```
 CHECKING HOST(S) AVAILABILITY
 -----------------------------

   expired.badssl.com:443                       => 104.154.89.105




 SCAN RESULTS FOR EXPIRED.BADSSL.COM:443 - 104.154.89.105
 ---------------------------------------------------------

 * OpenSSL CCS Injection:
                                        OK - Not vulnerable to OpenSSL CCS injection

 * TLS 1.2 Session Resumption Support:
      With Session IDs: NOT SUPPORTED (0 successful resumptions out of 5 attempts).
      With TLS Tickets: OK - Supported.

 * ROBOT Attack:
                                        OK - Not vulnerable.

 * TLS 1.0 Cipher Suites:
     Attempted to connect using 80 cipher suites.

     The server accepted the following 12 cipher suites:
        TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                256
        TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                128
        TLS_RSA_WITH_AES_256_CBC_SHA                     256
        TLS_RSA_WITH_AES_128_CBC_SHA                     128
        TLS_RSA_WITH_3DES_EDE_CBC_SHA                    168
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA               256       ECDH: prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA               128       ECDH: prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA              168       ECDH: prime256v1 (256 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA            256       DH (2048 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA            128       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA                 256       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA                 128       DH (2048 bits)

     The group of cipher suites supported by the server has the following properties:
       Forward Secrecy                   OK - Supported
       Legacy RC4 Algorithm              OK - Not Supported


 * Certificates Information:
       Hostname sent for SNI:            expired.badssl.com
       Number of certificates detected:  1


     Certificate #0 ( _RSAPublicKey )
       SHA1 Fingerprint:                 404bbd2f1f4cc2fdeef13aabdd523ef61f1c71f3
       Common Name:                      *.badssl.com
       Issuer:                           COMODO RSA Domain Validation Secure Server CA
       Serial Number:                    99565320202650452861752791156765321481
       Not Before:                       2015-04-09
       Not After:                        2015-04-12
       Public Key Algorithm:             _RSAPublicKey
       Signature Algorithm:              sha256
       Key Size:                         2048
       Exponent:                         65537
       DNS Subject Alternative Names:    ['*.badssl.com', 'badssl.com']

     Certificate #0 - Trust
       Hostname Validation:              OK - Certificate matches server hostname
       Android CA Store (9.0.0_r9):      FAILED - Certificate is NOT Trusted: certificate has
expired
       Apple CA Store (iOS 14, iPadOS 14, macOS 11, watchOS 7, and tvOS 14):FAILED - Certificate is
NOT Trusted: certificate has expired
       Java CA Store (jdk-13.0.2):       FAILED - Certificate is NOT Trusted: certificate has
expired
```

```
      Mozilla CA Store (2021-01-24):     FAILED - Certificate is NOT Trusted: certificate has
expired
      Windows CA Store (2021-02-08):     FAILED - Certificate is NOT Trusted: certificate has
expired
      Symantec 2018 Deprecation:         ERROR - Could not build verified chain (certificate
untrusted?)
      Received Chain:                    *.badssl.com --> COMODO RSA Domain Validation Secure
Server CA --> COMODO RSA Certification Authority
      Verified Chain:                    ERROR - Could not build verified chain (certificate
untrusted?)
      Received Chain Contains Anchor:    ERROR - Could not build verified chain (certificate
untrusted?)
      Received Chain Order:              OK - Order is valid
      Verified Chain contains SHA1:      ERROR - Could not build verified chain (certificate
untrusted?)

    Certificate #0 - Extensions
      OCSP Must-Staple:                  NOT SUPPORTED - Extension not found
      Certificate Transparency:          NOT SUPPORTED - Extension not found

    Certificate #0 - OCSP Stapling
                                         NOT SUPPORTED - Server did not send back an OCSP response

 * SSL 3.0 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

 * OpenSSL Heartbleed:
                                         OK - Not vulnerable to Heartbleed

 * TLS 1.1 Cipher Suites:
    Attempted to connect using 80 cipher suites.

    The server accepted the following 12 cipher suites:
       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                256
       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                128
       TLS_RSA_WITH_AES_256_CBC_SHA                     256
       TLS_RSA_WITH_AES_128_CBC_SHA                     128
       TLS_RSA_WITH_3DES_EDE_CBC_SHA                    168
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA               256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA               128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA              168       ECDH: prime256v1 (256 bits)
       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA            256       DH (2048 bits)
       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA            128       DH (2048 bits)
       TLS_DHE_RSA_WITH_AES_256_CBC_SHA                 256       DH (2048 bits)
       TLS_DHE_RSA_WITH_AES_128_CBC_SHA                 128       DH (2048 bits)

    The group of cipher suites supported by the server has the following properties:
      Forward Secrecy                  OK - Supported
      Legacy RC4 Algorithm             OK - Not Supported


 * TLS 1.2 Cipher Suites:
    Attempted to connect using 156 cipher suites.

    The server accepted the following 24 cipher suites:
       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                256
       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                128
       TLS_RSA_WITH_AES_256_GCM_SHA384                  256
       TLS_RSA_WITH_AES_256_CBC_SHA256                  256
       TLS_RSA_WITH_AES_256_CBC_SHA                     256
       TLS_RSA_WITH_AES_128_GCM_SHA256                  128
       TLS_RSA_WITH_AES_128_CBC_SHA256                  128
       TLS_RSA_WITH_AES_128_CBC_SHA                     128
       TLS_RSA_WITH_3DES_EDE_CBC_SHA                    168
       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384            256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384            256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA               256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256            128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256            128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA               128       ECDH: prime256v1 (256 bits)
```

```
        TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA              168       ECDH: prime256v1 (256 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA            256       DH (2048 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA            128       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_GCM_SHA384              256       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA256              256       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA                 256       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256              128       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA256              128       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA                 128       DH (2048 bits)

    The group of cipher suites supported by the server has the following properties:
      Forward Secrecy                   OK - Supported
      Legacy RC4 Algorithm              OK - Not Supported


 * SSL 2.0 Cipher Suites:
    Attempted to connect using 7 cipher suites; the server rejected all cipher suites.

 * TLS 1.3 Cipher Suites:
    Attempted to connect using 5 cipher suites; the server rejected all cipher suites.

 * Session Renegotiation:
      Client Renegotiation DoS Attack:   OK - Not vulnerable
      Secure Renegotiation:              OK - Supported

 * Deflate Compression:
                                         OK - Compression disabled

 * Elliptic Curve Key Exchange:
      Supported curves:                  prime256v1
      Rejected curves:                   X25519, X448, prime192v1, secp160k1, secp160r1, secp160r2,
secp192k1, secp224k1, secp224r1, secp256k1, secp384r1, secp521r1, sect163k1, sect163r1, sect163r2,
sect193r1, sect193r2, sect233k1, sect233r1, sect239k1, sect283k1, sect283r1, sect409k1, sect409r1,
sect571k1, sect571r1

 * Downgrade Attacks:
      TLS_FALLBACK_SCSV:                 OK - Supported


 SCAN COMPLETED IN 8.52 S
 ------------------------
```