

Telnet gebruiken

Door Ives van der Flaas

INHOUD

- 1) *Inleiding*
- 2) *Anonieme mails versturen*
- 3) *Mail ophalen*
- 4) *Valse mails herkennen*
- 5) *IRC gebruiken*

1) INLEIDING

Van www.WikiPedia.nl:

Telnet (terminal networking) is een netwerkprotocol dat het mogelijk maakt op afstand in te loggen op een machine en die via een opdrachtregel te besturen. De computer waarop de telnetclient uitvoert fungeert dan als terminal van de server.\n

Telnet is officieel gespecificeerd in IETF-document STD 8 (RFC 854 and RFC 855), en gebruikt gewoonlijk TCP/IP-poort 23.

telnet is de naam van de meest gebruikte telnetclient. telnet is sinds begin jaren '80 beschikbaar op Unix. Dit programma kan verbinding maken met andere TCP-poorten dan 23, en kan dus gebruikt worden als "handmatige" client voor andere netwerkprotocollen; de gebruiker moet dan zelf de commando's en output van het protocol invoeren en interpreteren. Ook is het mogelijk telnet in een script te gebruiken.

Het gebruik maken van telnet (het protocol of het programma) wordt ook wel "telnetten" genoemd.

Telnet was één van de twee eerste applicatieprotocollen op het ARPANET (de andere was FTP). Omdat telnet slecht beveiligd is (alle gegevens, meestal inclusief wachtwoorden, worden in leesbare vorm over het netwerk verstuurd) wordt het steeds minder gebruikt, en stappen steeds meer gebruikers over op het versleutelde alternatief SSH. De versleutelde variant van telnet, SSL-telnet, is nooit echt aangeslagen.

Van mezelf:

Het kan gebeuren dat in telnet niet word weergegeven wat je zelf typt. Dit noemt men een local echo. Je kan deze aanzetten door in telnet (terwijl je bent ingelogt op een server) de toetscombinatie CTRL +] te drukken. Je komt nu in een venster van telnet zelf, daar typ je in

```
-----  
set localecho  
-----
```

Op een lege lijn moet je op ENTER te drukken om terug naar de server te gaan (deze keer met local echo aan).

Telnet is ook niet case-sensitive, dus HELO is hetzelfde als helo als HeLo en als HELLO.

2) ANONIEME MAILS VERSTUREN

Mail versturen is één van de vele functies van Telnet. Eerst moet je een commando prompt starten, dat kan je doen via [Start] - [Uitvoeren] of door de sneltoets [WINDOWS] - [R]. Voor de minder ervaren mensen, de windows toets is de toets tussen [CTRL] en [ALT] met het windows symbooltje erop. Telnet heeft een vervelend kwaaltje, de backspace toets genereert enkel een storend vierkantje. Als je dus een typfout maakt dan kan je het beste het venster sluiten en opnieuw beginnen.

Dan moet je met de mailserver van je ISP (Internet Service Provider) connecten. Hotmail, GMail en vele andere gratis mail-providers hebben deze functionaliteit spijtig genoeg niet. Aangezien ik telenet heb moet ik intypen in de commandoregel:

```
-----  
telnet uit.telenet.be 25  
-----
```

waarbij 25 de poort is waarmee je connect met je uitbox. Als je dit niet van buiten weet, kan je dit opzoeken op <https://www.networking4all.com/nl/helpdesk/email/sntp+servers/>

Nu moet je kennis maken met de server, dit doe je door HELO (Inderdaad, niet hello, maar HELO) te typen met daarachter de naam van je pc. De waarheid is dat dit eigenlijk niet veel uitmaakt, er word niet veel mee rekening gehouden.

```
-----  
HELO Ives  
-----
```

Het wordt tijd om aan te geven van welk emailadres je een mail wil sturen, dit mag bijna elk emailadres zijn! Ik moet hier wel bij vermelden dat hotmail (bij mij toch niet) werkt, terwijl MSN dat dan weer wel doet.

```
-----  
MAIL FROM:bill@microsoft.com  
-----
```

De bestemming bepaal je zo:

```
-----  
RCPT TO:ives.vdf@gmail.com  
-----
```

Hierop volgt de inhoud van de mail zelf. Dit doe je door DATA te typen, een enter, en dan te tekst die je wil doorsturen. Om je bericht te beëindigen moet je een nieuwe regel beginnen en daar enkel een punt op typen.

```
-----  
DATA  
Dag Ives, ik zou graag 10 miljoen euro op je rekening storten, omdat je altijd zo trouw windows  
hebt gebruikt.  
Groetjes Bill  
.  
-----
```

Je bericht word pas verstuurd als je de verbinding verbreekt, en dat doe je zo:

```
-----  
QUIT  
-----
```

Als je alles goed hebt gedaan krijg je een melding die zegt dat je mail in de rij staat om verstuurd te worden.

Een voorbeeld om alles voor te doen. Ik zal eerst laten zien wat je ingeeft, daarachter komt wat er op je scherm komt te staan, inclusief antwoord van de server.

```
-----  
telnet uit.telenet.be 25  
HELO Ives  
MAIL FROM:webmaster@rootx.nl  
RCPT TO:ives.vdf@gmail.com  
DATA  
Wow, het is me een echte eer om jou als 1337-hacker te mogen ontvangen op ons forum. Jij  
bent echt mijn idool.  
Groetjes, webmaster van RootX.nl  
.  
QUIT  
EXIT  
-----
```

Het scherm:

```
-----  
C:\Documents and Settings\ives>telnet uit.telenet.be 25  
  
220 europa.telenet-ops.be ESMTP Postfix  
HELO Ives  
250 europa.telenet-ops.be  
MAIL FROM:webmaster@rootx.nl  
250 Ok  
RCPT TO:ives.vdf@gmail.com  
250 Ok  
DATA  
354 End data with <CR><LF>.<CR><LF>  
Wow, het is me een echte eer om jou als 1337-hacker te mogen ontvangen op ons forum. Jij  
bent echt mijn idool.  
Groetjes, webmaster van RootX.nl  
.  
250 Ok: queued as D17EE23434F  
QUIT  
221 Bye  
  
De verbinding met de host is verbroken.  
C:\Documents and Settings\ives>exit  
-----
```

Nu krijgt je slachtoffer de mail aan.

3) MAIL ONTVANGEN

Net zoals om mail te versturen, moet je eerst connecten met de server, dit keer met je inbox. Geef dit in een command prompt in:

```
-----  
telnet in.telenet.be 110  
-----
```

Waarbij je natuurlijk in.telenet.be vervangt door de pop3 server van je ISP, en 110 door de poort waarnaar je moet verbinden. Nu moet je jezelf indentificeren. Dit doe je zo:

```
-----  
USER jeGebruikersNaam  
PASS jePaswoord  
-----
```

De server reageert nu met de boodschap dat alles OK is, en dat je verder kan. Nu kan je een lijst opvragen van alle aangekregen mails, dit doe je door LIST in te typen.

```
-----  
LIST  
-----
```

Je ziet op je scherm een lijst met alle aangekregen mails, voorgegaan door een nummer.

Als je wil weten wat de inhoud is van een bepaalde mail, gebruik dan het commando RETR # waarbij # het getal is dat in de lijst voor je mail staat.

```
-----  
RETR 1  
-----
```

Haalt de eerste mail op. Soms wil je enkel het bovenste gedeelte van je mail zien, de header bijvoorbeeld. Dit gaat met het commando TOP #mail #lijnen, dus als je van de 3de mail de eerste 10 lijnen wil zien doe je zoiets (dit commando werkt niet op alle servers):

```
-----  
TOP 3 10  
-----
```

Je kan ook de volledige mail binnenhalen met het RETR # commando, met ipv. # het nummer van de mail.

```
-----  
RETR  
-----
```

Stel dat je de eerste mail wil verwijderen, gebruik dan het commando

```
-----  
DELE 1  
-----
```

Als je wat snel bent geweest, en teveel mails hebt verwijderd, dan heb je geluk, want je kan met het RSET commando alle mails die je hebt aangeduid voor te verwijderen terug normaal maken.

```
-----  
RSET  
-----
```

Dit zijn alle commando's die je nodig hebt om normale mails te ontvangen en te openen.

4) VALSE MAIL HERKENNEN

Ik zal eerst een valse mail sturen (met de manier getoont bovenaan dit bestand).

```
-----
01)X-Gmail-Received: 66189181e40dbd95cd55d61e129272a32370408d
02)Delivered-To: ives.vdf@gmail.com
03)Received: by 10.48.205.20 with SMTP id c20cs33472nfg;
04)    Sat, 25 Mar 2006 10:32:55 -0800 (PST)
05)Received: by 10.66.242.15 with SMTP id p15mr1256248ugh;
06)    Sat, 25 Mar 2006 10:32:55 -0800 (PST)
07)Return-Path: <bill@microsoft.com>
08)Received: from hoboe2bl1.telenet-ops.be (hoboe2bl1.telenet-ops.be [195.130.137.73])
09)    by mx.gmail.com with ESMTP id e1si89239ugf.2006.03.25.10.32.55;
10)    Sat, 25 Mar 2006 10:32:55 -0800 (PST)
11)Received-SPF: softfail (gmail.com: domain of transitioning bill@microsoft.com does not
12)designate 195.130.137.73 as permitted sender)
13)Received: from localhost (localhost.localdomain [127.0.0.1])
14)  by hoboe2bl1.telenet-ops.be (Postfix) with SMTP id 551E51247FB
15)  for <ives.vdf@Gmail.com>; Sat, 25 Mar 2006 19:32:55 +0100 (CET)
16)Received: from Ives (d54C0F11C.access.telenet.be [84.192.241.27])
17)  by hoboe2bl1.telenet-ops.be (Postfix) with SMTP id 7D23212487D
18)  for <ives.vdf@Gmail.com>; Sat, 25 Mar 2006 19:32:12 +0100 (CET)
19)Message-Id: <20060325183212.7D23212487D@hoboe2bl1.telenet-ops.be>
20)Date: Sat, 25 Mar 2006 19:32:12 +0100 (CET)
21)From: bill@microsoft.com
22)To: undisclosed-recipients: ;
23)
24)Hi Ives, you should really start paying for my software.
25)Greetings, Bill
-----
```

Op lijn 16 is er duidelijk te zien dat de mail eigenlijk niet van Microsoft komt, maar verstuurd door een telenet server met het "helo Ives" commando. De persoon die de mail heeft verstuurd verzond deze dus van 84.192.241.27 (ook te lezen op lijn 16). Deze hoofding verschilt natuurlijk van mail tot mail, maar met wat logisch verstand valt dit wel uit te zoeken.

5) IRC GEBRUIKEN

Dit is één van de ingewikkeldste dingen (vind ik) die je met telnet kan doen. Zoals altijd met telnet moet je eerst connecten met de server. Dit doe je (voor IRC) meestal op poort 6667. Als voorbeeld ga ik hier connecten met het IRC chatkanaal op server irc.wondernet.nu. Hiervoor start je opnieuw een commando prompt, waar je het volgende intypt.

```
-----  
telnet irc.wondernet.nu 6667  
-----
```

De server wil nu dat je duidelijk maakt wie je bent. Dit doe je zo:

```
-----  
USER Ives.vdf localhost localhost : Ives van der Flaas  
NICK Ives  
-----
```

Ives.vdf staat voor je gebruikersnaam, Ives van der Flaas moet je vervangen door je echte naam (natuurlijk kan je hier invullen wat je zelf wil).

De volgende regel bepaald je nickname, het zou kunnen dat de server zegt dat deze nick al bezet is, dan kan je gewoon het commando opnieuw uitvoeren, deze keer met een andere nickname.

Niet lang nadat je bent ingelogd zal de server het volgende bericht doorsturen:

```
-----  
PING :Ro.FL.US.WonderNet.nu  
-----
```

Hierop moet je antwoorden met PONG, met daarachter hetgeen dat achter de dubbele punt staat.

```
-----  
PONG Ro.FL.US.WonderNet.nu  
-----
```

Doe je dit niet, dan kan (en zal) de server je eraf gooien.

Chatten doe je altijd in een bepaald kanaal, dit kanaal kan je kiezen met het join commando. Vergeet de # voor het kanaal niet.

```
-----  
join #rootx  
-----
```

Vanaf dit moment zie je alles wat er wordt gezegd in die room. Als je zelf iets wil zeggen, gebruik dan de (iets wat ingewikkelde) syntax privmsg #channel : Bericht

```
-----  
privmsg #rootx :Is daar iemand?  
-----
```

Soms wil je een privé bericht sturen, dit doe je op dezelfde manier als een algemeen bericht.

```
-----  
privmsg Ontvanger : Prive bericht, gewoon aan het testen voor men tutorial :D.  
-----
```

De meeste commando's die je normaal in mIRC zou gebruiken werken ook in Telnet, maar dan zonder de /.