Activities Terminal Jan 28 20:27

bandit15@bandit: ~

```
bandit15@bandit:~$ man openssl
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Jan 27 16:44:16 2024 GMT
verify return:1
depth=0 CN = localhost
notAfter=Jan 27 16:44:16 2024 GMT
verify return:1
---
Certificate chain
 0 s:CN = localhost
   i:CN = localhost
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA1
   v:NotBefore: Jan 27 16:43:16 2024 GMT; NotAfter: Jan 27 16:44:16 2024 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDCzCCAfOgAwIBAgIEURMdljANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDAls
b2NhbGhvc3QwHhcNMjQwMTI3MTY0MzE2WhcNMjQwMTI3MTY0NDE2WjAUMRIwEAYD
VQQDDAlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDU
Z9QE6I7JcdyFMgoOiRdmAiBU0XEF8VuDlXEKjm6JD1irOr6Z/U3CWmK+FOQ/4P3U
wwyc0VjORutcz7OltTYmxDOOWaLY9BJCwRo6tYFRM5M3ILxR6QGwVtUtjPBR9ckA
mk+S4InJ40U7/YOJF/MV6KDVwmMHHgfeoyVGDstPyY6S2WXGlyYZsV9oFR2Wkfl7
kMCdxn0O32wuzGS4EKXxKlle2Jh97flNEl5snYrODcFy43PLYwlWed961Uxus8je
FWIOo+o+pNRFRsvTGoQYTADysGSU7Q02cydX/2TQZiI322OQvb1L72L47MrVE04z
bGUzjBSuW104Y/LGxh+3AgMBAAGjZTBjMBQGA1UdEQQNMAuCCWxvY2FsaG9zdDBL
BglghkgBhvhCAQ0EPhY8QXV0b21hdGljVWxseSBnZW5lcmF0ZWQgYnkgTmNhdC4g
U2VlIGh0dHBzOi8vbm1hcC5vcmcvbmNhdC8uMA0GCSqGSIb3DQEBBQUAA4IBAQAb
+Cu6UMEx3v+pml7qFalcLSpGRm3S6syfZf3YjX+Dd0oT0wZ9L0QQQ8rXVYB4IncM
FXIzS3wqMu9by0ozphoFS2+jlZYZlQqBrYWvzJ41pVL3NjsTKzYJUzVgZTnqm5w4
TSOsLWV9cnlxYPZMHPqf5vx495x0Zs1SVGCFhPXrNVLqe4DEFVznqLZ4QlbGtWcJ
9FgYDsBEp/OWp1ZUnczIwh5UH6murMVQIdgcd/CSFE6lPRwHm2CqvUiPoI9IfA2U
nmDzBr3er/bU4PoIBlBUK9qj7M+er4TRtCtpy5F2NoXtktutTvP2fkkGvkLdCzs7
DePfLKYUfyhVeVnNVFh9
-----END CERTIFICATE-----
subject=CN = localhost
issuer=CN = localhost
---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 1339 bytes and written 373 bytes
Verification error: certificate has expired
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
```

Activities Terminal Jan 28 20:27

bandit15@bandit: ~

```
    0060 - 95 9c c4 99 0b 7c 4f 97-fb f5 45 aa 62 32 6f dd   .....|O...E.b2o.
    0070 - ef 40 16 8d f0 14 83 7c-2f 46 28 a1 a5 15 fa dc   .@.....|/F(.....
    0080 - dc 64 14 cb 5b 05 e7 02-29 bf 9a c8 f2 7a 58 3f   .d..[...)....zX?
    0090 - 6c 8c 5c 4a 20 e2 8a 7a-f8 6f 31 9d b7 53 30 62   l.\J ..z.o1..S0b
    00a0 - b2 81 03 68 50 26 e8 1b-cb 7a 6d f9 2d 63 8d 21   ...hP&...zm.-c.!
    00b0 - 1c 4f 38 77 68 c7 15 57-ce 90 75 e7 ff dd e8 97   .O8wh..W..u.....
    00c0 - 7d 61 c3 b3 a6 90 89 95-c1 ae d9 a9 ba 39 0b 29   }a...........9.)

    Start Time: 1706473538
    Timeout   : 7200 (sec)
    Verify return code: 10 (certificate has expired)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: 3FD56003364D299F9529A8F C8D5BABF9D09E57B795CCEFFB7032E1435BE5D003
    Session-ID-ctx:
    Resumption PSK: 23EDCE311C49C0FD35FE68C9A3FFEDB9F1F027A5D741E32BA0595FE68F7ED797C48E8EC1E87CECB3378F8067C407D1C9
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - af 29 d5 03 4d fa b5 ff-df 95 1c 61 31 a1 d0 3c   .)..M......a1..<
    0010 - af 5e 07 87 33 09 43 80-d6 50 5b fb b0 54 99 96   .^..3.C..P[..T..
    0020 - f9 cd 6c 28 d2 8c 2e 0a-09 44 e3 05 fc d6 d8 e0   ..l(.....D......
    0030 - 14 c8 e0 ea df 9e 91 56-26 dc 23 ab bb 78 9d 8c   .......V&.#..x..
    0040 - 1b 79 f3 fa fc ae 6e 7d-0b 3c 25 a2 f4 7b db 61   .y....n}.<%..{.a
    0050 - 04 1a 88 df c3 a1 0f 59-a1 d2 a1 bf b4 5e 15 9f   .......Y.....^..
    0060 - 22 72 9f 7d a1 77 6a 03-c2 5f 98 e0 47 0e d8 99   "r.}.wj.._..G...
    0070 - 6f 92 ac 72 d8 c7 0b f6-5e da 91 af f3 1f 2e 81   o..r....^.......
    0080 - 55 6d 46 39 35 53 79 20-95 dc 7b 84 3a 69 d3 83   UmF95Sy ..{.:i..
    0090 - 08 8c 8c 0d a8 78 a0 da-21 75 93 9a 23 d7 f1 35   .....x..!u..#..5
    00a0 - b2 9d 2b 67 c9 75 a9 34-63 16 d7 79 a0 dd c7 2b   ..+g.u.4c..y...+
    00b0 - ff d2 60 2b af e2 11 35-32 a5 69 7c fd e0 8f 6e   ..`+...52.i|...n
    00c0 - b1 66 7e 10 a3 a0 97 0a-46 a9 f9 9e 49 26 ce e1   .f~.....F...I&..

    Start Time: 1706473538
    Timeout   : 7200 (sec)
    Verify return code: 10 (certificate has expired)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Correct!
JQttfApK4SeyHwDlI9SXGR50qclOAil1

closed
bandit15@bandit:~$
```