

Домашнее задание урок 6.

1. Найти любой не зашифрованный сайт, где требуется форма ввода пароля. Может злоумышленник перехватить этот пароль?

Пришлось воскресить мой старый проект) в который мы рубились одно время: <http://x.utea.ru>, он весь в кракрозьябрах, но думаю это не важно.

Определяем IP: ping x.utea.ru - 185.130.82.109

Ставим фильтр по назначению: ip.dst == 185.130.82.109

Переходим на сайт, вводим логин и пароль, нажимаем «enter».

Ну и собственно особо и искать не пришлось, сразу и видно, в запросе POST все передается в открытом виде:

The image shows a Wireshark packet capture of an HTTP POST request. The packet list shows a POST request from 192.168.25.107 to 185.130.82.109. The packet details pane shows the request body as an HTML Form URL Encoded string. The form items are: username=admin, password=passwords, and submit= (indicated by a key icon). The packet bytes pane shows the raw data, with the password field highlighted in red.

File Action Media Clipboard View Help

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 185.130.82.109

No.	Time	Source	Destination	Protocol	Length	Info
15747	1025.627529	192.168.25.107	185.130.82.109	TCP	54	58637 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
15748	1025.627576	192.168.25.107	185.130.82.109	TCP	54	58638 → 80 [FIN, ACK] Seq=475 Ack=3099 Win=130304 Len=0
15753	1025.628614	192.168.25.107	185.130.82.109	TCP	54	58637 → 80 [ACK] Seq=2 Ack=2 Win=131328 Len=0
15754	1025.628628	192.168.25.107	185.130.82.109	TCP	54	58638 → 80 [ACK] Seq=476 Ack=3100 Win=130304 Len=0
16569	1158.453981	192.168.25.107	185.130.82.109	TCP	66	58717 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
16570	1158.454242	192.168.25.107	185.130.82.109	TCP	66	58718 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
16572	1158.456271	192.168.25.107	185.130.82.109	TCP	54	58717 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
16574	1158.456315	192.168.25.107	185.130.82.109	TCP	54	58718 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
16575	1158.458847	192.168.25.107	185.130.82.109	HTTP	728	POST / HTTP/1.1 (application/x-www-form-urlencoded)
16576	1158.459721	192.168.25.107	185.130.82.109	TCP	54	58718 → 80 [ACK] Seq=675 Ack=230 Win=131072 Len=0
16580	1158.884262	192.168.25.107	185.130.82.109	TCP	54	58718 → 80 [ACK] Seq=675 Ack=940 Win=130304 Len=0
16584	1160.902358	192.168.25.107	185.130.82.109	HTTP	556	GET / HTTP/1.1
16587	1161.021067	192.168.25.107	185.130.82.109	TCP	54	58718 → 80 [ACK] Seq=1177 Ack=2655 Win=131328 Len=0
16590	1161.022398	192.168.25.107	185.130.82.109	TCP	54	58718 → 80 [ACK] Seq=1177 Ack=4037 Win=129792 Len=0
16621	1165.862275	192.168.25.107	185.130.82.109	TCP	54	58717 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
16622	1165.862368	192.168.25.107	185.130.82.109	TCP	54	58718 → 80 [FIN, ACK] Seq=1177 Ack=4037 Win=129792 Len=0
16627	1165.863551	192.168.25.107	185.130.82.109	TCP	54	58717 → 80 [ACK] Seq=2 Ack=2 Win=131328 Len=0
16628	1165.863573	192.168.25.107	185.130.82.109	TCP	54	58718 → 80 [ACK] Seq=1178 Ack=4038 Win=129792 Len=0

[Next request in frame: 16584]

File Data: 76 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

- > Form item: "username" = "admin"
- > Form item: "password" = "passwords"
- > Form item: submit = (key icon)

Key: submit

01d0	69 6d 61 67 65 2f 77 65	62 70 2c 69 6d 61 67 65	image/we bp,image
01e0	2f 61 70 6e 67 2c 2a 2f	2a 3b 71 3d 30 2e 38 2c	/apng,*/ *;q=0.8,
01f0	61 70 70 6c 69 63 61 74	69 6f 6e 2f 73 69 67 6e	applicat ion/sign
0200	65 64 2d 65 78 63 68 61	6e 67 65 3b 76 3d 62 33	ed-excha nge;v=b3
0210	3b 71 3d 30 2e 39 0d 0a	52 65 66 65 72 65 72 3a	;q=0.9... Referer:
0220	20 68 74 74 70 3a 2f 2f	78 2e 75 74 65 61 2e 72	http:// x.utea.r
0230	75 2f 0d 0a 41 63 63 65	70 74 2d 45 6e 63 6f 64	u/...Acce pt-Encod
0240	69 6e 67 3a 20 67 7a 69	70 2c 20 64 65 66 6c 61	ing: gzi p, defla
0250	74 65 0d 0a 41 63 63 65	70 74 2d 4c 61 6e 67 75	te...Acce pt-Langu
0260	61 67 65 3a 20 72 75 2d	52 55 2c 72 75 3b 71 3d	age: ru- RU,ru;q=
0270	30 2e 39 2c 65 6e 2d 55	53 3b 71 3d 30 2e 38 2c	0.9,en-ll S;q=0.8
0280	65 6e 3b 71 3d 30 2e 37	0d 0a 0d 0a 75 73 65 72	en;q=0.7 ...user
0290	6e 61 6d 65 3d 61 64 6d	69 6e 26 70 61 73 73 77	name=adm in&passw
02a0	6f 72 64 3d 70 61 73 73	77 6f 72 73 26 73 75 62	ord=pass wors&sub
02b0	6d 69 74 3d 25 45 46 25	42 46 25 42 44 25 45 46	mit=%EF% BF%BD%EF
02c0	25 42 46 25 42 44 25 45	46 25 42 46 25 42 44 25	Not %00% Not %00%
02d0	45 46 25 42 46 25 42 44		EF%BF%BD

Выводы: если у злоумышленника будет доступ к каналу передачи, он сможет получить пароль.

2. Использовать гугл хром. Нужно найти сайт с картинками не шифрованный. Сколько открыто TCP-сессий и зачем.

Ответа нет, как я ни силюсь я не понял, что от меня требуется. Буду ждать разбора ДЗ

3. Повторить задание 1 с https. Вопрос аналогичный.

При использовании https трафик шифруется и в wireshark мы видим кракрозьябры) Но! имея некоторые представления о шифровании я понимаю, что оба субъекта должны обменяться ключами для шифрования, следовательно, делаю предположение, что их можно перехватить. Немного углубившись в эту тему, я понял, что так и есть, если очень упрощенно, клиент используя открытый ключ сервера добавляя некоторую случайную информацию, обменивается с сервером сеансовыми ключами наверное теоретически и их тоже можно перехватить. В случае если есть доступ к локальной машине, то можно попросить браузер их сохранять и даже настроить wireshark для расшифровки трафика, на скрине обращение к сайту "citilink.ru" (178.248.234.66), форма авторизации там мы видим расшифрованный трафик, ну а раз смог wireshark смогут и другие:

Wireshark capture of an HTTPS session. The packet list shows a series of TLS and HTTP messages. Packet 1192 is selected, showing the HTTP POST request body with form data.

No.	Time	Source	Destination	Protocol	Length	Info
1175	115.132458	178.248.234.66	192.168.25.107	TLSv1.3	1471	Certificate, Certificate Verify, Finished
1176	115.132478	192.168.25.107	178.248.234.66	TCP	54	64989 → 443 [ACK] Seq=589 Ack=5514 Win=64240 Len=0
1177	115.132936	192.168.25.107	178.248.234.66	TLSv1.3	118	Change Cipher Spec, Finished
1178	115.135613	178.248.234.66	192.168.25.107	TLSv1.3	1471	Certificate, Certificate Verify, Finished
1179	115.135665	192.168.25.107	178.248.234.66	TCP	54	64988 → 443 [ACK] Seq=518 Ack=5514 Win=64240 Len=0
1188	115.140341	192.168.25.107	178.248.234.66	TLSv1.3	118	Change Cipher Spec, Finished
1190	115.140710	192.168.25.107	178.248.234.66	HTTP2	146	Magic, SETTINGS[0], WINDOW_UPDATE[0]
1191	115.141046	192.168.25.107	178.248.234.66	HTTP2	2536	HEADERS[1]: POST /auth/login/?_from=https://www.citilink.ru/
1192	115.141080	192.168.25.107	178.248.234.66	HTTP2	411	DATA[1] (application/x-www-form-urlencoded)
1193	115.144790	178.248.234.66	192.168.25.107	TCP	60	443 → 64992 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
1194	115.144815	192.168.25.107	178.248.234.66	TCP	54	64992 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1195	115.145055	192.168.25.107	178.248.234.66	TLSv1.3	571	Client Hello
1227	115.179376	178.248.234.66	192.168.25.107	TLSv1.3	325	New Session Ticket
1228	115.179411	178.248.234.66	192.168.25.107	TLSv1.3	325	New Session Ticket
1229	115.179411	178.248.234.66	192.168.25.107	HTTP2	116	SETTINGS[0], WINDOW_UPDATE[0]
1230	115.179437	192.168.25.107	178.248.234.66	TCP	54	64989 → 443 [ACK] Seq=653 Ack=6118 Win=63636 Len=0
1231	115.185901	178.248.234.66	192.168.25.107	TCP	60	443 → 64988 [ACK] Seq=5514 Ack=674 Win=30016 Len=0

Frame 1192: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on interface \Device\NPF_{25CF267E-C60D-45E1-958C-7E6A9DA40816}, id 0
Ethernet II, Src: Microsof f4:f4:02 (00:15:5d:f4:f4:02), Dst: MitacInt_48:bd:62 (00:22:4d:48:bd:62)
Internet Protocol Version 4, Src: 192.168.25.107, Dst: 178.248.234.66
Transmission Control Protocol, Src Port: 64988, Dst Port: 443, Seq: 3156, Ack: 5514, Len: 357
Transport Layer Security
HyperText Transfer Protocol 2
Stream: DATA, Stream ID: 1, Length 326
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "authorized" = "true"
Form item: "login" = "+79138884407"
Form item: "pass" = "password"
Form item: "token" = "3fUnKASbZEW5QLa0CKtZxv6/11ZEB1YGNkMdPdmz26RMcX07oPIE/3Gp8hc/YYfP6VMkElJw673PY00cwH850HZ2o3ZZNQ==_942f81789ff8d7fcc2fef2ee8a726440"
Form item: "csrf" = "d34a212b873c19f45f0b763916a1e8360d837ff4"
Form item: "version" = ""

0000 00 22 4d 48 bd 62 00 15 5d f4 f4 02 08 00 45 00 ..MH.b...].....E.
0010 01 8d 0d 1f 40 00 80 06 00 00 c0 a8 19 6b b2 f8 ...@... ..k..
0020 ea 42 fd dc 01 bb f0 1f 42 e0 c5 49 b8 16 50 18 .B.....B..I..P..
0030 fa f0 78 ce 00 00 17 03 03 01 60 0f 3e 23 1d e5 ...x.....>#..
0040 38 3d 5b 84 ab fd ef d5 94 09 79 3b 55 b2 ed 53 8=[.....;y;U..S
0050 6a fc e4 6c 12 b9 0e 37 8a b7 3d ae 52 0a 4c a9 j..1...7 ..=R..L..
0060 11 f9 10 fc 32 80 86 93 1e 1b 62 e7 70 1c b1 f72....b.p..
0070 64 4b ed e0 7e 12 df 11 01 d8 f4 dc fe 83 24 8e dK.....\$..
0080 34 eb 51 db 19 6f 5c 82 dd a1 af 25 38 f4 7f 84 4Q...o\...%8..
0090 e2 0c 17 45 9f 76 a6 40 61 fc f1 9b be 2d b8 3e ...E.v.@ a.....>

Frame (411 bytes) Decrypted TLS (335 bytes)

Вывод: На самом деле все конечно же сложнее, но не мне вам это объяснять) Если трафик слушается на локальной машине, то https полагаю не спасет). А вот если вклинится в сеть передачи, то задача сильно усложняется.