

Welcome to Network !

2nd Hack The Pods Write-up

問題概要

問題文

このファイルは、あるWebサイトへのアクセスログである

この中でやりとりされているメッセージを探し当ててくれ

file: plaintext.pcap

概要

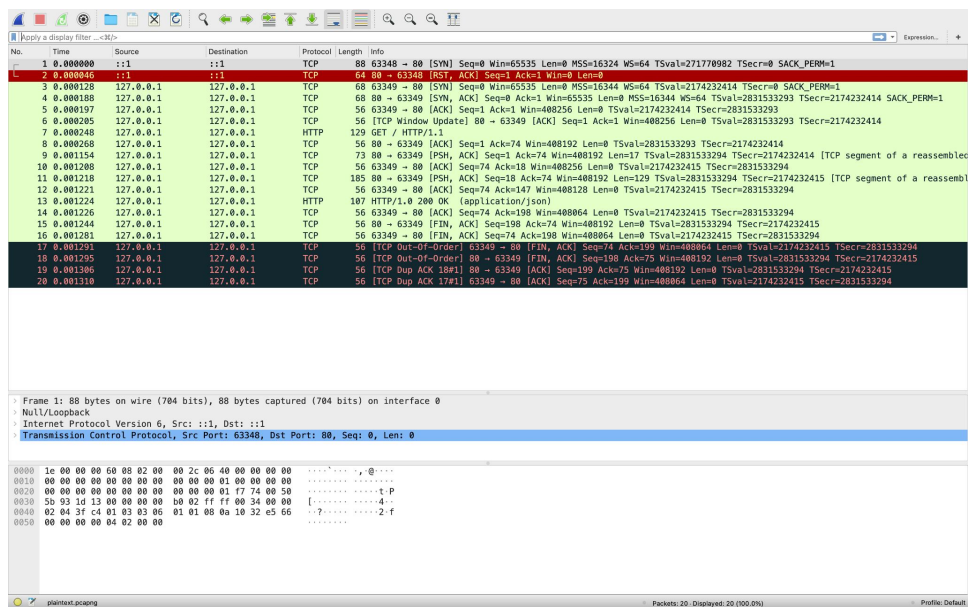
50点 - Network

pcapからやり取りされているメッセージを読み取る問題

pcapファイル

pcapファイルはパケットキャプチャファイル

ネットワーク上でやりとりされたデータが格納されている



The image shows a Wireshark packet capture analysis. The top pane displays a list of 20 network packets. Packet 1 is a TCP SYN packet from 192.168.1.1 to 192.168.1.1. Packet 2 is a TCP ACK packet from 192.168.1.1 to 192.168.1.1. Packet 3 is a TCP SYN packet from 192.168.1.1 to 192.168.1.1. Packet 4 is a TCP ACK packet from 192.168.1.1 to 192.168.1.1. Packet 5 is a TCP SYN packet from 192.168.1.1 to 192.168.1.1. Packet 6 is a TCP ACK packet from 192.168.1.1 to 192.168.1.1. Packet 7 is a TCP SYN packet from 192.168.1.1 to 192.168.1.1. Packet 8 is a TCP ACK packet from 192.168.1.1 to 192.168.1.1. Packet 9 is a TCP SYN packet from 192.168.1.1 to 192.168.1.1. Packet 10 is a TCP ACK packet from 192.168.1.1 to 192.168.1.1. Packet 11 is a TCP SYN packet from 192.168.1.1 to 192.168.1.1. Packet 12 is a TCP ACK packet from 192.168.1.1 to 192.168.1.1. Packet 13 is a TCP SYN packet from 192.168.1.1 to 192.168.1.1. Packet 14 is a TCP ACK packet from 192.168.1.1 to 192.168.1.1. Packet 15 is a TCP SYN packet from 192.168.1.1 to 192.168.1.1. Packet 16 is a TCP ACK packet from 192.168.1.1 to 192.168.1.1. Packet 17 is a TCP SYN packet from 192.168.1.1 to 192.168.1.1. Packet 18 is a TCP ACK packet from 192.168.1.1 to 192.168.1.1. Packet 19 is a TCP SYN packet from 192.168.1.1 to 192.168.1.1. Packet 20 is a TCP ACK packet from 192.168.1.1 to 192.168.1.1.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	:::1	:::1	TCP	88	63348 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=16324 WS=64 TSval=217170982 TSecr=0 SACK_PERM=1
2	0.000000	:::1	:::1	TCP	88	63348 → 80 [ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16324 WS=64 TSval=217170982 TSecr=0 SACK_PERM=1
3	0.000128	127.0.0.1	127.0.0.1	TCP	68	63349 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=64 TSval=2174232414 TSecr=0 SACK_PERM=1
4	0.000188	127.0.0.1	127.0.0.1	TCP	68	80 → 63349 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=64 TSval=2831533293 TSecr=2174232414 SACK_PERM=1
5	0.000197	127.0.0.1	127.0.0.1	TCP	56	63349 → 80 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=2174232414 TSecr=2831533293
6	0.000285	127.0.0.1	127.0.0.1	TCP	56	[TCP Window Update] 80 → 63349 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=2831533293 TSecr=2174232414
7	0.000248	127.0.0.1	127.0.0.1	HTTP	129	GET / HTTP/1.1
8	0.000268	127.0.0.1	127.0.0.1	TCP	56	80 → 63349 [ACK] Seq=1 Ack=74 Win=408192 Len=0 TSval=2831533293 TSecr=2174232414
9	0.001154	127.0.0.1	127.0.0.1	TCP	73	80 → 63349 [PSH, ACK] Seq=1 Ack=74 Win=408192 Len=17 TSval=2831533294 TSecr=2174232414 [TCP segment of a reassembled
10	0.001206	127.0.0.1	127.0.0.1	TCP	56	63349 → 80 [ACK] Seq=74 Ack=18 Win=408256 Len=0 TSval=2174232415 TSecr=2831533294
11	0.001218	127.0.0.1	127.0.0.1	TCP	185	80 → 63349 [PSH, ACK] Seq=18 Ack=74 Win=408192 Len=129 TSval=2831533294 TSecr=2174232415 [TCP segment of a reassemb
12	0.001221	127.0.0.1	127.0.0.1	TCP	56	63349 → 80 [ACK] Seq=74 Ack=147 Win=408128 Len=0 TSval=2174232415 TSecr=2831533294
13	0.001224	127.0.0.1	127.0.0.1	HTTP	107	HTTP/1.0 200 OK (application/json)
14	0.001226	127.0.0.1	127.0.0.1	TCP	56	63349 → 80 [ACK] Seq=74 Ack=198 Win=408064 Len=0 TSval=2174232415 TSecr=2831533294
15	0.001244	127.0.0.1	127.0.0.1	TCP	56	80 → 63349 [FIN, ACK] Seq=198 Ack=74 Win=408192 Len=0 TSval=2831533294 TSecr=2174232415
16	0.001281	127.0.0.1	127.0.0.1	TCP	56	63349 → 80 [FIN, ACK] Seq=74 Ack=198 Win=408064 Len=0 TSval=2174232415 TSecr=2831533294
17	0.001221	127.0.0.1	127.0.0.1	TCP	56	[TCP Out-Of-Order] 63349 → 80 [FIN, ACK] Seq=198 Ack=198 Win=408192 Len=0 TSval=2831533294 TSecr=2174232415
18	0.001295	127.0.0.1	127.0.0.1	TCP	56	[TCP Out-Of-Order] 80 → 63349 [FIN, ACK] Seq=198 Ack=75 Win=408192 Len=0 TSval=2831533294 TSecr=2174232415
19	0.001306	127.0.0.1	127.0.0.1	TCP	56	[TCP Dup ACK 18#1] 80 → 63349 [ACK] Seq=199 Ack=75 Win=408192 Len=0 TSval=2831533294 TSecr=2174232415
20	0.001310	127.0.0.1	127.0.0.1	TCP	56	[TCP Dup ACK 17#1] 63349 → 80 [ACK] Seq=75 Ack=199 Win=408064 Len=0 TSval=2174232415 TSecr=2831533294

Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
Ethernet II, Src: NuLi/Loopback
Internet Protocol Version 6, Src: :::1, Dst: :::1
Transmission Control Protocol, Src Port: 63348, Dst Port: 80, Seq: 0, Len: 0

0000 1c 00 00 00 60 00 02 00 00 2c 06 40 00 00 00 00: @
0010 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00: t P
0020 00 00 00 00 00 00 00 00 00 00 00 01 f7 00 50 00: 4
0030 50 93 1d 13 00 00 00 00 02 02 ff 00 34 00 00 00: 2 f
0040 02 04 3f c4 01 03 06 01 01 06 0a 10 32 e5 66: 2 f
0050 00 00 00 00 04 02 00 00 00 00 00 00 00 00 00 00: 2 f

packet.pcapng Packets: 20, Displayed: 20 (100.0%) Profile: Default

HTTPでやり取りされてる

7	0.000248	127.0.0.1	127.0.0.1	HTTP	129 GET / HTTP/1.1
---	----------	-----------	-----------	------	--------------------

12	0.001221	127.0.0.1	127.0.0.1	TCP	50 65549 → 80 [ACK] Seq=74 Ack=147 Win=48
13	0.001224	127.0.0.1	127.0.0.1	HTTP	107 HTTP/1.0 200 OK (application/json)
14	0.001226	127.0.0.1	127.0.0.1	TCP	56 63340 → 80 [ACK] Seq=74 Ack=108 Win=48

Apply a display filter ...<?/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	:::1	:::1	TCP	88	63348 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=16324 WS=64 TSval=271770982 TSecr=0 SACK_PERM=1
2	0.000046	:::1	:::1	TCP	64	80 → 63348 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	0.000128	127.0.0.1	127.0.0.1	TCP	68	63349 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=64 TSval=2174232414 TSecr=0 SACK_PERM=1
4	0.000188	127.0.0.1	127.0.0.1	TCP	68	80 → 63349 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=64 TSval=2831533293 TSecr=2174232414 SACK_PERM=1
5	0.000197	127.0.0.1	127.0.0.1	TCP	56	63349 → 80 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=2174232414 TSecr=2831533293
6	0.000205	127.0.0.1	127.0.0.1	TCP	56	[TCP Window Update] 80 → 63349 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=2831533293 TSecr=2174232414
7	0.000248	127.0.0.1	127.0.0.1	HTTP	129	GET / HTTP/1.1
8	0.000268	127.0.0.1	127.0.0.1	TCP	56	80 → 63349 [ACK] Seq=1 Ack=74 Win=408192 Len=0 TSval=2831533293 TSecr=2174232414
9	0.001154	127.0.0.1	127.0.0.1	TCP	73	80 → 63349 [PSH, ACK] Seq=1 Ack=74 Win=408192 Len=17 TSval=2831533294 TSecr=2174232414 [TCP segment of a reassembled
10	0.001208	127.0.0.1	127.0.0.1	TCP	56	63349 → 80 [ACK] Seq=74 Ack=18 Win=408256 Len=0 TSval=2174232415 TSecr=2831533294
11	0.001218	127.0.0.1	127.0.0.1	TCP	185	80 → 63349 [PSH, ACK] Seq=18 Ack=74 Win=408192 Len=129 TSval=2831533294 TSecr=2174232415 [TCP segment of a reassembled
12	0.001221	127.0.0.1	127.0.0.1	TCP	56	63349 → 80 [ACK] Seq=74 Ack=147 Win=408128 Len=0 TSval=2174232415 TSecr=2831533294
13	0.001224	127.0.0.1	127.0.0.1	HTTP	107	HTTP/1.0 200 OK (application/json)
14	0.001226	127.0.0.1	127.0.0.1	TCP	56	63349 → 80 [ACK] Seq=74 Ack=198 Win=408064 Len=0 TSval=2174232415 TSecr=2831533294
15	0.001244	127.0.0.1	127.0.0.1	TCP	56	80 → 63349 [FIN, ACK] Seq=198 Ack=74 Win=408192 Len=0 TSval=2831533294 TSecr=2174232415
16	0.001281	127.0.0.1	127.0.0.1	TCP	56	63349 → 80 [FIN, ACK] Seq=74 Ack=198 Win=408064 Len=0 TSval=2174232415 TSecr=2831533294
17	0.001291	127.0.0.1	127.0.0.1	TCP	56	[TCP Out-Of-Order] 63349 → 80 [FIN, ACK] Seq=74 Ack=199 Win=408064 Len=0 TSval=2174232415 TSecr=2831533294
18	0.001295	127.0.0.1	127.0.0.1	TCP	56	[TCP Out-Of-Order] 80 → 63349 [FIN, ACK] Seq=198 Ack=75 Win=408192 Len=0 TSval=2831533294 TSecr=2174232415
19	0.001306	127.0.0.1	127.0.0.1	TCP	56	[TCP Dup ACK 18#1] 80 → 63349 [ACK] Seq=199 Ack=75 Win=408192 Len=0 TSval=2831533294 TSecr=2174232415
20	0.001310	127.0.0.1	127.0.0.1	TCP	56	[TCP Dup ACK 17#1] 63349 → 80 [ACK] Seq=75 Ack=199 Win=408064 Len=0 TSval=2174232415 TSecr=2831533294

> Frame 13: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface 0

> Null/Loopback

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

> Transmission Control Protocol, Src Port: 80, Dst Port: 63349, Seq: 147, Ack: 74, Len: 51

> [3 Reassembled TCP Segments (197 bytes): #9(17), #11(129), #13(51)]

> Hypertext Transfer Protocol

> JavaScript Object Notation: application/json

```

0000 02 00 00 00 45 00 00 67 00 00 40 00 40 06 00 00  ....E...g...@...
0010 7f 00 00 01 7f 00 00 01 00 50 f7 75 5c e8 6c 54  ....P...u\..LT
0020 47 0e f4 e6 80 18 18 ea fe 5b 00 00 01 01 08 0a  G.....[.....
0030 a8 c5 c4 ee 81 98 27 5f 7b 22 66 6c 61 67 22 3a  ....'...{"flag":
0040 22 68 74 70 2d 63 74 66 7b 48 54 54 50 5f 43 4f  "http-ctf":{"HTTP_CO
0050 4d 4d 55 4e 49 43 41 54 45 53 5f 49 4e 5f 50 4c  MMUNICAT ES_IN_PL
0060 41 49 4e 54 45 58 54 7d 22 7d 0a  AINTEXT"}-

```

Frame (107 bytes) Reassembled TCP (197 bytes)

plaintext.pcapng

Packets: 20 · Displayed: 20 (100.0%) Profile: Default

0000	02 00 00 00 45 00 00 67	00 00 40 00 40 06 00 00E..g ..@·@...
0010	7f 00 00 01 7f 00 00 01	00 50 f7 75 5c e8 6c 54 ·P·u\·lT
0020	47 0e f4 e6 80 18 18 ea	fe 5b 00 00 01 01 08 0a	G..... ·[.....
0030	a8 c5 c4 ee 81 98 27 5f	7b 22 66 6c 61 67 22 3a'_"{"flag":
0040	22 68 74 70 2d 63 74 66	7b 48 54 54 50 5f 43 4f	"htp-ctf {HTTP_CO
0050	4d 4d 55 4e 49 43 41 54	45 53 5f 49 4e 5f 50 4c	MMUNICAT ES_IN_PL
0060	41 49 4e 54 45 58 54 7d	22 7d 0a	AINTEXT} "}.

0000	02 00 00 00 45 00 00 67	00 00 40 00 40 06 00 00E..g ..@.@...
0010	7f 00 00 01 7f 00 00 01	00 50 f7 75 5c e8 6c 54P.u\..lT
0020	47 0e f4 e6 80 18 18 ea	fe 5b 00 00 01 01 08 0a	G..... .[.....
0030	a8 c5 c4 ee 81 98 27 5f	7b 22 66 6c 61 67 22 3a'_ {"flag":
0040	22 68 74 70 2d 63 74 66	7b 48 54 54 50 5f 43 4f	"http-ctf {HTTP_CO
0050	4d 4d 55 4e 49 43 41 54	45 53 5f 49 4e 5f 50 4c	MMUNICAT ES_IN_PL
0060	41 49 4e 54 45 58 54 7d	22 7d 0a	AINTEXT} "}.·

http-ctf{HTTP_COMMUNICATES_IN_PLAINTEXT}

おきもち

パケットキャプチャするとやり取りされているデータが見える

HTTPはコンテンツが平文でやりとりされる

普通のページならいいけど，ログイン情報とかも抜ける

CTFdのログイン情報がハックできるって言ったのはこれが1つ

パケットキャプチャするだけなら犯罪じゃないのでたくさん覗こう！