

Shark 1 – Angstorm CTF 2022

In this challenge we received a pcap file that from what we can see there is a connection over an unsecure TCP, two IPs are talking to each other and at the end we can see the flag being sent in plain text.

The image shows a Wireshark packet capture of a file named 'shark1.pcapng'. The interface displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet is packet 22, which is a TCP segment from 10.0.2.15 to 10.0.2.4. The packet details pane shows the frame structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The data field contains 40 bytes of data. The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII column highlights the text 'Emactff{w ireshark_doo_doo_doo_doo_doo_doo }' in blue.

No.	Time	Source	Destination	Protocol	Length	Info
13	99.192923857	PcsCompu_95:bd:54	PcsCompu_17:92:53	ARP	42	10.0.2.4 is at 08:00:27:95:bd:54
14	99.196279745	PcsCompu_95:bd:54	PcsCompu_17:92:53	ARP	42	Who has 10.0.2.15? Tell 10.0.2.4
15	99.186857968	PcsCompu_17:92:53	PcsCompu_95:bd:54	ARP	60	10.0.2.15 is at 08:00:27:17:92:53
16	103.837344545	10.0.2.15	10.0.2.4	TCP	84	5555 → 56686 [PSH, ACK] Seq=1 Ack=8 Win=65280 Len=18 TSval=36...
17	103.837378729	10.0.2.4	10.0.2.15	TCP	60	56686 → 5555 [ACK] Seq=8 Ack=19 Win=64256 Len=0 TSval=3332523...
18	117.883241466	10.0.2.4	10.0.2.3	DHCP	330	DHCP Request - Transaction ID 0xce9424f5
19	117.886116847	10.0.2.3	10.0.2.4	DHCP	590	DHCP ACK - Transaction ID 0xce9424f5
20	122.994428919	PcsCompu_95:bd:54	PcsCompu_96:00:7f	ARP	42	Who has 10.0.2.3? Tell 10.0.2.4
21	122.994869270	PcsCompu_96:00:7f	PcsCompu_95:bd:54	ARP	60	10.0.2.3 is at 08:00:27:96:00:7f
22	183.264283970	10.0.2.15	10.0.2.4	TCP	100	5555 → 56686 [PSH, ACK] Seq=19 Ack=9 Win=65280 Len=40 TSval=3...
23	183.264232488	10.0.2.4	10.0.2.15	TCP	60	56686 → 5555 [ACK] Seq=8 Ack=59 Win=64256 Len=0 TSval=3332602...
24	188.274584594	PcsCompu_95:bd:54	PcsCompu_17:92:53	ARP	42	Who has 10.0.2.15? Tell 10.0.2.4
25	188.275877512	PcsCompu_17:92:53	PcsCompu_95:bd:54	ARP	60	10.0.2.15 is at 08:00:27:17:92:53
26	188.446869168	PcsCompu_17:92:53	PcsCompu_95:bd:54	ARP	60	Who has 10.0.2.4? Tell 10.0.2.15
27	188.446889865	PcsCompu_95:bd:54	PcsCompu_17:92:53	ARP	42	10.0.2.4 is at 08:00:27:95:bd:54

Frame 22: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_17:92:53 (08:00:27:17:92:53), Dst: PcsCompu_95:bd:54 (08:00:27:95:bd:54)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.4
Transmission Control Protocol, Src Port: 5555, Dst Port: 56686, Seq: 19, Ack: 8, Len: 40
Data (40 bytes)
Data: 010374667b7607265736861726b5f646f65f646f65f64
[Length: 40]

0000 00 00 27 95 bd 54 08 00 27 17 92 53 08 00 45 00 ...T...S..E
0010 00 5c fb 7e 40 00 40 06 27 00 0a 00 02 0f 0a 00 ...~@.@...
0020 02 04 15 b3 dd 6e 00 9f 18 1d 95 a7 42 fd 00 1b ...n...B...
0030 01 fe 84 2c 00 00 01 01 08 0a d8 ce 32 f9 c6 a2 ...2...
0040 45 6d 01 63 74 66 7b 77 69 72 65 73 68 61 72 6b Emactff{w ireshark
0050 5f 64 6f 6f 5f 64 6f 6f 5f 64 6f 6f 5f 64 6f 6f _doo_doo_doo_doo
0060 5f 64 6f 6f 5f 64 6f 6f 7d 0a _doo_doo }.

```
45 00  ..'.T..'.S..E.
9a 00  .\~@.@.'.....
80 18  .....n.....B...
c6 a2  ....,.....2...
72 6b  Emactff{w ireshark
6f 6f  _doo_doo_doo_doo
      _doo_doo }.
```