Labo computernetwerken 1 – Applicatielaag

Tijdens dit eerste practicum leren we hoe applicaties communiceren met elkaar, en waarom er voor elke applicatie aparte protocollen gespecifieerd zijn. We verkennen het soort commando's die uitgewisseld worden tussen de host die de client rol aanneemt, en de host die de server rol aanneemt. Kortom, we proberen te praten tegen een computer alsof wijzelf ook een computer zijn. Het biedt ons een inzicht in welke instructies er precies vervat zitten in een applicatielaagprotocol.

Interactieve verbinding met server: telnet / SSH

1) Telnet

Het uitwisselen van data tussen twee hosts op een betrouwbare manier kan in zijn essentie heel eenvoudig: je initieert een TCP-verbinding, en wisselt ASCII-karakters uit tussen de twee eindpunten. **`telnet`**[1] is een zeer eenvoudige tool om over het netwerk met andere hosts te praten aan de hand van een TCP verbinding. **`telnet`** stuurt alle tekst die je intypt rechtstreeks naar de server en toont alle tekst die de server terugstuurt op het scherm. Een voorbeeld:

```
home login: comnet1
Password:
Last login: Mon Feb 15 16:29:40 CET 2020 from dhcp242.intec.ugent.be on pts/3
Linux home 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u4 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
comnet1@home:~$ whoami
comnet1
comnet1@home:~$
```

Eenmaal ingelogd, worden alle instructies die worden doorgestuurd, uitgevoerd op de server. **`telnet`** stuurt wel alles in *plain text* door: wie de pakketten kan onderscheppen, kan alle instructies meelezen.

2) Secure Shell (SSH)

Nu bijna alle systemen op één of ander netwerk zijn aangesloten wordt nog slechts zelden ter plekke met servers gewerkt. Meestal worden deze servers via het netwerk aangestuurd. Secure Shell (SSH) is één van de meest gebruikte manieren om over het netwerk commando's uit te voeren op een remote server. Je zou hiervoor ook **`telnet`** kunnen gebruiken, maar Secure Shell is een stuk veiliger omdat alle communicatie tussen client en server geëncrypteerd wordt. Wie de pakketten onderschept, ziet enkel geëncrypteerde en dus onleesbare data.

Om een SSH sessie te starten hebben we uiteraard een SSH client nodig. Op Linux en Mac machines wordt deze software mee geïnstalleerd als het commando "ssh".

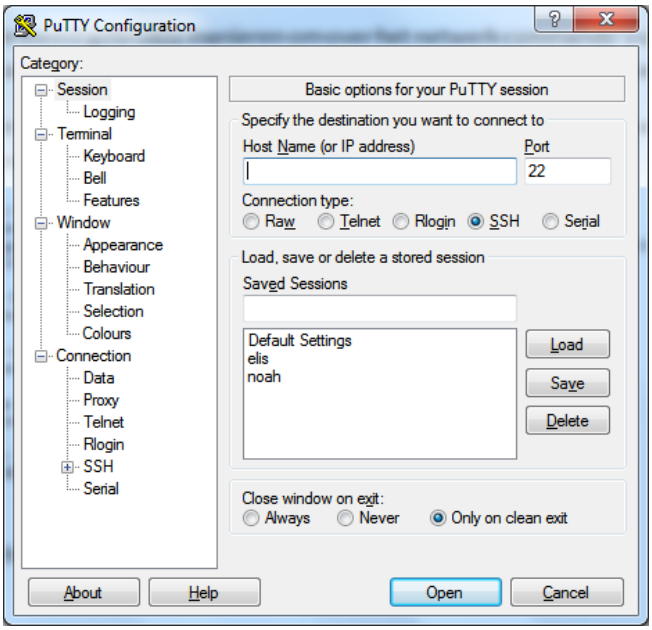
```
user@linux:~$ ssh comnet1@home.test.atlantis.ugent.be
student@CompNet:~$ ssh comnet1@home.test.atlantis.ugent.be
The authenticity of host 'home.test.atlantis.ugent.be (157.193.215.170)' can't
be established.
ECDSA key fingerprint is SHA256:w9IwLirJkBJsjwuPBv/WCOSnAbgYUe9mO1BKPH3yr1E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'home.test.atlantis.ugent.be,157.193.215.170'
(ECDSA) to the list of known hosts.
comnet1@home.test.atlantis.ugent.be's password:
Linux home 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

[1] Op Linux kan je deze software installeren met **`sudo apt install telnet`**

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Oct 15 11:52:53 2020 from 87.66.224.244
comnet1@home:~$
```

In het labo werken we vanop een Linux VM, waar SSH standaard aanwezig is op de CLI. Voor de volledigheid: niet op alle Windows machines is er standaard een SSH client aanwezig. We kunnen als alternatief PuTTY[2] gebruiken, een gratis SSH client voor Windows. Wie wil kan dit zelf uitproberen.



Telnet als service voor andere applicaties

`telnet` implementeert geen enkel protocol en kan dus gebruikt worden voor alle tekst gebaseerde protocollen. Het is voor vele andere protocollen (HTTP, SMTP, POP) een manier om instructies te transporteren tussen een client en een server.

3) Mail protocollen

In het klassieke mailsysteem, daterend uit begin de jaren '80, werken verschillende protocollen samen. SMTP laat toe om van een client een e-mail te sturen naar jouw mailserver. Tussen mailservers onderling wordt het e-mail bericht verder gepushed tot het op de mailserver van de bestemmeling aankomt. Daar blijft de e-mail wachten tot hij geraadpleegd wordt door de ontvanger. Raadplegen kan op twee manieren: via POP, dat e-mails downloadt naar de client, of via IMAP, dat synchronisatie toelaat tussen de server & de client. Deze laatste laat toe e-mails op meerdere plaatsen tegelijk te bewaren (server, een mailclient, een smartphone, …). Dit complexe protocol valt buiten de scope van dit labo. POP laat toe om e-mails af te halen van de server, en de inbox op de server te beheren door ze na het afhalen ofwel daar te laten, ofwel te verwijderen – zonder synchronisatie.

SMTP & POP zijn de twee protocollen die we bespreken. Zo kun je **`telnet`** gebruiken om met een SMTP mailserver te praten, op zijn server poort 25:

```
comnet1@home:~$ telnet mail.test.atlantis.ugent.be 25
Trying 157.193.215.172...
Connected to mail.test.atlantis.ugent.be.
Escape character is '^]'.
220 mail.test.atlantis.ugent.be ESMTP Postfix (Debian/GNU)
HELO mycomputer.homenet.be
250 mail.test.atlantis.ugent.be
```

[2] Online te vinden op http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

```
MAIL FROM: john.doe@intec.ugent.be
250 Ok
RCPT TO: comnet1@test.atlantis.ugent.be
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Dit is een mailtje
.
250 Ok: queued as BF0054BEDF
QUIT
221 Bye
Connection closed by foreign host.
comnet1@home:~$
```

Een mail die op deze manier is verstuurd kan via POP gelezen worden, zonder mail client kan ook hier **`telnet`** gebruikt worden om de commando's van het POP protocol door te geven aan de mailserver:

```
comnet1@home:~$ telnet mail.test.atlantis.ugent.be 110
Trying 157.193.215.172...
Connected to mail.test.atlantis.ugent.be.
Escape character is '^]'.
+OK Cubic Circle's v1.31 1998/05/13 POP3 ready <fa0e00009a9e5843@mail>
USER comnet1
+OK comnet1 selected
PASS p@sw00rd
+OK Congratulations!
STAT
+OK 1 1138
RETR 1
+OK 1138 octets
Received: by mail (mbox comnet1)
(with Cubic Circle's cucipop (v1.31 1998/05/13) Fri Oct 21 10:05:04 2020)
X-From : comnet1@test.atlantis.ugent.be Oct 21 10:04:42 2020
Return-Path: <comnet1@test.atlantis.ugent.be>
X-Original-To: comnet1@test.atlantis.ugent.be
Delivered-To: comnet1@test.atlantis.ugent.be
Received: from PCklasZ01 (pcklasz01.stud.atlantis.ugent.be [157.193.215.194])
by mail.test.atlantis (Postfix) with SMTP id 20ECE4BEDF
for <comnet1@test.atlantis.ugent.be>; Fri, 21 Oct 2020 10:04:42 +0200 (CEST)
Message-ID: <000b01c5d62d60e85b40c2d7c19d@PCklasZ01>
From: "Comnet1" <comnet1@test.atlantis.ugent.be>
To: "Comnet1" <comnet1@test.atlantis.ugent.be>
Subject: Mailtje
Date: Fri, 21 Oct 2020 12:51:23 +0200
MIME-Version: 1.0
Content-Type: text/plain;
format=flowed;
charset="iso-8859-1";
reply-type=response
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2527
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2527
ten behoeve van een voorbeeld
.
QUIT
+OK Was it as good for you, as it was for me? (clean as a baby)
Connection closed by foreign host.
comnet1@home:~$
```

4) HTTP

Ook HTTP gebruikt onderliggend telnet om zijn commando's door te geven aan een webserver. Met telnet kan je dus ook rudimentair surfen, zoals hieronder getoond wordt:

```
user@linux:~$ telnet portquiz.net 80
Trying 52.47.209.216...
Connected to portquiz.net.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Thu, 15 Oct 2020 09:44:03 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 3317
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<head>
<title>Outgoing Port Tester</title>
<style type="text/css">
[ ... (further server response)]
</body>

</html>
Connection closed by foreign host.
user@linux:~$
```

Bij HTTP-verbindingen is het vaak zo dat de echo, het tonen van wat precies aan de server wordt meegedeeld, uit staat. Wil je dit toch zien, moet je eerst het programma telnet opstarten, expliciet echo aanzetten, en dan pas de verbinding openen met de HTTP-server.

Surfen hoeft dus helemaal niet vanuit een GUI omgeving – ook met telnet kan je een webpagina downloaden. Specifiek zijn er andere twee andere programma's die beter omgaan met HTTP verbindingen: **`curl`** en **`lynx`**. Start deze twee programma's ook eens op naar dezelfde webserver.

Opdrachten met telnet: aan de slag

Voer de volgende opdrachten uit in je Linux VM en beschrijf jouw resultaten. Verwerk je resultaten in een persoonlijk verslag (e.g. Markdown gebaseerd (zie http://markdowntutorial.com/)). Je kan deze resultaten gebruiken op de test over dit onderwerp.

1. Verbind met home.test.atlantis.ugent.be op poort 23, maak op deze server in je thuismap een bestand aan met jouw naam en studentennummer er in, genaamd 'mijnInfo.txt'.
2. Verbind met deze zelfde server, maar nu op poort 13. Beschrijf de info die je ziet.
3. Hoe kan je met **`telnet`** testen of deze server ook een FTP daemon werkende heeft?

4. Verbind met **`telnet`** met de mailserver mail.test.atlantis.ugent.be en verstuur een mail naar jezelf vanuit deze telnet verbinding (welke poort?).
   Let wel: backspace werkt meestal niet bij dit soort verbindingen, dus werk met de precisie die ook een computerprogramma zou hanteren.
5. Lees nadien deze mail door met dezelfde server te verbinden, maar gebruik nu poort 110 (POP).
6. Stuur een mail naar gebruiker avmaele@test.atlantis.ugent.be. Kan je een subject[3] instellen (Labo 1 – mail)? Als inhoud van de mail stuur je één zin.
7. Wat doet het commando NOOP bij het POP protocol. Lees dit na in RFC 1939.

8. Download met behulp van **`wget`**[4] een script via HTTP:
   `wget www.test.atlantis.ugent.be/capture_syn.sh`
   Start op de CLI van jouw Virtuele Linux het script "./capture_syn.sh". Dit start Wireshark op, en captured enkel de start van een TCP verbinding – niks meer. Surf vervolgens met Firefox naar de site 'www.test.atlantis.ugent.be'. Kan je uit de Wireshark info afleiden welke versie van HTTP deze server ondersteunt? Leg uit.
9. Maak met **`telnet`** verbinding met dezelfde webserver (welke poort?) en vraag de hoofdpagina op door de HTTP commando's door te geven in je telnet verbinding.
10. Surf met Lynx naar de webserver; tegelijk capture je opnieuw het aantal TCP verbindingen met het script uit de voorgaande vraag. Is er een verschil. Kan je dit verklaren?

11. Download met behulp van **`wget`** een script via HTTP, dat je in het volgende luik kan gebruiken:
    `wget www.test.atlantis.ugent.be/capture_dns.sh`

[3] De originele RFC kan je vertellen hoe precies - https://tools.ietf.org/html/rfc821
[4] Jawel: **`sudo apt install wget`**

DNS queries

Een DNS client wordt door bijna elke applicatie gebruikt: een achterliggend programma vraagt aan een DNS-server op welk IP-adres correspondeert met de URL die werd opgegeven in het programma. Dit proces heet men *resolving*. Hoewel dit bijna overal achterliggend gebeurt, vindt deze *resolving* plaats bij quasi elke aanvraag die de computer start naar de buitenwereld – je merkt het gewoon niet…
Ook manueel kan een DNS request getriggerd worden met een programma als **`nslookup`**[5]:

```
comnet1@home:~$ nslookup www.ugent.be
Server:  ugdns1.ugent.be
Address:  157.193.40.37

Non-authoritative answer:
Name:   www.ugent.be
Address: 157.193.43.50
```

Bij het resolven wordt hier de default DNS-server gebruikt, die ingesteld is op de host (e.g. door DHCP). De naam en het IP-adres van de DNS-server die ons deze informatie aanlevert worden eerst weergegeven, gevolgd door de naam en het IP-adres van de URL die werd opgevraagd.

Wie expliciet een andere server wil gebruiken om informatie op te vragen, kan dit door bij het commando ook het server adres (of naam) mee te geven:

```
comnet1@home:~$ nslookup <gezochte URL> [DNS-server IP-adres of naam]
comnet1@home:~$ nslookup www.ugent.be 157.193.40.42
Server:  ugdns2.ugent.be
Address:  157.193.40.42

Non-authoritative answer:
Name:    www.ugent.be
Address:  157.193.43.50
```

Behalve het nslookup commando, dat zowel werkt op Linux als op Windows, kan men op Linux ook het **`host`** commando gebruiken (kortere output), of het **`dig`** commando (extensieve output).

Met **`dig`** kan je ook extra informatie opvragen, zoals bvb. de servers die verantwoordelijk zijn voor de details van een bepaald domein (a.k.a. de authoritative server):

```
comnet1@home:~$ dig +short NS ugent.be
ugdns3.ugent.be.
ugdns1.ugent.be.
ugdns2.ugent.be.
ns.belnet.be.
```

Opdrachten met DNS: aan de slag

Vul je (markdown?) verslag aan met volgende opdrachten:

1. Welk IP-adres heeft www.ugent.be? Welke servers zijn verantwoordelijk voor dit domein?
2. www.belnet.be geeft een IP-adres terug, maar als je dit IP-adres probeert om te zetten in een URL (reverse lookup) merk je dat de server een andere naam heeft. Welke?
   Licht toe hoe je dit vond.
3. Resolve de URL www.tinder.com verschillende keren na elkaar, en gebruik verschillende nameservers. Herhaal hetzelfde op de home server (log in met SSH), die andere DNS-servers gebruikt. Beschrijf wat je ziet - waarom gaat een groot bedrijf op deze manier te werk?
4. Start in je Linux VM het script **`capture_dns.sh`**[6] op dat je downloadde; voer de lookup naar www.tinder.com opnieuw uit. Hoeveel DNS requests werden er naar de server gestuurd, hoeveel antwoorden kreeg je terug?

[5] Installatie op Linux: **`sudo apt install dnsutils`**
[6] Je kan een script opstarten door er bash voor te tikken (**`bash capture_dns.sh`**), ofwel door de juiste execute permissies toe te kennen m.b.v. **`chmod`**