Huiswerk Linux: Telnet hacking

De opdracht is: erachter komen wat voor webserver er gebruikt wordt voor een aantal web-sites. Ook zouden we graag willen weten of er een scripting-taal, zoals PHP of .NET gebruikt wordt. We gebruiken daarvoor de commando's *telnet*, *tee* en het *pipe*-symbool.

Over telnet

Telnet is de moeder van alle internet programma's. Met het commando *telnet* kun je een conversatie met een willekeurige server starten en de "ruwe data" van het internet zien. Standaard maakt telnet contact via poort 23 (telnet). Je krijgt dan command-line toegang tot een Linux server. In het kader van deze opdracht gaan wij een conversatie starten met een aantal web-servers over poort 80 (HTTP).

Cygwin gebruikers

Het *telnet* commando is onderdeel van het *inetutils* package. Dit wordt niet standaard in Cygwin geïnstalleerd. We gaan ons Linux systeem uitbreiden met het *inetutils* package.

Open een Cygwin terminal **Als administrator** en gebruik het *apt-get* installatieprogramma om het *inetutils* package te installeren:

```
apt-get install inetutils
```

Andere Linux gebruikers

Ook in de andere Linux versies wordt *telnet* niet standaard geïnstalleerd. Open een terminal met **<Ctrl><Alt>-T** en installeer het *telnet* package met het *apt-get* installatieprogramma:

```
sudo apt-get install telnet
```

We gebruiken hier het *sudo* mechanisme, zodat de bestanden met de juiste toegangsrechten geïnstalleerd worden.

Home-page opvragen

Om te zien hoe *telnet* werkt, gaan we eerst de complete home-pagina van mijn web-server neerladen. Type de volgende regel en geef <Enter>:

```
telnet www.boland.nl 80
```

We maken nu contact met mijn web-server en krijgen het volgende antwoord:

```
Trying 85.92.128.191...
Connected to www.boland.nl.
Escape character is '^]'.
```

De server wacht nu op jouw *request* (aanvraag). Type nu de volgende aanvraag in, gevolgd door **twee keer** <Enter>:

```
GET / HTTP/1.0
```

In dit geval doen we een *GET* aanvraag en we willen de home-pagina ("/"), volgens het *HyperText Transfer Protocol* (HTTP), versie 1.0.

De server geeft antwoord door de home-pagina op te sturen en beëindigt de verbinding. Maximaliseer het terminal venster, zodat je het volgende kunt zien:

```
HTTP/1.1 200 OK
Date: Sat, 15 Aug 2015 09:00:08 GMT
Server: Apache/1.3.29 (Unix) mod_ssl/2.8.16 OpenSSL/0.9.7j
Last-Modified: Sun, 11 Mar 2007 01:31:55 GMT
ETag: "5c3015d6d87ec583ff7a85d5925ff511f1ec540a"
Accept-Ranges: bytes
Content-Length: 2216
Connection: close
Content-Type: text/html

<!doctype html public "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Test Page for Apache Installation</title>
</head>
<body bgcolor="#ffffff">
```

```
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
    <td bgcolor="99ffff">
<a href="http://www.openbsd.org/"><img alt="[OpenBSD]" border="0" height=30 width=141
      SRC="smalltitle.gif"></a><br>
<b><font color="#ee0000" size="18"> Apache</font></b>
    </td>
</tr>
<tr>
    <td bgcolor="0000cc"> </td>
</tr>
</table>

<h1 align="center">It Worked!</h1>
<p>
    If you can see this page, then the people who own this host have just
    activated the <a href="http://www.apache.org/">Apache Web server</a>
    software included with their <a href="http://www.openbsd.org/">
    OpenBSD System</a>. They now have to add content to this directory
    and replace this placeholder page, or else point the server at their real
    content.
</p>

<p align="center">
    <img src="manual/images/mod_ssl_sb.gif">
    <img src="manual/images/openssl_ics.gif">
</p>
</body>
</html>
Connection closed by foreign host.
```

We zien twee stukken tekst, gescheiden door een lege regel. Het onderste stuk tekst is HTML, herkenbaar aan de *<html>* en *</html>* tags. Dit wordt normaal door je browser visueel gemaakt.

Het bovenste stuk noemen we de *MIME* header. Die is voor ons interessant, want we kunnen nu zien om welke server en versie het gaat (Microsoft-IIS/8.0).

Alleen MIME header opvragen

Eigenlijk zijn we alleen geïnteresseerd in de MIME informatie, niet de hele web-pagina. HTTP heeft daar de *HEAD request* (aanvraag) voor. Deze wordt vaak gebruikt door web-crawlers, zoals Google, om te kijken of de pagina is gewijzigd.

Haal het *telnet* commando terug met de *omhoog*-pijltjestoets en geef <Enter>:

telnet www.boland.nl 80

We krijgen opnieuw antwoord van mijn web-server:

```
Trying 85.92.128.191...
Connected to www.boland.nl.
Escape character is '^]'.
```

Geef nu de *HEAD* aanvraag in, en toets **twee keer** <Enter>:

HEAD / HTTP/1.0

De server stuurt nu alleen de MIME header en beëindigt de verbinding:

```
HTTP/1.1 200 OK
Date: Sat, 15 Aug 2015 09:00:08 GMT
Server: Apache/1.3.29 (Unix) mod_ssl/2.8.16 OpenSSL/0.9.7j
Last-Modified: Sun, 11 Mar 2007 01:31:55 GMT
ETag: "5c3015d6d87ec583ff7a85d5925ff511f1ec540a"
Accept-Ranges: bytes
Content-Length: 2216
Connection: close
Content-Type: text/html

Connection closed by foreign host.
```

MIME header in bestand opslaan

We gaan in de les de header-informatie nader bekijken. Sla daarom de conversatie met de server op in een tekstbestand door een pijpleiding te crëeren tussen het *telnet* commando en het *tee* commando. Toets daarna <Enter>:

```
telnet www.boland.nl 80 | tee bestand_a.txt
```

We krijgen opnieuw antwoord van mijn web-server:

```
Trying 85.92.128.191...
Connected to www.boland.nl.
Escape character is '^]'.
```

Geef opnieuw de *HEAD* aanvraag in en toets **twee keer** <Enter>:

```
HEAD / HTTP/1.0
```

Het antwoord van mijn web-server staat nu in het bestand, genaamd *bestand_a.txt*.

Opdracht

Sla de *MIME* header op van de volgende web-sites. Verander steeds de bestandsnaam (bestand_b.txt, bestand_c.txt, etc.), zodat de informatie per web-site in verschillende bestandjes terecht komt.

www.twitter.com
www.xs4all.nl
www.gnu.org
www.linux.org
www.lighttpd.net
www.skype.com
www.dropbox.com

Voeg ook een aantal websites van je eigen keuze toe. Hoe obscuurder, hoe beter. Succes!