如何利用Wireshark解密TLS加密报文

应用审计 孔凡安 3天前 发表

回题描述

如何利用Wireshark工具解密TLS加密报文:

- 1. 需要有服务器的key文件;
- 2. 涉及ECDHE算法的报文无法解密

1. 打开首选项				
在Wireshark中,	前往 Edit -> Preferences	或按键盘快捷键	Ctrl + Shift +	P 开启首选
项窗口。				

2. 导航到 TLS 设置 在首选项窗口中,导航到 Protocols -> TLS 部分。

3. 导入 RSA 私钥 在 TLS 选项中,找到 RSA keys list 选项,点击 Edit 按钮。

步骤详细说明: 点击 New:打开新建一个新的私钥配置条目。

填写相应信息:

IP Address: 输入服务器的 IP 地址。 Port: 输入端口号 (通常是 443, 代表 HTTPS 流量)。 Protocol: 通常输入 http 或其他协议。 Key File: 通过浏览按钮选择你的 RSA 私钥文件路径 (例 如: /path/to/your/private_key.pem)。 确认并保存:点击 OK 进行保存,返回上层界面,再次点击 OK 确认所有配置。

AT			•	× 4
桶台		1.	Б	~コ
用于	トノノ	\sim	J	12

实践操作:

▲ Wireshark · 首选项		ACK1 Sen=91 Ack=1826 Win=819	92 Len=14
TACACS+ ^ Transport Laver Security		ACK] Seg=1551 Ack=1826 Win=8	8192 Len=
TALI		ACK] Seq=1826 Ack=3011 Win=2	259072 Le
, TAPA RSA keys list Edit		Update] 2159 → 443 [ACK] Sec	q=1826 Ac
TCAP TLS debug file			
TCP	36(105)	Done	
TCPCL	Allacini	ACK1 Son=1826 Ack=4040 Win=2	261056 Le
TCPENCAP Reassemble TLS records spanning multiple T	C a its becrypt	^ ,	, Finishe
TDMAE Reassemble TLS Application Data spanning i	mi in addama	K 61-	
		Key File	262080 Le
TDS	e 180.168.8.180 443 tcp L	D:/1- B/chinasws.com.	d43c2b8d5
TeamSpeak Pre-Shared Key		2	7128 Len=
TECMP (Pre)-Master-Secret log filename			
TELNET	-		
Teredo	-		03 fc
TETRA			3d 06
TFP			02 04
TFTP			00 00
Thread			
Thrift			
Tibia			
TIME			
TIPC			
IWoConne I	<	>	
THE			
INS			
· ·	+	C\Users\k25855\AppData\Roaming\Wireshark\ssl_keys	
		确定 复制自 取消 帮助	

解密效果如下:

TLS协商的算法:



解密后的报文如下,关注目标端口为443.但是报文内容明文显示。如下:

HTTP/1.1

<	
> Frame 18: 805 bytes on wire (6440 bits), 805 bytes captured (6440 bits)	▲ 0000 00 00 01 40 00 00 04 40 20 43 30 83 81 00 03 fc ····@···@··CO·····
> Ethernet II, Src: NewH3CTechno 43:30:83 (84:40:a9:43:30:83), Dst: Xerox 40:00:00 (00:00:01:40:00:00)	0010 81 88 93 b6 88 99 45 88 93 ef 88 99 40 99 3d 86 ·····E·····₽····
> 802.10 Virtual LAN, PRI: 0, DEI: 0, ID: 1020	0020 01 95 0a 00 71 18 b4 a8 08 b4 08 61 01 bb a4 10
> 802.10 Virtual LAN, PRI: 0, DEI: 0, ID: 950	0030 46 36 02 CC 12 41 50 18 10 00 44 03 00 00 17 03 F ···· AP· ··D····
> Internet Protocol Version 4, Src: 10.0.113.248, Dst: 180 180	0050 32 f9 75 a6 8c 87 d1 b2 e2 89 75 53 d3 b8 81 73 2-uuSCS
> Transmission Control Protocol, Src Port: 2156, Det Port: 443, Sec. 2144, Ack: 4091, Len: 743	0060 0d 60 03 eb bd 61 48 b6 6e 1b 7f 33 8e 8a 7c d9 · · · · aH· n · · 3 · ·
Y Transport Laver Security	0070 a7 8d 72 b0 84 5f 36 a9 9f 7d 3a 21 9c 61 09 0a ··r··6··):!.a··
 Timoport Legen Josef Anglication Data Bratoval: Transmission Control Protoval 	0000 ac 8b 41 fb 0d c0 8c da 62 e1 b0 ee dc 7d 46 a8 ··A···· b····}F·
Instant work of Lapid a spin of the formation of the	0000 e8 1c a9 2f c7 d4 8b 7f bd 64 17 86 18 98 46 c2/dF
Content Type: Application bata (25)	0000 b3 c4 06 at 31 d6 e0 48 8d 39 08 d5 16 4c eb aa ····1··H ·9···L··
Version: 1.2 (000005)	0000 67 01 25 10 01 66 76 11 10 02 60 07 02 14 01 11 1 10 17 10 10
Length: /38	0010 05 ro 13 as 04 de r1 dd dr 35 6e ad 46 50 ab 3e
Encrypted Application Data [truncated]: 000000000000000000aaf0d02a3432f975a60c87d1b2e209755343b881730d6003ebbd6148b66e1b7f338e8	5000 de a3 a6 52 33 c0 e4 45 2f c0 a4 3b cf b7 9c 30 N 83 F (0
[Application Data Protocol: Transmission Control Protocol]	00f0 e2 8a 7f 4b 3d 71 36 4a 0b 47 a8 57 8d 6e c7 f9 ···K=q67 ·G·W·n··
 Hypertext Transfer Protocol 	0100 fd 53 61 9a 88 68 86 15 82 0c f8 3c 5d fc c9 63 -Sa-h
> GET /iiot-prod/mahl-/sociocas/fractionades-shoulds-shoulds-should are utrain 1\r\n	0110 89 43 cf ca e1 8f 74 7a 52 7b 69 74 87 5f 23 82 -Ctz R{it-#-
Host: mobile.communectm.com	0120 80 01 0c d6 3e 5b 66 ac f1 f7 5c 2f 1b c7 59 84 ····>[f···\/··Y·
Connection: keep-alive\r\n	0130 ee 60 20 8T 0C De 8T 3C 3e T2 48 /1 30 88 T3 19
sec-ch-ua: "Not/A)Brand";y="8", "Chromium";y="126", "Google Chrome";y="126"\n\n	0140 10 30 00 70 47 00 00 47 45 77 20 00 55 02 55 00 00 - 77 00 °C °, 55 °
DWT: 1\r\n	0100 59 98 74 d1 2a a1 58 35 97 58 88 17 89 69 85 f4 Y-L-* X5 P
sec-ch-ua-mobile: 20\r\n	0170 56 53 a0 4e a0 37 8a d1 49 98 fb 87 29 70 ed 79 VS-N-7 I)p-y
line Apart: Mavilla/5 & /Mavinterh: Total Mar OS Y 18 15 7) Apalakabrit/527 26 (WHTML like Sarka) (hopen/126 & 8 & Safari/527 2	0180 06 64 4d 42 4a 0f 72 7d a0 62 d9 f0 4d b0 aa f6 dM83 r) - b - M
and spine interactions and the or a reaction of the second s	0190 Sa 64 e8 20 96 f8 06 13 f3 e2 c3 8b 7a 24 b4 29 Zd ·······z\$·)
according particular in according to a section of the section of t	0100 1e f6 b8 af 9b 38 48 23 68 ec 5c 25 07 1a f9 a6
Accel: 1 melley act, 1melley accel, 1 melley acle 208-001, 1 melley, 208-001, 1 melley, 1, 1 diore (1, 1)	0100 5e 3e 3e dd c7 ab 4b 8b 87 66 7e dd 08 20 be 39 ^>>K -++9
Sec-Fetch-Site: cross-site\r\n	0100 43 /C 00 5/ TT 76 /6 2T 90 5T /0 3/ 0C 18 18 3C C[-N-V/ - [/C
Sec-Fetch-Hode: no-cors\r\n	0100 14 06 07 05 05 44 76 50 CC 9C 65 60 07 74 45 05
Sec-Fetch-Dest: image\n\n	01f0 ad 9a 87 9e a2 2c a7 d0 ca 83 ee 29 f9 e5 3b 41
Referer: http://localhost:81/\r\n	0200 0e 38 7b 34 24 d4 fa c9 f9 e6 4f b0 25 1b 69 15 8(4\$0%1
Accept-Encoding: gzip, deflate, br, zstd\r\n	0210 06 ea 9b 06 4c 57 47 05 4d 05 41 1f 2b fa 5a 77LWG- H-A-+-ZW
Accept-Language: en-US,enjq-0.0 zh-CNjq-0.8,zhjq-0.7,kojq-0.6,zh-TWjq-0.5,amjq-0.4,frjq-0.3\r\n	0220 95 c0 c9 10 bb 39 29 c0 0e d4 44 e4 09 ce 81 92 ·····9)· ··D·····
\r\n	v
	P STOPPE C A PRODUCTION OF PERSON AND A STOPPE A CONTRACT OF A STOPPE A S