

# CTF Questions

1.

## 3.pcap

1. There is a Flag in a TCP Packet. Identify the flag. (Hint: Search for the keyword Flag)

```
Activities | Text Editor | Sep 10 16:58 | log.txt [Read-Only] | ~/Downloads | Save | [Menu] | [Close] | 40 %
Open | [Find]
1816013 | |Type Of Service : 0
1816014 | |IP Total Length : 50 Bytes(Size of Packet)
1816015 | |Identification : 1
1816016 | |TTL : 64
1816017 | |Protocol : 6
1816018 | |Checksum : 11869
1816019 | |Source IP : 18.192.188.189
1816020 | |Destination IP : 111.121.13.114
1816021 |
1816022 | TCP Header
1816023 | |Source Port : 1911
1816024 | |Destination Port : 11120
1816025 | |Sequence Number : 0
1816026 | |Acknowledge Number : 0
1816027 | |Header Length : 5 DWORDS or 20 BYTES
1816028 | |Urgent Flag : 0
1816029 | |Acknowledgement Flag : 0
1816030 | |Push Flag : 0
1816031 | |Reset Flag : 0
1816032 | |Synchronise Flag : 1
1816033 | |Finish Flag : 0
1816034 | |Window : 8192
1816035 | |Checksum : 35779
1816036 | |Urgent Pointer : 0
1816037 |
1816038 | DATA Dump
1816039 | IP Header
1816040 | 00 00 5E 00 01 F6 F8 63 3F 7D 2C 1A 08 00 45 00 | ..^....c?},...E.
1816041 | 00 32 00 01 | .2..
1816042 | TCP Header
1816043 | 00 00 40 06 2E 5D 12 C0 BC BD 6F 79 0D 72 07 77 | ..@..]....oy.r.w
1816044 | 2B 70 00 00 | +p..
1816045 | Data Payload
1816046 | 46 6C 61 67 3A 20 41 64 61 6D | Flag: Adam
1816047 |
1816048 | #####
1816049 |
Plain Text | Tab Width: 8 | Ln 1816046, Col 67 | INS
```

```
3 | DATA Dump
9 | IP Header
9 | 00 00 5E 00 01 F6 F8 63 3F 7D 2C 1A 08 00 45 00 | ..^....c?},...E.
1 | 00 32 00 01 | .2..
2 | TCP Header
3 | 00 00 40 06 2E 5D 12 C0 BC BD 6F 79 0D 72 07 77 | ..@..]....oy.r.w
4 | 2B 70 00 00 | +p..
5 | Data Payload
6 | 46 6C 61 67 3A 20 41 64 61 6D | Flag: Adam
7 |
```

2. My username is secret, Identify my secret.

3. I have a TCP checksum "0x46a4". I have instructions in my path.

```

2976685 #####
2976686
2976687 *****TCP Packet*****
2976688
2976689 Ethernet Header
2976690   |-Destination Address : 00-00-5E-00-01-F6
2976691   |-Source Address      : F8-63-3F-7D-2C-1A
2976692   |-Protocol           : 8
2976693
2976694 IP Header
2976695   |-Protocol : 6
2976696   |-Checksum : 39549
2976697   |-Source IP  : 118.142.111.129
2976698   |-Destination IP : 138.123.111.130
2976699
2976700 TCP Header
2976701   |-Source Port : 9291
2976702   |-Destination Port : 1303
2976703
2976704             DATA Dump
2976705 IP Header
2976706   00 00 5E 00 01 F6 F8 63 3F 7D 2C 1A 08 00 45 00   ..^....c?},...E.
2976707   00 6D 00 01                                       .m..
2976708 TCP Header
2976709   00 00 40 06 9A 7D 76 8E 6F 81 8A 7B 6F 82 24 4B   ..@..}v.o..{o.$K
2976710   05 17 00 00                                       ....
2976711 Data Payload
2976712   47 45 54 20 2F 20 48 54 54 50 2F 31 2E 31 0D 0A   GET / HTTP/1.1..
2976713   43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 50 41   Content-Type: PA
2976714   53 53 57 4F 52 44 2D 52 69 6F 0D 0A 4F 72 69 67   SSWORD-Rio..Orig
2976715   69 6E 3A 20 77 77 77 2E 63 73 34 33 33 2E 63 6F   in: www.cs433.co
2976716   6D 0D 0A 0D 0A                                       m....

```

4. My device has an IP Address “131.144.126.118”. Sum of my connection ports will lead you to a person.

```

01 *****TCP Packet*****
02
03 Ethernet Header
04   |-Destination Address : 00-00-5E-00-01-F6
05   |-Source Address      : F8-63-3F-7D-2C-1A
06   |-Protocol            : 8
07
08 IP Header
09   |-Protocol : 6
10   |-Checksum : 15121
11   |-Source IP : 123.118.56.78
12   |-Destination IP : 11.128.128.78
13
14 TCP Header
15   |-Source Port : 60237
16   |-Destination Port : 443
17
18           DATA Dump
19 IP Header
20   00 00 5E 00 01 F6 F8 63 3F 7D 2C 1A 08 00 45 00   ..^....c?},...E.
21   00 54 00 01                                       .T..
22 TCP Header
23   00 00 40 06 3B 11 7B 76 38 4E 0B 80 80 4E EB 4D   ..@.;.{v8N.\80\80N.M
24   01 BB 00 00                                       ....
25 Data Payload
26   54 68 65 20 70 65 72 73 6F 6E 20 79 6F 75 20 61   The person you a
27   72 65 20 6C 6F 6F 6B 69 6E 67 20 66 6F 72 20 69   re looking for i
28   73 20 4A 6F 68 6E 20 4B 65 61 74 73               s John Keats

```

5. I come from localhost, I requested a milkshake. Find my flavour.

```

75 *****TCP Packet*****
76
77 Ethernet Header
78   |-Destination Address : 00-00-5E-00-01-F6
79   |-Source Address      : F8-63-3F-7D-2C-1A
80   |-Protocol            : 8
81
82 IP Header
83   |-Protocol : 6
84   |-Checksum : 59659
85   |-Source IP   : 127.0.0.1
86   |-Destination IP : 198.33.76.78
87
88 TCP Header
89   |-Source Port      : 121
90   |-Destination Port : 60116
91
92                               DATA Dump
93 IP Header
94   00 00 5E 00 01 F6 F8 63 3F 7D 2C 1A 08 00 45 00   ..^....c?},...E.
95   00 7B 00 01                                       .{..
96 TCP Header
97   00 00 40 06 E9 0B 7F 00 00 01 C6 21 4C 4E 00 79   ..@...[REDACTED]....!LN.y
98   EA D4 00 00                                       ....
99 Data Payload
100  47 45 54 20 2F 6D 69 6C 6B 73 68 61 6B 65 20 48   GET /milkshake H
101  54 54 50 2F 31 2E 31 0D 0A 43 6F 6E 74 65 6E 74   TTP/1.1..Content
102  2D 54 79 70 65 3A 20 66 6C 61 76 6F 72 2D 20 50   -Type: flavor- P
103  69 6E 65 61 70 70 6C 65 0D 0A 43 6F 6F 6B 69 65   ineapple..Cookie
104  3A 20 75 73 65 72 3A 63 75 73 74 6F 6D 65 72 0D   : user:customer.
105  0A 0D 0A                                           ...

```