

Отчет анализа дампа Серов Глеб Ильич

1. Участвующие хосты

В дампе присутствуют следующие основные узлы:

IP-адрес	Роль
192.168.118.129	Клиент
192.168.118.128	Сервер
192.168.118.1	Предполагаемый шлюз (ответов не наблюдается в дампе)

Сеть относится к диапазону 192.168.118.0/24.

2. Общая картина взаимодействия.

Взаимодействие между клиентом и сервером происходит в несколько этапов:

1. ARP-резолвинг (клиент пытается определить MAC-адреса других узлов).
2. HTTP-соединение (порт 1337) – передача данных в открытом виде.
3. TLS-соединение (порт 1338) – защищенный канал.

3. Анализ переданных данных.

ARP-трафик

В дампе наблюдаются ARP-запросы вида “Who has 192.168.118.1?/Who has 192.168.118.128?”. Ответы получены только от сервера 192.168.118.128 (рис. 1).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	VMware_23:75:b6	Broadcast	ARP	42	Who has 192.168.118.1? Tell 192.168.118.129
2	3.005975	VMware_23:75:b6	Broadcast	ARP	42	Who has 192.168.118.1? Tell 192.168.118.129
3	4.004544	VMware_23:75:b6	Broadcast	ARP	42	Who has 192.168.118.1? Tell 192.168.118.129
4	5.004453	VMware_23:75:b6	Broadcast	ARP	42	Who has 192.168.118.1? Tell 192.168.118.129
5	8.009009	VMware_23:75:b6	Broadcast	ARP	42	Who has 192.168.118.1? Tell 192.168.118.129
6	9.008399	VMware_23:75:b6	Broadcast	ARP	42	Who has 192.168.118.1? Tell 192.168.118.129
7	9.509763	VMware_23:75:b6	Broadcast	ARP	42	Who has 192.168.118.128? Tell 192.168.118.129
8	9.511210	VMware_ff:a1:64	VMware_23:75:b6	ARP	60	192.168.118.128 is at 00:0c:29:ff:a1:64

Рисунок 1 – Ответ от сервера на ARP запрос.

В дампе не наблюдается защиты ARP (по типу ARP ACL, DAI), то есть, в сети отсутствуют механизмы предотвращения ARP-spoofing.

HTTP-трафик (порт 1337).

Клиент выполняет HTTP-запрос “GET /k3y HTTP/1.1”. Ответ сервера содержит закрытый криптографический ключ в формате PEM (рис. 2).

```
0120 3d 35 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e =5, max= 100..Con
0130 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c nection: Keep-Al
0140 69 76 65 0d 0a 0d 0a 2d 2d 2d 2d 42 45 47 49 ive....- ----BEGI
0150 4e 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d N PRIVAT E KEY---
0160 2d 2d 0a 4d 49 49 45 76 41 49 42 41 44 41 4e 42 ---.MIIEv AIBADANB
0170 67 6b 71 68 6b 69 47 39 77 30 42 41 51 45 46 41 gkqhkiG9 w0BAQEFA
0180 41 53 43 42 4b 59 77 67 67 53 69 41 67 45 41 41 ASCBKYwg gSiAgEAA
0190 6f 49 42 41 51 43 78 68 75 63 63 64 65 42 6a 35 oIBAQCxh uccdeBj5
01a0 76 6b 6c 0a 74 66 68 4d 69 6a 4d 64 33 77 4b 38 vkl.tfhM iJMd3wK8
01b0 4c 53 4e 77 56 63 64 49 4c 6f 65 78 72 54 46 4e LSNwVcdI LoexrTFN
01c0 45 46 79 6c 47 4d 4c 37 30 38 51 68 51 6f 63 35 EFylGML7 08QhQoc5
01d0 2f 44 46 68 6a 6b 64 6c 36 35 38 48 52 4e 34 58 /DFhjkdL 658HRN4X
01e0 79 6a 65 67 0a 2f 38 6a 70 67 57 78 64 49 41 6c yjeg./8j pgWxdIAL
01f0 72 71 6b 6b 56 43 33 47 5a 46 42 6d 45 45 53 57 rqqkVC3G ZFBmEESW
0200 49 51 38 42 58 57 4e 73 2b 65 58 4f 6c 51 44 51 IQ8BXWns +eX0lQDQ
0210 39 59 36 79 42 53 4c 43 58 71 73 78 30 66 42 71 9Y6yBSLC Xqsx0fBq
0220 70 34 54 38 33 0a 4a 51 6f 46 5a 52 6a 45 33 57 p4T83.JQ oFZRjE3W
0230 45 45 6f 39 6b 54 6c 38 74 36 39 55 74 73 56 6c EEo9kTl8 t69UtsVL
0240 53 46 63 5a 5a 4c 7a 39 35 45 4c 68 45 73 4d 46 SFCZZLz9 5ELhEsMF
0250 6f 74 66 53 47 64 4d 36 4c 62 32 35 66 52 79 34 otfSGdM6 Lb25fRy4
0260 46 57 4b 53 65 41 0a 37 58 30 77 79 5a 67 5a 4e FwKSeA.7 X0wyZgZN
0270 70 6e 74 45 75 76 53 6f 71 61 64 7a 36 79 48 47 pntEuvSo qad26yHG
0280 79 46 37 35 7a 73 66 38 77 75 69 70 51 4c 48 6d yF75zsf8 wuipQLHm
0290 45 43 4e 5a 36 73 75 31 2f 70 30 31 39 35 75 71 ECNZ6su1 /p0195uq
02a0 61 73 4f 38 6e 47 62 0a 6e 38 2b 45 71 4d 45 38 as08nGb. n8+EqME8
02b0 4c 70 58 51 4c 52 50 53 61 56 69 76 2b 64 4c 46 LpXQLRPS aViv+dLF
02c0 48 2f 43 63 4e 54 6e 6d 35 63 43 52 30 62 30 39 H/CcNTnm 5cCR0b09
02d0 67 7a 32 76 68 73 2b 68 35 34 61 74 51 31 49 6f gz2vhs+h 54atQ1Io
02e0 66 35 76 71 63 71 57 6f 0a 7a 4f 6a 73 33 67 6d f5vqcqWo .z0js3gm
02f0 50 41 67 4d 42 41 41 45 43 67 67 45 41 61 33 32 PAgMBAAE CggEAa32
0300 6c 66 6d 51 5a 5a 43 51 38 67 34 72 31 4e 31 4d lfmQZZCQ 8g4r1N1M
0310 4f 74 47 32 4e 2b 47 62 55 61 48 5a 6e 33 64 72 OtG2N+Gb UaH2n3dr
0320 65 71 73 53 56 62 33 59 53 0a 77 70 79 46 6f 33 eqsSVb3Y S.wpyFo3
```

Рисунок 2 - Ответ сервера

Данный ключ передается без шифрования, что является критической утечкой секретной информации.

TLS-трафик (порт 1338).

После получения ключа клиент устанавливает TLS-соединение с сервером. Можно проследить следующий используемый параметр (рис. 3): Cipher Suite (TLS_RSA_WITH_AES_256_CBC_SHA) – используется RSA key exchange, отсутствует Perfect Forward Secrecy (что достигается с помощью

DHE/ECDHE). То есть, RSA применяется для шифрования premaster secret, который генерируется клиентом, шифруется публичным ключом сервера, расшифровывается сервером приватным ключом, и далее из premaster secret вычисляются master secret, session keys. То есть, безопасность сессии зависит от приватного ключа сервера.

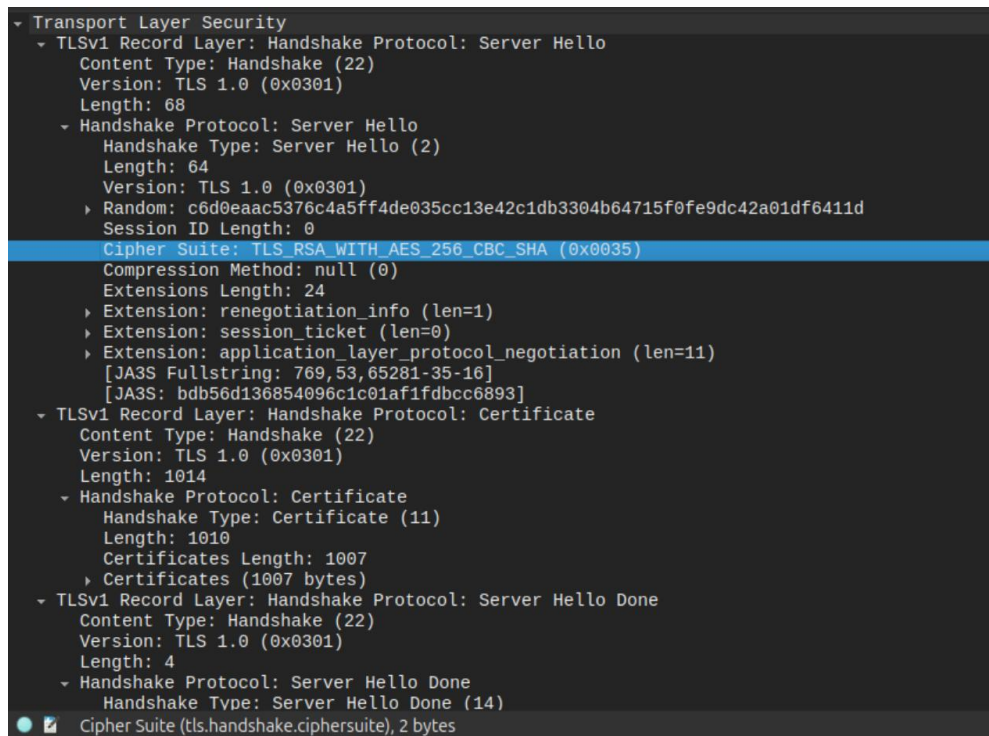


Рисунок 3 – Используемый Cipher Suite

Далее возникла идея расшифровать TLS. Был скопирован полученный ранее ключ, проверен на валидность (рис. 4).

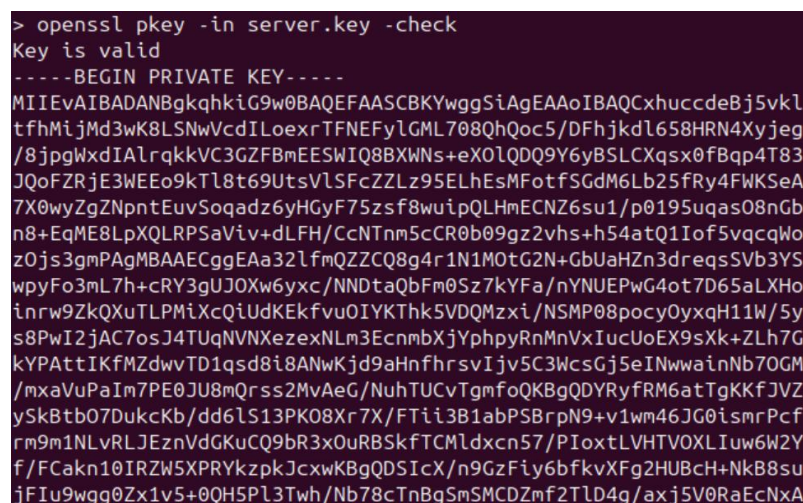


Рисунок 4 – Проверка ключа на валидность

Далее в Wireshark был расшифрован TLS (рис. 5)

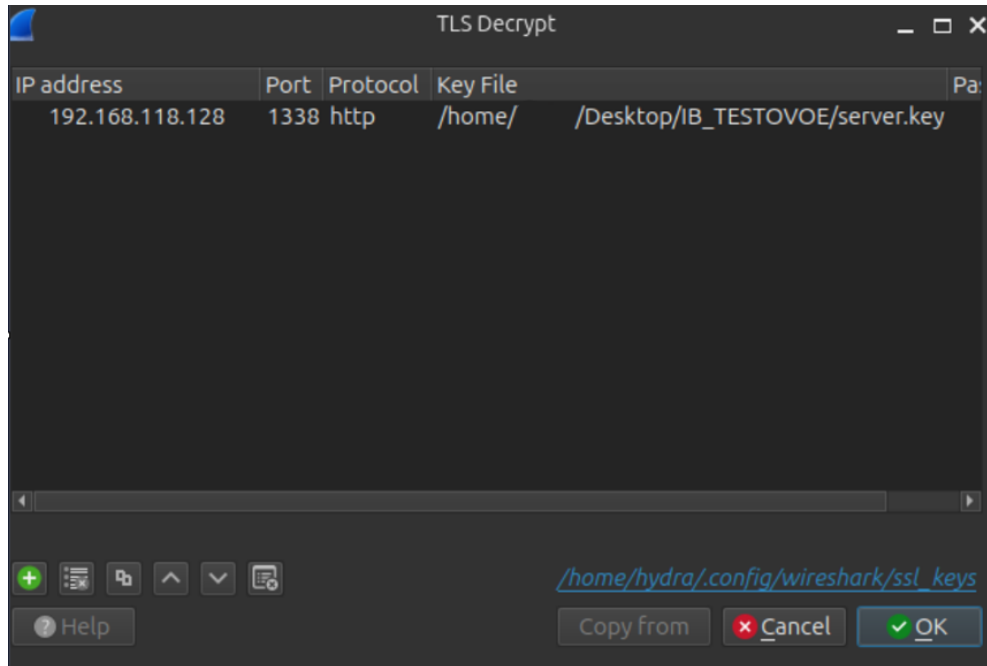


Рисунок 5 – Расшифровка TLS

В результате расшифрования обнаружен еще один GET запрос (рис. 6).

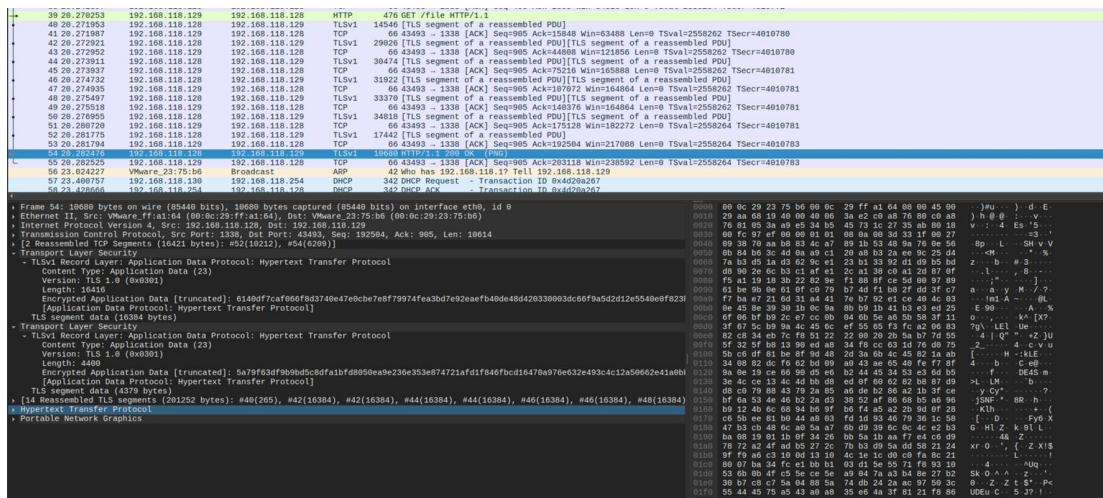


Рисунок 6 – GET-request

В ответе – PNG файл (рис. 7).

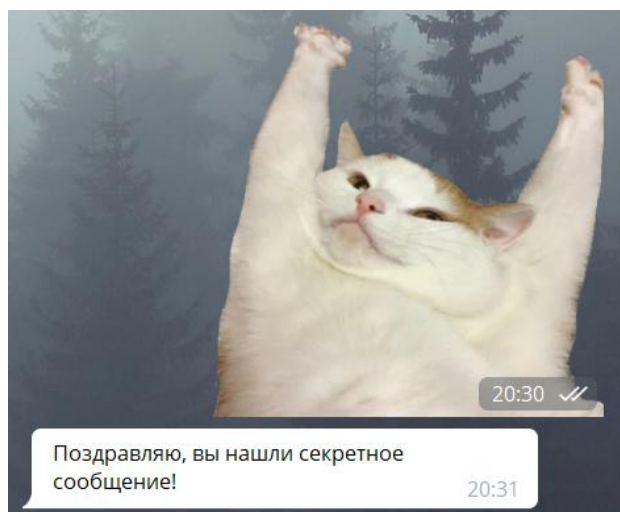


Рисунок 7 – Полученный PNG файл

5. Итоговые выводы

В дампе зафиксировано клиент-серверное взаимодействие. Передавались ARP-requests, HTTP-requests, закрытый RSA-ключ, TLS-трафик, бинарный PNG-файл. В результате произошла утечка закрытого ключа, TLS-трафик был расшифрован.

Из уязвимостей можно отметить отсутствие защиты от MITM в локальной сети (ARP без механизмов защиты). Закрытый ключ передается по HTTP – наиболее критичная уязвимость. Закрытый RSA-ключ передается в открытом виде, компрометируется вся модель доверия TLS. Также используется устаревший Cipher Suite.

Также HTTP-headers раскрывают тип сервера и версию ПО, что потенциально облегчает подбор известных уязвимостей.