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

  hostedscan.com:443                      => 35.231.210.182




SCAN RESULTS FOR HOSTEDSCAN.COM:443 - 35.231.210.182
---------------------------------------------------

* Elliptic Curve Key Exchange:
      Supported curves:                  X25519, prime256v1
      Rejected curves:                   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

* OpenSSL Heartbleed:
                                         OK - Not vulnerable to Heartbleed

* TLS 1.0 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* TLS 1.3 Cipher Suites:
    Attempted to connect using 5 cipher suites.

    The server accepted the following 3 cipher suites:
       TLS_CHACHA20_POLY1305_SHA256                    256       ECDH: X25519 (253 bits)
       TLS_AES_256_GCM_SHA384                          256       ECDH: X25519 (253 bits)
       TLS_AES_128_GCM_SHA256                          128       ECDH: X25519 (253 bits)


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

* TLS 1.1 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

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

    The server accepted the following 3 cipher suites:
       TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256     256       ECDH: X25519 (253 bits)
       TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384           256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256           128       ECDH: prime256v1 (256 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 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, RSA cipher suites not supported.

* Deflate Compression:
                                         OK - Compression disabled

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

```
 * Certificates Information:
       Hostname sent for SNI:             hostedscan.com
       Number of certificates detected:   1


     Certificate #0 ( _EllipticCurvePublicKey )
       SHA1 Fingerprint:                  d2bfb3b850576f3f6dbadf9367aded5c2e9ba992
       Common Name:                       *.hostedscan.com
       Issuer:                            R3
       Serial Number:                     299870597081835010164541621944005284379299
       Not Before:                        2023-07-19
       Not After:                         2023-10-17
       Public Key Algorithm:              _EllipticCurvePublicKey
       Signature Algorithm:               sha256
       Key Size:                          256
       Curve:                             secp256r1
       DNS Subject Alternative Names:     ['*.hostedscan.com', 'hostedscan.com']

     Certificate #0 - Trust
       Hostname Validation:               OK - Certificate matches server hostname
       Android CA Store (9.0.0_r9):       OK - Certificate is trusted
       Apple CA Store (iOS 14, iPadOS 14, macOS 11, watchOS 7, and tvOS 14):OK - Certificate is
trusted
       Java CA Store (jdk-13.0.2):        OK - Certificate is trusted
       Mozilla CA Store (2021-01-24):     OK - Certificate is trusted
       Windows CA Store (2021-02-08):     OK - Certificate is trusted
       Symantec 2018 Deprecation:         OK - Not a Symantec-issued certificate
       Received Chain:                    *.hostedscan.com --> R3 --> ISRG Root X1
       Verified Chain:                    *.hostedscan.com --> R3 --> ISRG Root X1
       Received Chain Contains Anchor:    OK - Anchor certificate not sent
       Received Chain Order:              OK - Order is valid
       Verified Chain contains SHA1:      OK - No SHA1-signed certificate in the verified certificate
chain

     Certificate #0 - Extensions
       OCSP Must-Staple:                  NOT SUPPORTED - Extension not found
       Certificate Transparency:          WARNING - Only 2 SCTs included but Google recommends 3 or
more

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

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

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


 SCAN COMPLETED IN 5.81 S
 ------------------------
```