Files

main

Go to file t

1337UP_2022
UTCTF_2022
beginner
baby_shark
img
README.md
baby_shark1.pcap
baby_shark_p2
img
README.md
baby_shark2.pcap

LambdaMamba Added writeup for UTCTF 2022 Baby Shark P2 — 12d3294 · 2 years ago — History

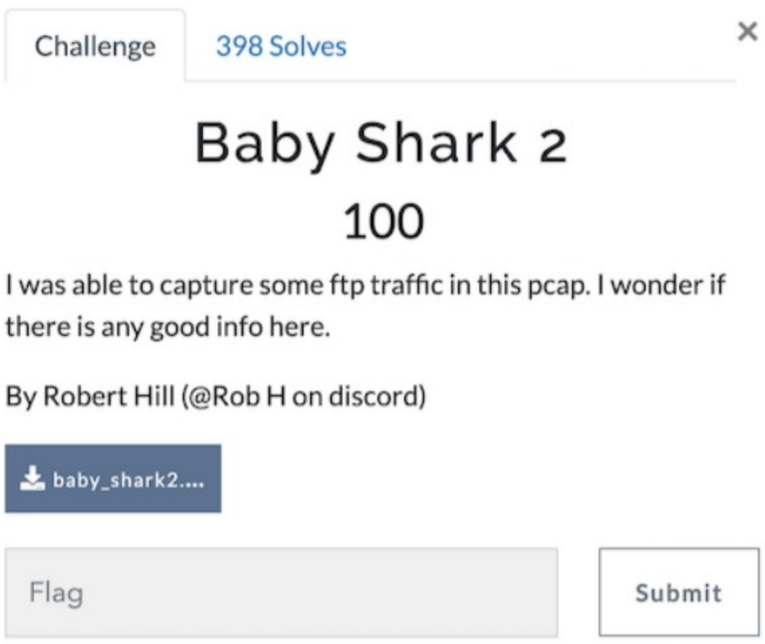
Name	Last commit message	Last commit date
..		
img	Added writeup for UTCTF 2022 Baby Shark P2	2 years ago
README.md	Added writeup for UTCTF 2022 Baby Shark P2	2 years ago
baby_shark2.pcap	Added writeup for UTCTF 2022 Baby Shark P2	2 years ago

README.md

UTCTF 2022 Baby Shark P2 (Category: Beginner)

The challenge is the following,

The challenge is the following,



Here, we are given the file baby_shark2.pcap. The challenge description says `I was able to capture some ftp traffic in this pcap. I wonder if there is any good info here.`, so we will look at the ftp traffic.

Opening this up on Wireshark shows the following,

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.24.0.1	172.24.0.2	TCP	76	53610 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1
2	0.000012	172.24.0.1	172.24.0.2	TCP	76	[TCP Out-Of-Order] 53610 → 21 [SYN] Seq=0 Wi
3	0.000062	172.24.0.2	172.24.0.1	TCP	76	21 → 53610 [SYN, ACK] Seq=0 Ack=1 Win=65160
4	0.000062	172.24.0.2	172.24.0.1	TCP	76	[TCP Out-Of-Order] 21 → 53610 [SYN, ACK] Seq
5	0.000097	172.24.0.1	172.24.0.2	TCP	68	53610 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0
6	0.000103	172.24.0.1	172.24.0.2	TCP	68	[TCP Dup ACK 5#1] 53610 → 21 [ACK] Seq=1 Ack
7	0.007628	172.24.0.2	172.24.0.1	FTP	117	Response: 220 ProFTPD Server (Debian) [::fff
8	0.007628	172.24.0.2	172.24.0.1	TCP	117	[TCP Retransmission] 21 → 53610 [PSH, ACK] S
9	0.007684	172.24.0.1	172.24.0.2	TCP	68	53610 → 21 [ACK] Seq=1 Ack=50 Win=65536 Len=
10	0.007692	172.24.0.1	172.24.0.2	TCP	68	[TCP Dup ACK 9#1] 53610 → 21 [ACK] Seq=1 Ack
11	0.008172	172.24.0.1	172.24.0.2	FTP	82	Request: USER gpshark
12	0.008181	172.24.0.1	172.24.0.2	TCP	82	[TCP Retransmission] 53610 → 21 [PSH, ACK] S
13	0.008212	172.24.0.2	172.24.0.1	TCP	68	21 → 53610 [ACK] Seq=50 Ack=15 Win=65280 Len
14	0.008212	172.24.0.2	172.24.0.1	TCP	68	[TCP Dup ACK 13#1] 21 → 53610 [ACK] Seq=50 A
15	0.008554	172.24.0.2	172.24.0.1	FTP	103	Response: 331 Password required for gpshark
16	0.008554	172.24.0.2	172.24.0.1	TCP	103	[TCP Retransmission] 21 → 53610 [PSH, ACK] S
17	0.008576	172.24.0.1	172.24.0.2	TCP	68	53610 → 21 [ACK] Seq=15 Ack=85 Win=65536 Len
18	0.008583	172.24.0.1	172.24.0.2	TCP	68	[TCP Dup ACK 17#1] 53610 → 21 [ACK] Seq=15 A
19	1.775550	172.24.0.1	172.24.0.2	FTP	102	Request: PASS utflag{sharkbait_hoo_ha_ha}
20	1.775563	172.24.0.1	172.24.0.2	TCP	102	[TCP Retransmission] 53610 → 21 [PSH, ACK] S
21	1.775647	172.24.0.2	172.24.0.1	TCP	68	21 → 53610 [ACK] Seq=85 Ack=49 Win=65280 Len
22	1.775647	172.24.0.2	172.24.0.1	TCP	68	[TCP Dup ACK 21#1] 21 → 53610 [ACK] Seq=85 A
23	1.785848	172.24.0.2	172.24.0.1	FTP	96	Response: 230 User gpshark logged in
24	1.785848	172.24.0.2	172.24.0.1	TCP	96	[TCP Retransmission] 21 → 53610 [PSH, ACK] Seq=85

```
0000  00 04 00 01 00 06 02 42  60 04 71 99 00 00 08 00   ·······B `·q·····
0010  45 10 00 56 2b 89 40 00  40 06 b6 d5 ac 18 00 01   E··V+·@· @·······
0020  ac 18 00 02 d1 6a 00 15  41 cc 6d 8a c7 7b 98 08   ·····j·· A·m··{··
0030  80 18 40 00 58 7c 00 00  01 01 08 0a f8 09 42 6c   ··@·X|·· ·····Bl
0040  23 1d 7c 9c 50 41 53 53  20 75 74 66 6c 61 67 7b   #·|·PASS  utflag{
0050  73 68 61 72 6b 62 61 69  74 5f 68 6f 6f 5f 68 61   sharkbai t_hoo_ha
0060  5f 68 61 7d 0d 0a                                 _ha}··
```

FTP packet 19 shows,

`PASS utflag{sharkbait_hoo_ha_ha}`

Therefore, the flag is,

`utflag{sharkbait_hoo_ha_ha}`