VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Návrh, správa a bezpečnost počítačových sítí 2020/2021

7. laboratórne cvičenie

26. marca 2021

Alex Sporni (xsporn01)

1 Zadanie

Cieľom tejto laboratórnej úlohy je vyskúšať si cielené 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[1]. Existujú základné 3 typy útokov:

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

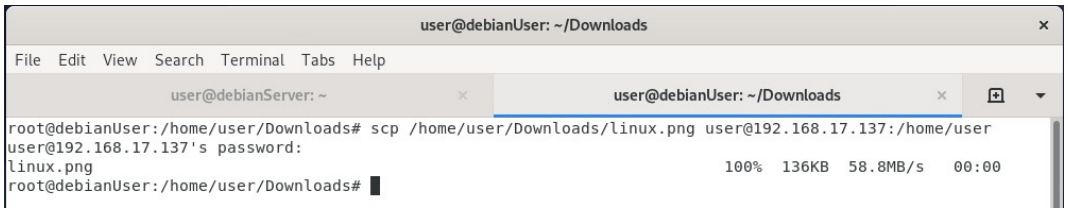
2 Nastavenie pracoviska

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

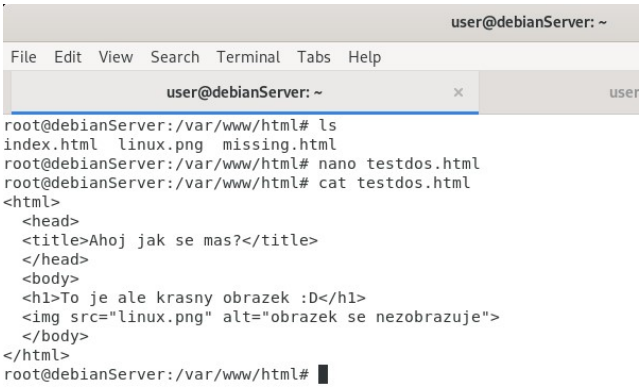
Tabuľka 1: Nastavenie pracoviska

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 viď. 2.



Obr. 1: Prekopírovanie obrázka na server



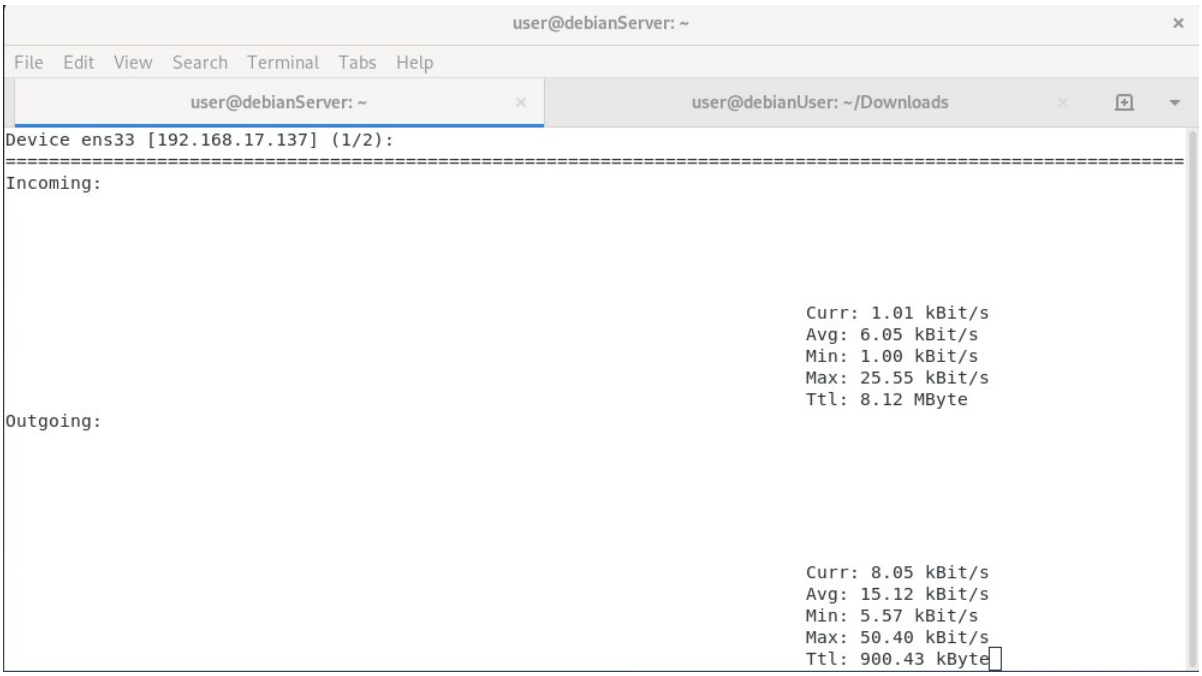
Obr. 2: Obsah adresára `/var/www/html` a zobrazenie obsahu súboru `testdos.html`

[1] `https://paper.dropbox.com/doc/7-CV-VOmrcgNfAN712pb6Syw0w`

Následne cez odkaz `https://192.168.17.137/testdos.html` je možné si danú stránku zobraziť 3.

Obr. 3: `testdos.html`

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

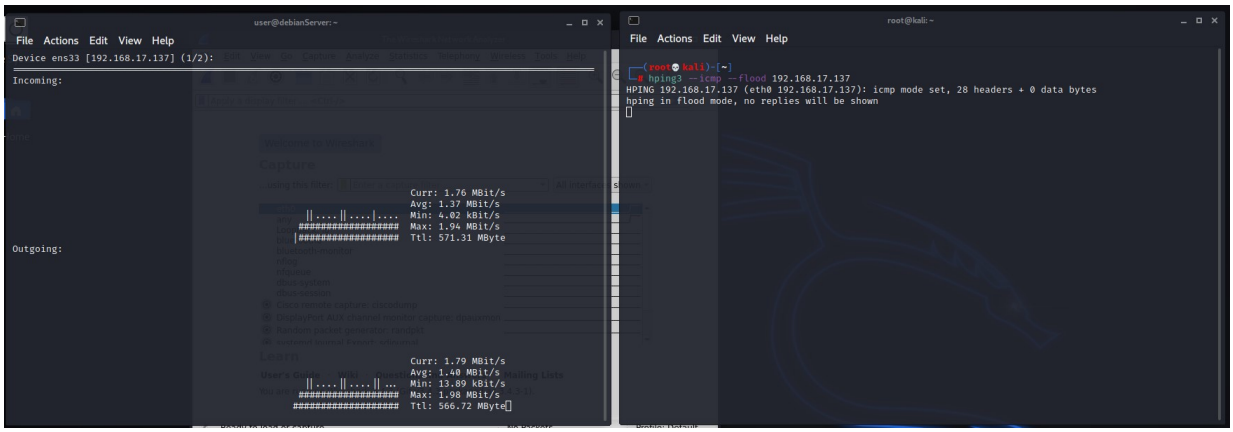


Obr. 4: Program **nload**

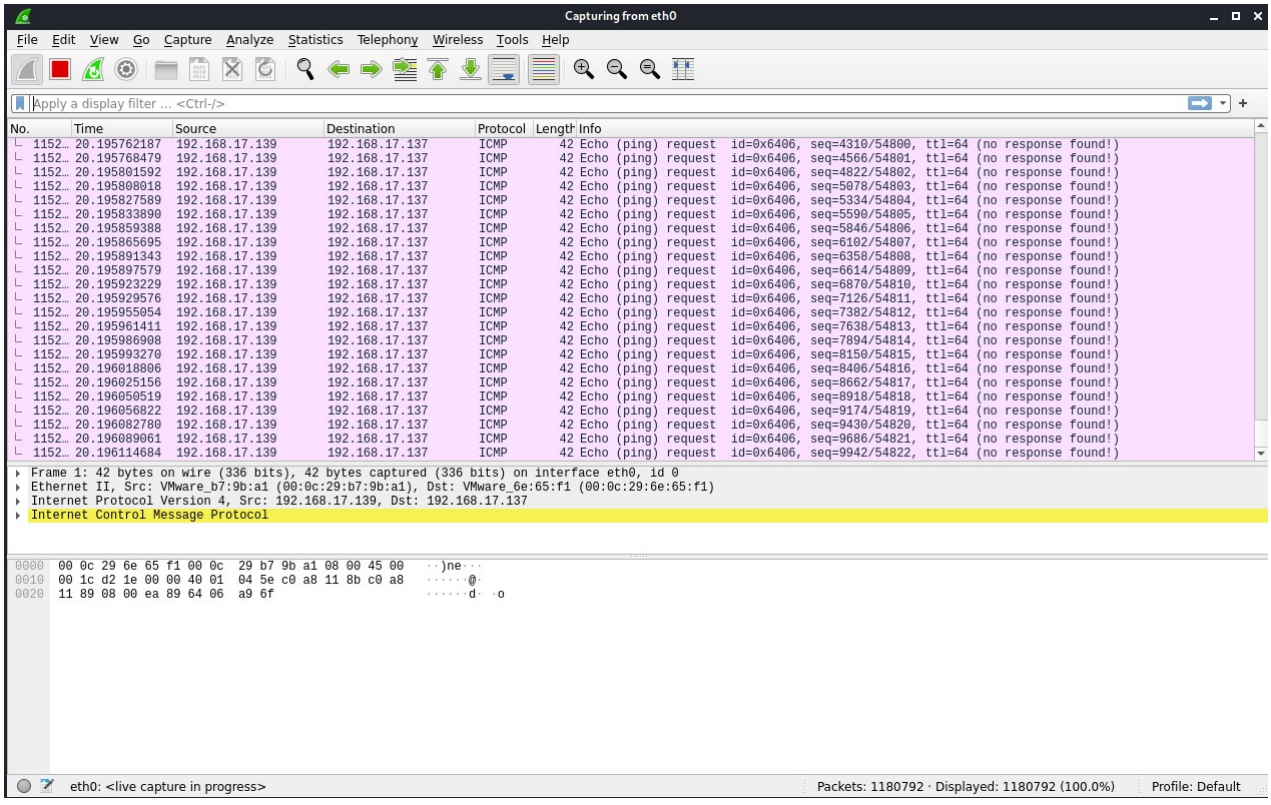
4 Záplavové útoky

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

4.1 ICMP flood



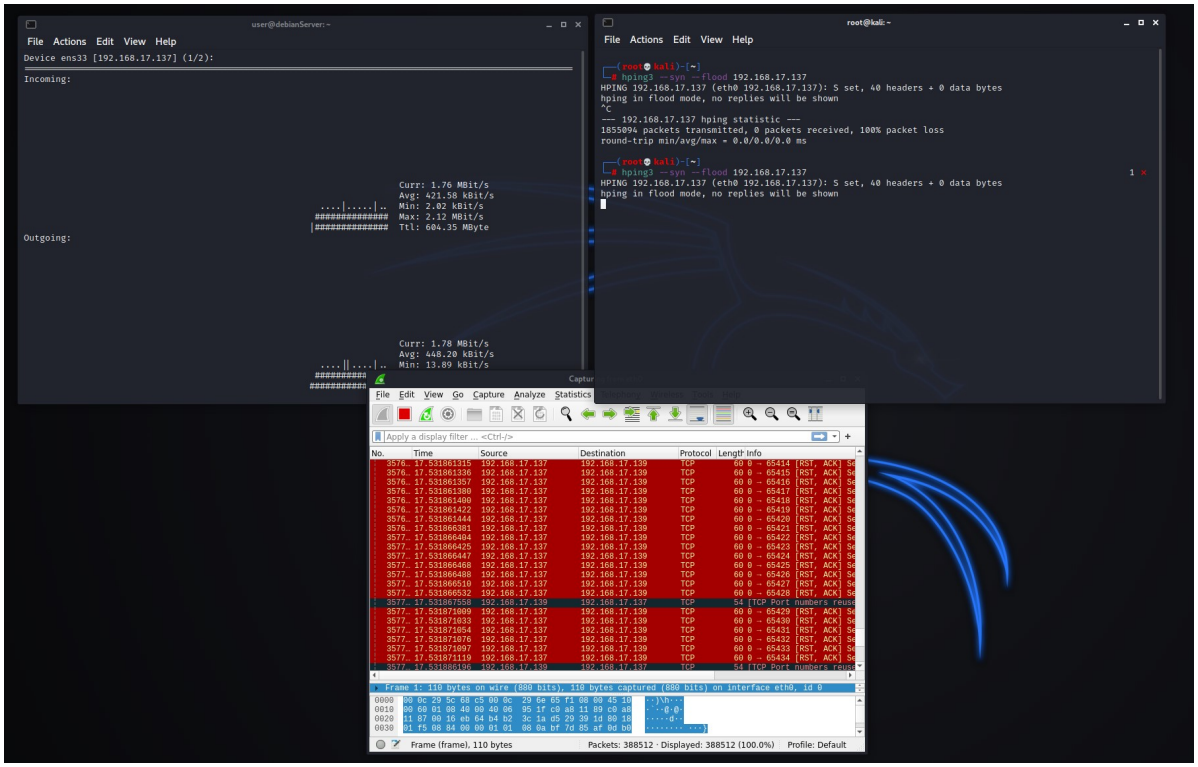
Obr. 5: Program `hping3 --icmp --flood 192.168.17.137`



Obr. 6: Záznam v programe Wireshark

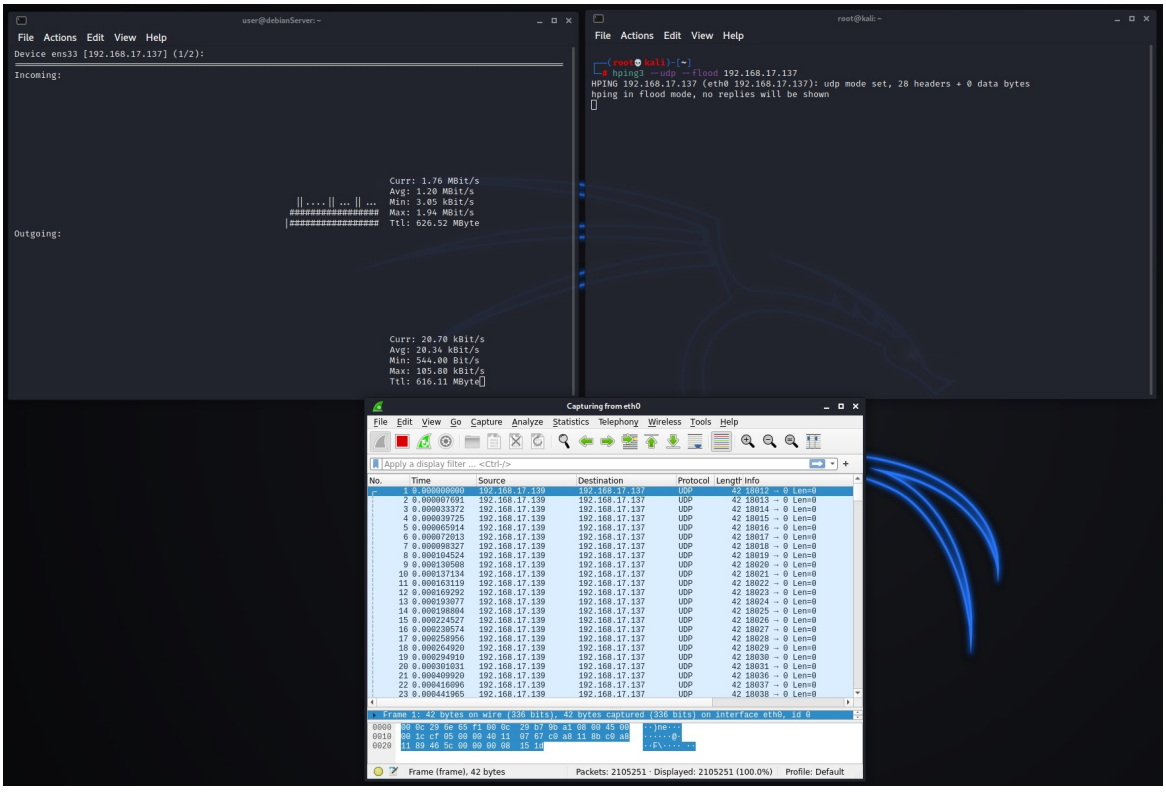
4.2 SYN flood

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



Obr. 7: SYN flood útok

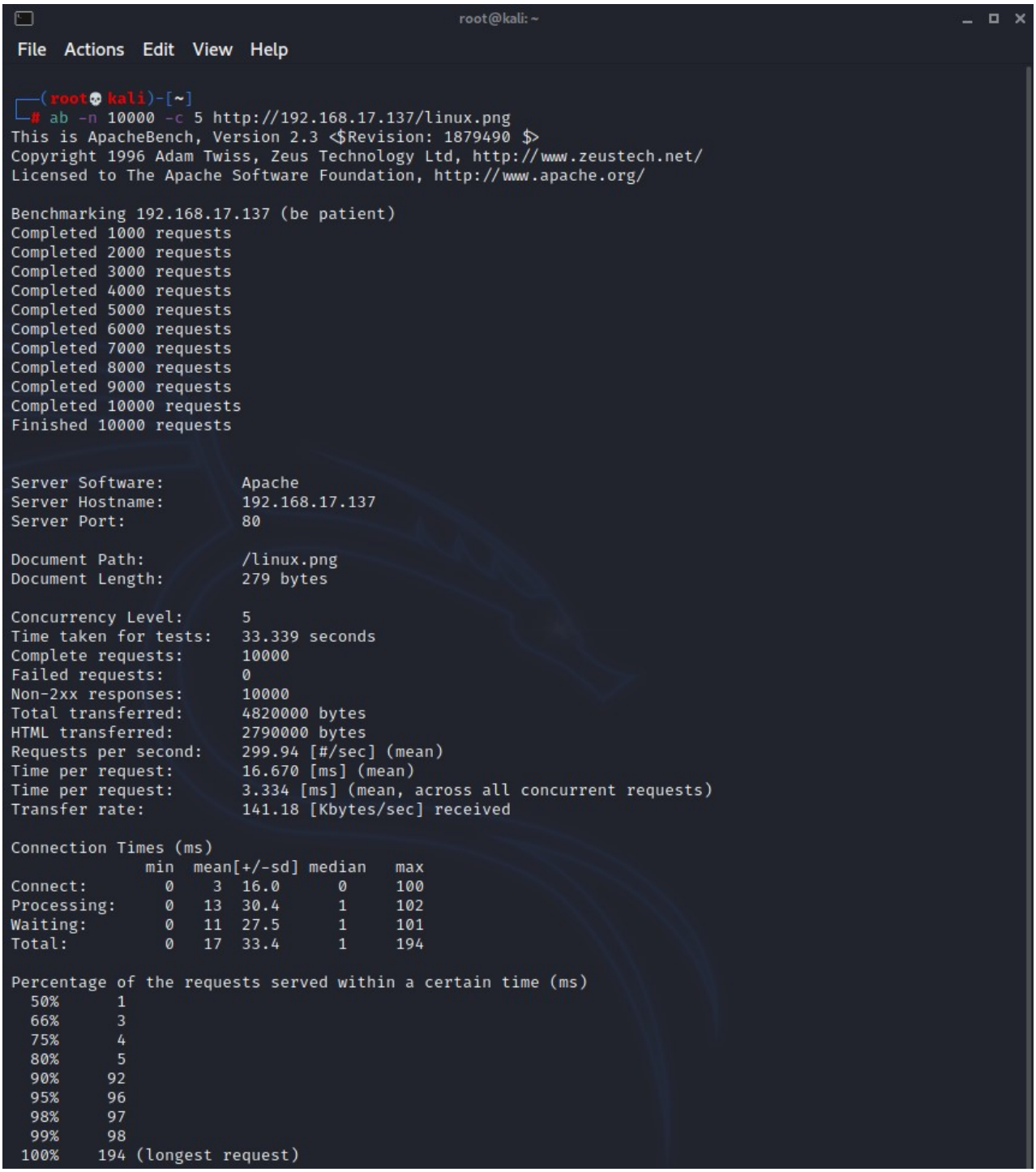
4.3 UDP flood



Obr. 8: UDP flood útok

4.4 ApacheBench(ab)

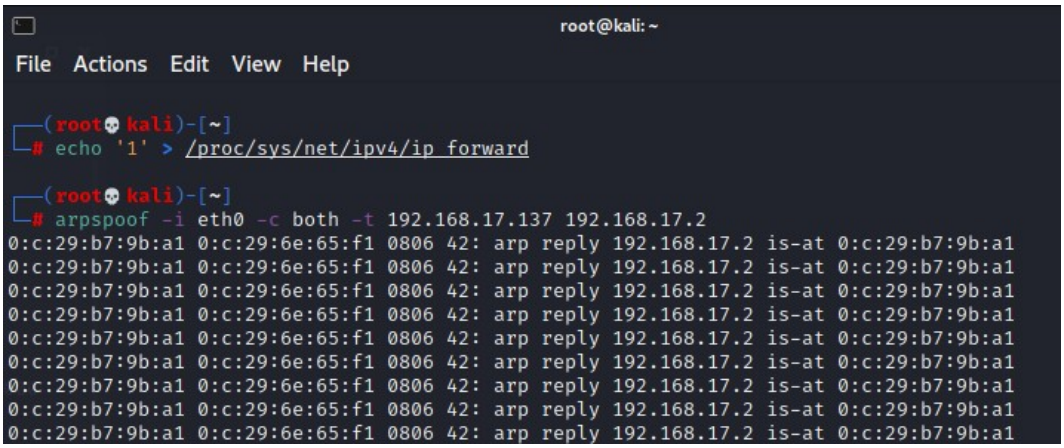
Jedná sa v podstate o záplavový útok, ktorý cieli na vyťaženosť výstupnej linky zo strany webového serveru. Útočník si vyberie na webovej stránke veľký obrázok a z botnetu spustí požiadavku GET na tento obrázok.



Obr. 9: ApacheBench útok

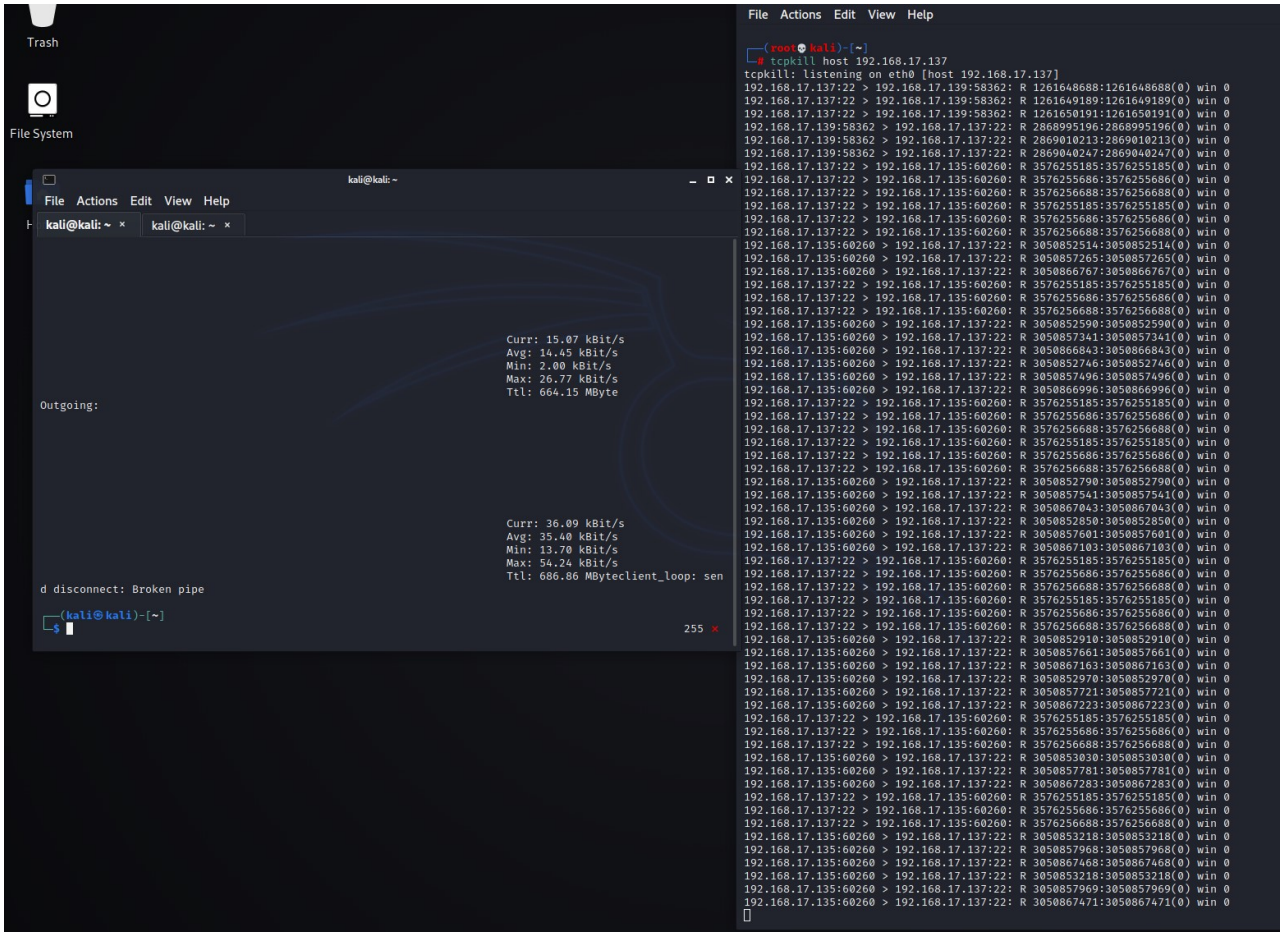
4.5 Man in the Middle útok

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



Obr. 10: Otrava ARP tabuľky

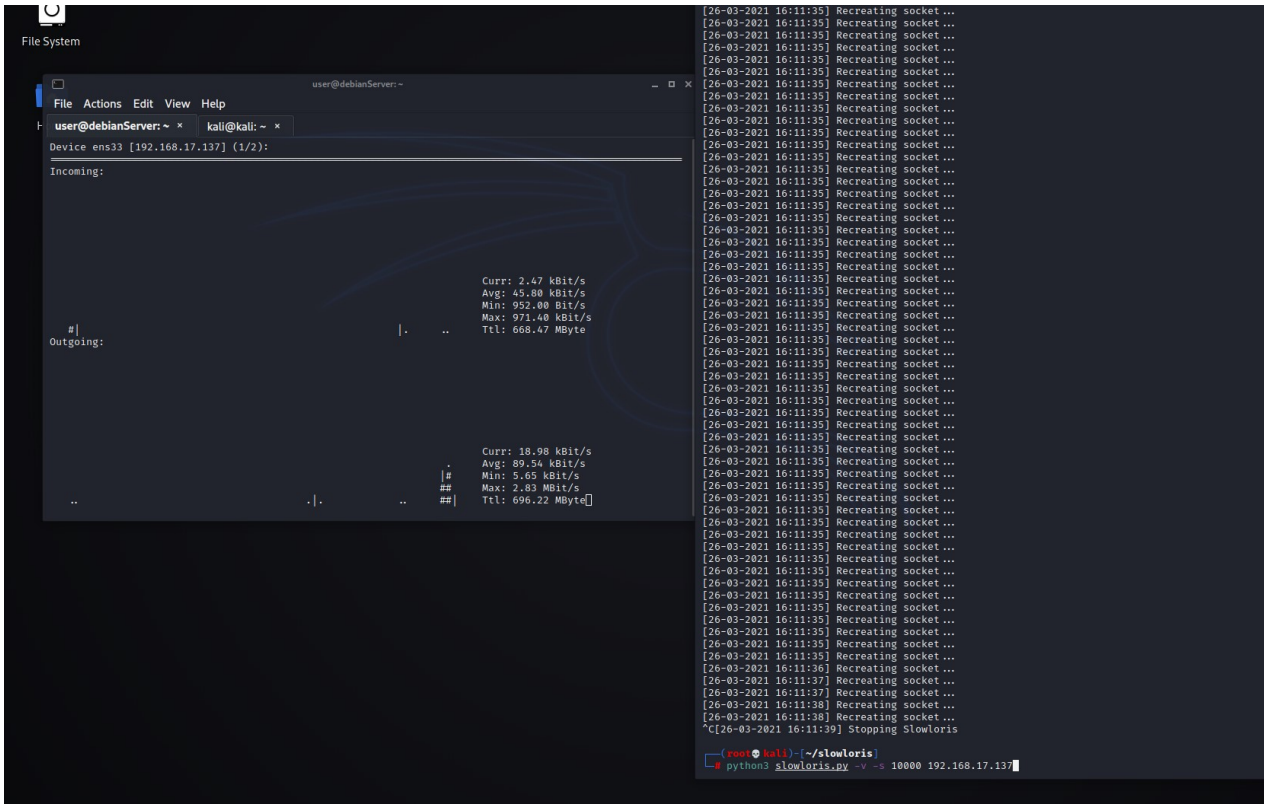
Následne je možné spojenie medzi Kali linuxom a DebianServerom prerušiť pomocou príkazu `tcpkill host 192.168.17.137` viď. 11.



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

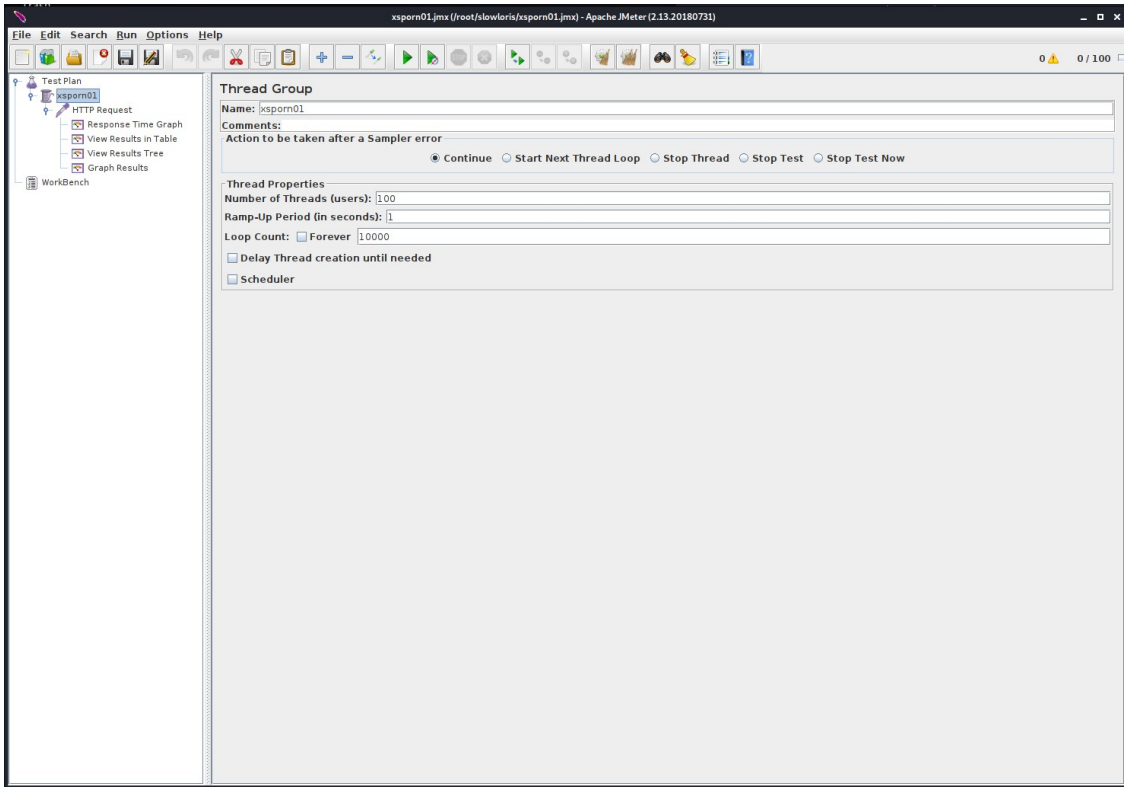


Obr. 12: SlowLoris útok

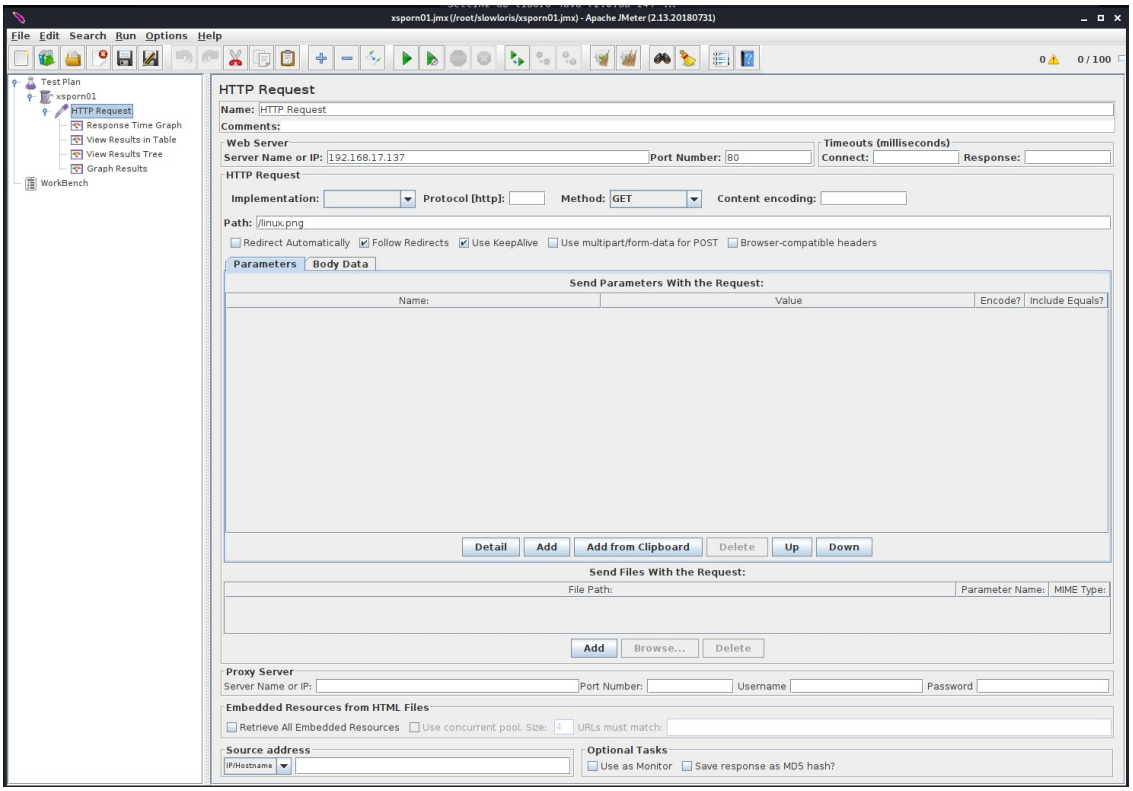
6 Samostatná úloha

6.1 Záťažové testovanie Apache Jmeter

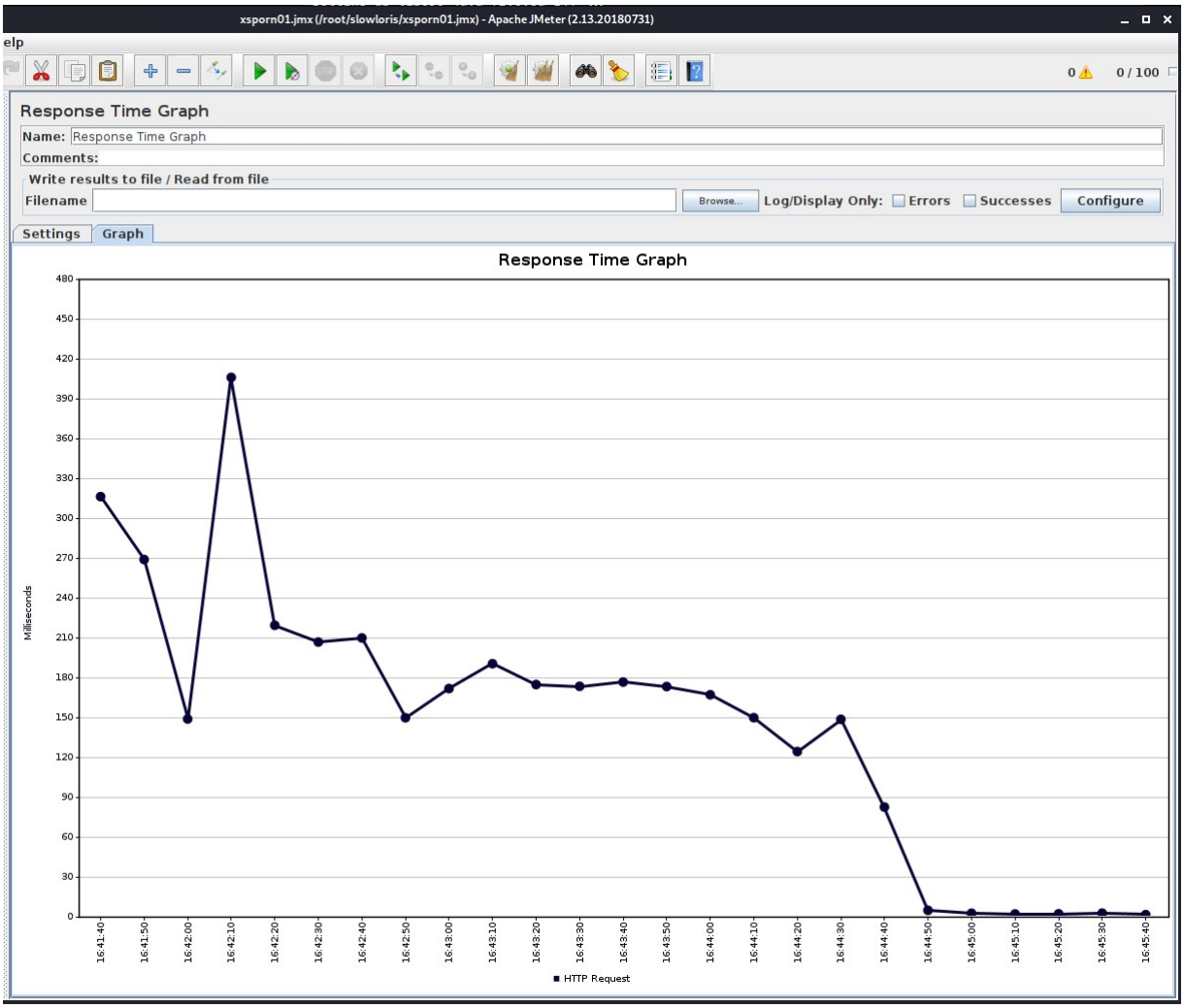
Vytvoríme nový **Thread Group**, ktorý nastavíme nasledovne viď. 13. HTTP request 14 a Response Time Graph 15.



Obr. 13: Thread Group



Obr. 14: HTTP request



Obr. 15: Response time graph