

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNOLOGIÍ



Návrh, správa a bezpečnost počítačových sítí
2020/2021

7. laboratorné cvičenie

1 Zadanie

Cieľom tejto laboratórnej úlohy je vyskúšať si ciele útoky na odoprenie služieb *DDoS* (Distributed Denial of Service). Vyskúšať si záťažové testovanie webového serveru, poprípade aplikácie. Zoznámiť sa s najznámejšími nástrojmi **ab** a **Jmeter**. Celé zadanie laboratórnej úlohy je možné nájsť v e-learningu na karte predmetu alebo na [Dropboxe](https://paper.dropbox.com/doc/7-CV-V0mrcgNfAN712pb6Syw0w)¹. Existujú základné 3 typy útokov:

- vyčerpanie zdrojov serveru (CPU, RAM, transakcie, atď...),
- vyčerpanie kapacity linky (záplavové Flood),
- logické útoky (slowLoris, cieľ na chybu protokolu).

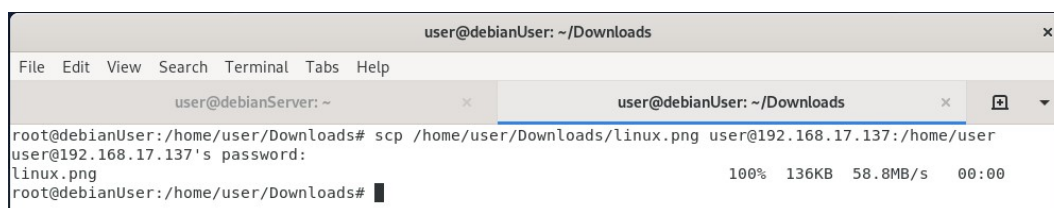
2 Nastavenie pracoviska

| Pracovisko | Kali | Debian klient | Debian server |
|------------|-------------------|-------------------|-------------------|
| IP | 192.168.17.139 | 192.168.17.135 | 192.168.17.137 |
| MAC | 00:0C:29:B7:9B:A1 | 00:0C:29:5C:68:C5 | 00:0C:29:6E:65:F1 |

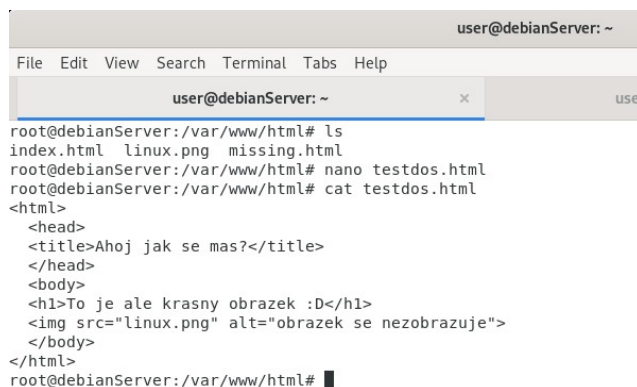
Tabuľka 1: Nastavenie pracoviska

3 Príprava pracoviska

V prvom rade je potrebné si daný obrázok prekopírovať z usera na server ako je možné vidieť na obrázku 1. Následne je potrebné si presunúť obrázok do správnej zložky a vytvoriť požadovanú HTML stránku vid' 2.



Obr. 1: Prekopírovanie obrázka na server



Obr. 2: Obsah adresára /var/www/html a zobrazenie obsahu súboru testdos.html

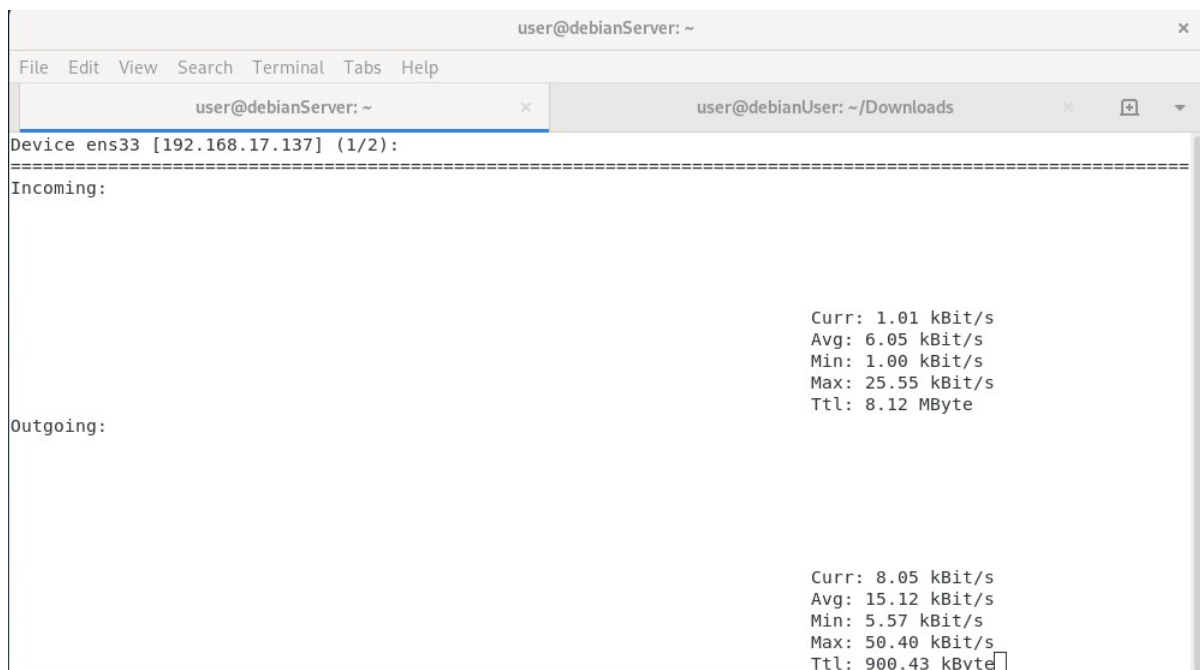
¹<https://paper.dropbox.com/doc/7-CV-V0mrcgNfAN712pb6Syw0w>

Následne cez odkaz <https://192.168.17.137/testdos.html> je možné si danú stránku zobrazíť 3.



Obr. 3: testdos.html

Na monitorovanie serveru je potrebné si nainštalovať program *nload* cez príkaz `apt-get install nload`.

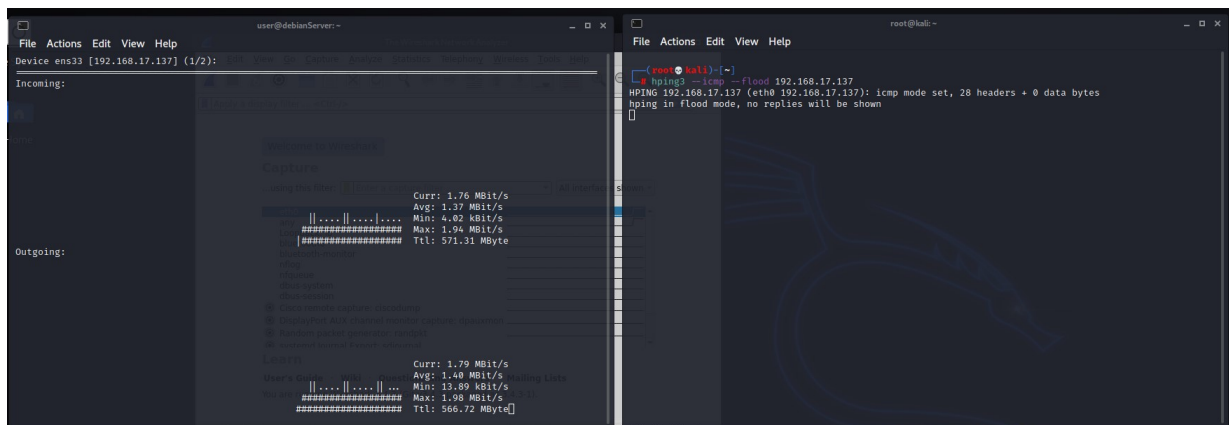


Obr. 4: Program **nload**

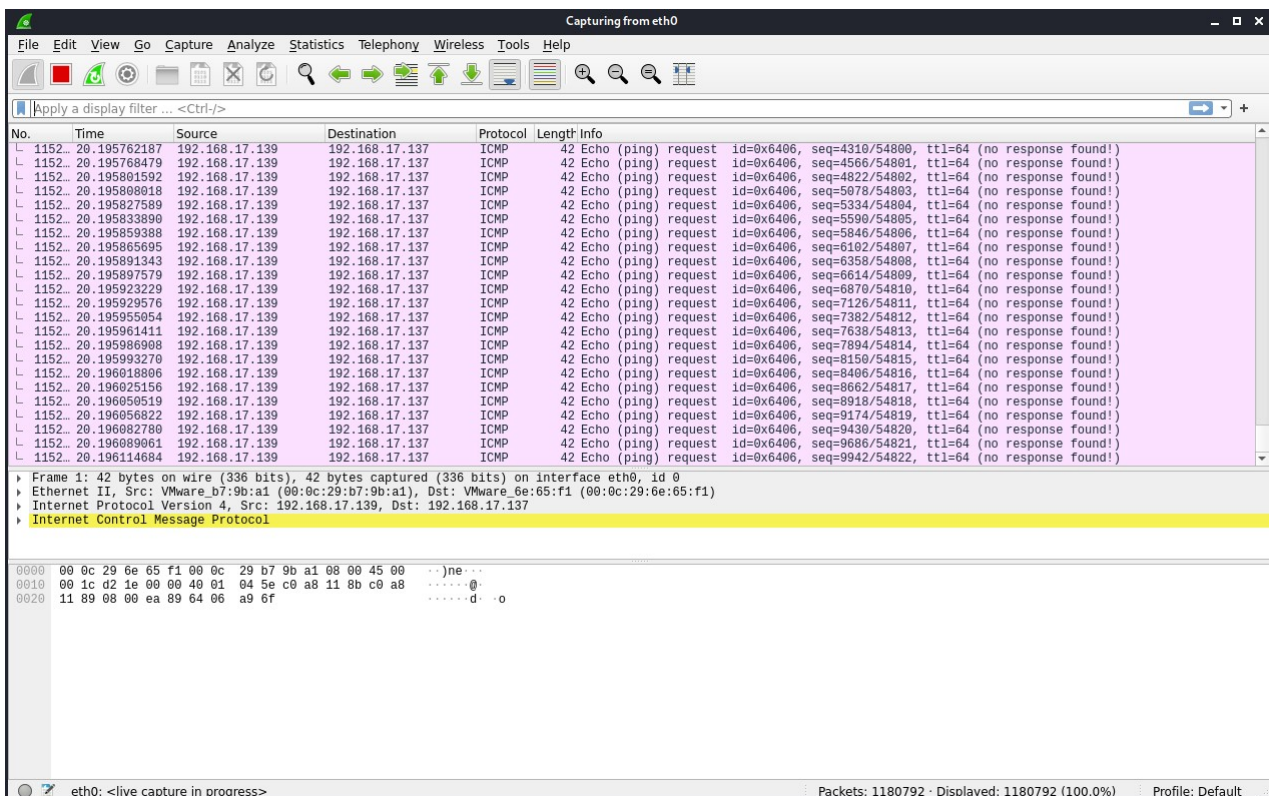
4 Záplavové útoky

Na generovanie záplavových útorok bude použitý program *hping3*. Najprv si vyskúšame záplavu ICMP paketov typu ping, server odpovie ICMP Reply

4.1 ICMP flood



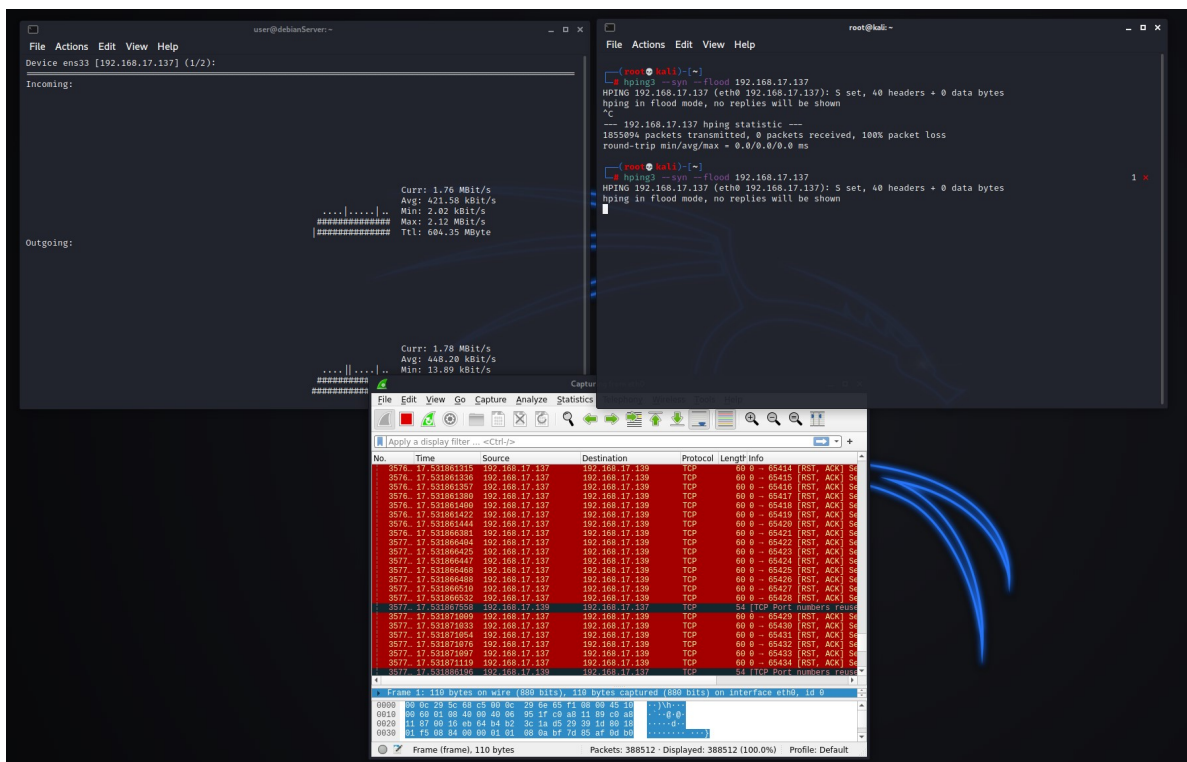
Obr. 5: Program hping3 --icmp --flood 192.168.17.137



Obr. 6: Záznam v programe Wireshark

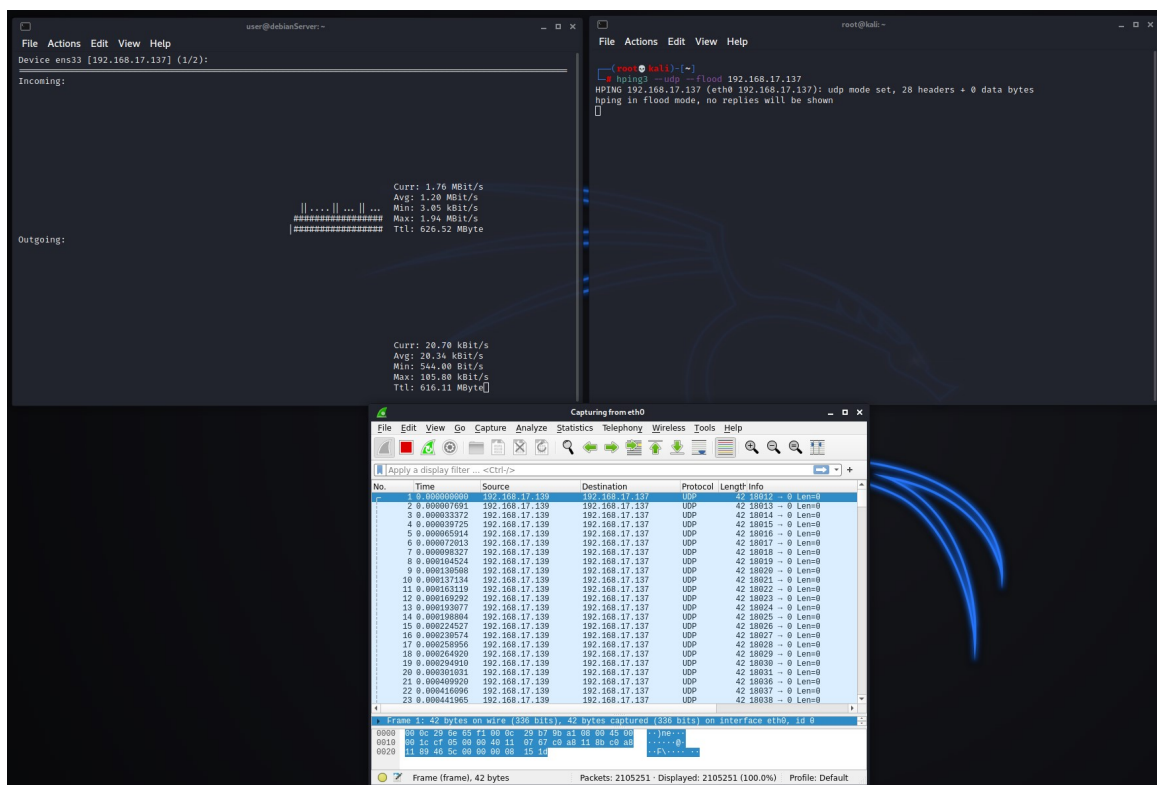
4.2 SYN flood

Ďalším typom útoku je *SYN Flood*. Princíp tohto útoku spočíva vo využití protokolu TCP. Útočník neustále posíla na server žiadosti o pripojenie cez SYN pakety čím dochádza k zahľteniu serveru. Útok cieľi na zraniteľnosť v handshake procese.



Obr. 7: SYN flood útok

4.3 UDP flood



Obr. 8: UDP flood útok

4.4 ApacheBench(ab)

Jedná sa v podstate o záplavový útok, ktorý cieľi na vyťaženosť výstupnej linky zo strany webového serveru. Útočník si vyberie na webovej stránke veľký obrázok a z botnetu spustí požiadavku GET na tento obrázok.

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)~  
# ab -n 10000 -c 5 http://192.168.17.137/linux.png  
This is ApacheBench, Version 2.3 <$Revision: 1879490 $>  
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/  
Licensed to The Apache Software Foundation, http://www.apache.org/  
  
Benchmarking 192.168.17.137 (be patient)  
Completed 1000 requests  
Completed 2000 requests  
Completed 3000 requests  
Completed 4000 requests  
Completed 5000 requests  
Completed 6000 requests  
Completed 7000 requests  
Completed 8000 requests  
Completed 9000 requests  
Completed 10000 requests  
Finished 10000 requests  
  
Server Software:      Apache  
Server Hostname:     192.168.17.137  
Server Port:         80  
  
Document Path:       /linux.png  
Document Length:     279 bytes  
  
Concurrency Level:    5  
Time taken for tests:  33.339 seconds  
Complete requests:    10000  
Failed requests:      0  
Non-2xx responses:    10000  
Total transferred:    4820000 bytes  
HTML transferred:    2790000 bytes  
Requests per second:  299.94 [#/sec] (mean)  
Time per request:     16.670 [ms] (mean)  
Time per request:     3.334 [ms] (mean, across all concurrent requests)  
Transfer rate:        141.18 [Kbytes/sec] received  
  
Connection Times (ms)  
      min   mean[+/-sd] median   max  
Connect:    0     3  16.0      0    100  
Processing:  0    13  30.4      1    102  
Waiting:    0    11  27.5      1    101  
Total:      0    17  33.4      1    194  
  
Percentage of the requests served within a certain time (ms)  
 50%    1  
 66%    3  
 75%    4  
 80%    5  
 90%   92  
 95%   96  
 98%   97  
 99%   98  
100%  194 (longest request)
```

Obr. 9: ApacheBench útok

Ďalší útok o ktorý sa jedná je tzv. *Man in the Middle attack* pomocou otravy ARP tabuľky.

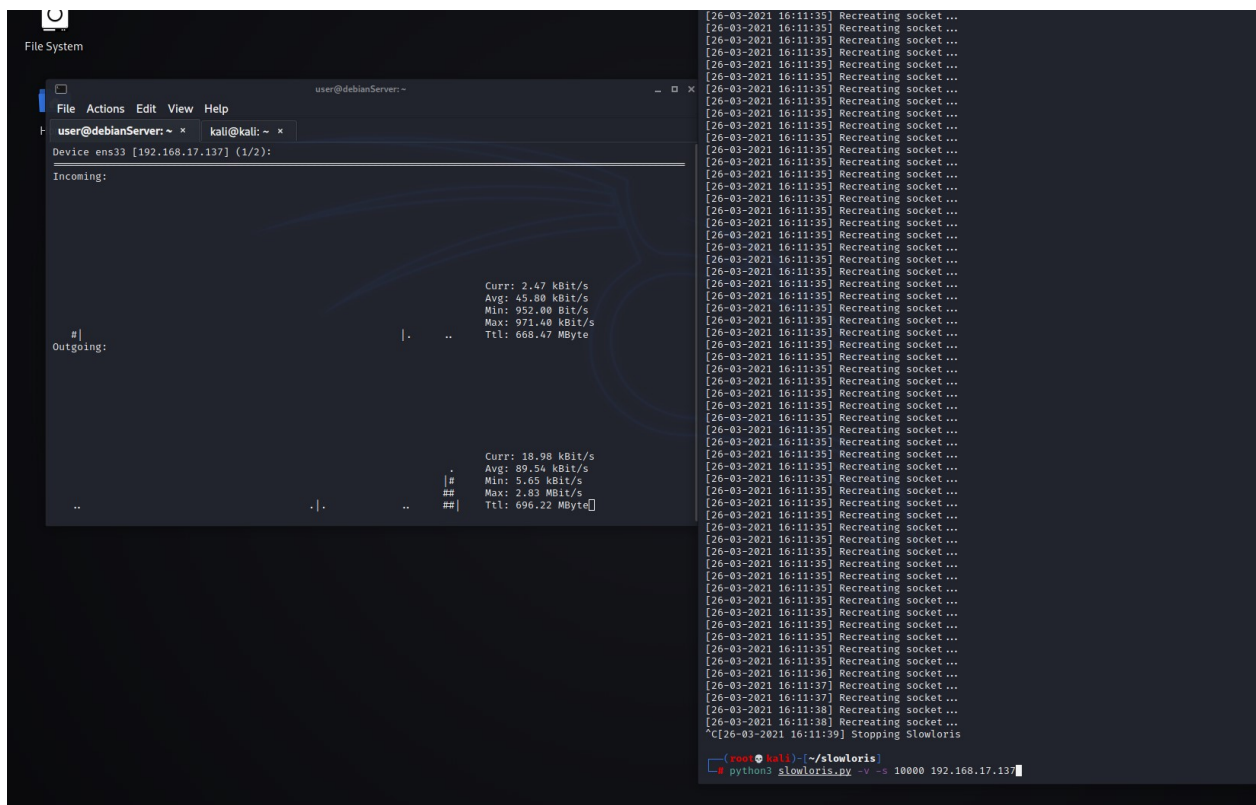
Obr. 10: Otrava ARP tabuľky

The image shows a Kali Linux desktop environment. On the left, there is a sidebar with icons for 'Trash' and 'File System'. The main window is a file manager titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help) and a toolbar. It displays a directory listing of files and folders. Below the listing, there is a summary of statistics: Curr: 15.07 kBit/s, Avg: 14.45 kBit/s, Min: 2.00 kBit/s, Max: 26.77 kBit/s, and Ttl: 664.15 Mbyte. The status bar at the bottom indicates 'Outgoing: d disconnect: Broken pipe'. On the right side of the desktop, there is a terminal window titled '(kali@kali)-[~]' showing a netstat command output. The output lists various network connections, including established connections to 192.168.17.137 and 192.168.17.135, and listening connections on eth0 and 192.168.17.137. The terminal window has a menu bar (File, Actions, Edit, View, Help) and a toolbar. The status bar at the bottom of the terminal shows '255 x'.

Obr. 11: Prerušenie spojenia

5 Logické úlohy

Ďalším útokom bude pomalý útok *SlowLoris*. Tento typ útoku je založený na DDoS útoku. Slowloris sa snaží otvoriť čo najviac http spojení medzi serverom a útočníkom a udržať ich otvorené. Tým zabraňuje serveru obslúžiť ďalšie požiadavky klientov. Tento útok nevyťažuje server cez šírku pásma. Prenosová rýchlosť je cca 14-16 kBit/s

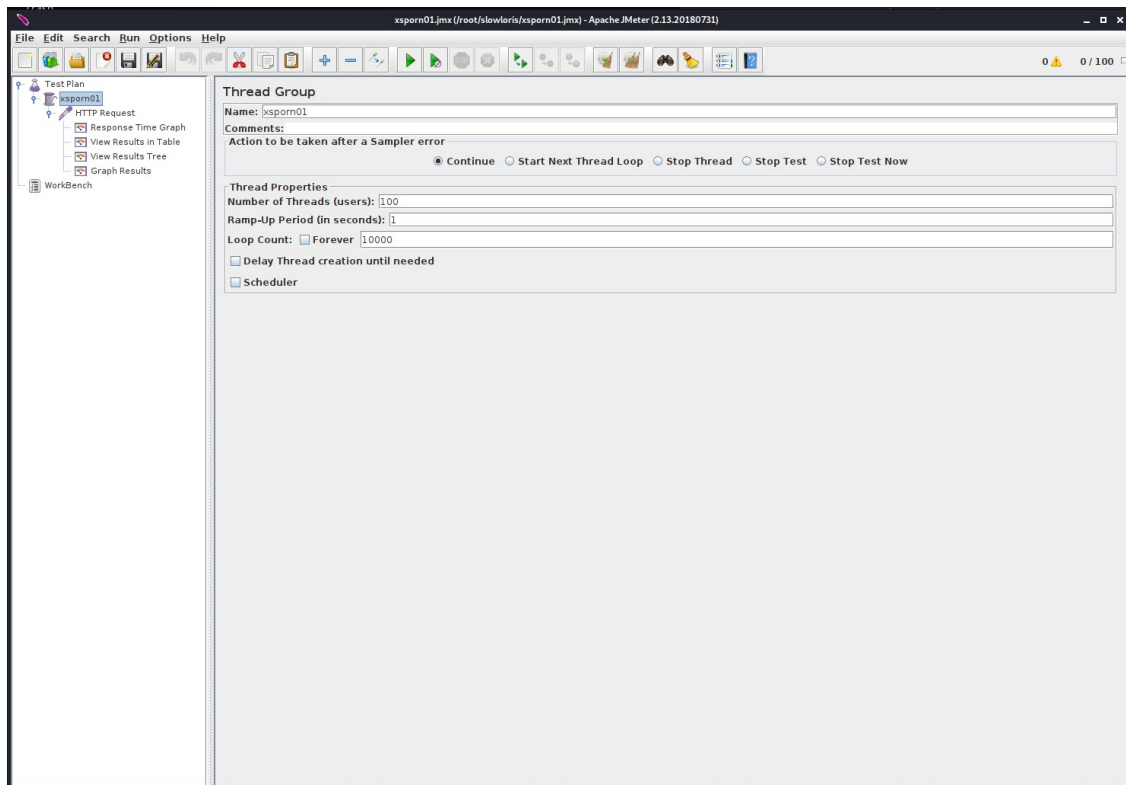


Obr. 12: SlowLoris útok

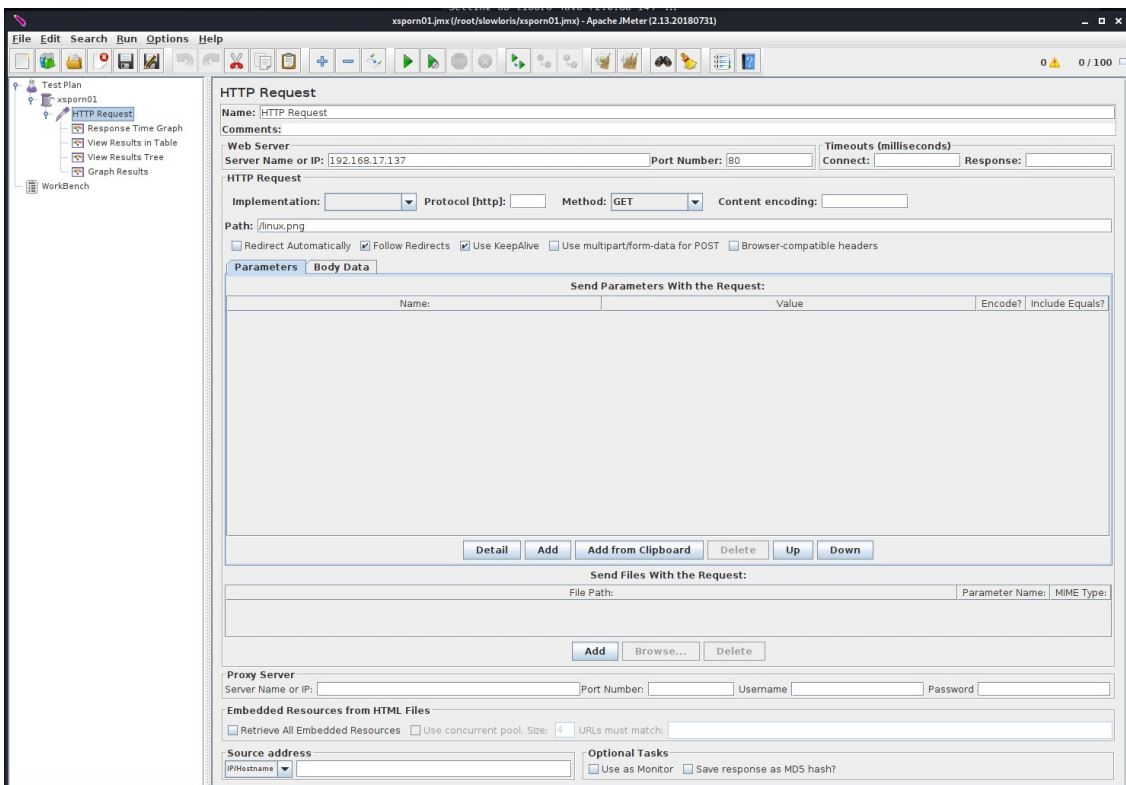
6 Samostatná úloha

6.1 Záťažové testovanie Apache Jmeter

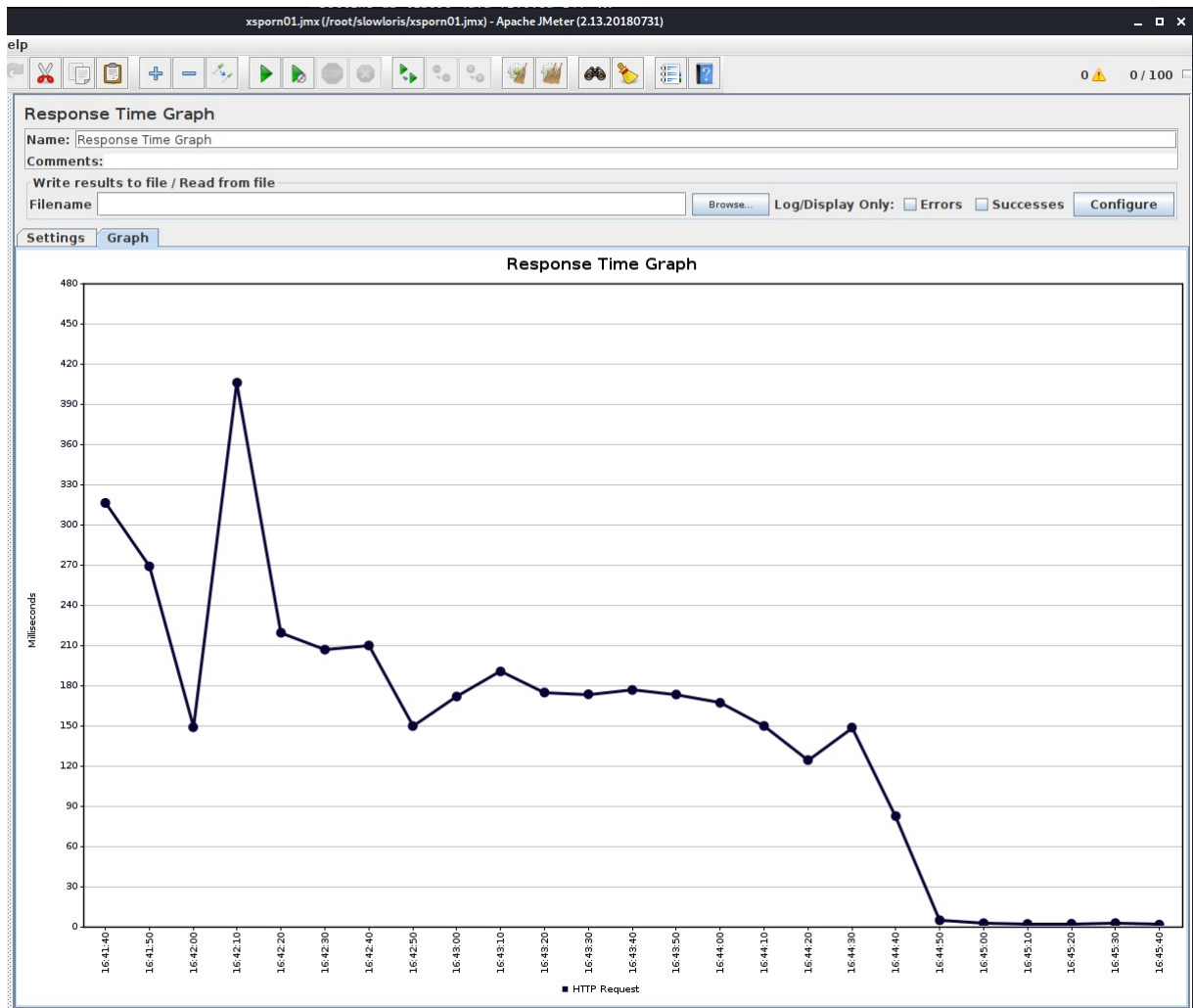
Vytvoríme nový **Thread Group**, ktorý nastavíme nasledovne vid'. 13. HTTP request 14 a Response Time Graph 15.



Obr. 13: Thread Group



Obr. 14: HTTP request



Obr. 15: Response time graph