24.5.2 POP3 Konsole 2

Eine verschlüsselte TCP-Verbindung zu einem POP3-Server funktioniert zuverlässig, wenn Sie zum Beispiel den SSL-Client 'openssl' einsetzen. Als Port-Nummer für POP3 über SSL müssen Sie Port 995 verwenden.

24.5.2.1 Beispiel

```
[1]  hans@linux:~$ openssl s_client -quiet -connect mx.freenet.de:995
[2]  depth=2 C = DE, O = Deutsche Telekom AG, OU = T-TeleSec Trust Center, CN = Deutsche Telekom Root CA 2
[3]  verify error:num=19:self signed certificate in certificate chain verify return:0
[4]  +OK <500.1448880155@mx.freenet.de>
[5]  USER POP3Username
[6]  +OK user ok
[7]  PASS POP3PASSWORT
[8]  +OK 2 messages (5377 octets).
[9]  LIST
[10] +OK
[11] 1 2572
[12] 2 2805
[13] .
[14] RETR 1
[15] +OK 2572 octets
[16] [ KOPFZEILEN – HEADER ]
[17]
[18] This is a MIME multipart/mixed message.
[19]
[20] --|1B031C1B1A9321EF01|
[21] Content-Type: text/plain;charset=UTF-8
[22] Content-Disposition: inline
[23] Content-Transfer-Encoding: quoted-printable
[24] Content-Length: 72
[25]
[26] Hallo!
[27] =
[28]
[29] Im Anhang liegt die Datei acht.png
[30] =
[31]
[32] Mit freundlichem Gru=C3=9F
[33] =
[34]
[35] Hans
[36]
[37] --|1B031C1B1A9321EF01|
[38] Content-Type: image/png; name="acht.png"
[39] Content-Disposition: attachment
[40] Content-Transfer-Encoding: base64
[41] Content-Length: 116
[42]
[43] iVBORw0KGgoAAAANSUhEUgAAAAgAAAAICAYAAADED76LAAAAO0lEQVQYlX2PyQ0AMAjDnKr7
[44] r5x+egvIEyxwZDBFOoASxJoAEWUB0J6Zhedi5QFSh/0lkDnAd/pWK2sORyMOEhaL7BAAAAAA
[45] SUVORK5CYII=
[46]
[47] --|1B031C1B1A9321EF01|--
[48]
[49] .
[50] NOOP
[51] +OK
[52] QUIT
[53] +OK
[54] hans@linux:~$
```

Kommentar:

- In der Zeile 1 wird eine verschlüsselte Verbindung zum POP3-Server 'mx.freenet.de' auf dem Port 995 aufgebaut und in der Zeile 4 bestätigt.
- Anschließend erfolgt in den Zeilen 5 bis 8 die Identifizierung und Authentifizierung des Benutzers am POP3-Server.
- Mit 'USER POP3Username' wird der Username (Zeile 5) für das entsprechende EMail-Konto übergeben und im Klartext (!) gesendet – jetzt aber durch einen SSL-Tunnel.
- Wenn der Benutzer auf dem POP3-Server bekannt ist, +OK in Zeile 6, dann können Sie mit 'PASS POP3Passwort' das Passwort – auch wieder im Klartext – senden.
- Mit dem Befehl LIST in der Zeile 9 fragen Sie nach einer Liste der auf dem POP3-Server gespeicherten EMails und erhalten hier eine Liste mit zwei Zeilen, wobei in jeder Zeile eine (fortlaufende) Nummer und die Größe der EMail (Byte) steht.

- Mit 'RETR 1' in der Zeile 15 wird die erste EMail vom POP3-Server geladen und die vollständige Mime-Nachricht angezeigt. Auf die Anzeige der sehr vielen Kopfzeilen wurde teilweise verzichtet. Der Text des Bodys der Mime-Nachricht steht in den Zeilen 20 bis 54.
- Die Verbindung zwischen POP3-Client und POP3-Server wird mit dem Befehl 'QUIT' geschlossen.
- Der Text-Abschnitt im Body (Zeilen 26 bis 35) ist nach dem Verfahren 'quoted-printable' kodiert, worüber in der Zeile 23 im Sub-Header-Feld mit dem Feldnamen 'Content-Transfer-Encoding' mitgeteilt wird.
- Gute Informationen zu dieser Kodierung finden Sie hier → https://de.wikipedia.org/wiki/Quoted-printable.
- Vom Bild im Anhang (Zeilen 38 bis 41 und 43 bis 45) werden Sie nichts sehen, denn es ist base64-kodiert und somit blanker Text. Sie müssten den Text in den Zeilen 43 bis 45 erst base64-dekodieren und als Bild abspeichern.

Das ist der Konsole schnell getan:

```
echo iVBORw0KGgoAAAANSUhEUgAAAAgAAAAICAYAAADED76LAAAAO0lEQVQYlX2PyQ0AMAjDnKr7r5x+egvIEyxwZDBFOoASxJoAE \
WUB0J6Zhedi5QFSh/0lkDnAd/pWK2sORyMOEhaL7BAAAAAASUVORK5CYII= | base64 --decode > acht.png
```

Anschließend sehen Sie das Bild in Ihrem Home-Verzeichnis:

Abbildung 24.5.2.1.1: Winziges 8x8-Pixel-Bild

24.5.2.2 Authentifizierung über APOP

Wenn ein POP3-Server die Authentifizierung über *Authenticated Post Office Protocol* (APOP) anbietet, so wird zwar der POP3-User-Name im Klartext im SSL-Tunnel gesendet, aber das POP3-Passwort wird verschlüsselt übertragen und darauf kommt es unter dem Aspekt Sicherheit bei der Authentifizierung am POP3-Server an.

Die Authentifizierung über APOP basiert auf dem Challenge-Response-Verfahren, das nach einem Beitrag auf *https://de.wikipedia.org/wiki/Challenge-Response-Authentifizierung* "als ein sicheres Authentifizierungsverfahren eines Teilnehmers auf der Basis von Wissen" angesehen werden kann.

```
[1]  hans@linux:~$ openssl s_client -quiet -connect mx.freenet.de:995
[2]  depth=2 C = DE, O = Deutsche Telekom AG, OU = T-TeleSec Trust Center, CN = Deutsche Telekom Root CA 2
[3]  verify error:num=19:self signed certificate in certificate chain
[4]  verify return:0
[5]  +OK <31534.1448457450@mx.freenet.de>
[6]  APOP User-Name Has-Wert
[7]  +OK 3 messages (1147469 octets).
[8]  LIST
[9]  +OK
[10] 1 382310
[11] 2 382307
[12] 3 382852
[13] .
[14] QUIT
[15] +OK
[16] hans@linux:~$
```

Hinweise:

- Wenn ein POP3-Server nach dem Verbindungsaufbau mit einer *Willkommensnachricht* antwortet (Zeile 5), die der Syntax '+OK <process-id.timestamp@hostname>' folgt, dann können Sie sicher sein, dass der POP3-Server auch die Authentifizierung über APOP ermöglicht.
- Der POP3-Server übermittelt in der APOP-Willkommensnachricht nach dem +OK und einem Leerzeichen auch die Aufforderung <31534.1448457450@mx.freenet.de>.
- Aus dieser Server-Aufforderung muss der Client unter Einbeziehung des POP3-User-Passwortes einen Hash-Wert als Teil der Antwort berechnen. Später wird die Antwort gesendet – ohne darin das Passwort selbst zu übertragen!
- Die Berechnung des Hash-Wertes als Teil der Antwort erfolgt zum Beispiel in einer (weiteren) Konsole mit dieser Anweisung:

```
hans@linux:~$ echo -n "<31534.1448457450@mx.freenet.de>POP3-PASSWORD" | openssl md5
```

- Anschließend kann die vollständige Antwort aus 'User-Name<space>Hash-Wert' nach dem Befehl APOP an den POP3-Server (Zeile 6) gesendet werden:

```
APOP User-Name Hash-Wert
```

- War die Authentifizierung erfolgreich, dann sendet der POP3-Server (Zeile 7) nach dem +OK die Anzahl der EMails im Postfach sowie deren Gesamtgröße in Byte.

- Schlägt die Authentifizierung fehl, dann erhalten Sie diese Antwort vom POP3-Server:

```
-ERR permission denied
```