PENETRATION TEST LAB part 1

Pentest Report Analysis

Preparation

The test has been performer between two laptops, alternately one laptop is the item under test, the other one is the instrument used by penetration tester to perform the test, then the roles has been swapped.

System under test: Hp Pro Book Laptop with Ubuntu 16.04 (with Kernel 4.4);

Pen test goal: discover common vulnerability of the system under test.

Scanning Description

Has been performed a network scanning using *Nmap* tool:

Penetration tester laptop ip address	`iaddr:192.168.43.249`
Device under test ip address	`addr:192.168.43.56`
Output for default nmap	nmap 192.168.43.56 Starting Nmap 7.01 (https://nmap.org) at 2018-04-27 17:30 CEST Nmap scan report for davide-Ubuntu (192.168.43.56) Host is up (0.029s latency). Not shown: 999 closed ports PORT STATE SERVICE 902/tcp open iss-realsecure Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
Output for "aggressive" nmap	nmap -A 192.168.43.56 Starting Nmap 7.01 (https://nmap.org) at 2018-04-27 17:30 CEST Nmap scan report for davide-Ubuntu (192.168.43.56) Host is up (0.50s latency). Not shown: 999 closed ports PORT STATE SERVICE VERSION 902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)

The same operation has been performed with another similar laptop.

Vulnerable software

During the test, has been tracked following software installed on devices under test:

- VMware 1.10
- OpenSSH 7.2p2

Vulnerability type

Since VMware will be uninstalled , the team will consider only the vulnerabilities on OpenSSH software.

Type of vulnerability taken in charge: Denial Of Service (**hypothesis**).

Vulnerability severity

For educational purpose has been searched common vulnerabilities using online database and has been taken in charge the *CVE- 2016-65-15* (see https://www.cvedetails.com/cve/CVE-2016-6515/ link).

With reference to this vulnerability, the score is high (7.8 on CVSS scoring, the cpu usage can have 100% usage peaks) affecting Availability property of the CIA model.

Exploits availability/accessibility

From CVE:

- Authentication is not required to exploit the vulnerability;
- very little knowledge or skill is required to exploit (accessing with a password crafted in length);
- some script are available online.

Origin cause

The cause of this vulnerability is a software bug: the check on password length has been missed.

Affected software

OpenSSH version prior to 7.3 (vendor confirmed).

Products Affected by CVE-2016-6515: Fedora 24.

Impact

As reported by CVE- 2016-65-15:

Confidentiality Impact: none

Integrity Impact: none

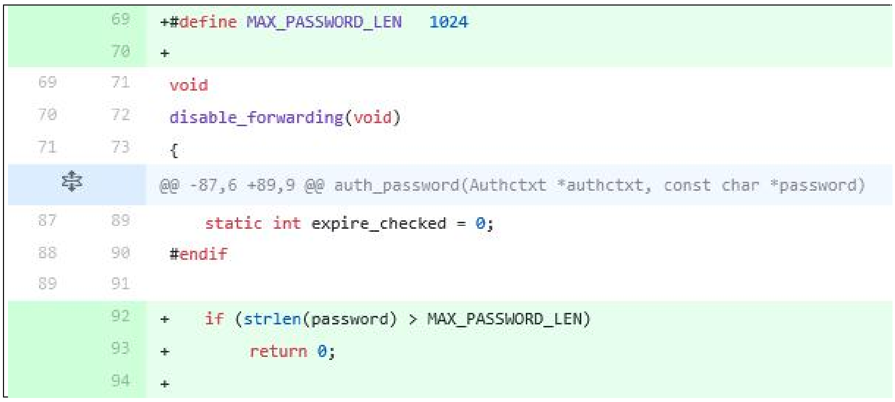
Availability Impact: **Complete** (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)

Solution availability/accessibility

The fix is already available on 7.3 version.

For detail on fix see: https://github.com/openssh/openssh-portable/commit/fcd135c9df440bcd2d5870405ad3311743d78d97

Fix description: the file auth-passwd.c has been modified in order to refuse password bigger than 1024 character as showed in the picture below:



```
+#define MAX_PASSWORD_LEN   1024
+
 void
 disable_forwarding(void)
 {
@@ -87,6 +89,9 @@ auth_password(Authctxt *authctxt, const char *password)
     static int expire_checked = 0;
 #endif

+    if (strlen(password) > MAX_PASSWORD_LEN)
+        return 0;
+
```

Description of the problem

If the device under test (used as a remote machine) is installed and running OpenSSH version prior to 7.3, it does not limit the password length (in auth-passwd.c file) for authentication. A remote attacker can exploit this vulnerability sending a crafted data which for example 90000 characters in length to the 'password' field while attempting to log in to cause a denial of service (high crypt CPU consumption).

Description of the used methods

The method used to discover vulnerabilities (Nmap tool) is described in *Scanning Description* paragraph.

Suggestions and notes

The vendor has issued a fix (7.3 version).

Outcome

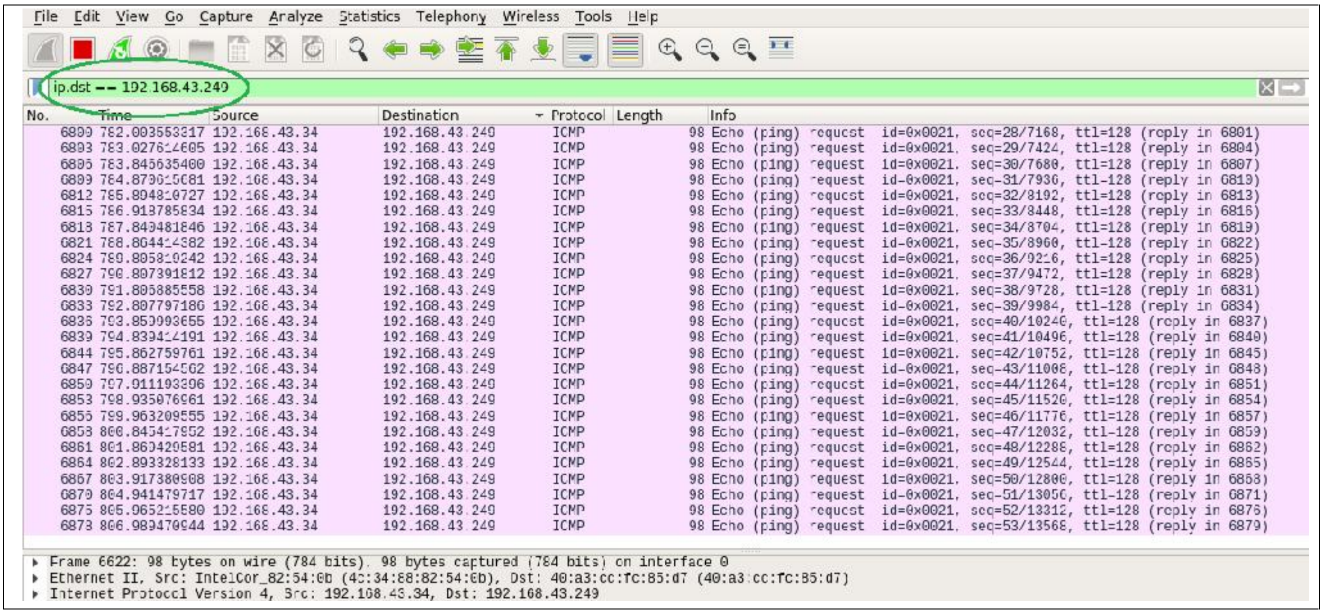
Penetration Tester recommendation:

- Update all remote devices with OpenSSH 7.3 version
- Uninstall VMware version.

PENETRATION TEST LAB part 2

Introduction

The second part of lab has been used to familiarize with *Wireshark* network communication sniffing tool. Here below is reported an example of Wireshark *display filter* on destination ip address applied at ping scanning acquisition:



ip.dst == 192.168.43.249

```
No.        Time          Source           Destination      Protocol Length Info
      6800 782.003553217 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=28/7168, ttl=128 (reply in 6801)
      6803 783.027614605 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=29/7424, ttl=128 (reply in 6804)
      6806 783.845635400 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=30/7680, ttl=128 (reply in 6807)
      6809 784.870615081 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=31/7936, ttl=128 (reply in 6810)
      6812 785.894810727 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=32/8192, ttl=128 (reply in 6813)
      6815 786.918785834 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=33/8448, ttl=128 (reply in 6816)
      6818 787.849481846 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=34/8704, ttl=128 (reply in 6819)
      6821 788.864414382 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=35/8960, ttl=128 (reply in 6822)
      6824 789.805810242 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=36/9216, ttl=128 (reply in 6825)
      6827 790.807391812 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=37/9472, ttl=128 (reply in 6828)
      6830 791.805885558 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=38/9728, ttl=128 (reply in 6831)
      6833 792.807797186 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=39/9984, ttl=128 (reply in 6834)
      6836 793.850993655 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=40/10240, ttl=128 (reply in 6837)
      6839 794.839414191 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=41/10496, ttl=128 (reply in 6840)
      6844 795.862759761 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=42/10752, ttl=128 (reply in 6845)
      6847 796.887154562 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=43/11008, ttl=128 (reply in 6848)
      6850 797.911193396 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=44/11264, ttl=128 (reply in 6851)
      6853 798.935076961 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=45/11520, ttl=128 (reply in 6854)
      6856 799.963209555 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=46/11776, ttl=128 (reply in 6857)
      6858 800.845417952 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=47/12032, ttl=128 (reply in 6859)
      6861 801.869420581 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=48/12288, ttl=128 (reply in 6862)
      6864 802.893328133 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=49/12544, ttl=128 (reply in 6865)
      6867 803.917380908 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=50/12800, ttl=128 (reply in 6868)
      6870 804.941479717 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=51/13056, ttl=128 (reply in 6871)
      6875 805.965215580 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=52/13312, ttl=128 (reply in 6876)
      6878 806.989470944 192.168.43.34    192.168.43.249   ICMP       98 Echo (ping) request  id=0x0021, seq=53/13568, ttl=128 (reply in 6879)

▸ Frame 6622: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: IntelCor_82:54:6b (40:34:88:82:54:6b), Dst: 40:a3:cc:fc:85:d7 (40:a3:cc:fc:85:d7)
▸ Internet Protocol Version 4, Src: 192.168.43.34, Dst: 192.168.43.249
```

Preparation description

Wireshark has been used to analyze the TLS communication between client (the browser) and a web server. In order to decrypt the packets, the Session Key shall be loaded.

Step performed:

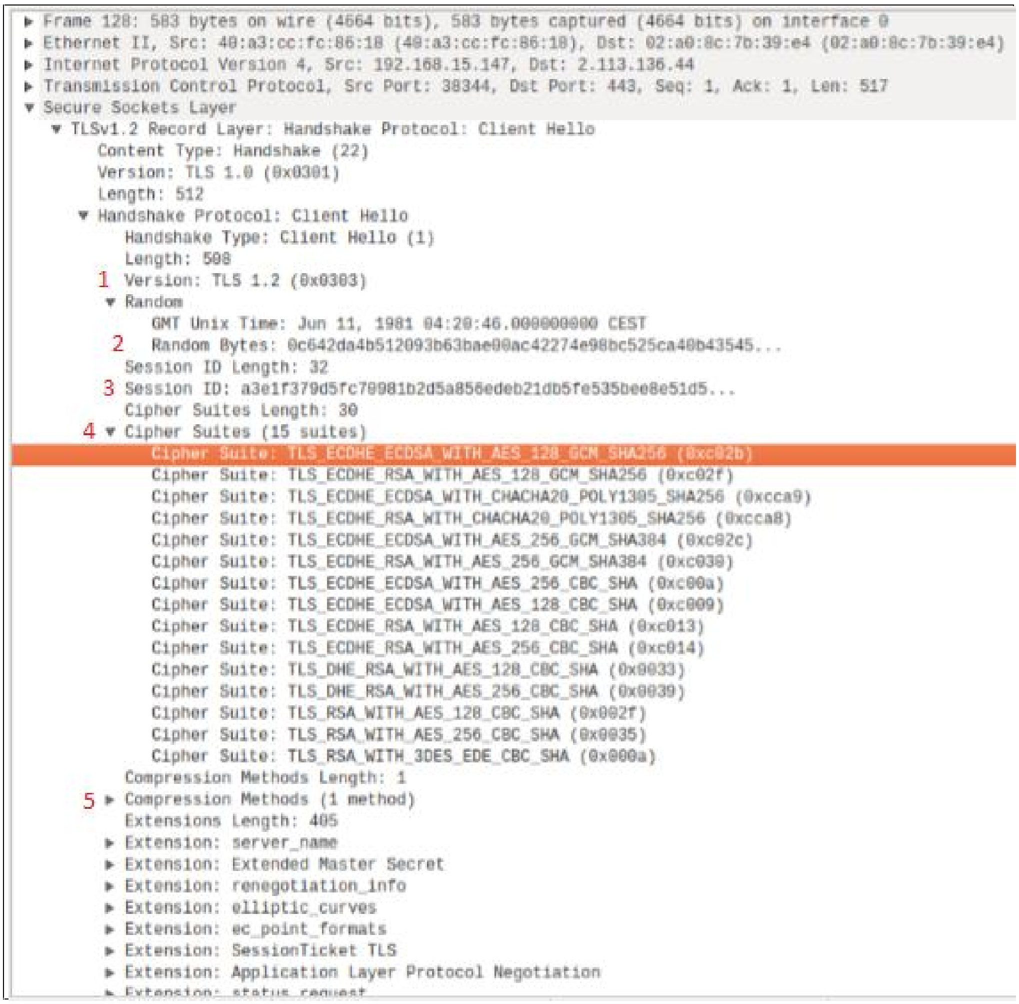
- Session key has been exported using environment variable (*export SSLKEYLOGFILE=sslkeylog.log*);
- The browser and wireshark tool has been launched;
- Wireshark has been setup with session key (Edit->preferences->protocols->SSL->(Pre)-Master-Secret log filename);
- connection is performed (www.bancadalba.it).

The transmission data has been postprocessed using *.pcapng* files saved during TLS transmission.

Analysis description

Here below is reported an example of *Client hello* message send by client during handshake. During the sniffing has been checked the main field of this message:

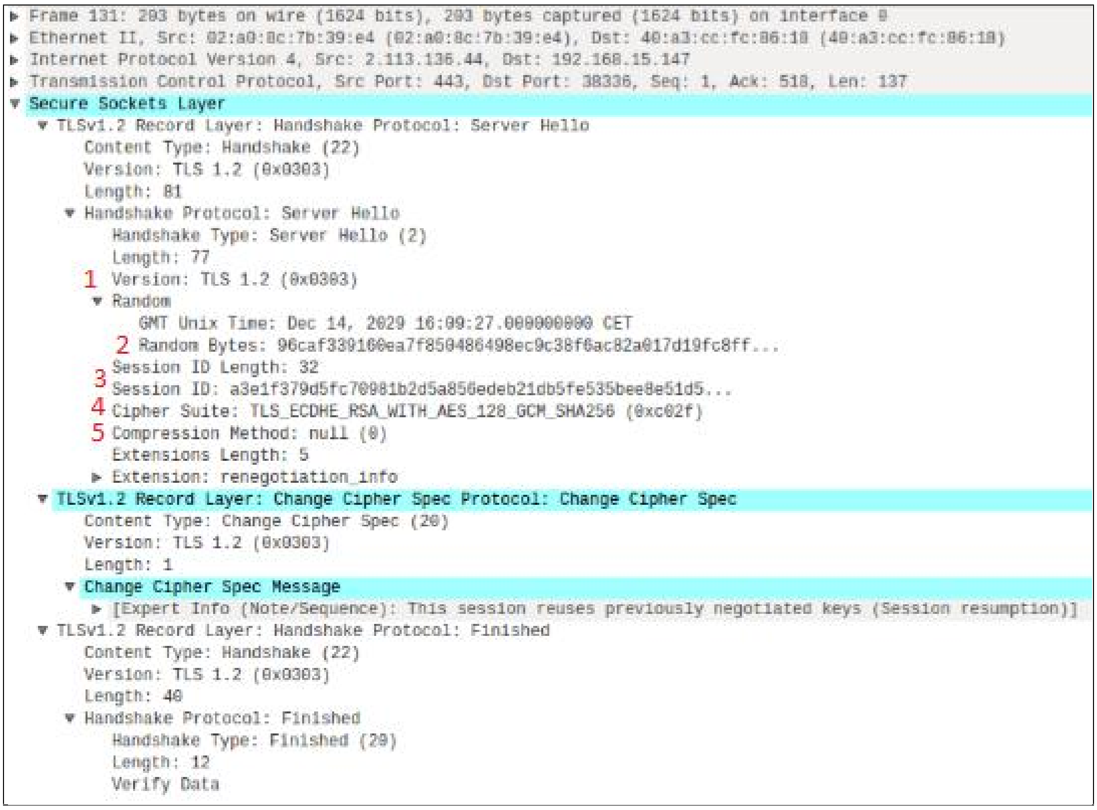
1. SSL version preferred by client;
2. Random byte;
3. Session Id (different from zero since client is asking to reload an existing session);
4. Cipher suite supported by client;
5. List of compression method supported by client.



```
▶ Frame 128: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0
▶ Ethernet II, Src: 40:a3:cc:fc:86:18 (40:a3:cc:fc:86:18), Dst: 02:a0:8c:7b:39:e4 (02:a0:8c:7b:39:e4)
▶ Internet Protocol Version 4, Src: 192.168.15.147, Dst: 2.113.136.44
▶ Transmission Control Protocol, Src Port: 38344, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    ▼ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 508
      1 Version: TLS 1.2 (0x0303)
      ▼ Random
          GMT Unix Time: Jun 11, 1981 04:20:46.000000000 CEST
       2  Random Bytes: 0c642da4b512093b63bae00ac42274e98bc525ca40b43545...
        Session ID Length: 32
      3 Session ID: a3e1f379d5fc70981b2d5a856edeb21db5fe535bee8e51d5...
        Cipher Suites Length: 30
    4 ▼ Cipher Suites (15 suites)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
          Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
          Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
          Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
          Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
          Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
          Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
        Compression Methods Length: 1
    5 ▶ Compression Methods (1 method)
        Extensions Length: 405
      ▶ Extension: server_name
      ▶ Extension: Extended Master Secret
      ▶ Extension: renegotiation_info
      ▶ Extension: elliptic_curves
      ▶ Extension: ec_point_formats
      ▶ Extension: SessionTicket TLS
      ▶ Extension: Application Layer Protocol Negotiation
      ▶ Extension: status_request
```

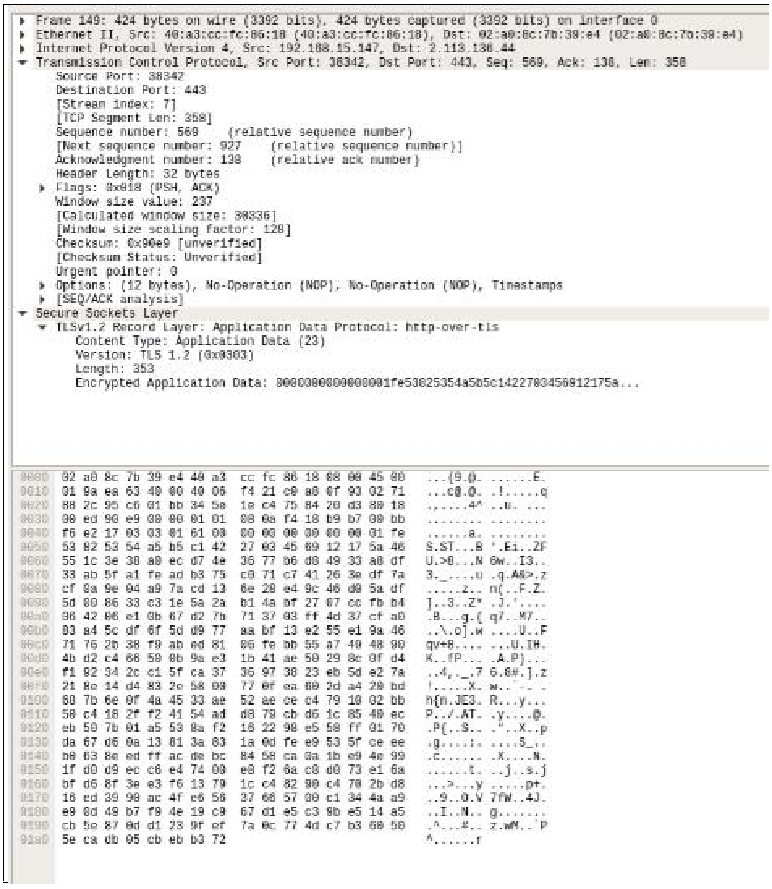
The equivalent "*Server hello*" message, sent by server, contains:

1. SSL version fixed by server;
2. Random byte;
3. Session Id (the same proposed by client since server approved to reload that session);
4. Cipher suite chosen by server;
5. List of compression method chosen by server.



```
▶ Frame 131: 203 bytes on wire (1624 bits), 203 bytes captured (1624 bits) on interface 0
▶ Ethernet II, Src: 02:a0:8c:7b:39:e4 (02:a0:8c:7b:39:e4), Dst: 40:a3:cc:fc:86:18 (40:a3:cc:fc:86:18)
▶ Internet Protocol Version 4, Src: 2.113.136.44, Dst: 192.168.15.147
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 38336, Seq: 1, Ack: 518, Len: 137
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 81
    ▼ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 77
      1 Version: TLS 1.2 (0x0303)
      ▼ Random
          GMT Unix Time: Dec 14, 2029 16:09:27.000000000 CET
        2 Random Bytes: 96caf339160ea7f850486498ec9c38f6ac82a017d19fc8ff...
        Session ID Length: 32
      3 Session ID: a3e1f379d5fc70981b2d5a856edeb21db5fe535bee8e51d5...
      4 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      5 Compression Method: null (0)
        Extensions Length: 5
      ▶ Extension: renegotiation_info
  ▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
    ▼ Change Cipher Spec Message
      ▶ [Expert Info (Note/Sequence): This session reuses previously negotiated keys (Session resumption)]
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Finished
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
    ▼ Handshake Protocol: Finished
        Handshake Type: Finished (20)
        Length: 12
        Verify Data
```

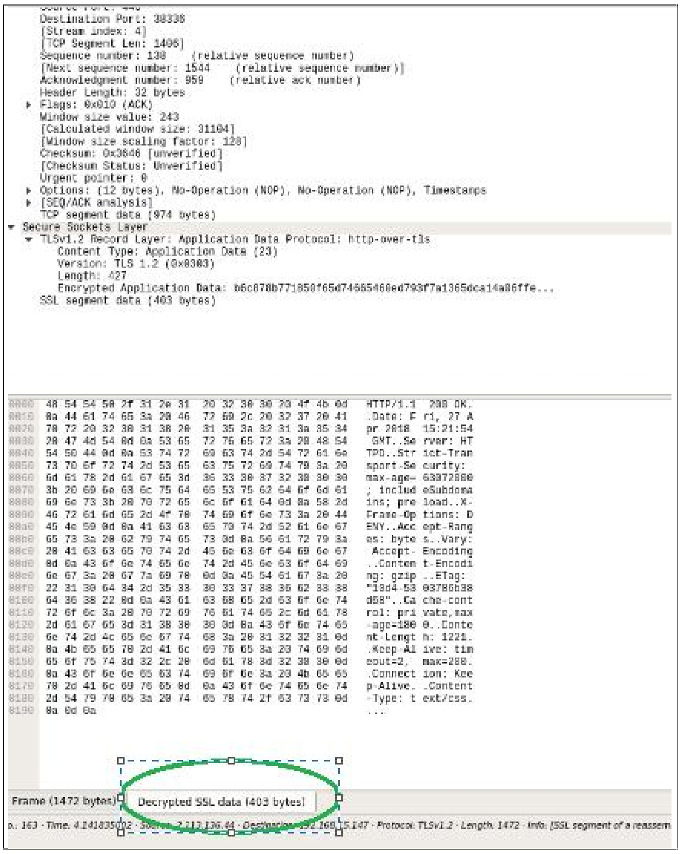
After the client *"change chiper spec message"* the payload is ciphered; here below is reported an image of TLS payload without availability of session ID key (messages, are ciphered, only transport level is available):



```
▶ Frame 149: 424 bytes on wire (3392 bits), 424 bytes captured (3392 bits) on interface 0
▶ Ethernet II, Src: 40:a3:cc:fc:86:18 (40:a3:cc:fc:86:18), Dst: 02:a0:8c:7b:39:e4 (02:a0:8c:7b:39:e4)
▶ Internet Protocol Version 4, Src: 192.168.15.147, Dst: 2.113.136.44
▼ Transmission Control Protocol, Src Port: 38342, Dst Port: 443, Seq: 569, Ack: 138, Len: 358
    Source Port: 38342
    Destination Port: 443
    [Stream index: 7]
    [TCP Segment Len: 358]
    Sequence number: 569    (relative sequence number)
    [Next sequence number: 927    (relative sequence number)]
    Acknowledgment number: 138    (relative ack number)
    Header Length: 32 bytes
  ▶ Flags: 0x018 (PSH, ACK)
    Window size value: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x90e9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ [SEQ/ACK analysis]
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 353
      Encrypted Application Data: 0000000000000001fe53825354a5b5c14227034569121175a...

0000  02 a0 8c 7b 39 e4 40 a3  cc fc 86 18 08 00 45 00   ...{9.@. ......E.
0010  01 9a ea 63 40 00 40 06  f4 21 c0 a8 0f 93 02 71   ...c@.@. .!.....q
0020  88 2c 95 c6 01 bb 34 5e  1e c4 75 84 20 d3 80 18   .,....4^ ..u. ...
0030  00 ed 90 e9 00 00 01 01  08 0a f4 18 b9 b7 00 bb   ........ ........
0040  f6 e2 17 03 03 01 61 00  00 00 00 00 00 00 01 fe   ......a. ........
0050  53 82 53 54 a5 b5 c1 42  27 03 45 69 12 17 5a 46   S.ST...B '.Ei..ZF
0060  55 1c 3e 30 a0 ec d7 4e  36 77 b6 d0 49 33 a0 df   U.>0...N 6w..I3..
0070  33 ab 5f a1 fe ad b3 75  c0 71 c7 41 26 3e df 7a   3._....u .q.A&>.z
0080  cf 0a 9e 04 a9 7a cd 13  6e 28 e4 9c 46 d0 5a df   .....z.. n(..F.Z.
0090  5d 80 86 33 c3 1e 5a 2a  b1 4a bf 27 07 cc fb b4   ]..3..Z* .J.'....
00a0  06 42 06 e1 0b 67 d2 7b  71 37 03 ff 4d 37 cf a0   .B...g.{ q7..M7..
00b0  03 a4 5c df 6f 5d d9 77  aa bf 13 e2 55 e1 9a 46   ..\.o].w ....U..F
00c0  71 76 2b 38 f9 ab ed 81  86 fe bb 55 a7 49 48 90   qv+8.... ...U.IH.
00d0  4b d2 c4 66 50 0b 9a e3  1b 41 ae 50 29 8c 0f d4   K..fP... .A.P)...
00e0  f1 82 34 2c c1 5f ca 37  36 97 38 23 eb 5d e2 7a   ..4,._.7 6.8#.].z
00f0  21 8e 14 d4 83 2e 58 08  77 0f ea 60 2d a4 20 bd   !.....X. w..`-. .
0100  68 7b 6e 0f 4a 45 33 ae  52 ae ce c4 79 10 02 bb   h{n.JE3. R...y...
0110  50 c4 18 2f f2 41 54 ad  d8 79 cb d6 1c 85 40 ec   P../.AT. .y....@.
0120  eb 50 7b 01 a5 53 8a f2  16 22 98 e5 58 ff 01 70   .P{..S.. ."..X..p
0130  da 67 d6 0a 13 81 3a 83  1a 0d fe e9 53 5f ce ee   .g....:. ....S_..
0140  b0 63 8e ed ff ac de bc  84 58 ca 0a 1b e0 4e 99   .c...... .X....N.
0150  1f d0 d9 ec c6 e4 74 00  e0 f2 6a c8 d0 73 e1 6a   ......t. ..j..s.j
0160  bf d6 8f 3e e3 f6 13 79  1c c4 82 90 c4 70 2b d8   ...>...y .....p+.
0170  18 ed 39 90 ac 4f e6 56  37 66 57 80 c1 34 4a a9   ..9..O.V 7fW..4J.
0180  e9 0d 49 b7 f9 4e 19 c9  67 d1 e5 c3 9b e5 14 a5   ..I..N.. g.......
0190  cb 5e 87 0d d1 23 9f ef  7a 0c 77 4d c7 b3 60 50   .^...#.. z.wM..`P
01a0  5e ca db 05 cb eb b3 72                            ^......r
```

In order to decipher the payload it has been loaded the session ID key as described into "Preparation description" paragraph. Here below is reported an example of deciphered TLS payload:

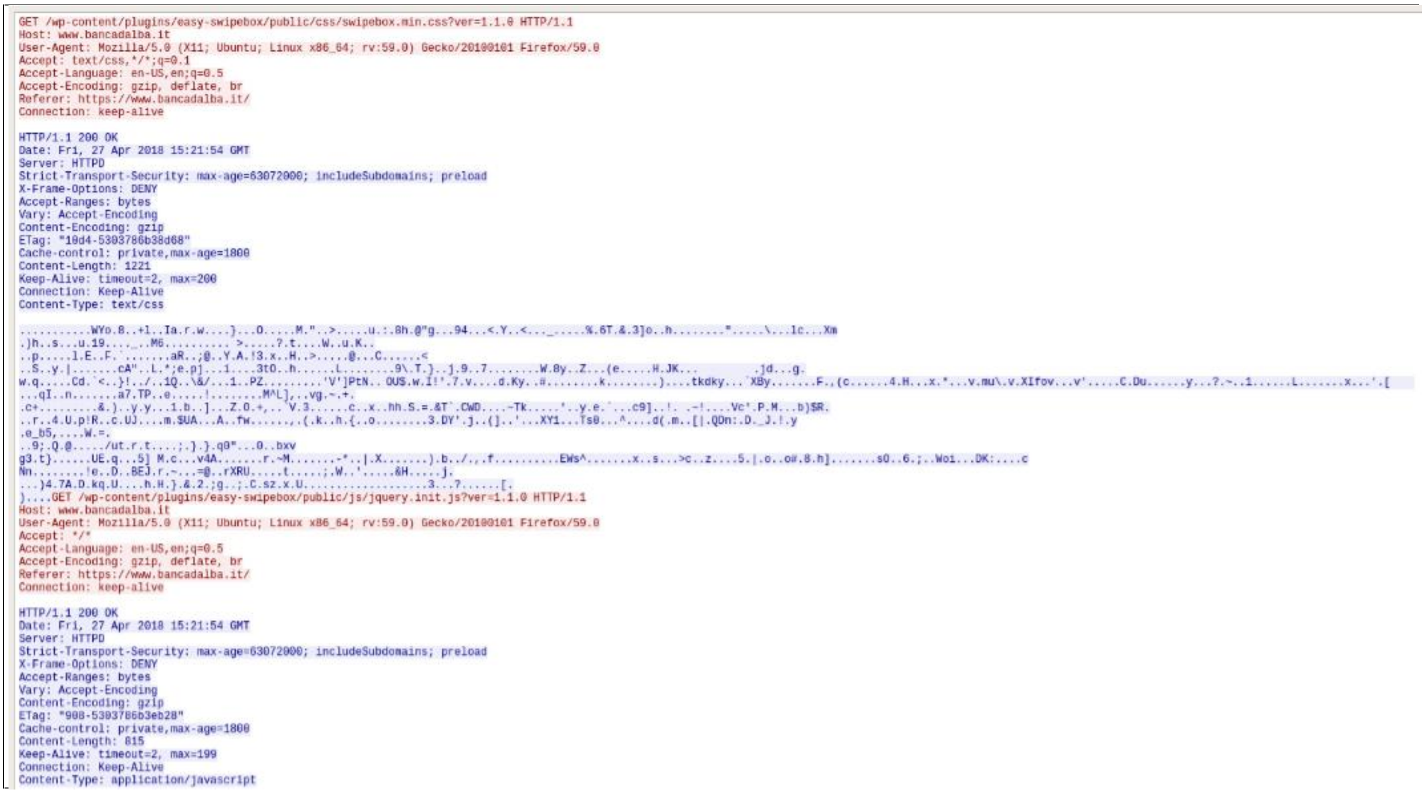


```
    Destination Port: 38338
    [Stream index: 4]
    [TCP Segment Len: 1406]
    Sequence number: 138    (relative sequence number)
    [Next sequence number: 1544    (relative sequence number)]
    Acknowledgment number: 959    (relative ack number)
    Header Length: 32 bytes
  ▸ Flags: 0x010 (ACK)
    Window size value: 243
    [Calculated window size: 31104]
    [Window size scaling factor: 128]
    Checksum: 0x3846 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
    TCP segment data (974 bytes)
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 427
      Encrypted Application Data: b6c878b771850f65d74665460ed793f7a1365dca14a86ffe...
    SSL segment data (403 bytes)

0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
0010  0a 44 61 74 65 3a 20 46  72 69 2c 20 32 37 20 41   .Date: F ri, 27 A
0020  70 72 20 32 30 31 38 20  31 35 3a 32 31 3a 35 34   pr 2018  15:21:54
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 48 54    GMT..Se rver: HT
0040  54 50 44 0d 0a 53 74 72  69 63 74 2d 54 72 61 6e   TPD..Str ict-Tran
0050  73 70 6f 72 74 2d 53 65  63 75 72 69 74 79 3a 20   sport-Se curity: 
0060  6d 61 78 2d 61 67 65 3d  36 33 30 37 32 30 30 30   max-age= 63072000
0070  3b 20 69 6e 63 6c 75 64  65 53 75 62 64 6f 6d 61   ; includ eSubdoma
0080  69 6e 73 3b 20 70 72 65  6c 6f 61 64 0d 0a 58 2d   ins; pre load..X-
0090  46 72 61 6d 65 2d 4f 70  74 69 6f 6e 73 3a 20 44   Frame-Op tions: D
00a0  45 4e 59 0d 0a 41 63 63  65 70 74 2d 52 61 6e 67   ENY..Acc ept-Rang
00b0  65 73 3a 20 62 79 74 65  73 0d 0a 56 61 72 79 3a   es: byte s..Vary:
00c0  20 41 63 63 65 70 74 2d  45 6e 63 6f 64 69 6e 67    Accept- Encoding
00d0  0d 0a 43 6f 6e 74 65 6e  74 2d 45 6e 63 6f 64 69   ..Conten t-Encodi
00e0  6e 67 3a 20 67 7a 69 70  0d 0a 45 54 61 67 3a 20   ng: gzip ..ETag: 
00f0  22 31 30 64 34 2d 35 33  30 33 37 38 36 62 33 38   "10d4-53 03786b38
0100  64 36 38 22 0d 0a 43 61  63 68 65 2d 63 6f 6e 74   d68"..Ca che-cont
0110  72 6f 6c 3a 20 70 72 69  76 61 74 65 2c 6d 61 78   rol: pri vate,max
0120  2d 61 67 65 3d 31 38 30  30 0d 0a 43 6f 6e 74 65   -age=180 0..Conte
0130  6e 74 2d 4c 65 6e 67 74  68 3a 20 31 32 32 31 0d   nt-Lengt h: 1221.
0140  0a 4b 65 65 70 2d 41 6c  69 76 65 3a 20 74 69 6d   .Keep-Al ive: tim
0150  65 6f 75 74 3d 32 2c 20  6d 61 78 3d 32 30 30 0d   eout=2,  max=200.
0160  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 4b 65 65   .Connect ion: Kee
0170  70 2d 41 6c 69 76 65 0d  0a 43 6f 6e 74 65 6e 74   p-Alive. .Content
0180  2d 54 79 70 65 3a 20 74  65 78 74 2f 63 73 73 0d   -Type: t ext/css.
0190  0a 0d 0a                                           ...
```

```
o. 163 · Time: 4.241835002 · Source: 2.113.136.44 · Destination: 192.168.15.147 · Protocol: TLSv1.2 · Length: 1472 · Info: [SSL segment of a reassem
```

In case you want to see all decrypted http response stream flow, as reported in the following picture: *right click on a message -> Follow ->SSL Stream.*



```
GET /wp-content/plugins/easy-swipebox/public/css/swipebox.min.css?ver=1.1.0 HTTP/1.1
Host: www.bancadalba.it
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.bancadalba.it/
Connection: keep-alive

HTTP/1.1 200 OK
Date: Fri, 27 Apr 2018 15:21:54 GMT
Server: HTTPD
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Frame-Options: DENY
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
ETag: "10d4-5303786b38d68"
Cache-control: private,max-age=1800
Content-Length: 1221
Keep-Alive: timeout=2, max=200
Connection: Keep-Alive
Content-Type: text/css

...........WYo.8..+l..Ia.r.w....}...O.....M."..>.....u.:.8h.@"g...94...<.Y..<..._.....%.6T.&.3]o..h........"......\...lc...Xm
.)h..s...u.19...._..M6.......... >.....?.t....W..u.K..
..p.....l.E..F.`.......aR..;@..Y.A.!3.x..H..>.....@...C......<
..S..y.|.......cA"..L.*;e.p]...1....3tO..h......L........9\.T.}..j.9..7........W.8y..Z...(e.....H.JK...         .jd...g.
w.q.....Cd.`<..}!../..1Q..\&/...1..PZ.........'V']PtN.. OUS.w.I!'.7.v....d.Ky..#........k........)....tkdky...`XBy.......F.,(c......4.H...x.*...v.mu\.v.XIfov...v'.....C.Du......y...?.~..1......L.......x...'.[
...qI..n.......a7.TP..e.....!........M^L],..vg.~.+.
.c+.........&.)..y.y...1.b..]...Z.O.+,.. V.3......c..x..hh.S.=.&T`.CWD....~Tk.....'..y.e.`...c9]..!. .-!....Vc'.P.M...b)$R.
..r..4.U.p!R..c.UJ....m.$UA...A..fw.......(.k..h.{..o........3.DY'.j..(]..'...XY1...Ts0...^....d(.m..[|.QDn:.D._J.!.y
.e_b5,....W.=.
..9;.Q.@...../ut.r.t....;.}.}.q0"...0..bxv
g3.t}......UE.q...5] M.c...v4A.......r.~M.......-*..|.X.......).b../.,.f..........EWs^.......x..s...>c..z....5.|.o..o#.8.h]......s0..6.;..Wo1...DK:....c
Nn........!e..D..BEJ.r.~...=@..rXRU.....t.....;.W..'.....&H.....j.
...)4.7A.D.kq.U....h.H.}.&.2.;g..;.C.sz.x.U...................3...?......[.
)....GET /wp-content/plugins/easy-swipebox/public/js/jquery.init.js?ver=1.1.0 HTTP/1.1
Host: www.bancadalba.it
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.bancadalba.it/
Connection: keep-alive

HTTP/1.1 200 OK
Date: Fri, 27 Apr 2018 15:21:54 GMT
Server: HTTPD
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Frame-Options: DENY
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
ETag: "908-5303786b3eb28"
Cache-control: private,max-age=1800
Content-Length: 815
Keep-Alive: timeout=2, max=199
Connection: Keep-Alive
Content-Type: application/javascript
```