

Sieci komputerowe - Warsztaty 6

Jakub Grobelny 300481

Zadanie do zaprezentowania (2 pkt.)

Dodajemy nowy wiersz do `/etc/hosts`:

```
root@virbian: /home/user
root@virbian:/home/user# vim /etc/hosts
root@virbian:/home/user# cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    virbian

# The following lines are desirable for IPv6 capable hosts
::1    localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

156.17.4.30  sieci.ii.uni.wroc.pl
```

Dodajemy wpis na stronie:

Testowy formularz - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Testowy formularz x +

Testowy formularz

sieci.ii.uni.wroc.pl/index.php

HTTP Header Live x

Connection: keep-alive
Upgrade-Insecure-Requests: 1
POST: HTTP/1.1 200 OK
Date: Mon, 18 May 2020 19:30:15 GMT
Server: Apache/2.4.38 (Debian)
Expires: now
Last-Modified: Mon, 18 May 2020 19:30:15GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 7269
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

http://sieci.ii.uni.wroc.pl/favicon.ico
Host: sieci.ii.uni.wroc.pl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) C
Accept: image/webp,*/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
GET: HTTP/1.1 404 Not Found
Date: Mon, 18 May 2020 19:21:53 GMT
Server: Apache/2.4.38 (Debian)
Content-Length: 282
Content-Type: text/html; charset=iso-8859-1

Clear Options File Save Record Data autoscroll

Formularz testowy na podstawie hydeparku Tomasza Wierzbickiego

Dodaj uwagę

Wyślij Wyczyść

Bieżące wpisy

33714: 18-05-2020, 21:30:15
1234567890

33713: 18-05-2020, 21:29:50
To jest test.

33712: 18-05-2020, 21:29:18
To jest test.

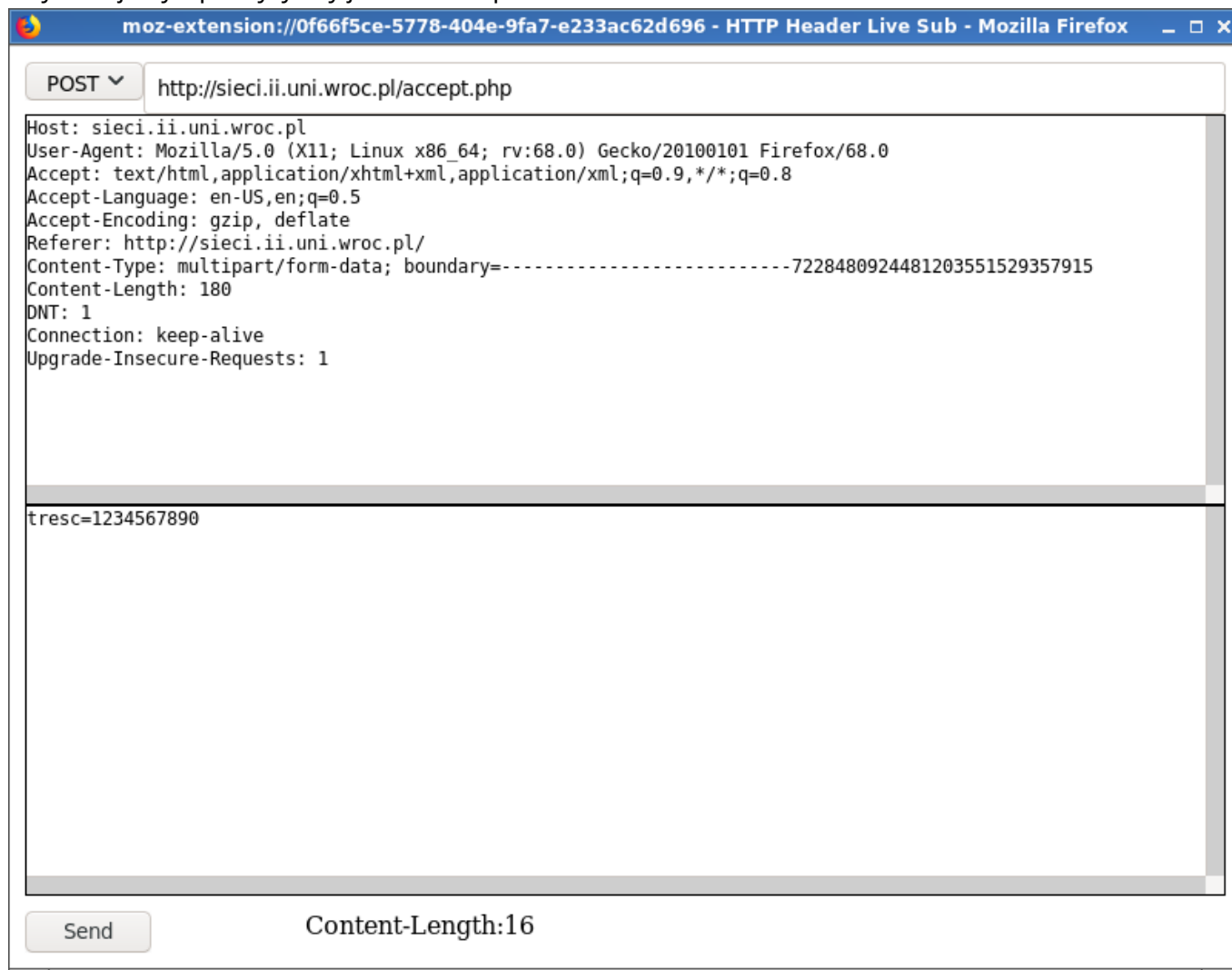
33711: 18-05-2020, 21:28:36
To jest test.

33710: 18-05-2020, 21:25:36
test tescik tesciuno

33709: 18-05-2020, 21:08:06
W dniach 30 września i 1 października zapraszamy na dni adaptacyjne odbywających się w budynku Instytutu Informatyki UW., ul. Joliot-Curie 15.

33708: 18-05-2020, 21:07:15
W dniach 30 września i 1 października zapraszamy na dni adaptacyjne odbywających się w budynku Instytutu Informatyki UW., ul. Joliot-Curie 15.

Gdy dodajemy wpis wysyłany jest POST request.



moz-extension:///0f66f5ce-5778-404e-9fa7-e233ac62d696 - HTTP Header Live Sub - Mozilla Firefox

POST http://sieci.ii.uni.wroc.pl/accept.php

Host: sieci.ii.uni.wroc.pl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://sieci.ii.uni.wroc.pl/
Content-Type: multipart/form-data; boundary=-----7228480924481203551529357915
Content-Length: 180
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

tresc=1234567890

Send Content-Length:16

Uruchamiamy polecenie:

```
V0$> nc -l -p 8888 | tee http request
```

Zmieniamy proxy na `localhost:8888`.



☒ Manual proxy configuration

HTTP Proxy Port

Po tej zmianie wpis nie zostaje dodany.

The screenshot shows a terminal window on the left and a Mozilla Firefox browser window on the right. The terminal displays an nc listener on port 8888 that has received a POST request from http://sieci.ii.uni.wroc.pl/accept.php. The request headers include Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Referer, Content-Type, Content-Length, DNT, Connection, and Upgrade-Insecure-Requests. The body of the request is a multipart/form-data with a single field named 'tresc' containing the value 'jakaś uwaga'. The browser window shows the 'Testowy formularz' page at sieci.ii.uni.wroc.pl/index.php. The page title is 'Formularz testowy na podstawie hydeparku Tomasza Wierzbickiego'. It contains a text input field with the placeholder 'jakaś uwaga', two buttons labeled 'Wyślij' and 'Wyczyść', and a section titled 'Bieżące wpisy' showing a single entry: '33722: 18-05-2020, 21:38:43'. The status bar at the bottom of the browser indicates 'Waiting for sieci.ii.uni.wroc.pl...'.

Dzieje się to dlatego, że requesty zostają przekierowane do serwera działającego na **localhost** na porcie **8888**, który z nimi nic nie robi, a przeglądarka nie dostaje nigdy odpowiedzi.

Zawartość pliku **http_request**:

```
root@virbian:/home/user# cat http_request
POST http://sieci.ii.uni.wroc.pl/accept.php HTTP/1.1
Host: sieci.ii.uni.wroc.pl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://sieci.ii.uni.wroc.pl/index.php
Content-Type: multipart/form-data; boundary=-----60867723014932348251633710471
Content-Length: 184
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
-----60867723014932348251633710471
Content-Disposition: form-data; name="tresc"

jakaś uwaga
-----60867723014932348251633710471--
root@virbian:/home/user#
```

Jak widać znajduje się w nim request POST, który wysłała przeglądarka w momencie próby dodania nowego wpisu.

Po ręcznym wysłaniu zapytania wpis pojawił się na stronie:

```
root@virbian: /home/user
root@virbian:/home/user# nc -q 3 sieci.ii.uni.wroc.pl 80 < http_request
HTTP/1.1 302 Found
Date: Mon, 18 May 2020 20:08:31 GMT
Server: Apache/2.4.38 (Debian)
Location: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

root@virbian:/home/user#
```

Bieżące wpisy

33737: 18-05-2020, 22:08:31
jakaś uwaga

Zmieniamy komunikat i pole **Content-Length** w pliku **http_request** a następnie wysyłamy zapytanie.

```
root@virbian: /home/user
root@virbian:/home/user# cat http_request
POST http://sieci.ii.uni.wroc.pl/accept.php HTTP/1.1
Host: sieci.ii.uni.wroc.pl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://sieci.ii.uni.wroc.pl/index.php
Content-Type: multipart/form-data; boundary=-----60867723014932348251633710471
Content-Length: 202
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----60867723014932348251633710471
Content-Disposition: form-data; name="tresc"

recznie zmieniony http_request
-----60867723014932348251633710471--
root@virbian:/home/user# nc -q 3 sieci.ii.uni.wroc.pl 80 < http_request
HTTP/1.1 302 Found
Date: Mon, 18 May 2020 20:23:45 GMT
Server: Apache/2.4.38 (Debian)
Location: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

root@virbian:/home/user#
```

Bieżące wpisy

33756: 18-05-2020, 22:23:45
recznie zmieniony http_request

Zadanie do zaprezentowania (3 pkt.)

Sprawdzamy poleceniem **dig** adres IP przypisany do domeny **www.debian.org**.

```
root@virbian:/home/user# dig www.debian.org +short
130.89.148.77
```

W jednym terminalu uruchamiamy polecenie

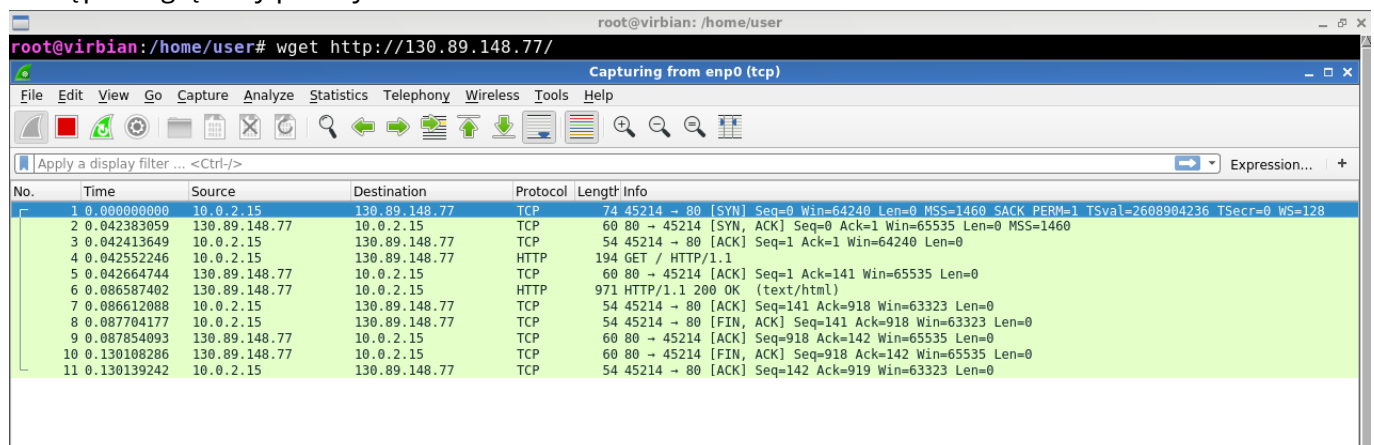
```
V0$> (while true; do netstat -tan | grep 130.89.148.77 ; done) | tee tcp
log
```

a w drugim

```
V0$> wget http://130.89.148.77/
```

W pliku **tcp_log** znajdują się stany **SYN_SENT**, **ESTABLISHED**, **FIN_WAIT2** i **TIME_WAIT**.

Następnie oglądamy pakiety IP w Wiresharku.



- Jakie gniazda tworzone są do pobierania pliku przez HTTP?
 - Tworzone są gniazda strumieniowe używające protokołu TCP.
- Jaki jest port źródłowy a jaki docelowy połączenia?
 - Port źródłowy: 45214, port docelowy: 80
- 1.
 - Włączone flagi: **SYN**
 - Przesyłane bajty: (numer sekwencyjny = 0)
 - Potwierdzone bajty:
 - Zmiana stanu: klient: **SYN_SENT** (widoczne w **tcp_log**)
- 2.
 - Włączone flagi: **ACK, SYN**
 - Przesyłane bajty: (numer sekwencyjny = 0)
 - Potwierdzone bajty: 1
 - Zmiana stanu: serwer: **SYN_RECEIVED**
- 3.
 - Włączone flagi: **ACK**
 - Przesyłane bajty:
 - Potwierdzone bajty: 1

- Zmiana stanu: klient: **ESTABLISHED** (widoczne w **tcp_log**)
 - 4. ◦ Włączone flagi: **ACK**
 - Przesyłane bajty:
 - Potwierdzone bajty: 141
 - Zmiana stanu: serwer: **ESTABLISHED**
 - 5. ◦ Włączone flagi: **ACK**
 - Przesyłane bajty:
 - Potwierdzone bajty: 918
 - Zmiana stanu:
 - 6. ◦ Włączone flagi: **FIN, ACK**
 - Przesyłane bajty:
 - Potwierdzone bajty: 918
 - Zmiana stanu: **FIN WAIT2** (widoczne w **tcp_log**)
 - 7. ◦ Włączone flagi: **ACK**
 - Przesyłane bajty:
 - Potwierdzone bajty:
 - Zmiana stanu: serwer: **CLOSE WAIT**
 - 8. ◦ Włączone flagi: **FIN, ACK**
 - Przesyłane bajty:
 - Potwierdzone bajty: 918
 - Zmiana stanu:
 - 9. ◦ Włączone flagi: **ACK**
 - Przesyłane bajty:
 - Potwierdzone bajty: 919
 - Zmiana stanu: klient: **TIME WAIT** (widoczne w **tcp_log**)
 - Klient dokonuje otwarcia aktywnego.
 - Klient dokonuje zamknięcia aktywnego (wysyłając **FIN**).
-