

The shark

Description: There is pcapng file. Can you reveal the authentication credentials?

Level: Level 1

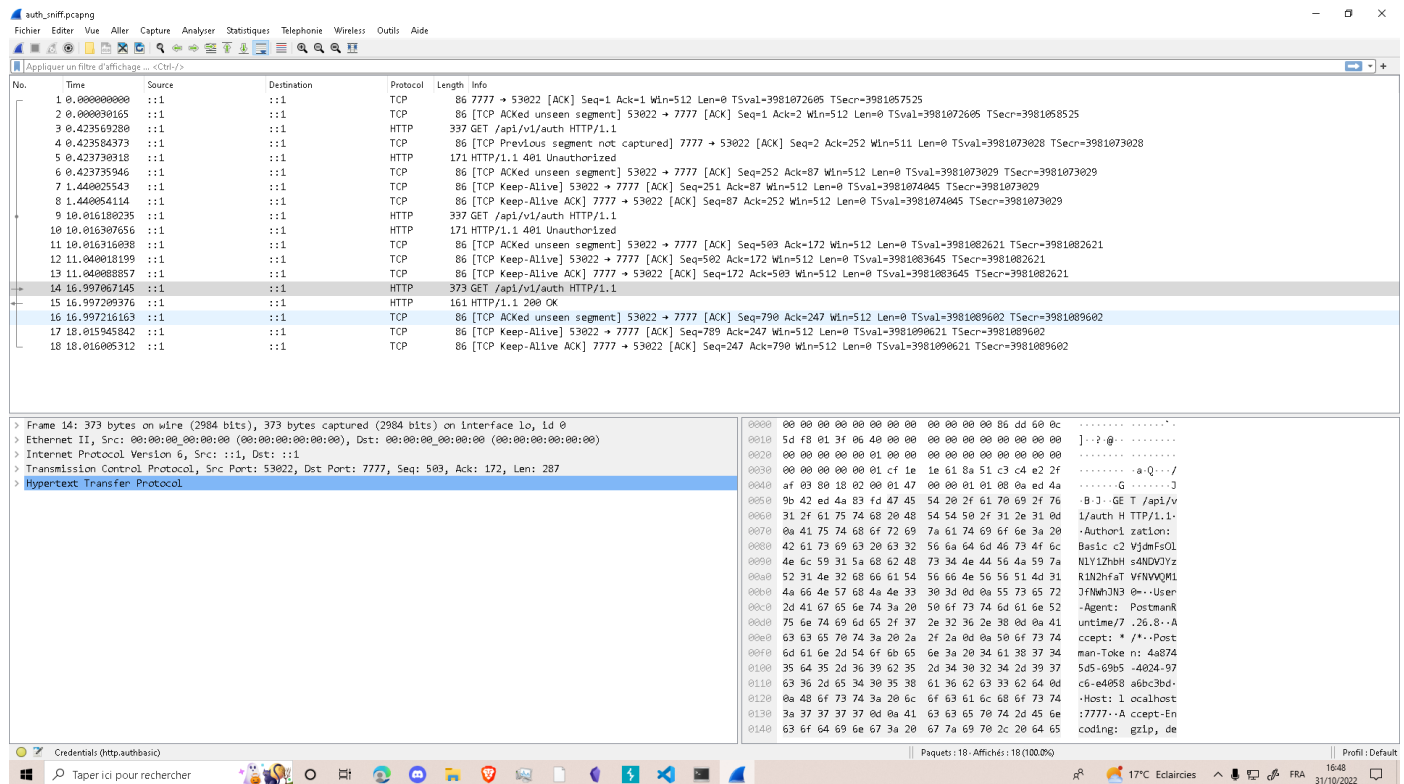
Type: network

Link: <https://ctf.securityvalley.org/dashboard>

So the only thing we got is a `.pcap` file that we can open with

Wireshark

When opening the file we can see the network snapshot:



We are looking for an authorization token, so we can see a `200 OK` "header" which means that everything is ok, so that the user is logged in. By taking a look at the line before, we can see that it is where the user log in

auth_sniff.pcapng

Fichier Editer Vue Aller Capture Analyser Statistiques Telephone Wireless Outils Aide

Appliquer un filtre d'affichage ... <Ctrl>/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	:::1	:::1	TCP	86	7777 → 53022 [ACK] Seq=1 Ack=1 Win=512 Len=0 TSval=3981072605 TSecr=3981057525
2	0.000000165	:::1	:::1	TCP	86	[TCP ACKED unseen segment] 53022 → 7777 [ACK] Seq=1 Ack=2 Win=512 Len=0 TSval=3981072605 TSecr=3981058525
3	0.423569280	:::1	:::1	HTTP	337	GET /api/v1/auth HTTP/1.1
4	0.423568373	:::1	:::1	TCP	86	[TCP Previous segment not captured] 7777 → 53022 [ACK] Seq=2 Ack=252 Win=511 Len=0 TSval=3981073028 TSecr=3981073028
5	0.423736918	:::1	:::1	HTTP	171	HTTP/1.1 401 Unauthorized
6	0.423735946	:::1	:::1	TCP	86	[TCP ACKED unseen segment] 53022 → 7777 [ACK] Seq=252 Ack=87 Win=512 Len=0 TSval=3981073029 TSecr=3981073029
7	1.440825543	:::1	:::1	TCP	86	[TCP Keep-Alive] 53022 → 7777 [ACK] Seq=251 Ack=87 Win=512 Len=0 TSval=3981074045 TSecr=3981073029
8	1.440854114	:::1	:::1	TCP	86	[TCP Keep-Alive ACK] 7777 → 53022 [ACK] Seq=87 Ack=252 Win=512 Len=0 TSval=3981074045 TSecr=3981073029
9	10.016180235	:::1	:::1	HTTP	337	GET /api/v1/auth HTTP/1.1
10	10.016180756	:::1	:::1	HTTP	171	HTTP/1.1 401 Unauthorized
11	10.016131608	:::1	:::1	TCP	86	[TCP ACKED unseen segment] 53022 → 7777 [ACK] Seq=503 Ack=172 Win=512 Len=0 TSval=3981082621 TSecr=3981082621
12	11.040018199	:::1	:::1	TCP	86	[TCP Keep-Alive] 53022 → 7777 [ACK] Seq=502 Ack=172 Win=512 Len=0 TSval=3981083645 TSecr=3981082621
13	11.040088857	:::1	:::1	TCP	86	[TCP Keep-Alive ACK] 7777 → 53022 [ACK] Seq=172 Ack=503 Win=512 Len=0 TSval=3981083645 TSecr=3981082621
14	16.997067145	:::1	:::1	HTTP	373	GET /api/v1/auth HTTP/1.1
15	16.997209376	:::1	:::1	HTTP	161	HTTP/1.1 200 OK
16	16.997216163	:::1	:::1	TCP	86	[TCP ACKED unseen segment] 53022 → 7777 [ACK] Seq=790 Ack=247 Win=512 Len=0 TSval=3981089602 TSecr=3981089602
17	17.015945842	:::1	:::1	TCP	86	[TCP Keep-Alive] 53022 → 7777 [ACK] Seq=789 Ack=247 Win=512 Len=0 TSval=3981089621 TSecr=3981089602
18	18.016005312	:::1	:::1	TCP	86	[TCP Keep-Alive ACK] 7777 → 53022 [ACK] Seq=247 Ack=790 Win=512 Len=0 TSval=3981089621 TSecr=3981089602

Frame 14: 373 bytes on wire (2984 bits), 373 bytes captured (2984 bits) on Interface lo, Id 0

Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

Internet Protocol Version 6, Src: ::1, Dst: ::1

Transmission Control Protocol, Src Port: 53022, Dst Port: 7777, Seq: 503, Ack: 172, Len: 287

Hypertext Transfer Protocol

Credentials (http.auth.basic)

Taper ici pour rechercher

Paquets: 18 - Affichés: 18 (100.0%)

Profil: Default

16:51 31/10/2022

And by taking a closer look, we can see in **Authorization > Credentials** the flag !

auth_sniff.pcapng

Fichier Editer Vue Aller Capture Analyser Statistiques Telephone Wireless Outils Aide

Appliquer un filtre d'affichage ... <Ctrl>/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	:::1	:::1	TCP	86	7777 → 53022 [ACK] Seq=1 Ack=1 Win=512 Len=0 TSval=3981072605 TSecr=3981057525
2	0.000000165	:::1	:::1	TCP	86	[TCP ACKED unseen segment] 53022 → 7777 [ACK] Seq=1 Ack=2 Win=512 Len=0 TSval=3981072605 TSecr=3981058525
3	0.423569280	:::1	:::1	HTTP	337	GET /api/v1/auth HTTP/1.1
4	0.423568373	:::1	:::1	TCP	86	[TCP Previous segment not captured] 7777 → 53022 [ACK] Seq=2 Ack=252 Win=511 Len=0 TSval=3981073028 TSecr=3981073028
5	0.423736918	:::1	:::1	HTTP	171	HTTP/1.1 401 Unauthorized
6	0.423735946	:::1	:::1	TCP	86	[TCP ACKED unseen segment] 53022 → 7777 [ACK] Seq=252 Ack=87 Win=512 Len=0 TSval=3981073029 TSecr=3981073029
7	1.440825543	:::1	:::1	TCP	86	[TCP Keep-Alive] 53022 → 7777 [ACK] Seq=251 Ack=87 Win=512 Len=0 TSval=3981074045 TSecr=3981073029
8	1.440854114	:::1	:::1	TCP	86	[TCP Keep-Alive ACK] 7777 → 53022 [ACK] Seq=87 Ack=252 Win=512 Len=0 TSval=3981074045 TSecr=3981073029
9	10.016180235	:::1	:::1	HTTP	337	GET /api/v1/auth HTTP/1.1
10	10.016180756	:::1	:::1	HTTP	171	HTTP/1.1 401 Unauthorized
11	10.016131608	:::1	:::1	TCP	86	[TCP ACKED unseen segment] 53022 → 7777 [ACK] Seq=503 Ack=172 Win=512 Len=0 TSval=3981082621 TSecr=3981082621
12	11.040018199	:::1	:::1	TCP	86	[TCP Keep-Alive] 53022 → 7777 [ACK] Seq=502 Ack=172 Win=512 Len=0 TSval=3981083645 TSecr=3981082621
13	11.040088857	:::1	:::1	TCP	86	[TCP Keep-Alive ACK] 7777 → 53022 [ACK] Seq=172 Ack=503 Win=512 Len=0 TSval=3981083645 TSecr=3981082621
14	16.997067145	:::1	:::1	HTTP	373	GET /api/v1/auth HTTP/1.1
15	16.997209376	:::1	:::1	HTTP	161	HTTP/1.1 200 OK
16	16.997216163	:::1	:::1	TCP	86	[TCP ACKED unseen segment] 53022 → 7777 [ACK] Seq=790 Ack=247 Win=512 Len=0 TSval=3981089602 TSecr=3981089602
17	17.015945842	:::1	:::1	TCP	86	[TCP Keep-Alive] 53022 → 7777 [ACK] Seq=789 Ack=247 Win=512 Len=0 TSval=3981089621 TSecr=3981089602
18	18.016005312	:::1	:::1	TCP	86	[TCP Keep-Alive ACK] 7777 → 53022 [ACK] Seq=247 Ack=790 Win=512 Len=0 TSval=3981089621 TSecr=3981089602

Frame 14: 373 bytes on wire (2984 bits), 373 bytes captured (2984 bits) on Interface lo, Id 0

Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

Internet Protocol Version 6, Src: ::1, Dst: ::1

Transmission Control Protocol, Src Port: 53022, Dst Port: 7777, Seq: 503, Ack: 172, Len: 287

Hypertext Transfer Protocol

GET /api/v1/auth HTTP/1.1

Authorization: Basic c2VjdFMsOlNlY1ZhbH54NDVzRlN2hfaTVFNWQMLjFmMhN30=

Credentials: secval:SecVal{845Ic4u7h_i5_5UP3R_5hI7}

User-Agent: PostmanRuntime/7.26.8

Accept: */*

Postman-Token: 4a8745d5-69b5-4802-97c6-e4058a6bc3bd

Host: localhost:7777

Accept-Encoding: gzip, deflate

Connection: keep-alive

Full request URI: http://localhost:7777/api/v1/auth

[HTTP request 3/3]

[Prev request in frame: 9]

[Response in frame: 15]

Outils: 06-08 Request Method (http.request.method)

Taper ici pour rechercher

Paquets: 18 - Affichés: 18 (100.0%)

Profil: Default

16:50 31/10/2022

So, the flag is: **SecVal{845Ic4u7h_i5_5UP3R_5hI7}**