VULNERABILITA TROVATE:

Critical: NFS Exported Share Information Disclosure

NFS (Network File System) ed SMB (Server Message Block) sono **protocolli o regole di archiviazione di accesso ai file per una condivisione efficiente dei file su una rete**.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.

Solution:

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Soluzione
Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

Output

- The following NFS shares could be mounted:
- È possibile montare le seguenti condivisioni NFS
-

```
  + /
    + Contents of / :
      - .
      - ..
      - bin
      - boot
      - cdrom
      - dev
      - etc
      - home
      - initrd
      - initrd.img
      - lib
      - lost+found
      - media
      - mnt
      - nohup.out
      - opt
      - proc
      - root
      - sbin
      - srv
      - sys
      - tmp
      - usr
      - var
      - vmlinuz
```

Critical: VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Descrizione

Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema.

Solution

Secure the VNC service with a strong password.

Proteggi il servizio VNC con una password complessa.

Output

- Nessus logged in using a password of "password".

  Nessus ha effettuato l'accesso utilizzando la password "password".

Critical: SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Descrizione

Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici, tra cui:

- Uno schema di riempimento non sicuro con cifrari CBC.

- Schemi di rinegoziazione e ripresa delle sessioni non sicuri.

Un utente malintenzionato può sfruttare queste falle per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato e i client.

Sebbene SSL/TLS disponga di un mezzo sicuro per scegliere la versione più alta supportata del protocollo (in modo che queste versioni vengano utilizzate solo se il client o il server non supportano niente di meglio), molti browser Web lo implementano in un modo non sicuro che consente a un utente malintenzionato di effettuare il downgrade di una connessione (come in POODLE). Pertanto, si consiglia di disattivare completamente questi protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. Alla data di entrata in vigore stabilita nel PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia avanzata" del PCI SSC.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Soluzione

Consultare la documentazione dell'applicazione per disattivare SSL 2.0 e 3.0. Utilizza invece TLS 1.2 (con suite di crittografia approvate) o versioni successive.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568

Output

```
- SSLv2 is enabled and the server supports at least one cipher.

  Low Strength Ciphers (<= 64-bit key)

    Name                         Code            KEX          Auth     Encryption            MAC
    ---------------------        ----------      ---          ----     --------------------  ---
    EXP-RC2-CBC-MD5                              RSA(512)     RSA      RC2-CBC(40)           MD5       export
    EXP-RC4-MD5                                  RSA(512)     RSA      RC4(40)               MD5       export

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

    Name                         Code            KEX          Auth     Encryption            MAC
    ---------------------        ----------      ---          ----     --------------------  ---
    DES-CBC3-MD5                                 RSA          RSA      3DES-CBC(168)         MD5

  High Strength Ciphers (>= 112-bit key)

    Name                         Code            KEX          Auth     Encryption            MAC
    ---------------------        ----------      ---          ----     --------------------  ---
    RC4-MD5                                      RSA          RSA      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}

- SSLv3 is enabled and the server supports at least one cipher.
       Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Low Strength Ciphers (<= 64-bit key)

    Name                         Code            KEX          Auth     Encryption            MAC
    ---------------------        ----------      ---          ----     --------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA                      DH(512)      RSA      DES-CBC(40)           SHA1      export
    EDH-RSA-DES-CBC-SHA                          DH           RSA      DES-CBC(56)           SHA1
    EXP-ADH-DES-CBC-SHA                          DH(512)      None     DES-CBC(40)           SHA1      export
    EXP-ADH-RC4-MD5                              DH(512)      None     RC4(40)               MD5       export
    ADH-DES-CBC-SHA                              DH           None     DES-CBC(56)           SHA1
    EXP-DES-CBC-SHA                              RSA(512)     RSA      DES-CBC(40)           SHA1      export
    EXP-RC2-CBC-MD5                              RSA(512)     RSA      RC2-CBC(40)           MD5       export
    EXP-RC4-MD5                                  RSA(512)     RSA      RC4(40)               MD5       export
    DES-CBC-SHA                                  RSA          RSA      DES-CBC(56)           SHA1

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

    Name                         Code            KEX          Auth     Encryption            MAC
    ---------------------        ----------      ---          ----     --------------------  ---
    EDH-RSA-DES-CBC3-SHA                         DH           RSA      3DES-CBC(168)         SHA1
    ADH-DES-CBC3-SHA                             DH           None     3DES-CBC(168)         SHA1
    DES-CBC3-SHA                                 RSA          RSA      3DES-CBC(168)         SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                         Code            KEX          Auth     Encryption            MAC
    ---------------------        ----------      ---          ----     --------------------  ---
    DHE-RSA-AES128-SHA                           DH           RSA      AES-CBC(128)          SHA1
    DHE-RSA-AES256-SHA                           DH           RSA      AES-CBC(256)          SHA1
    ADH-AES128-SHA                               DH           None     AES-CBC(128)          SHA1
    ADH-AES256-SHA                               DH           None     AES-CBC(256)          SHA1
    ADH-RC4-MD5                                  DH           None     RC4(128)              MD5
    AES128-SHA                                   RSA          RSA      AES-CBC(128)          SHA1
    AES256-SHA                                   RSA          RSA      AES-CBC(256)          SHA1
    RC4-MD5                                      RSA          RSA      RC4(128)              MD5
    RC4-SHA                                      RSA          RSA      RC4(128)              SHA1

The fields above are :

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

Critical: Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Descrizione

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Soluzione

Verifica se l'host remoto è stato compromesso e, se necessario, reinstalla il sistema.

Output

- Nessus was able to execute the command "id" using the following request :

```
This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

------------------------------ snip ------------------------------
```

Critical: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Descrizione

Il certificato x509 remoto sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto al fatto che un packager Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man in the middle.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Soluzione

Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

See Also

http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Output

- No output recorded.

Critical: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Descrizione
La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto al fatto che un packager Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man in the middle.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Soluzione

Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

See Also

http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Output

- No output recorded.

Critical: rlogin Service Detection

Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.
Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Descrizione

Il servizio rlogin è in esecuzione sull'host remoto. Questo servizio è vulnerabile poiché i dati vengono passati tra il client e il server rlogin in chiaro. Un utente malintenzionato man-in-the-middle può sfruttare questa situazione per sniffare login e password. Inoltre, potrebbe consentire accessi scarsamente autenticati senza password. Se l'host è vulnerabile all'ipotesi del numero di sequenza TCP (da qualsiasi rete) o allo spoofing IP (incluso il dirottamento ARP su una rete locale), potrebbe essere possibile ignorare l'autenticazione.
Infine, rlogin è un modo semplice per trasformare l'accesso in scrittura su file in accessi completi tramite i file .rhosts o rhosts.equiv.

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Soluzione

Commentare la riga 'login' in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilita questo servizio e utilizza invece SSH.

Output

- No output recorded.

Critical: Samba Badlock Vulnerability

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Descrizione

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali RPC (Remote Procedure Call). Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come visualizzare o modificare dati sensibili di sicurezza nel database di Active Directory (AD) o disabilitare servizi critici.

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

See Also

http://badlock.org

https://www.samba.org/samba/security/CVE-2016-2118.html

Output

- Nessus detected that the Samba Badlock patch has not been applied.

Critical: NFS Shares World Readable

Description

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

Descrizione

Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base a nome host, IP o intervallo IP).

Solution

Place the appropriate restrictions on all NFS shares.

Soluzione

Posizionare le opportune restrizioni su tutte le condivisioni NFS.

See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

Output

- The following shares have no access restrictions :

  / *

-Vulnerabilita meno critiche trovata nello scan a metasploitablet 2

Medium: TLS Version 1.0 Protocol Detection

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Descrizione

Il servizio remoto accetta connessioni crittografate utilizzando TLS 1.0. TLS 1.0 presenta numerosi difetti di progettazione crittografica. Le moderne implementazioni di TLS 1.0 mitigano questi problemi, ma le versioni più recenti di TLS come 1.2 e 1.3 sono progettate contro questi difetti e dovrebbero essere utilizzate quando possibile.

A partire dal 31 marzo 2020, gli endpoint che non sono abilitati per TLS 1.2 e versioni successive non funzioneranno più correttamente con i principali browser Web e i principali fornitori.

PCI DSS v3.2 richiede che TLS 1.0 sia completamente disabilitato entro il 30 giugno 2018, ad eccezione dei terminali POS POI (e dei punti terminali SSL/TLS a cui si connettono) che possono essere verificati come non suscettibili ad eventuali exploit noti.

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Soluzione

Abilita il supporto per TLS 1.2 e 1.3 e disabilita il supporto per TLS 1.0.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Output

- TLSv1 is enabled and the server supports at least one cipher.

Medium: Unencrypted Telnet Server.

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Descrizione

L'host remoto esegue un server Telnet su un canale non crittografato.

Non è consigliabile utilizzare Telnet su un canale non crittografato poiché login, password e comandi vengono trasferiti in chiaro. Ciò consente a un utente malintenzionato remoto, man-in-the-middle, di intercettare una sessione Telnet per ottenere credenziali o altre informazioni sensibili e modificare il traffico scambiato tra un client e un server.

SSH è preferito a Telnet poiché protegge le credenziali dalle intercettazioni e può eseguire il tunneling di flussi di dati aggiuntivi come una sessione X11.

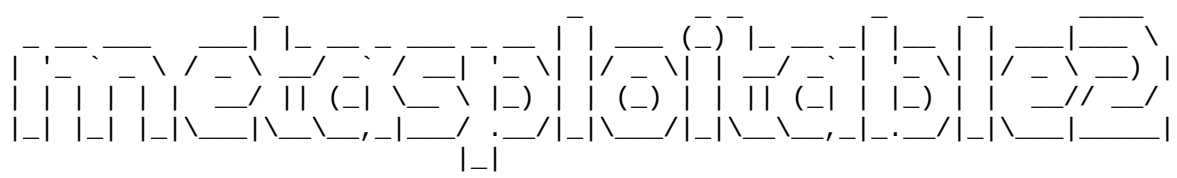
Soluzione

Disattiva il servizio Telnet e utilizza invece SSH.

Output

- Nessus collected the following banner from the remote Telnet server :

  ------------------------------ snip ------------------------------



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
------------------------------ snip ------------------------------
```

Medium: SSL Anonymous Cipher Suites Supported

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

Descrizione

L'host remoto supporta l'uso di crittografie SSL anonime. Sebbene ciò consenta a un amministratore di impostare un servizio che crittografa il traffico senza dover generare e configurare certificati SSL, non offre alcun modo per verificare l'identità dell'host remoto e rende il servizio vulnerabile a un attacco man-in-the-middle.

Nota: questo è molto più semplice da sfruttare se l'aggressore si trova sulla stessa rete fisica.

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Soluzione

```
Se possibile, riconfigurare l'applicazione interessata per evitare l'uso di
codici deboli.
```

See Also

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

Output:

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

crittografia debole insieme a una serie di connessioni appositamente predisposte a un server SSLv2 che utilizza la stessa chiave privata

Solution

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

Soluzione

Disabilita SSLv2 e le suite di crittografia di livello di esportazione. Assicurati che le chiavi private non vengano utilizzate da nessuna parte con software server che supporti le connessioni SSLv2.

See Also

https://drownattack.com/
https://drownattack.com/drown-attack-paper.pdf

Output

- The remote host is affected by SSL DROWN and supports the following vulnerable cipher suites :

```
  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth
Encryption             MAC
    ----------------------        ----------       ---           ----
--------------------  ---
    EXP-RC2-CBC-MD5               0x04, 0x00, 0x80 RSA(512)      RSA
RC2-CBC(40)            MD5       export
    EXP-RC4-MD5                   0x02, 0x00, 0x80 RSA(512)      RSA
RC4(40)                MD5       export

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth
Encryption             MAC
    ----------------------        ----------       ---           ----
--------------------  ---
    RC4-MD5                       0x01, 0x00, 0x80 RSA           RSA
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}
```