BAB III

METODE PENELITIAN

3.1 Desain Penelitian

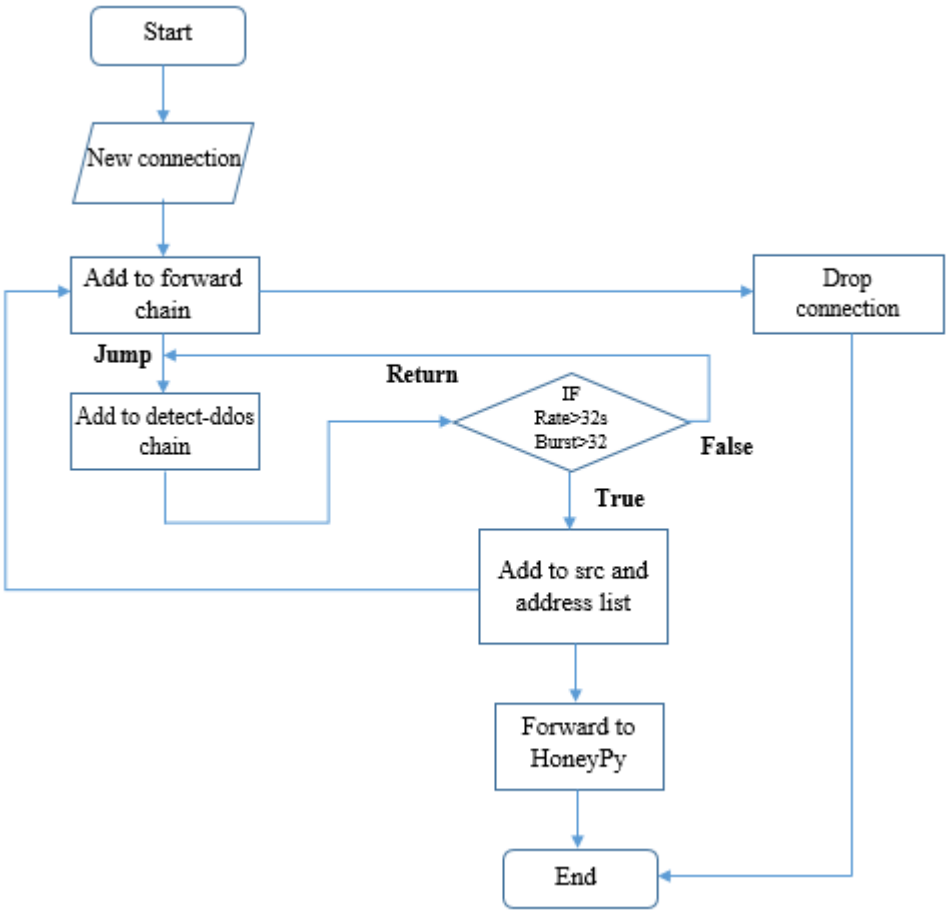
Penelitian ini bertujuan untuk meminimalisir serangan *Slowloris* terhadap *webserver* dengan menggunakan mekanisme pertahanan yang merupakan kombinasi dari *firewall* dan *honeypot*. Penelitian ini dilaksanakan dengan menggunakan metode *quasi experimental* dimulai dari mendesain topologi jaringan berdasarkan desain referensi. Desain jaringan dibuat dalam tiga kondisi, yaitu ketika trafik normal, ketika *webserver* diserang tanpa mekanisme pertahanan dan dengan mekanisme pertahanan. Kemudian, dilakukan eksperimen dalam tiga kondisi tersebut. Apabila serangan *Slowloris* berhasil diminimalisir, maka dilakukan analisa dari hasil eksperimen. Hasil eksperimen berupa paket-paket data yang terekam menggunakan *software* Winbox Mikrotik SIA, tcpdump, tshark dan Wireshark.

3.2 Mekanisme Pertahanan untuk Meminimalisir Serangan *Slowloris*

Mekanisme pertahanan untuk meminimalisir serangan *Slowloris* adalah dengan kombinasi *firewall* dan *low interaction honeypot*. *Firewall* yang digunakan merupakan *Stateless Firewall* diatur dengan *software* Winbox dalam *router* MikroTik dan *honeypot* sebagai *server* palsu. *Firewall* yang digunakan berfungsi untuk memantau dan memblokir paket data bersadarkan alamat sumber (*source*) dan tujuan (*destination*) dan pengaturan statis lainnya (Mojidra, 2016). *Firewall* ini menggunakan beberapa *rule*. Sedangkan *Honeypot* yang digunakan adalah *HoneyPy* yang merupakan *low interaction honeypot*. *Honeypot* menjalankan *full service*, untuk *port* 80 dibuka pada *port* 10080. Gambar 3.1 menunjukkan algoritma *flowchart* mekanisme pertahanan.

Setiap koneksi yang melewati *router* akan dideteksi yang kemudian trafik paket data diproses di *firewall chain*. Trafik paket data masuk dan dikelola terlebih dahulu di *forward chain*, kemudian *chain* berganti ke *detect-ddos chain*. *Limit connection*

rate = 32/s dan *burst* = 32 untuk trafik paket data yang terdeteksi *connection rate* 32 paket setiap detik dengan mencocokkan setiap 32 paket dengan *firewall rule* DDoS *Attack Detection and Blocking* dalam interval satu detik. *Burst* adalah jumlah paket untuk setiap *flow* (MikroTik, 2019a). Apabila terdeteksi melebihi jumlah itu, maka IP *Address* pengirim akan dimasukkan ke *address list* sebagai "ddoser" dalam *Source Address* (Src. *Address*) begitu pula dengan IP *Address* yang menjadi tujuan serangan dimasukkan ke *address list* sebagai "ddosed" dalam *Destination Address* (Dst. *Address*). *Address list* ýang terdeteksi memiliki *timeout* sebesar sepuluh menit (MikroTik, 2011). Kemudian, sebagian trafik paket data dari pengirim diproses untuk diblokir (*drop*) tanpa sepengathuan si pengirim dan sebagian lagi di *forward* ke *honeypot*.



Gambar 3. 1 Algoritma *flowchart* mekanisme pertahanan

3.3 Peralatan Penunjang

Peralatan penunjang yang diperlukan untuk melakukan eksperimen diantaranya sebagai berikut:

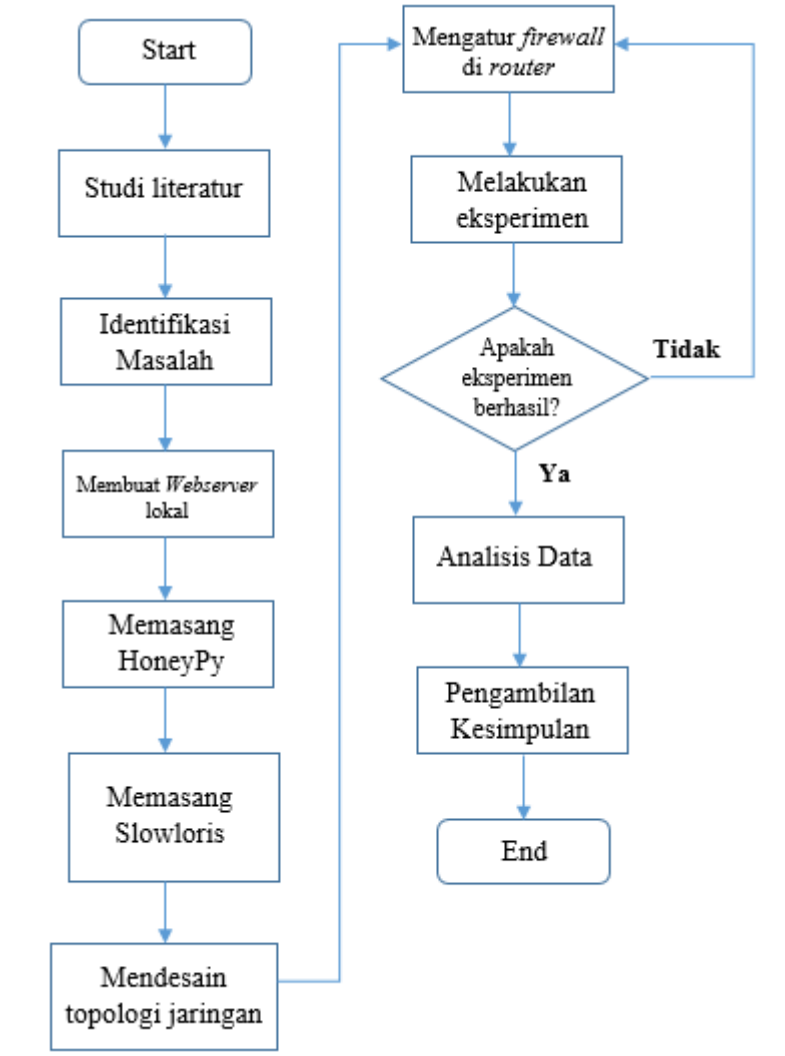
1. *Personal Computer*
2. *Raspberry Pi 2 Model B* dengan *operating system* Raspbian Stretch
3. *Raspberry Pi 3 Model B+* dengan *operating system* Raspbian Stretch
4. Monitor HDMI
5. *Keyboard*
6. *Mouse*
7. RouterBOARD 951 2n MikroTik
8. Kabel RJ45
9. *Switch*
10. Kabel HDMI

Perangkat lunak yang diperlukan untuk melakukan eksperimen diantaranya sebagai berikut:

1. Winbox Mikrotik SIA
2. *Apache* 2.2 (*Webserver*)
3. *Wireshark*
4. *Tshark*
5. 7zip
6. SD *Card Formatter* 5
7. HoneyPy
8. *Slowloris*
9. tcpdump
10. WinDisk32*Imager*
11. *Raspbian Stretch*
12. NOOBS v3.01
13. Ubuntu 18.04

3.4 Diagram Alur Penelitian

Penelitian yang ditempuh dalam Tugas Akhir ini dimulai dengan mengkaji literatur yang mengenai serangan *Slowloris* dan metode mengurangi serangan *Slowloris.* Literatur-literatur tersebut berupa jurnal ilmiah, buku, dan artikel. Literatur-literatur tersebut yang didapat dari situs-situs seperti *IEEE, Science Direct, Google scholar* dan situs khusus mengenai *cybersecurity*. Langkah kedua, mempelajari algoritma dan mengidentifikasi metode penyerangan yang diakukan oleh program *Slowloris*. Langkah ketiga, membuat *webserver* pada *RaspberryPi 2 Model B* dengan *Apache*. Kemudian langkah keempat, memasang aplikasi *HoneyPy* sebagai *honeypot* pada *RaspberryPi 3 Model B+*. Langkah kelima, memasang program *Slowloris* pada sebuah komputer berbasis *Ubuntu*. Langkah keenam, mendesain topologi jaringan untuk melakukan simulasi dalam tiga kondisi yang berbeda, yaitu kondisi ketika trafik normal, ketika *webserver* diserang, dan ketika telah dipasang *honeypot* dalam jaringan. Langkah terakhir, melakukan simulasi dan menganalisa hasil simulasi tersebut untuk diambil kesimpulan.



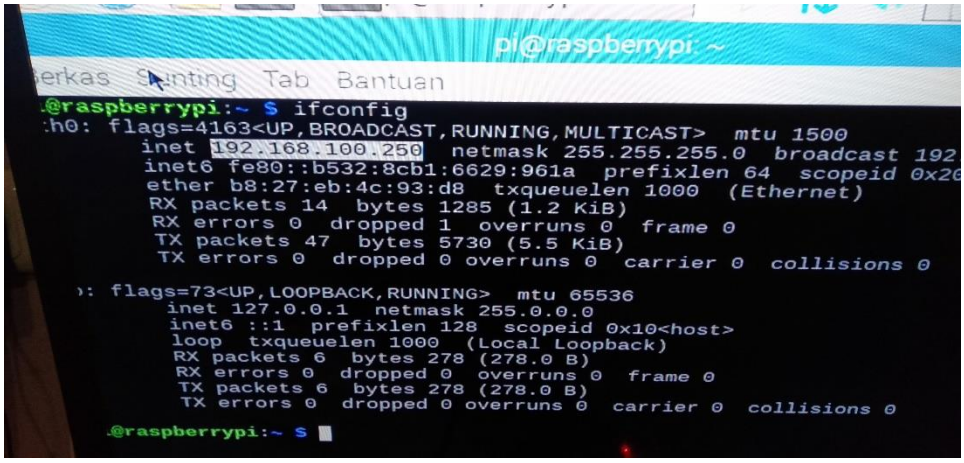
Gambar 3. 2 Diagram Alur Penelitian

3.5 Prosedur Penelitian

3.5.1 *Web Server* Lokal Apache

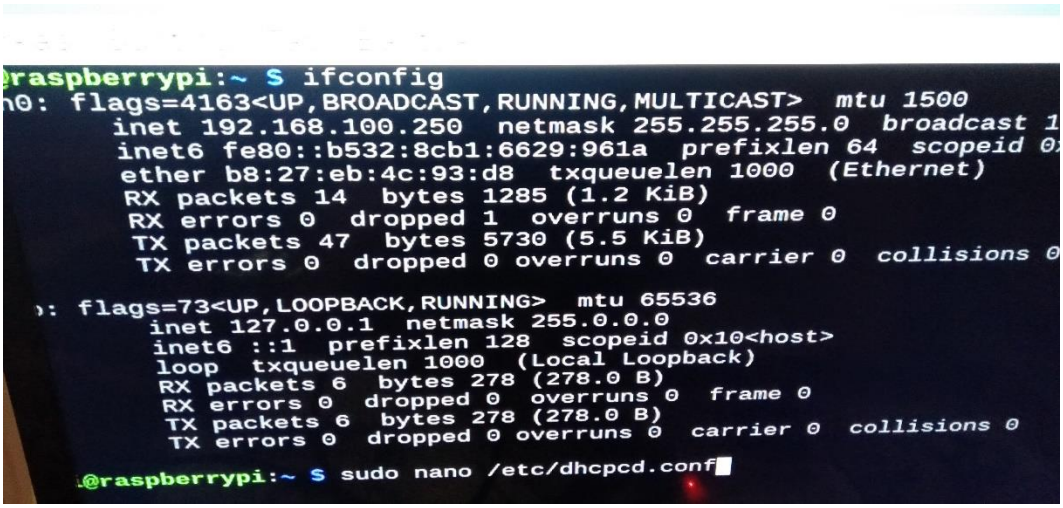
Web server yang dipakai adalah Apache dengan menggunakan *Raspberry Pi 2 Model B* dengan *operating system* Raspbian Stretch. Langkah-langkah pembuatan *web server* menggunakan *Raspberry Pi 2 Model B* diantaranya adalah sebagai berikut:

1. Masukkan perintah ifconfig melalui Terminal seperti pada Gambar 3.3. Perintah itu tersebut dimaksudkan untuk mengetahui IP *Address Raspberry Pi* 2 yang nantinya akan diakses melalui *browser* dan sebagai alamat IP yang akan menjadi target penyerangan.



Gambar 3. 3 IP Address *web server*

2. Masukkan perintah sudo nano /etc/networks/dhcpcd.conf untuk mengatur IP *Address* menjadi *static* seperti pada Gambar 3.4.



Gambar 3. 4 Perintah pengaturan IP *Address Static*

3. Masukkan data berikut ke dalam konfigurasi seperti pada Gambar 3.5.

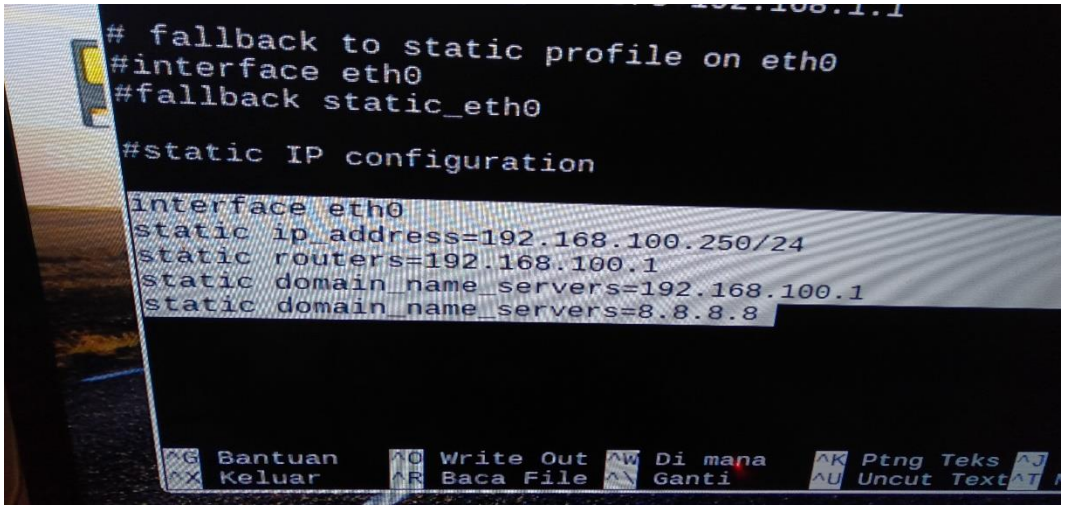
   interface eth0

   static ip_address=192.168.100.250/24

   static routers=192.168.100.1

   static domain_name_servers=192.168.100.1

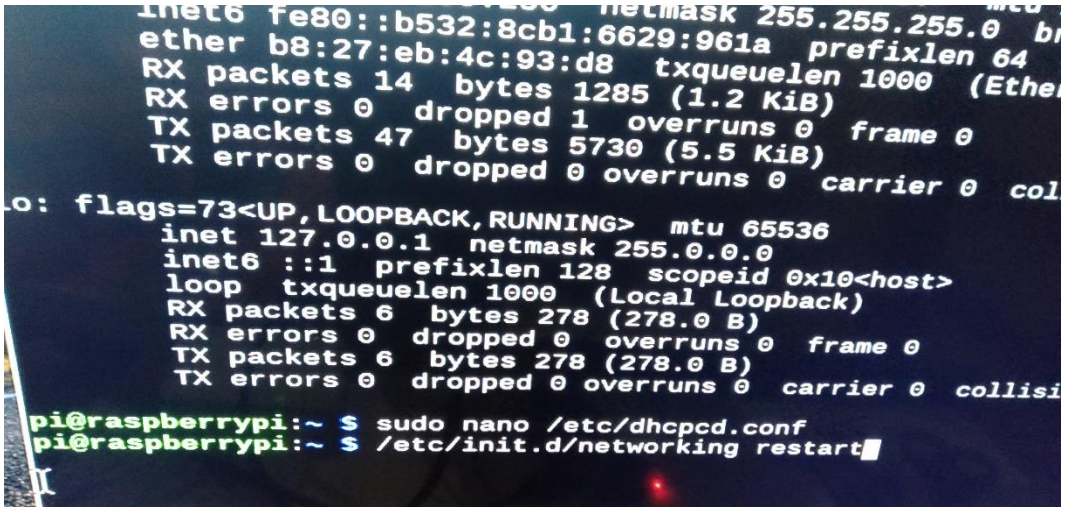
   static domain_name_servers=8.8.8.8



Gambar 3. 5 IP *configuration*

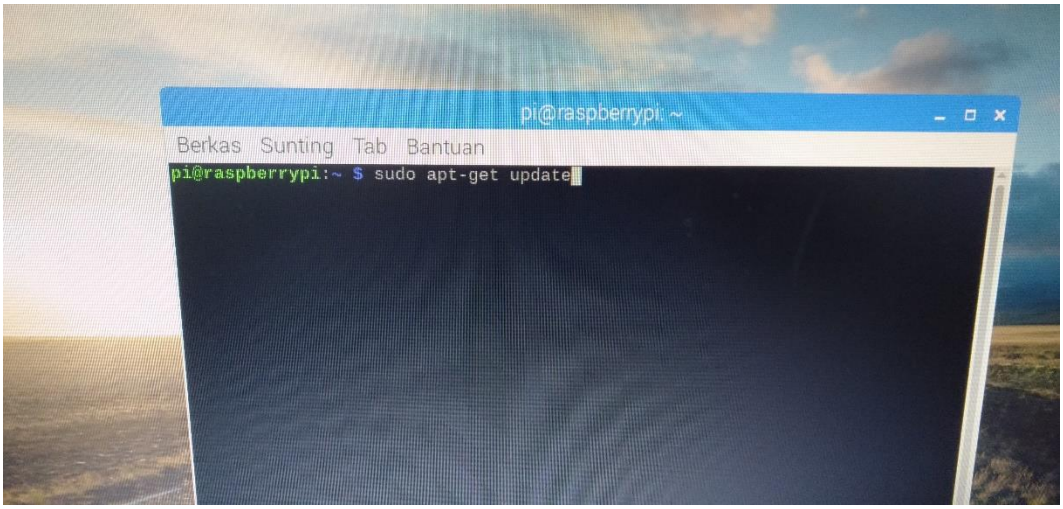
Kemudian, tekan Ctrl+O untuk menyimpan konfigurasi dan Ctrl+X keluar dari nano.

4. Masukkan perintah /etc/init.d/networking restart seperti pada Gambar 3.6 untuk melakukan *restart networking* di *Raspberry Pi*



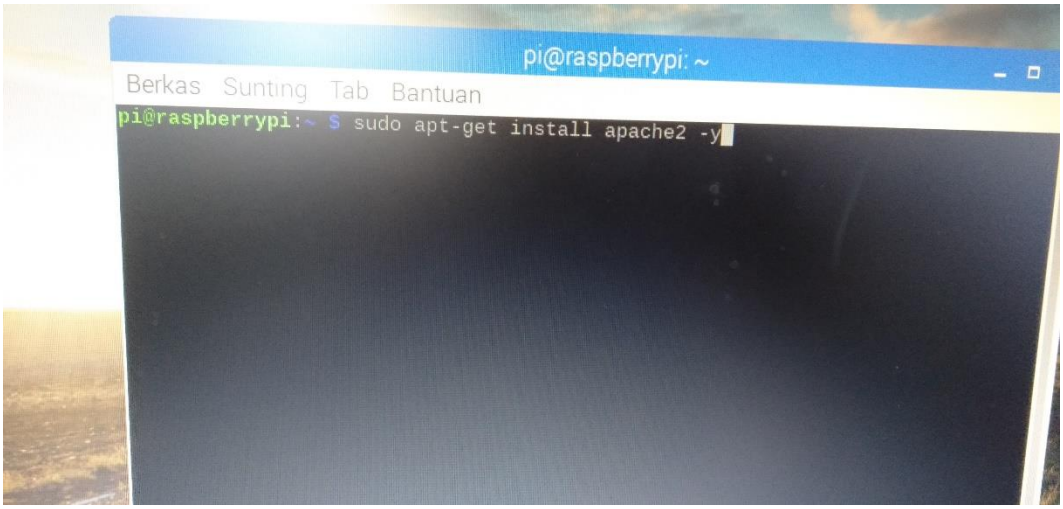
Gambar 3. 6 *Restart Networking*

5. Masukkan perintah sudo apt-get update kemudian tekan Enter untuk memperbaharui *Raspberry Pi* seperti pada Gambar 3.7.



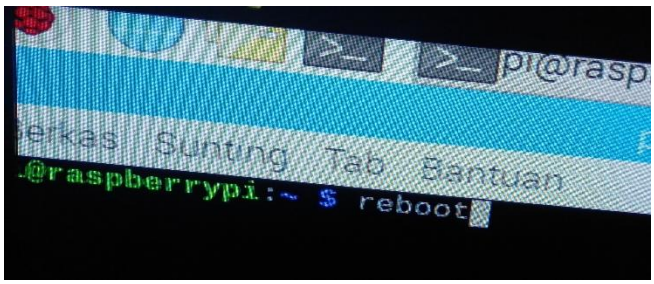
Gambar 3. 7 Perintah *update Raspberry Pi*

6. Masukkan perintah sudo apt-get install apache2 –y untuk memasang Apache pada *Raspberry Pi* seperti pada Gambar 3.8.



Gambar 3. 8 Pemasangan *Apache Web Server*

7. Masukkan perintah *reboot* pada terminal seperti pada Gambar 3.9.

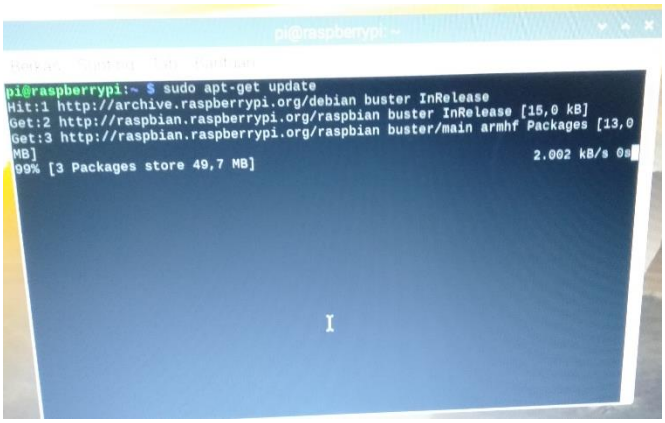


Gambar 3. 9 *Reboot*

3.5.2 Memasang HoneyPy

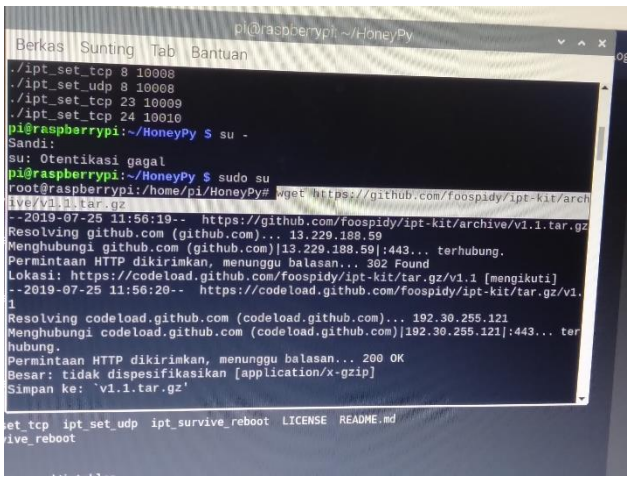
HoneyPy merupakan perangkat lunak *honeypot* yang dipasang dalam *Raspberry Pi 3 Model B+* berbasis *Raspbian* dengan langkah-langkah sebagai berikut:

1. Melalui Terminal, masukkan perintah sudo apt-get update untuk memperbaharui *Raspbian* seperti pada Gambar 3.10.



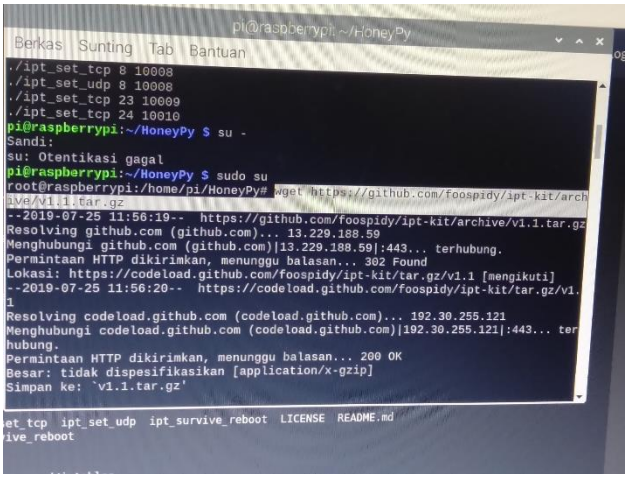
Gambar 3. 10 *Update Raspbian*

2. Masuk sebagai *root* dengan perintah sudo su seperti pada Gambar 3.11.



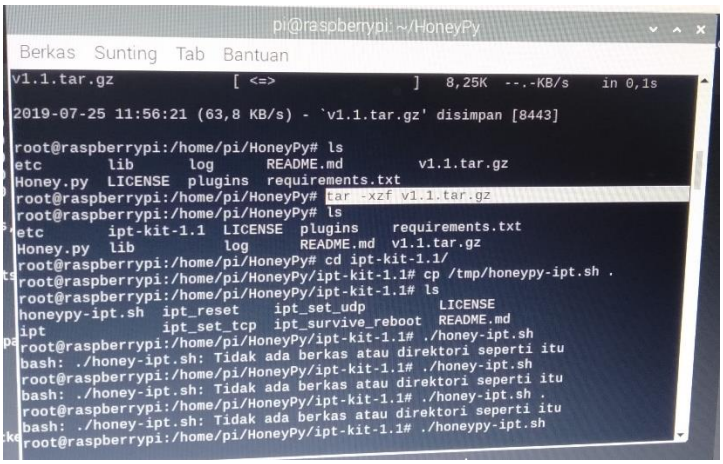
Gambar 3. 11 *Root*

3. Kemudian, mengunduh HoneyPy dengan memasukkan perintah wget https://github.com/foospidy/HoneyPy/archive/0.4.8.tar.gz seperti pada Gambar 3.12. *File* yang diunduh dalam format .zip



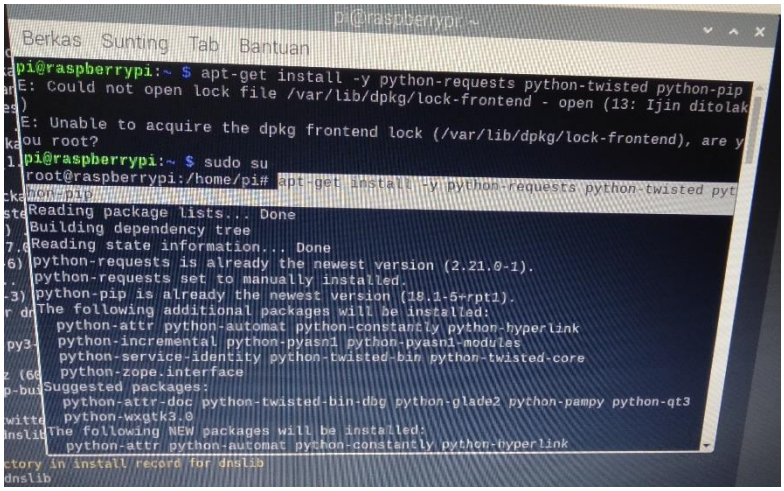
Gambar 3. 12 Mengunduh HoneyPy

4. *Unzip file* yang diunduh dengan perintah tar -xzf 0.4.8.tar.gz seperti pada Gambar 3.13.



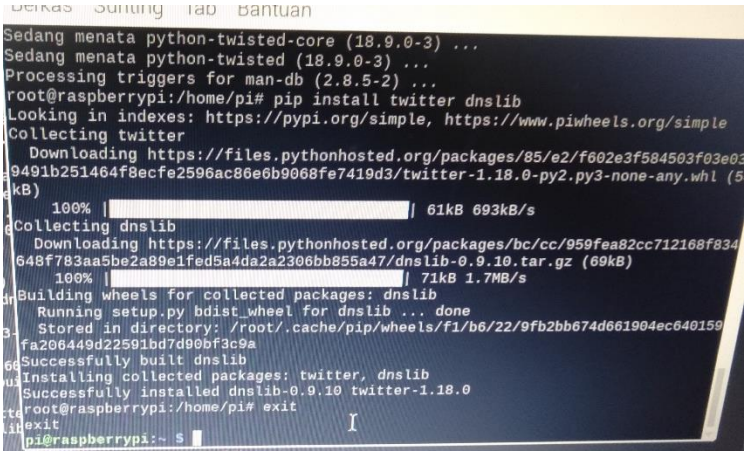
Gambar 3. 13 *Unzip*

5. Mengunduh *Python dependencies* dengan memasukkan perintah apt-get install -y python-requests python-twisted python-pip seperti pada Gambar 3.14.



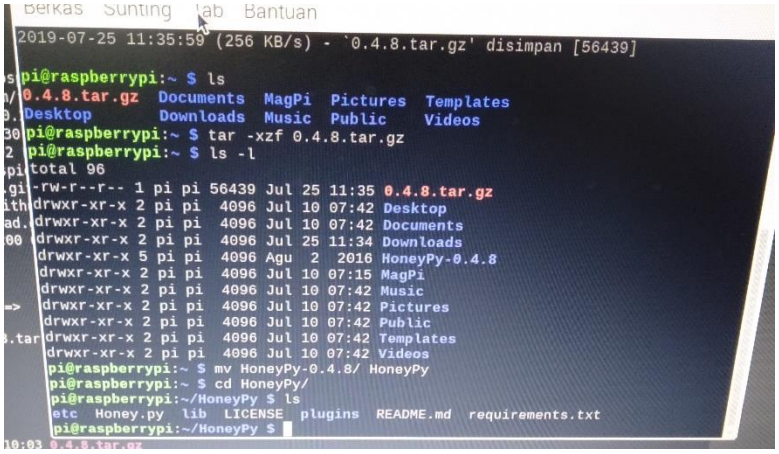
Gambar 3. 14 *Dependencies*

6. Masukkan perintah pip install twitter dnslib seperti pada Gambar 3.15.



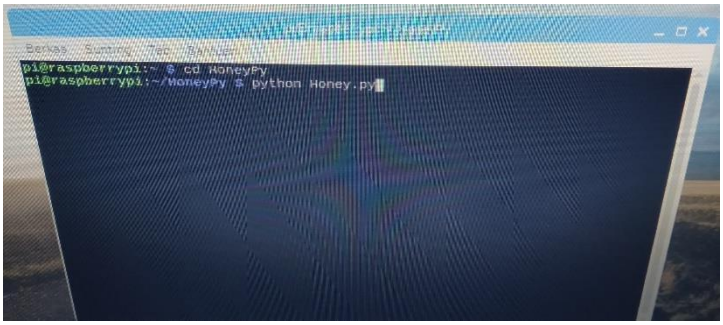
Gambar 3. 15 *Twitter Dependencies*

7. Masukkan perintah exit untuk keluar sebagai *root*. Kemudian masukkan perintah ls –l, selanjutnya masukkan perintah mv HoneyPy-0.4.8/ HoneyPy untuk memindahkan folder HoneyPy ke dalam *folder home* dengan nama HoneyPy seperti pada Gambar 3.16.



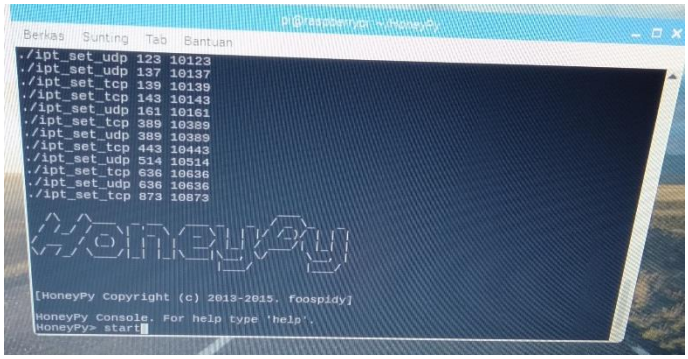
Gambar 3. 16 *Folder* HoneyPy

8. Jalankan HoneyPy tanpa *root* dengan memasukkan perintah cd HoneyPy seperti pada Gambar 3.17



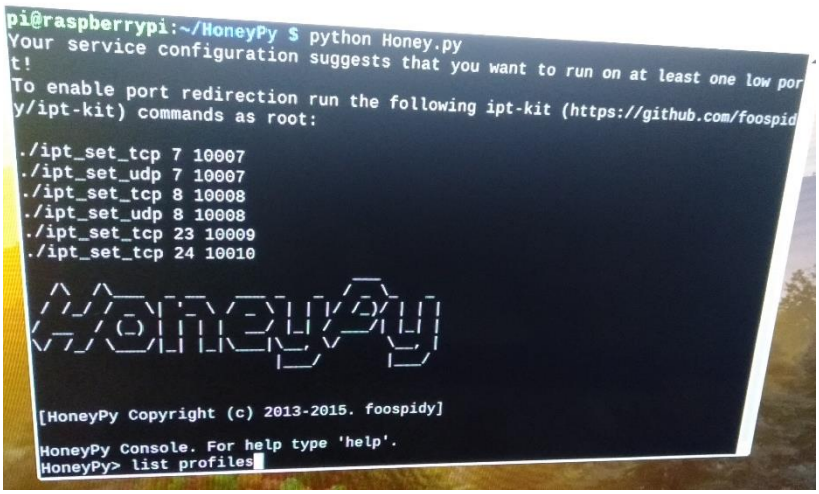
Gambar 3. 17 Menjalankan HoneyPy

Kemudian masukkan perintah python Honey.py kemudian muncul tampilan HoneyPy seperti pada Gambar 3.18.



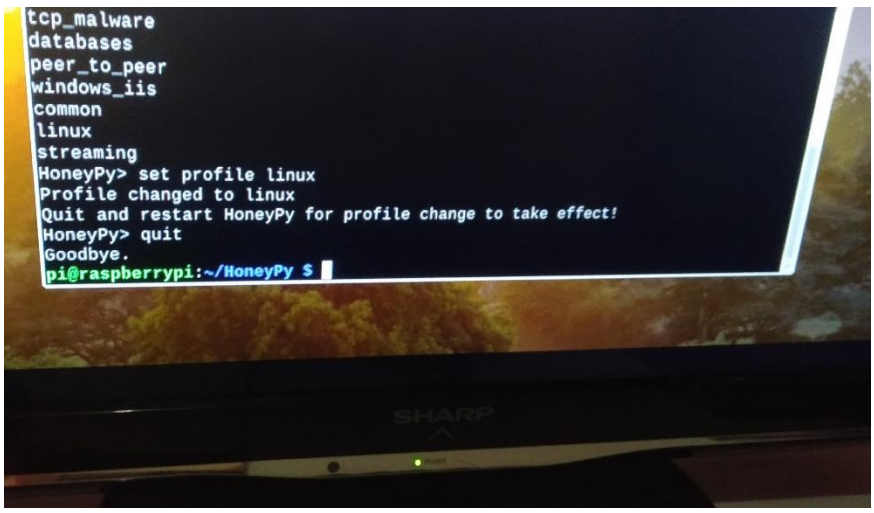
Gambar 3. 18 HoneyPy

9. Masukkan perintah list profiles untuk melihat *service profile* pada *honeypot* seperti pada Gambar 3.19.



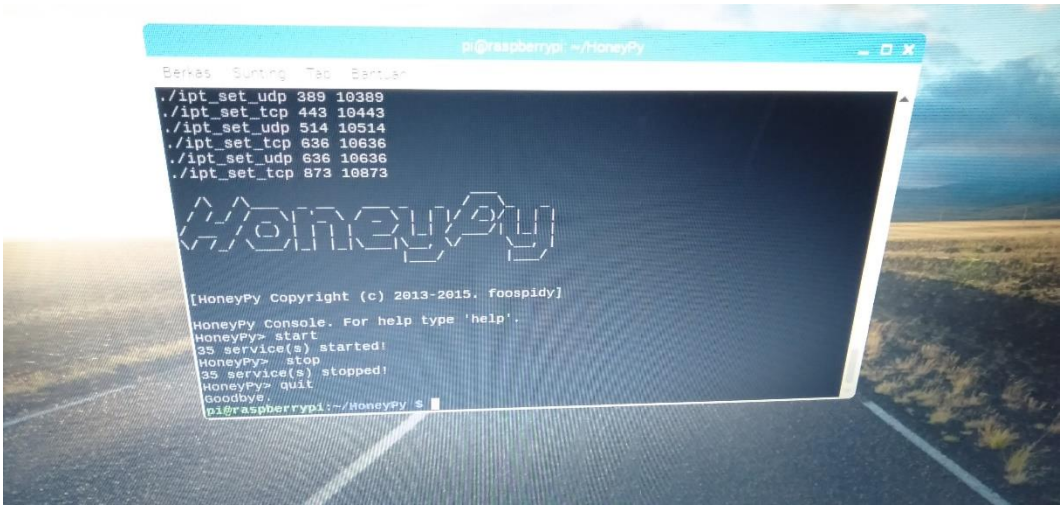
Gambar 3. 19 *List profiles*

10. Masukkan perintah set profile linux untuk memilih *honeypot* menjalankan sebagai linux *server full service* seperti pada Gambar 3.20. Kemudian masukkan perintah quit untuk melakukan *restart* pada HoneyPy.



Gambar 3. 20 *Linux Full Service*

11. Untuk menjalankan HoneyPy, masukkan perintah start, stop untuk memberhentikan layanan dan quit untuk keluar dari HoneyPy seperti ditunjukkan pada Gambar 3.21.

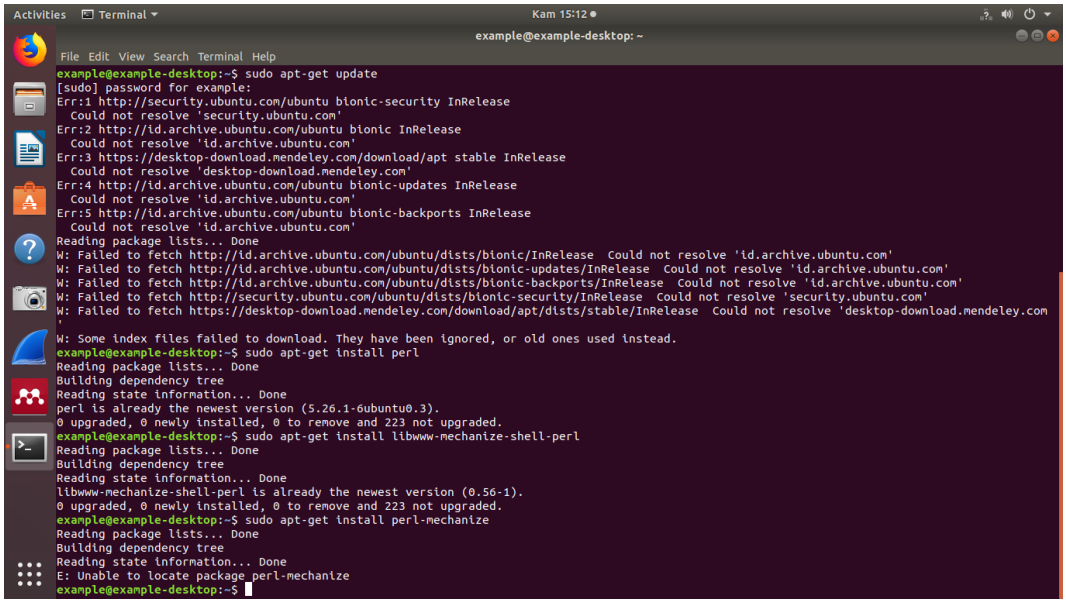


Gambar 3. 21 HoneyPy

3.5.3 Memasang Slowloris

Program serangan *Denial of Service* (DoS) yang akan dilakukan pada penelitian ini adalah *Slowloris*. Pemasangan dilakukan pada komputer dengan *operating system* Ubuntu 18.04 seperti pada Gambar 3.6 dengan langkah-langkah sebagai berikut:

1. Melalui Terminal, masukkan perintah sudo apt-get update untuk memperbaharui *Ubuntu*.
2. Kemudian, masukkan perintah sudo apt-get install perl untuk memasang program perl.
3. Kemudian, masukkan perintah sudo apt-get install libwww-mechanize-shell-perl untuk *library perl dependencies*.
4. Kemudian masukkan perintah sudo apt-get install perl-mechanize.

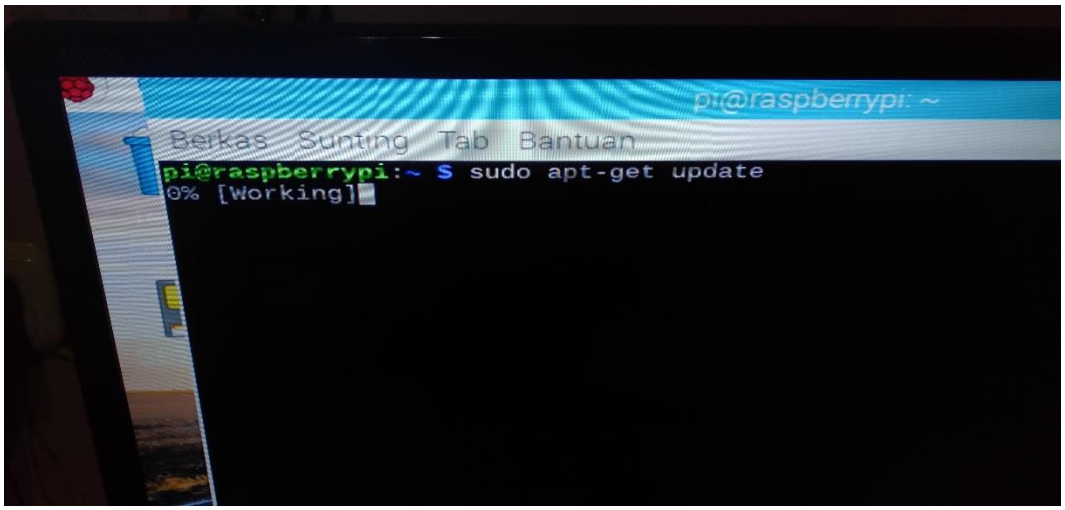


Gambar 3. 22 Pemasangan *Slowloris*

3.5.4 Memasang Tcpdump

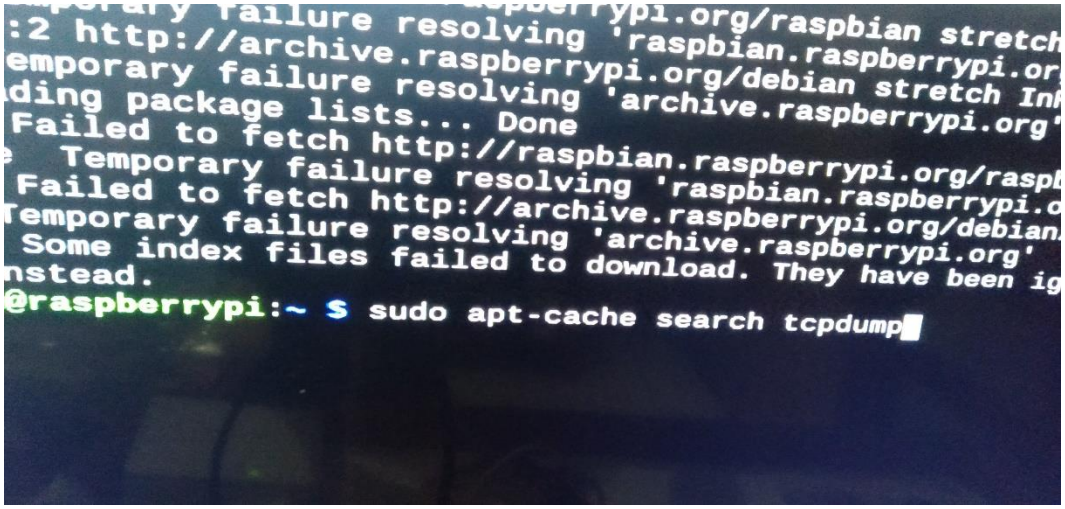
Tcpdump digunakan untuk merekam trafik yang masuk ke web server. Tcpdump dipasang di dalam web server. Berikut ini adalah langkah-langkah memasang Tcpdump:

1. Masukkan perintah sudo apt-get update untuk melakukan update Raspbian seperti pada Gambar 3.23.



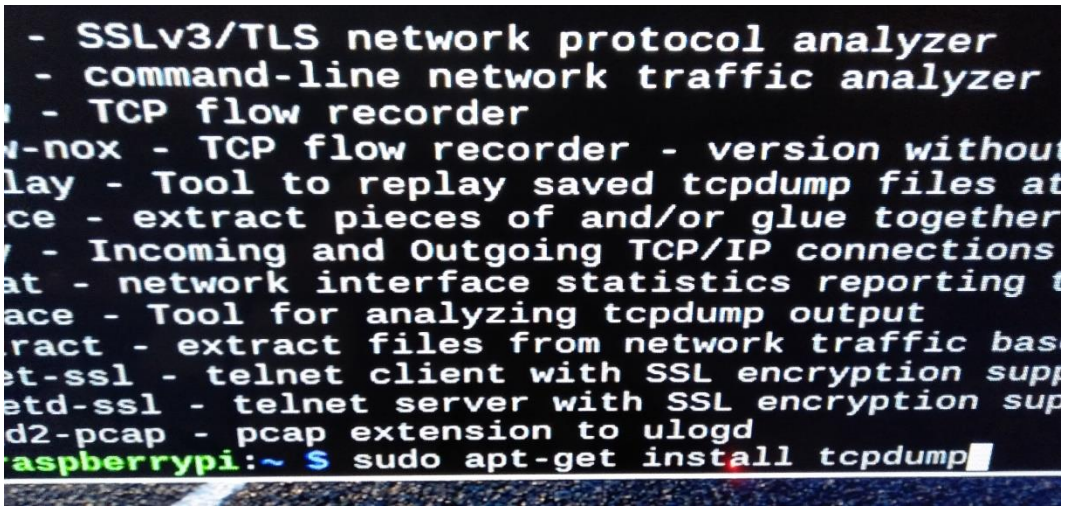
Gambar 3. 23 *Raspbian Update*

2. Masukkan perintah sudo apt-cache search tcpdump untuk mencari program tcpdump pada library Raspbian seperti pada Gambar 3.24.



Gambar 3. 24 *Search tcpdump*

3. Masukkan perintah sudo apt-get install tcpdump untuk memasang Tcpdump seperti pada Gambar 3.25.

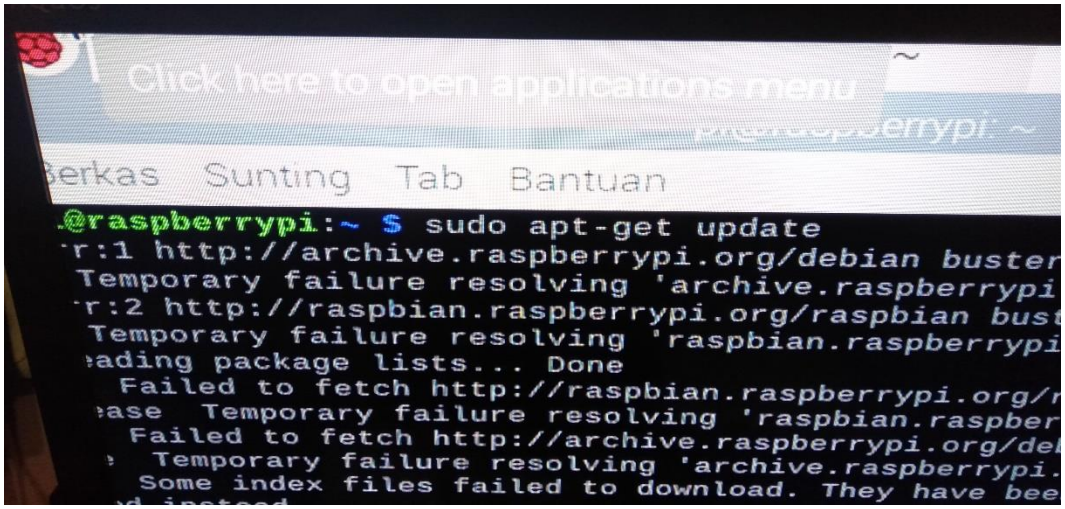


Gambar 3. 25 *Install tcpdump*

3.5.5 Memasang Tshark

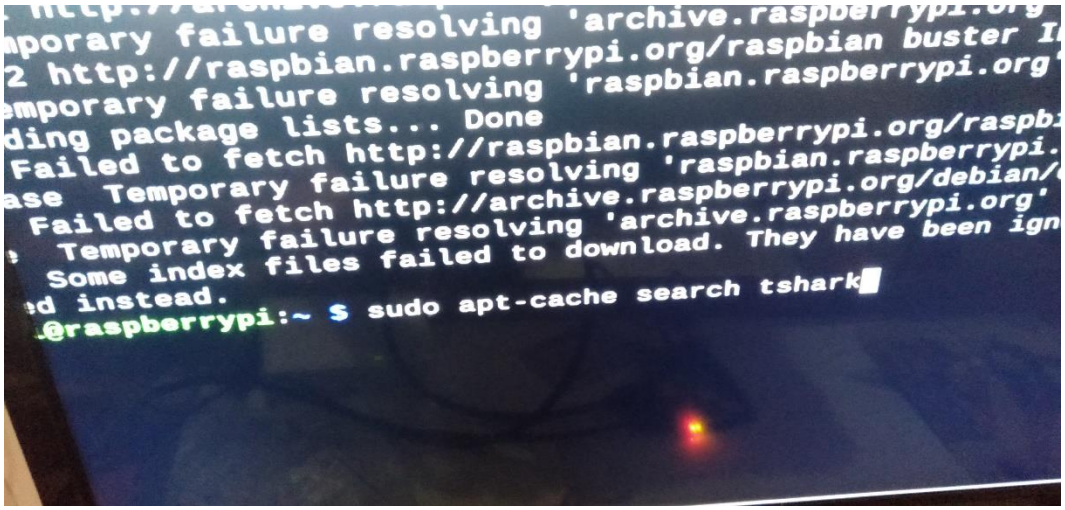
Tshark digunakan untuk merekam trafik yang masuk ke dalam honeypot. Berikut ini langkah-langkah memasang Tshark:

1. Masukkan perintah sudo apt-get update untuk melakukan *update* pada *Raspbian* seperti pada Gambar 3.26.



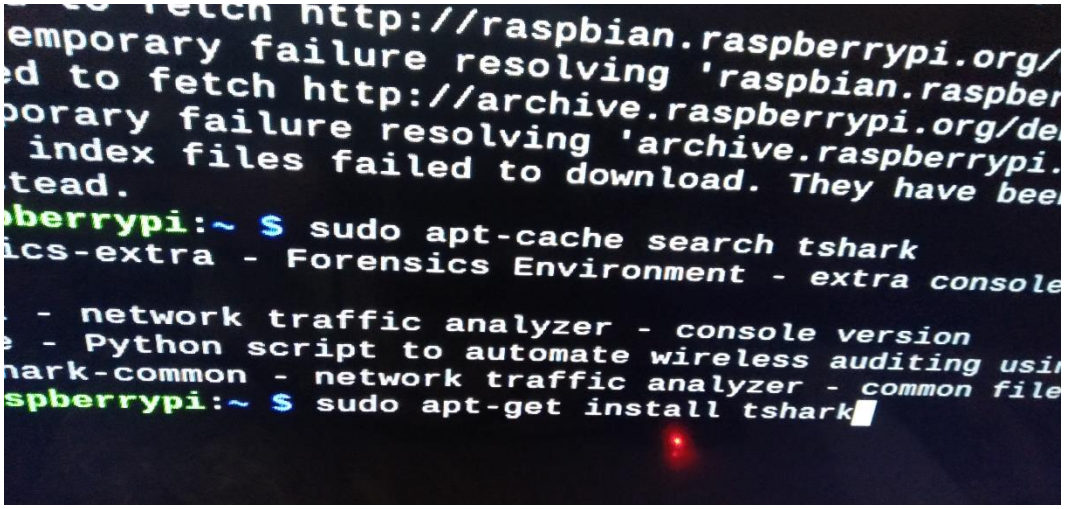
Gambar 3. 26 *Raspbian update*

2. Masukkan perintah sudo apt-cache search tshark untuk mencari program *tshark* pada *library Raspbian* seperti pada Gambar 3.27.



Gambar 3. 27 *Search Tshark*

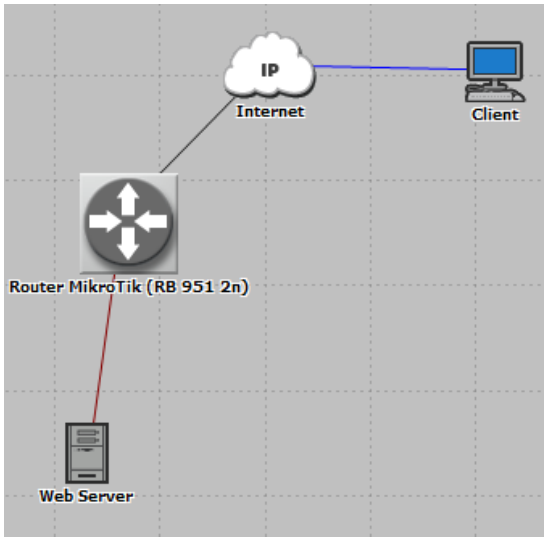
3. Masukkan perintah sudo apt-get install tshark untuk memasang *Tshark* seperti pada Gambar 3.28.



Gambar 3. 28 *Install Tshark*

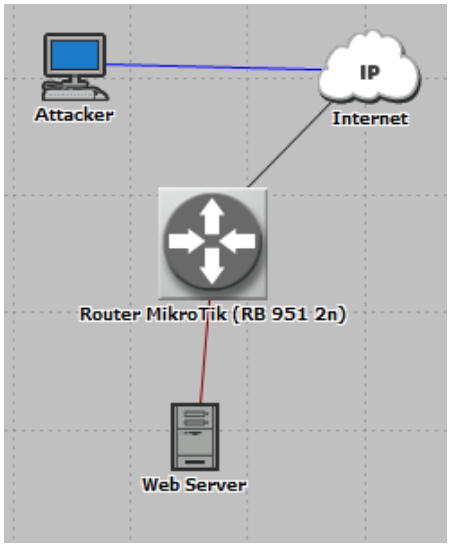
3.5.6 Mendesain Topologi Jaringan

Topologi jaringan untuk penelitian ini didesain berdasarkan referensi dalam tiga kondisi, kondisi normal, kondisi pnyerangan tanpa dan dengan mekanisme pertahanan.



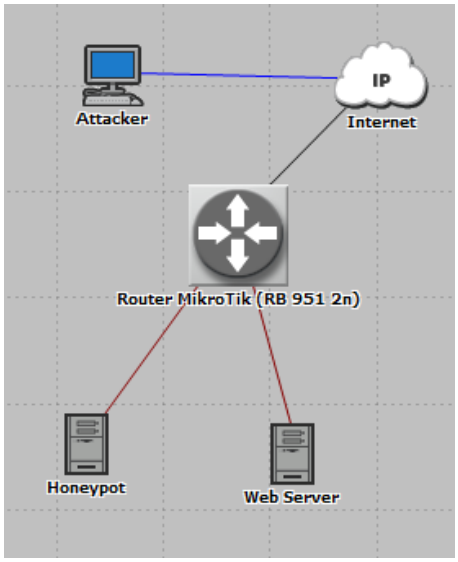
Gambar 3. 29 Topologi jaringan kondisi normal dimana tidak ada *attacker* dan *honeypot* di dalam jaringan

Pada kondisi normal, topologi jaringan hanya terdiri dari *router*, *web server* dan satu buah *laptop* sebagai *client* seperti yang ditunjukkan pada Gambar 3.29. Aktivitas pada jaringan hanya *browsing* dengan *browser* pada satu buah *laptop*. Tidak ada penyerangan terhadap *web server*.



Gambar 3. 30 Topologi jaringan kondisi ketika dilakukan serangan terhadap *webserver*

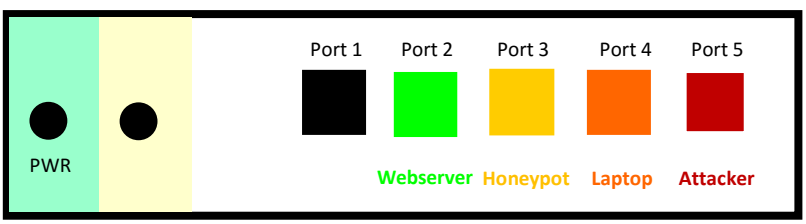
Pada kondisi terjadi penyerangan pada *web server*, topologi jaringan terdiri dari *router*, *web server* dan satu buah komputer sebagai *attacker* tanpa adanya mekanisme pertahanan seperti pada Gambar 3.30. Penyerangan dilakukan selama lima menit dengan satu buah komputer berbasis Ubuntu.



Gambar 3. 31 Topologi jaringan ketika *honeypot* di dalam jaringan

Pada kondisi terjadi penyerangan pada *web server* dengan mekanisme pertahanan, topologi jaringan terdiri dari *router*, *web server*, satu buah komputer sebagai *attacker* dan satu buah *honeypot* seperti pada Gambar 3.31. Mekanisme pertahanan merupakan kombinasi dari *firewall* pada *router* dan *honeypot*. Dilakukan perbandingan hasil antara *firewall* dan kombinasi *firewall* dan *honeypot*. Penyerangan dilakukan selama lima menit dengan satu buah komputer berbasis Ubuntu.

Topologi jaringan ini merupakan jaringan lokal tak terhubung dengan internet yang terdiri dari satu buah komputer yang menjadi *attacker*, 1 buah *laptop* untuk mengawasi dan mengatur *firewall* pada *router*, *RaspberryPi 3 Model B+* yang menjadi *honeypot*, *RaspberryPi 2 Model B* sebagai *webserver* dan *Router* MikroTik (RB 951 2n). Eksperimen dilakukan sebagai simulasi jaringan yang terhubung dengan internet. Gambar 3.32 menunjukkan *port-port* yang terhubung dengan *router*.



Gambar 3. 32 Port-port yang terhubung pada Router MikroTik (RB 951 2n)

Router memiliki IP *Address* 192.168.100.1/24 dengan *port* 2 hingga *port* 4 merupakan *bridge*. *Port* 5 dilepas dari *bridge* sebagai simulasi *attacker* menyerang dari internet dengan IP *Address* 192.168.25.1/24. *Port* 2 terhubung dengan *web server*, *port* 3 terhubung dengan *honeypot*, *port* 4 terhubung dengan *laptop*, sedangkan p*ort* 5 terhubung dengan komputer sebagai *attacker*. *Web server* beralamatkan 192.168.100.250, *honeypot* beralamatkan 192.168.100.244 dan *attacker* beralamatkan 192.168.25.252.

3.5.7 Mengatur *firewall router*

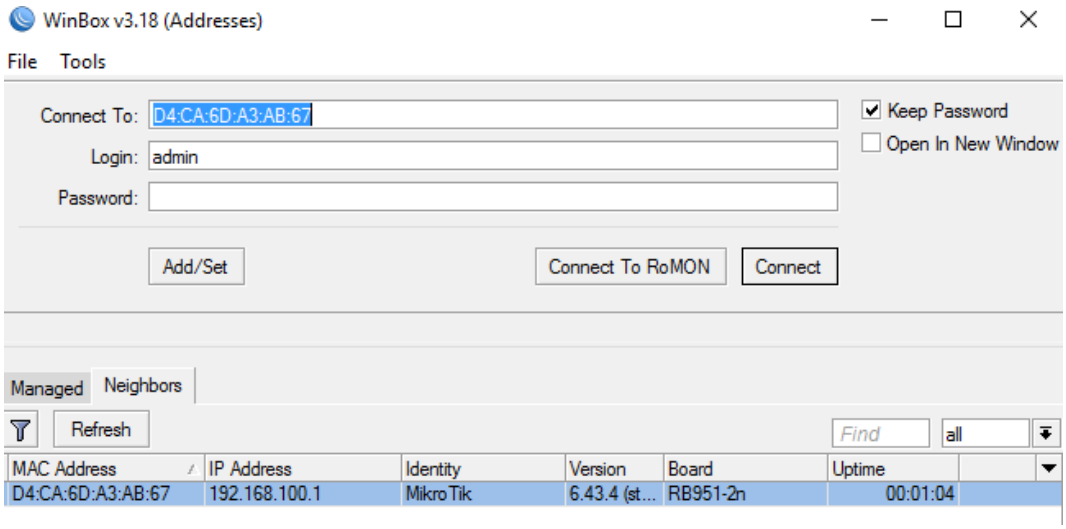
Router yang dipakai adalah Mikrotik RB 951 2n. *Firewall* diatur menggunakan *software* WinBox Mikrotik SIA dengan menghubungkan *router* dan *laptop* pada *port* 4. Beberapa *Firewall rules* merupakan *default configuration*. *Firewall* yang akan digunakan adalah *firewall DDoS Detection and Blocking*. Berikut ini langkah-langkah mengaktifkan *firewall DDoS Detection and Blocking* (MikroTik, 2011):

1. Hubungkan *laptop* dengan *router* menggunakan kabel RJ45 pada *port* 4 seperti pada Gambar 3.33 dan Gambar 3.34

Gambar 3. 33 *Laptop* dihubungkan dengan *Router*

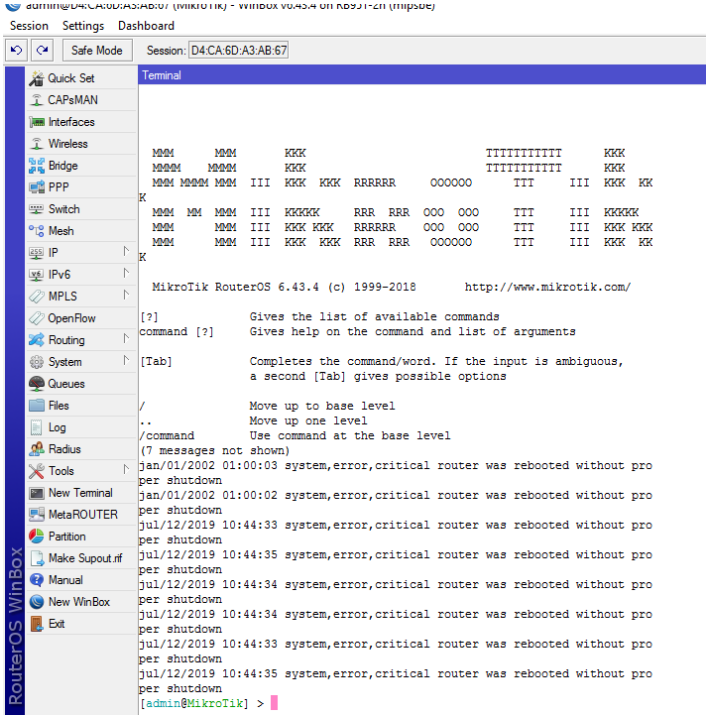
Gambar 3. 34 *Port* 4

2. Masuk ke *software* Winbox kemudian klik *connect* pada MAC *Address router* seperti pada Gambar 3.35.



Gambar 3. 35 Tampilan Winbox

3. Masuk ke menu Terminal seperti pada Gambar 3.36.



Gambar 3. 36 *New Terminal* pada *Winbox*

4. Kemudian, masukkan perintah berikut seperti pada Gambar 3.37:

   /ip firewall filter

   add chain=forward connection-state=new action=jump jump-target=detect-ddos

5. Kemudian, untuk setiap pasangan ”SrcIP:DstIP” diizinkan untuk beberapa koneksi baru dengan pengecualian seperti *web server* agar tidak terblokir dengan perintah berikut:

   add chain=detect-ddos dst-limit=32,32,src-and-dst-addresses/10s action=return

   add chain=detect-ddos src-address=192.168.100.250 action=return

6. Kemudian, memasukkan perintah berikut untuk mendeteksi penyerang (ddoser) dan target (ddosed) dengan IP Address yang selanjutnya dimasukkan ke dalam *address lists* dengan *timeout* sebesar sepuluh menit:

   add chain=detect-ddos action=add-dst-to-address-list address-list=ddosed address-list-timeout=10m

   add chain=detect-ddos action=add-src-to-address-list address-list=ddoser address-list-timeout=10m

7. Kemudian, proses paket kembali ke *forward chain*, dimana paket-paket yang datang dari ‘ddoser’ menuju ‘ddosed’ diblokir atau di-*drop* dengan memasukkan perintah berikut:

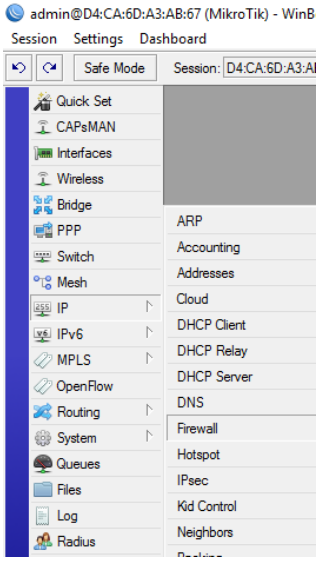
   add chain=forward connection-state=new src-address-list=ddoser dst-address-list=ddosed action=drop

```
[admin@MikroTik] /ip firewall filter> add chain=forward connection-state=new actio
n=jump jump-target=detect-ddos
[admin@MikroTik] /ip firewall filter> add chain=detect-ddos dst-limit=32,32,src-an
d-dst-addresses/10s action=return
[admin@MikroTik] /ip firewall filter> add chain=detect-ddos src-address=192.168.10
0.250 action=return
[admin@MikroTik] /ip firewall filter> add chain=detect-ddos action=add-dst-to-addr
ess-list address-list=ddosed address-list-timeout=10m
[admin@MikroTik] /ip firewall filter> add chain=detect-ddos action=add-src-to-addr
ess-list address-list=ddoser address-list-timeout=10m
[admin@MikroTik] /ip firewall filter> add chain=forward connection-state=new src-a
ddress-list=ddoser dst-address-list=ddosed action=drop
```

Gambar 3. 37 Perintah-perintah *firewall* DDoS *Detection and Blocking*

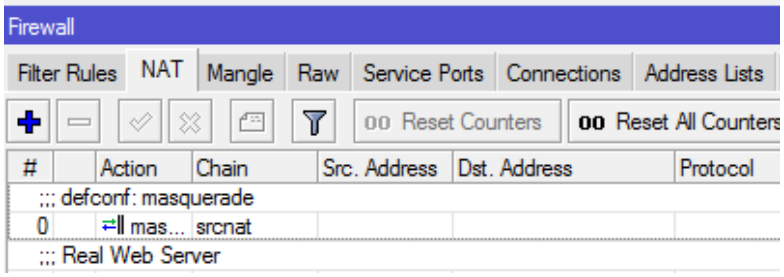
Port Forwarding ke *Honeypot* diatur dengan *Firewall* NAT *Rule*, dibawah ini merupakan langkah-langkah *port forwarding*:

1. Masuk ke menu IP lalu pilih *Firewall* seperti pada Gambar 3.38.



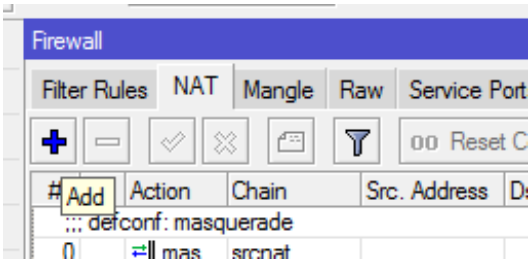
Gambar 3. 38 *Firewall* menu

2. Kemudian, pilih NAT seperti pada Gambar 3.39.



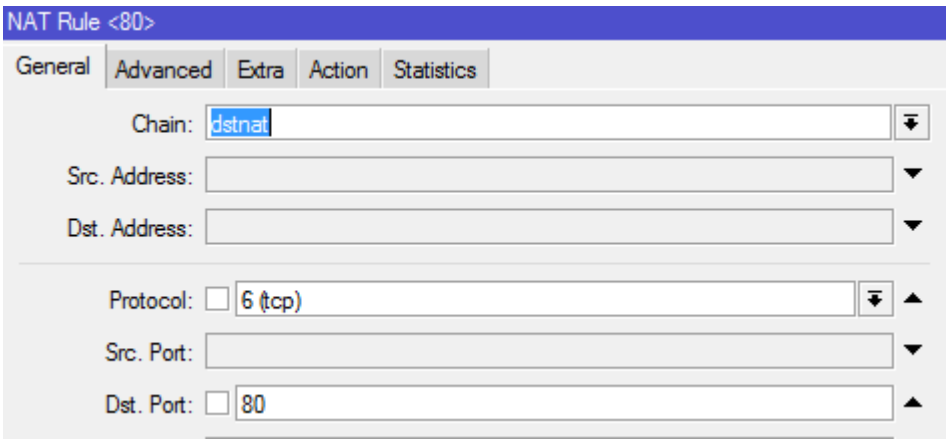
Gambar 3. 39 NAT

3. Kemudian, klik tanda plus biru untuk menambahkan NAT *Rule* baru seperti pada Gambar 3.40.



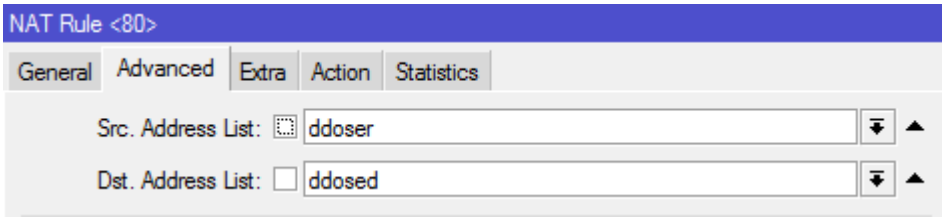
Gambar 3. 40 *Add New* NAT *Rule*

4. Di Tab General, masukkan chain dst nat, protocol tcp dan port 80 seperti pada Gambar 3.41



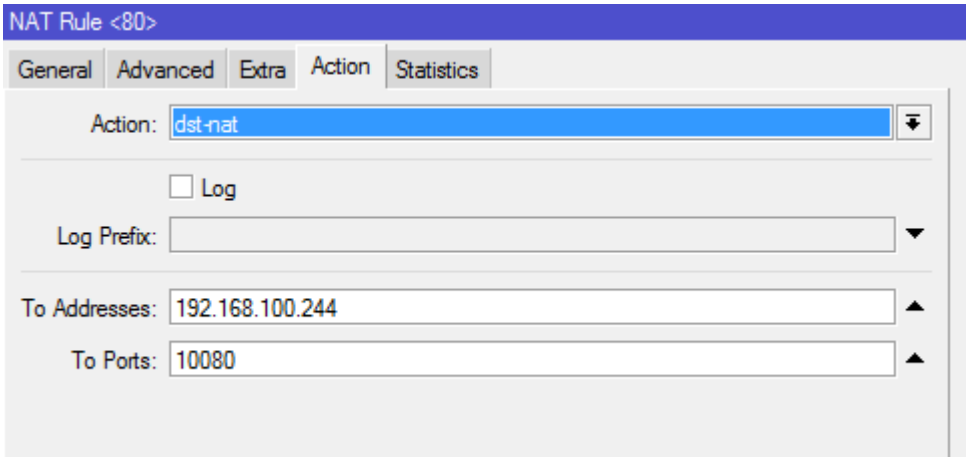
Gambar 3. 41 NAT *Rule General*

5. Di *Tab Advanced*, masukkan ddoser dalam Src. *Address List* dan ddosed di Dst. *Address List* seperti pada Gambar 3.42.



Gambar 3. 42 NAT *Rule Advanced*

6. Di *tab Action*, masukkan dst-nat pada *action*, *to addresses* adalah IP *Address Honeypot* dan *to Ports* adalah 10080 karena port 80 pada *honeypot* adalah 10080 seperti pada Gambar 3.43.



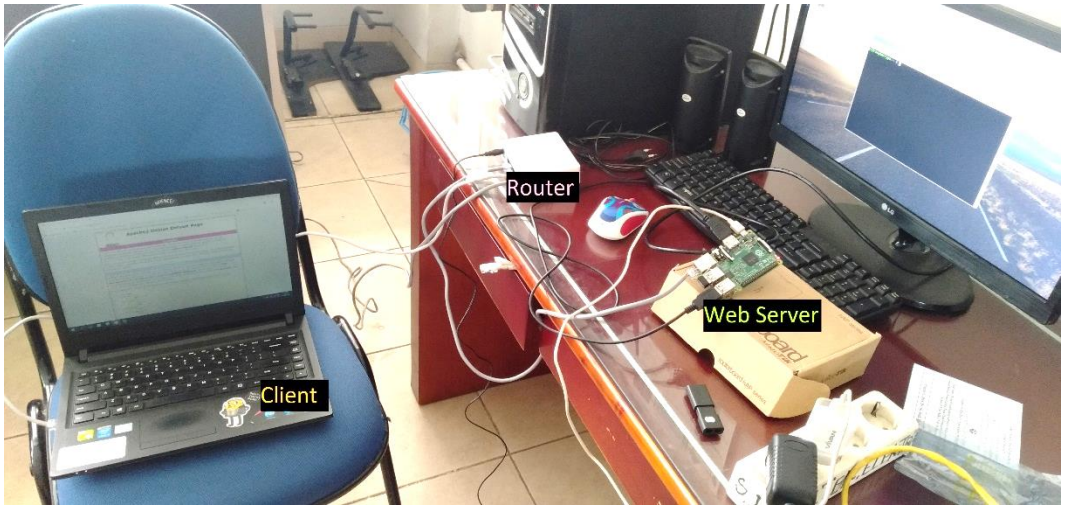
Gambar 3. 43 NAT *Rule Action*

3.5.8 Melakukan Eksperimen

Eksperimen dilakukan dalam tiga kondisi, yaitu ketika trafik normal, ketika terjadi penyerangan tanpa mekanisme pertahanan dan ketika mekanisme pertahanan dipasang.

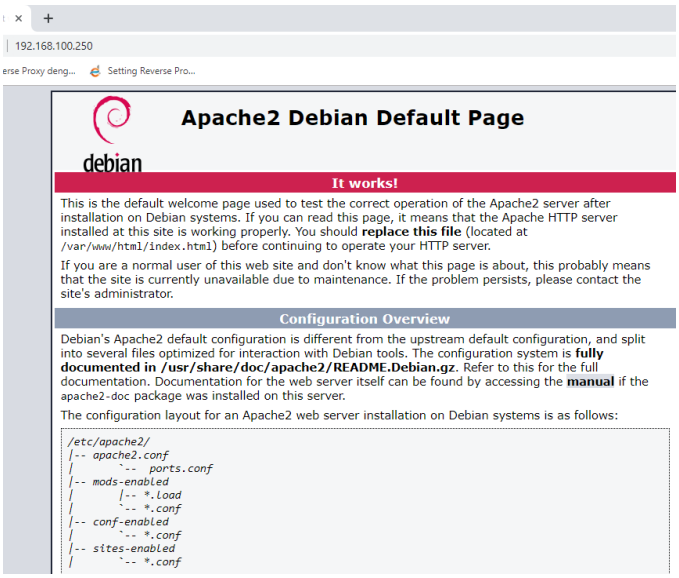
1. Kondisi trafik normal

   Kondisi dimana tidak ada penyerangan sama sekali, hanya *client* yang meangkses *web server*. Pada penelitian ini, satu buah laptop digunakan untuk mengakses *web server* seperti pada Gambar 3.44.



Gambar 3. 44 Kondisi Trafik Normal

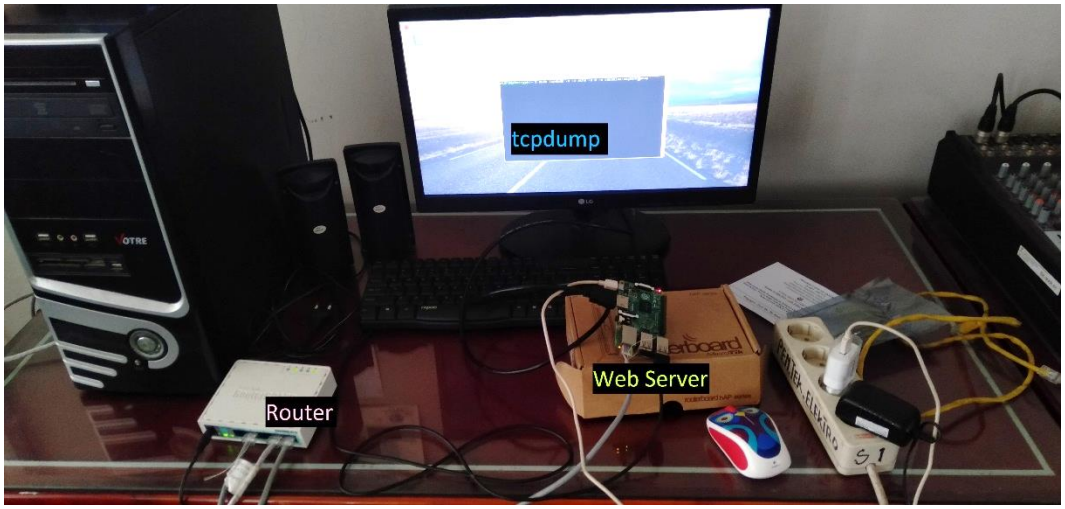
Halaman *web* diakses dengan memasukkan IP *Address web server* 192.168.100.250 pada kolom URL. Gambar 3.45 menunjukkan halaman *web* ketika diakses melalui *laptop* ketika tidak ada gangguan atau serangan menuju *web server*.



Gambar 3. 45 Halaman *web*

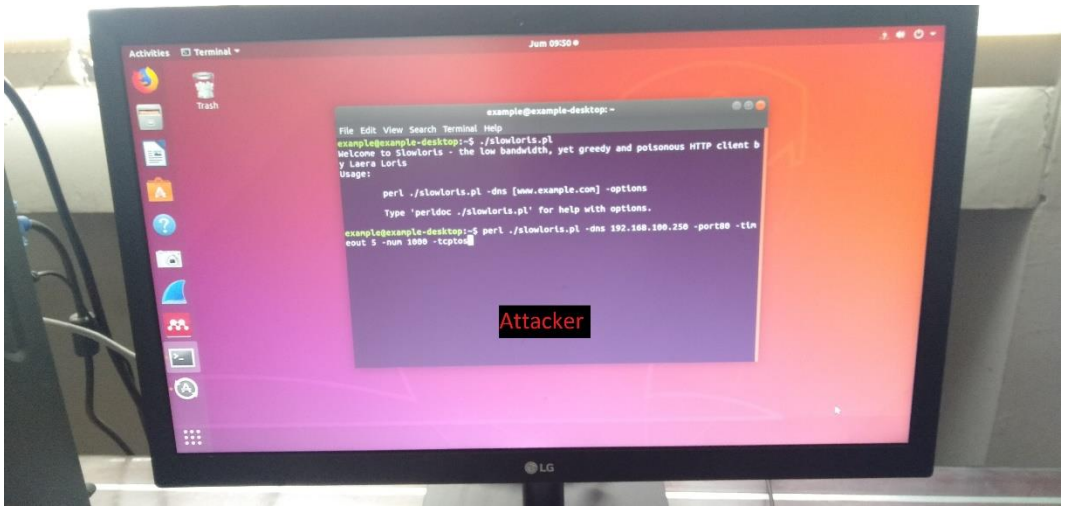
2. Kondisi penyerangan tanpa mekanisme pertahanan

   Kondisi ini dimana terjadi penyerangan tanpa mekanisme pertahanan seperti pada Gambar 3.46.



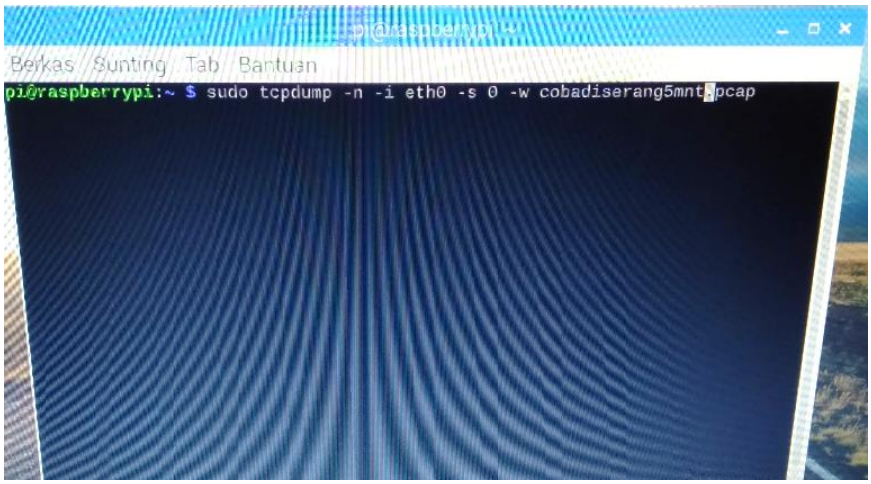
Gambar 3. 46 Kondisi ketika terjadi penyerangan

Penyerangan terhadap *web server* dilakukan selama lima menit dengan jumlah koneksi sebesar 1000 koneksi dan *timeout* lima detik pada *port* 80. Penyerangan dilakukan memasukkan perintah perl ./slowloris.pl –dns 192.168.100.250 –port 80 –timeout 5 –num 1000 –tcpto 5 (Arafat & Alam, 2015) dalam Terminal seperti pada Gambar 3.47.



Gambar 3. 47 Program *Slowloris*

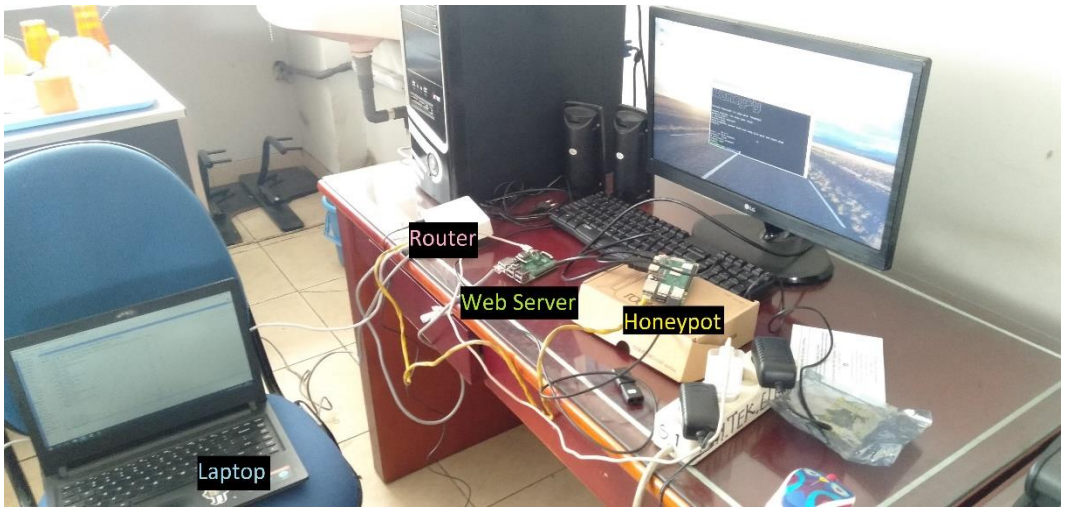
Trafik paket data yang masuk ke *web server* direkam dengan *software* tcpdump, kemudian hasilnya disimpan dalam *format* .pcap dengan memasukkan perintah sudo tcpdump –n –i eth0 –s 0 –w (nama file).pcap (Arafat & Alam, 2015) seperti pada Gambar 3.48.



Gambar 3. 48 tcpdump pada *web server*

3. Kondisi penyerangan dengan mekanisme pertahanan

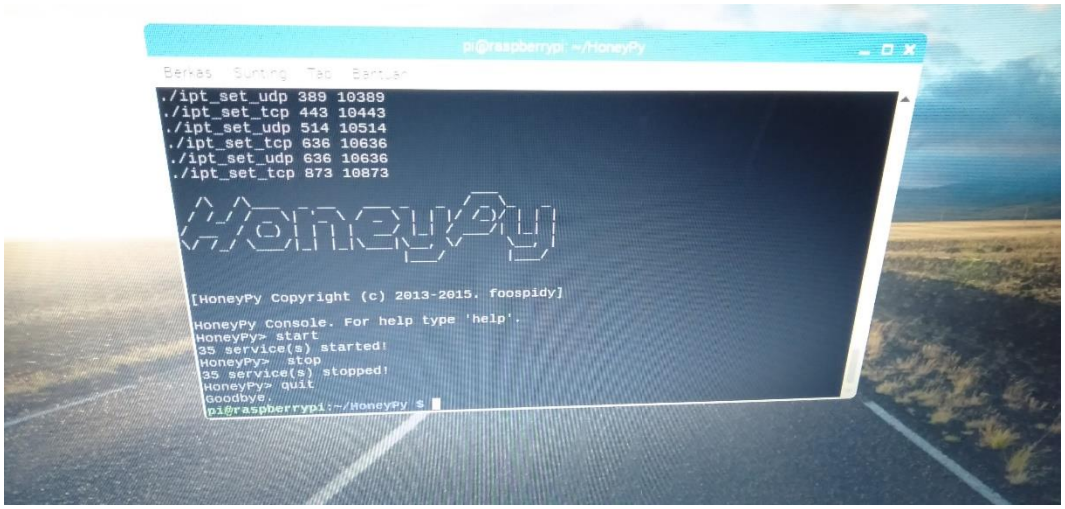
   Kondisi ini dimana terjadi penyerangan dengan mekanisme pertahanan seperti pada Gambar 3.49. Kondisi ini akan dibagi menjadi dua kondisi, yaitu dimana hanya *firewall* saja sebagai mekanisme pertahanan, kemudian ketika digabungkan dengan *honeypot*. Laptop digunakan sebagai *monitor* trafik paket data yang di *forward* menuju *honeypot*.



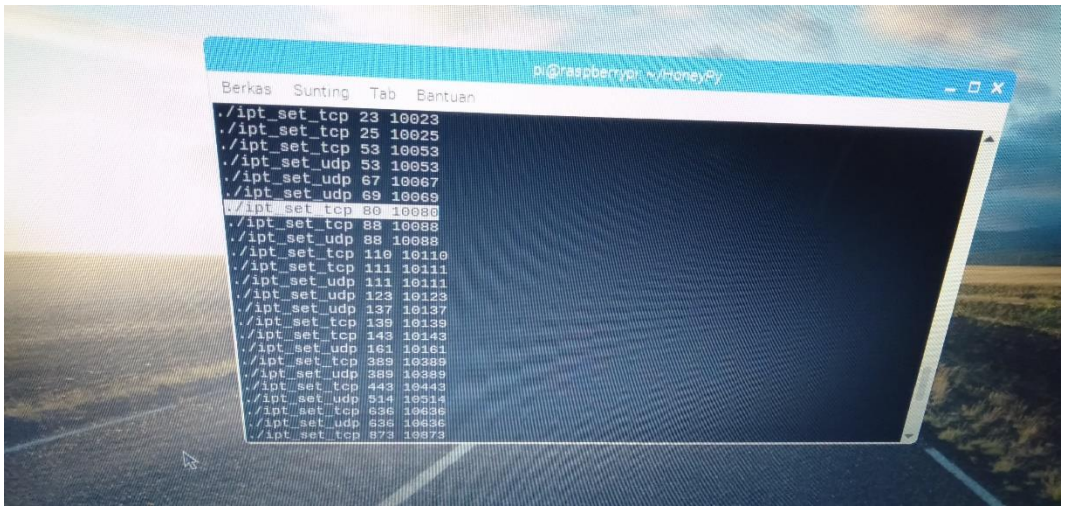
Gambar 3. 49 Kondisi ketika telah dipasang mekanisme pertahanan

Honeypot yang digunakan adalah HoneyPy, yang merupakan *low to medium interaction honeypot*. HoneyPy dijalankan *full service* sebagai Linux *server* seperti

pada Gambar 3.50 dengan tiruan *port* 80 untuk layanan HTTP pada *port* 10080 seperti pada Gambar 3.51.

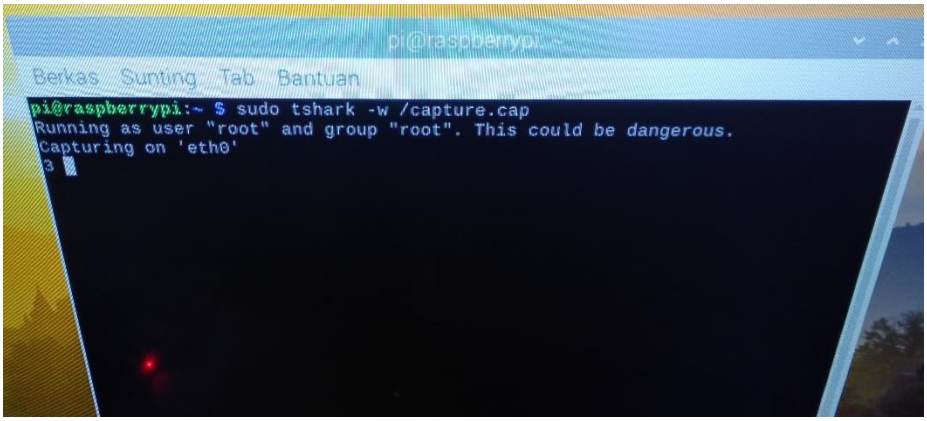


Gambar 3. 50 HoneyPy



Gambar 3. 51 Tiruan *Port* 80 pada *port* 10080

Trafik paket data yang masuk ke dalam *honeypot* direkam dalam format .cap dengan menggunakan Tshark dengan memasukkan perintah sudo tshark –w /(nama file).cap seperti pada Gambar 3.52. Kemudian, trafik paket data yang terekam dianalisa menggunakan *Wireshark*.



Gambar 3. 52 Menjalankan Tshark

3.6 Analisis Data

Trafik paket data hasil eksperimen dari tiga kondisi direkam dalam *web server* menggunakan *program* tcpdump. Trafik paket data dalam jaringan direkam dalam tiga kondisi, yaitu trafik normal, trafik kondisi penyerangan tanpa mekanisme pertahanan dan dengan mekanisme pertahanan. Kemudian trafik paket data yang terekam dianalisa menggunakan program *wireshark*. Kemudian, dilakukan perbandingan tiga kondisi tersebut, apakah dengan diterapkannya *honeypot* sebagai mekanisme pertahanan mengurangi serangan *Slowloris* terhadap *web server*. Dilakukan perekaman trafik yang masuk ke dalam *web server* dan *Honeypot* dengan menggunakan *software tcpdump* dan *Tshark* yang masih menjadi bagian dari *Wireshark*.