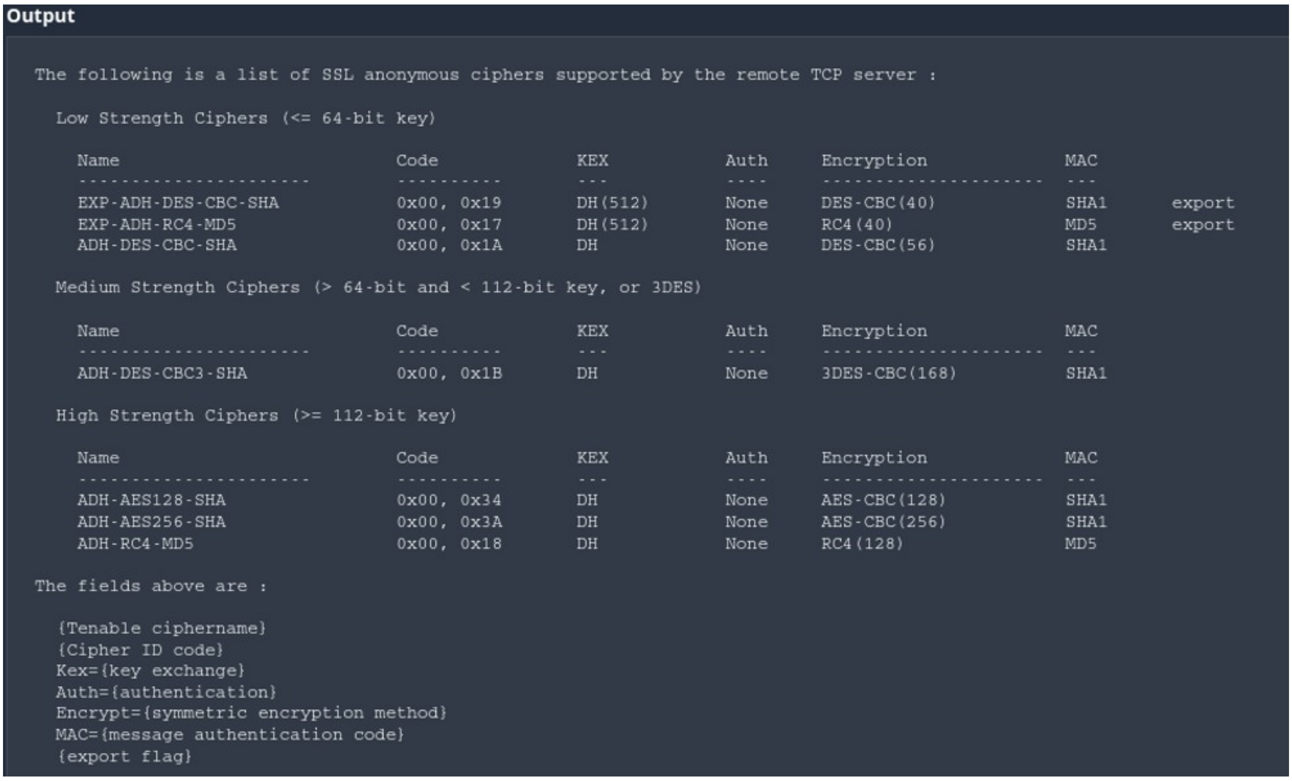
**See Also**

http://www.nessus.org/u?3a040ada

**Output**:



```
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)            SHA1       export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5        export
    ADH-DES-CBC-SHA               0x00, 0x1A       DH            None     DES-CBC(56)            SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)          SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    ADH-AES128-SHA                0x00, 0x34       DH            None     AES-CBC(128)           SHA1
    ADH-AES256-SHA                0x00, 0x3A       DH            None     AES-CBC(256)           SHA1
    ADH-RC4-MD5                   0x00, 0x18       DH            None     RC4(128)               MD5

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## Medium: SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

**Description**

The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key

**Descrizione**

L'host remoto supporta SSLv2 e pertanto potrebbe essere interessato da una vulnerabilità che consente un attacco Oracle di riempimento di Bleichenbacher tra protocolli noto come DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). Questa vulnerabilità esiste a causa di un difetto nell'implementazione Secure Sockets Layer Versione 2 (SSLv2) e consente di decrittografare il traffico TLS catturato. Un utente malintenzionato può sfruttare questa situazione per decrittografare la connessione TLS utilizzando il traffico precedentemente catturato e la