | DNIS | 128 Standard query response 0x1322 A 26rsfb.dnslog.cn A 127.0.0.1 |
| | | | | | |

通过刚刚的HTTP请求的序号,这里的DNS肯定就是后面点的

试了好几个,最后发现是最后一个域名

26rsfb.dnslog.cn

把域名当密码解压ZIP

得到flag