BAB 4
IMPLEMENTASI DAN PENGUJIAN SISTEM

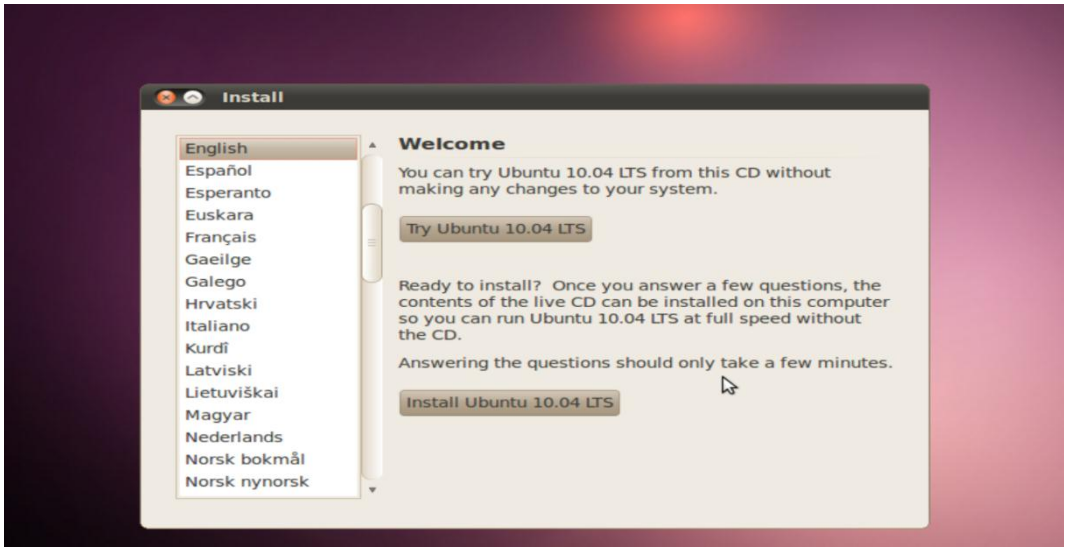
Pada bab ini akan dilakukan implementasi dan pengujian terhadap sistem keamanan jaringan IPS dan *Honeypot* yang dibangun. Implementasi dilakukan berdasarkan analisis, permasalahan dan perancangan yang telah dibuat. Setelah implementasi selesai, maka akan dilakukan pengujian kinerja dari sistem yang telah dibangun.

4.1 Instalasi Linux Ubuntu

Linux ubuntu adalah sistem operasi yang akan digunakan untuk membangun sistem keamanan jaringan IPS dan *Honeypot*, dimana akan terdapat satu pc akan di *install* linux ubuntu, PSAD, dan *Fwsnort* yang berfungsi sebagai IPS dan satu pc lainnya akan di *install* linux Ubuntu dan *HoneyD* yang berfungsi sebagai *honeypot*.

4.1.1 Instalasi Komputer IPS

Pada tahap ini akan melakukan instalasi linux Ubuntu yang akan digunakan sebagai sistem IPS. Dibawah ini adalah tahapan-tahapan instalasi linux ubuntu untuk sistem IPS.



Gambar 4.1 Tahap awal instalasi pc IPS

Pada gambar 4.1 dapat dilihat tahap awal dalam melakukan instalasi linux ubuntu untuk sistem IPS, pada tahap awal tersebut sebelum melakukan instalasi harus memilih bahasa yang akan digunakan kemudian lanjut dengan memilih *install* ubuntu. Berikut adalah tahap selanjutnya yang dapat dilihat pada gambar 4.2.



Gambar 4.2 Pemilihan zona waktu

Pada gambar 4.2 dapat dijelaskan untuk tahap instalasi selanjutnya yaitu pemilihan zona waktu, dimana sebaiknya zona waktu yang dipilih sesuai dengan

keberadaan sistem akan diimplementasikan atau dibangun agar tidak terjadi kejanggalan. Untuk tahap selanjutnya dapat dilihat pada gambar 4.3



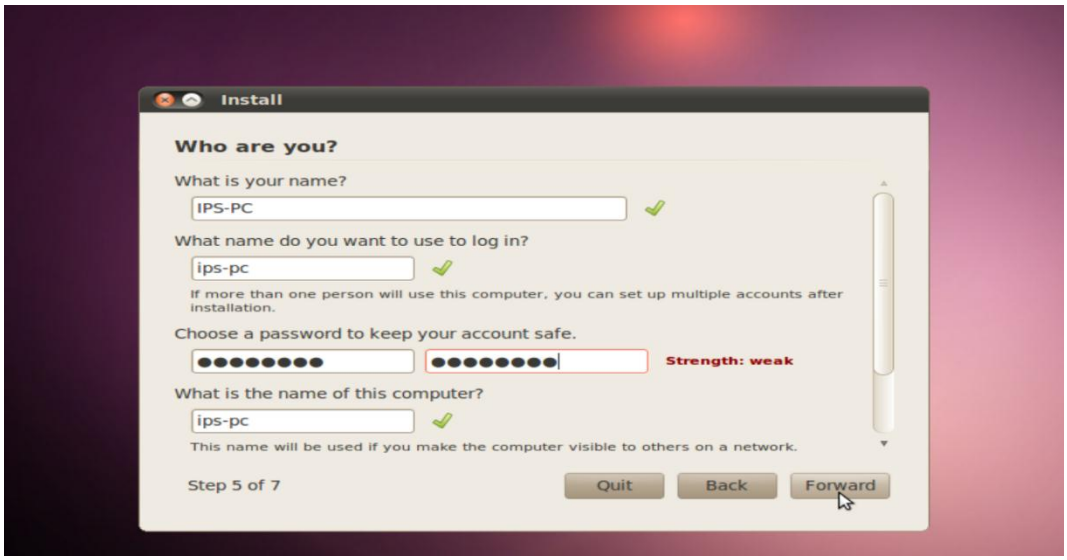
Gambar 4.3 Pemilihan layout keyboard

Pada gambar 4.3 dapat dijelaskan pemilihan *layout keyboard* yang akan digunakan, secara *default* sistem operasi linux ubuntu akan menyarankan menggunakan *layout keyboard* USA yang dimana menjadi *default layout keyboard* dari kebanyakan sistem operasi. Setelah memilih *layout keyboard* yang akan digunakan tahap selanjutnya dapat dilihat pada gambar 4.4.



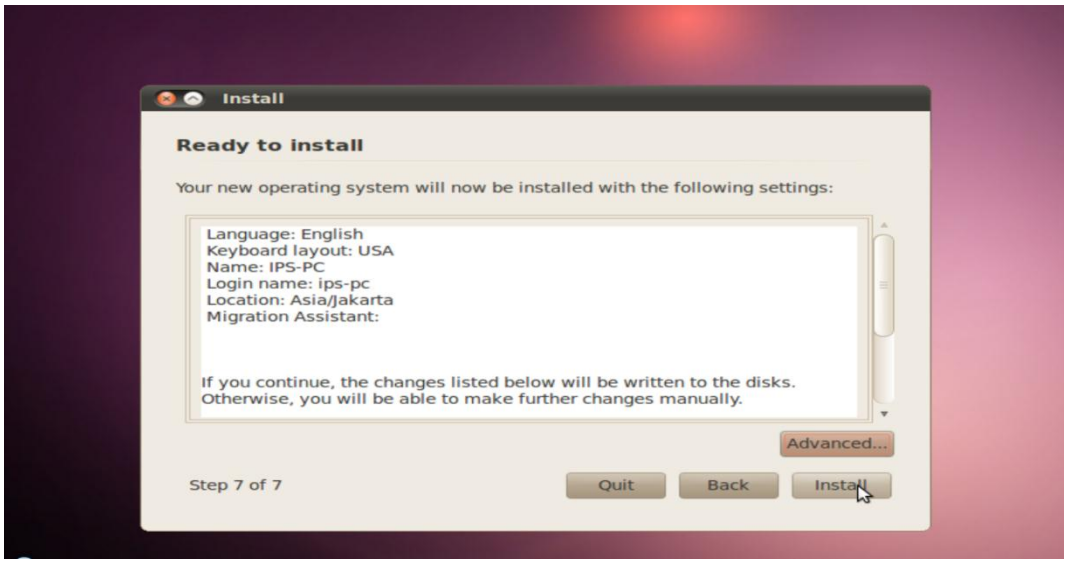
Gambar 4.4 Pembuatan partisi dan ukuran pada harddisk

Pada gambar 4.4 menjelaskan setelah pemilihan *layout keyboard* tahap selanjutnya yaitu pembuatan partisi dan ukuran *harddisk* yang akan digunakan untuk instalasi linux ubuntu, dikarenakan untuk komputer atau pc IPS hanya bekerja sebagai sistem keamanan dan tidak dipergunakan untuk menyimpan data, maka partisi *harddisk* hanya dibuat satu dan menggunakan ukuran *harddisk* sebesar 4 Gb. Setelah melakukan pembuatan partisi dan ukuran *harddisk* tahap selanjutnya dapat dilihat pada gambar 4.5.



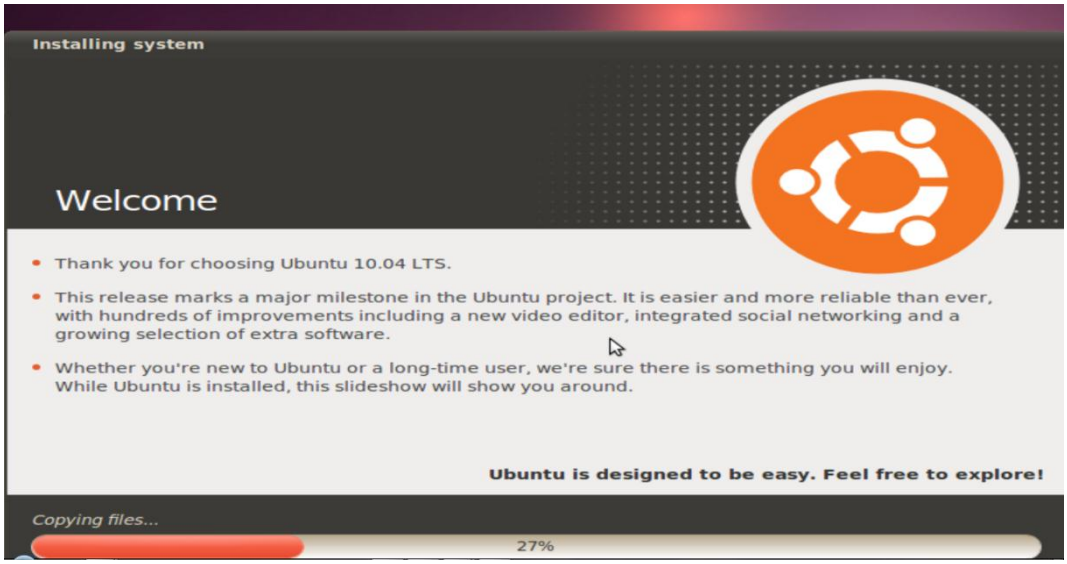
Gambar 4.5 Penamaan pc IPS dan Pemberian Password

Berdasarkan gambar 4.5 dapat dijelaskan untuk tahap selanjutnya yaitu penamaan, *username* login dan *password* untuk komputer atau pc IPS, pada tahap ini penamaan dan *username* untuk *login* yang akan digunakan adalah IPS-PC dan menggunakan *password* untuk menambah keamanan pc IPS. Tahap selanjutnya dapat dilihat pada gambar 4.6.



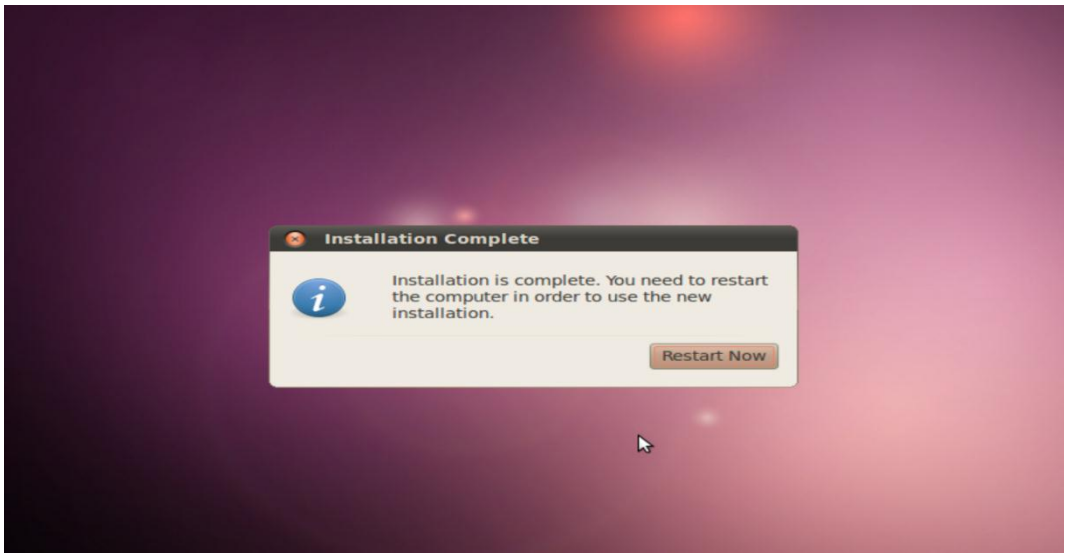
Gambar 4.6 Pengecekan konfigurasi instalasi sistem operasi

Berdasarkan gambar 4.6 pada tahap ini dilakukan pengecekan kembali apakah konfigurasi untuk sistem operasi yang akan di *install* sudah sesuai dengan yang diinginkan, apabila terdapat konfigurasi atau setelan yang tidak cocok dapat diubah kembali sebelum instalasi sistem operasi dilakukan. Setelah konfigurasi atau setelan sudah sesuai dengan keinginan maka instalasi dapat dilakukan dengan memilih tombol *install.* Berikut dibawah ini adalah tahap selanjutnya yang dapat dilihat pada gambar 4.7.



Gambar 4.7 Proses berjalannya instalasi sistem operasi

Pada gambar 4.7 dapat dilihat pada tahap ini adalah proses berjalannya instalasi sistem operasi linux ubuntu, apabila terdapat data yang kurang atau *corrupt* pada dvd atau file sistem operasi linux ubuntu maka proses instalasi akan berhenti. Tahap selanjutnya dapat dilihat pada gambar 4.8 dibawah.

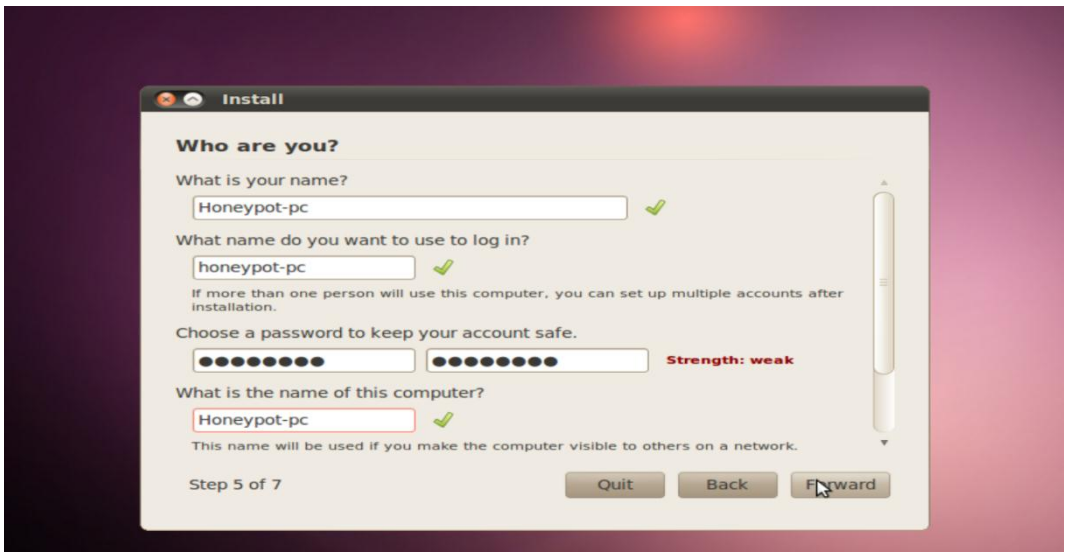


Gambar 4.8 Tahap akhir instalasi sistem operasi

Pada gambar 4.8 dapat dilihat tahap akhir dari instalasi sistem operasi, apabila instalasi berhasil dengan lancar maka sistem akan meminta untuk melakukan *restart*, pada tahap ini instalasi sudah selesai maka file atau dvd instalasi dapat dikeluarkan dari komputer dan lakukan *restart*.

4.1.2 Instalasi Komputer *Honeypot*

Pada tahapan instalasi komputer *Honeypot* tidak berbeda jauh dengan tahapan-tahapan pada saat melakukan instalasi komputer IPS, namun yang membedakan hanyalah pada tahap penamaan komputer atau pc *Honeypot* saja. Berikut adalah tahap dari penamaan untuk komputer *Honeypot* yang dapat dilihat pada gambar 4.9.



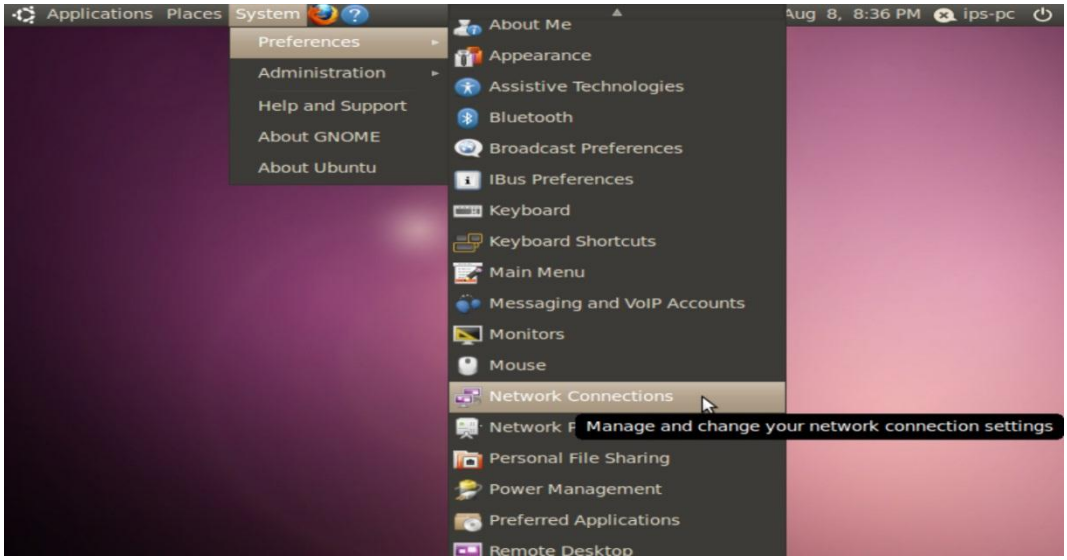
Gambar 4.9 Tahap penamaan pc honeypot

Berdasarkan gambar 4.9 dapat dilihat tahap untuk penamaan komputer atau pc *Honeypot*, penamaan dan *username* untuk *login* akan diberi nama Honeypot-pc dan akan diberi password untuk keamanan komputer tersebut.

4.2 Konfigurasi IP Address PC IPS

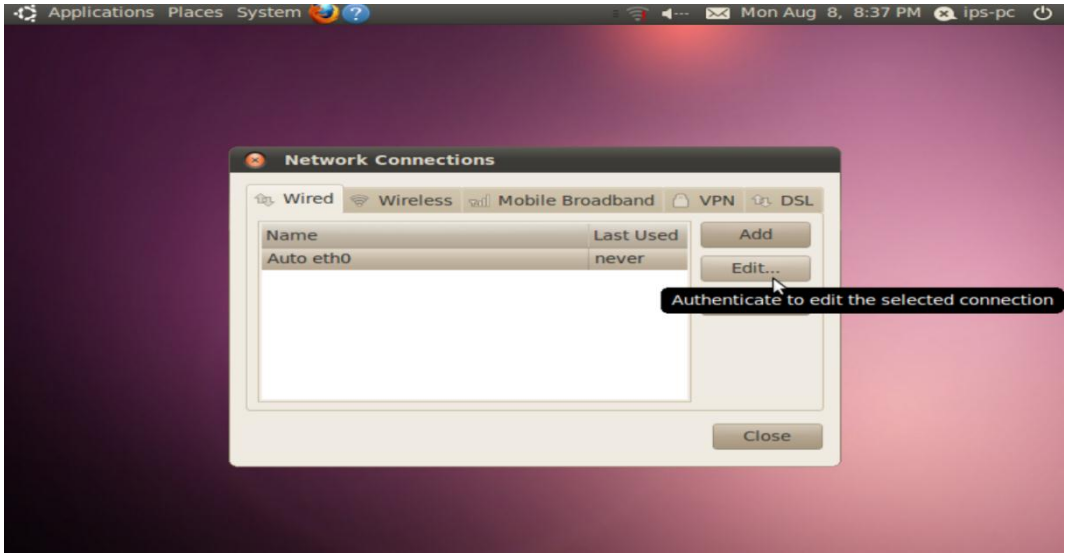
Berikut ini adalah tahapan-tahapan konfigurasi untuk pengalamatan ip address komputer atau pc IPS :

1. Masuk ke *Network Connections* untuk memasukan alamat ip pc yang terdapat pada *system* > *preferences* > *network connection* seperti yang dapat dilihat pada gambar 4.10.



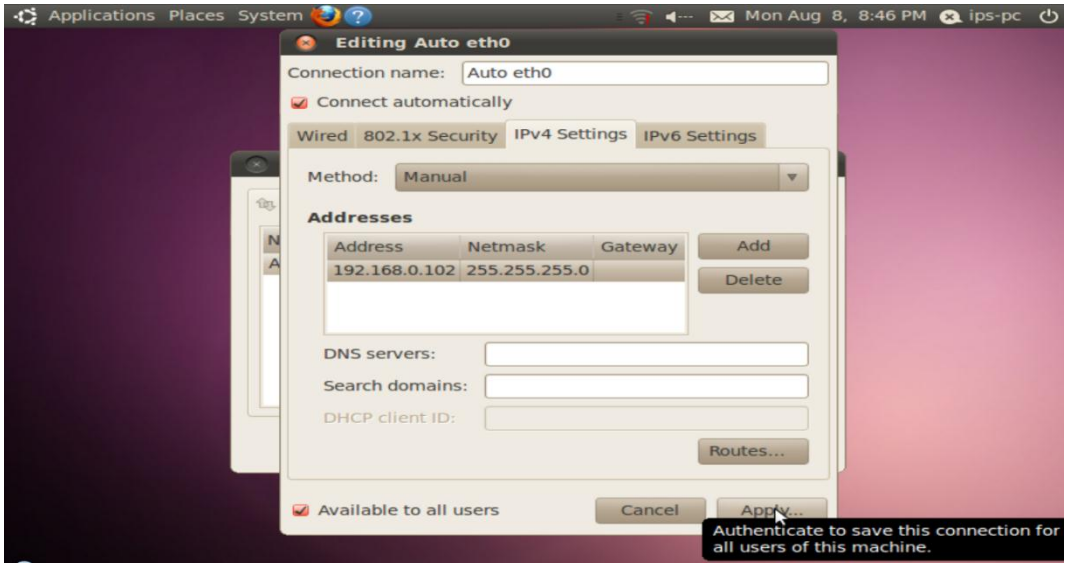
Gambar 4.10 Network connection pc IPS

2. Pilih *auto eth0* sebagai koneksi *Ethernet* atau jaringan yang akan digunakan kemudian klik edit untuk mengubah alamat ip seperti yang dapat dilihat pada gambar 4.11.



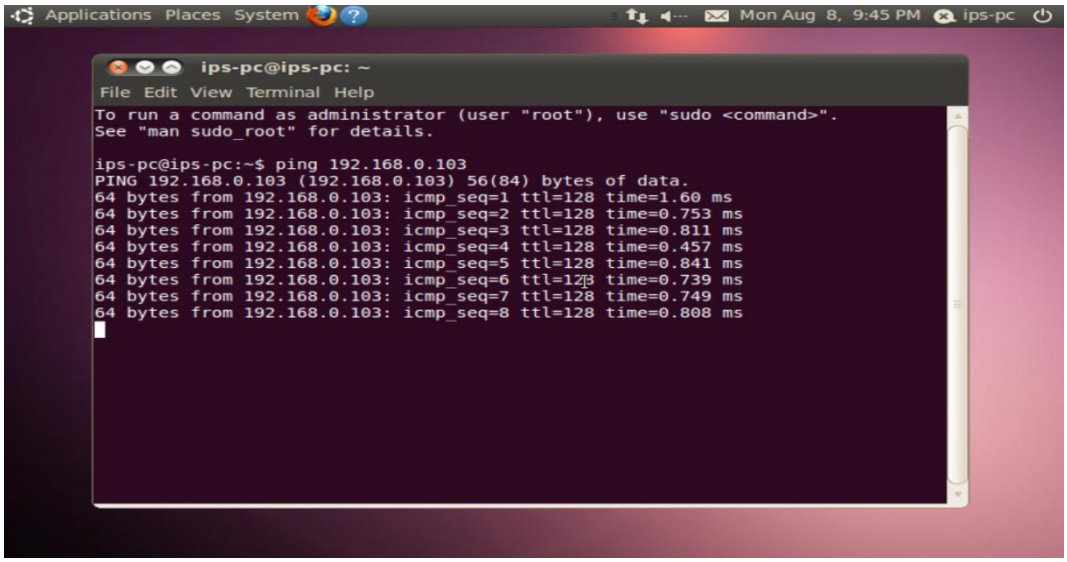
Gambar 4.11 Edit alamat ip pada pc IPS

3. Kemudian pilih IPv4 *Setting*, kemudian pilih *manual* pada bagian *method* agar pengalamatan ip dilakukan secara manual. Setelah itu masukan alamat ip yang akan digunakan yaitu 192.168.0.102 dan *netmask* 255.255.255.0 karena menggunakan ip kelas C kemudian klik *apply* seperti yang dapat dilihat pada gambar 4.12.



Gambar 4.12 Masukan alamat ip yang akan digunakan pc IPS

4. Setelah alamat ip diubah saatnya melakukan tes ping pada pc *server* yang beralamatkan 192.168.0.103 dengan cara membuka terminal kemudian ketik "*ping 192.168.0.103*" seperti yang dapat dilihat pada gambar 4.13.

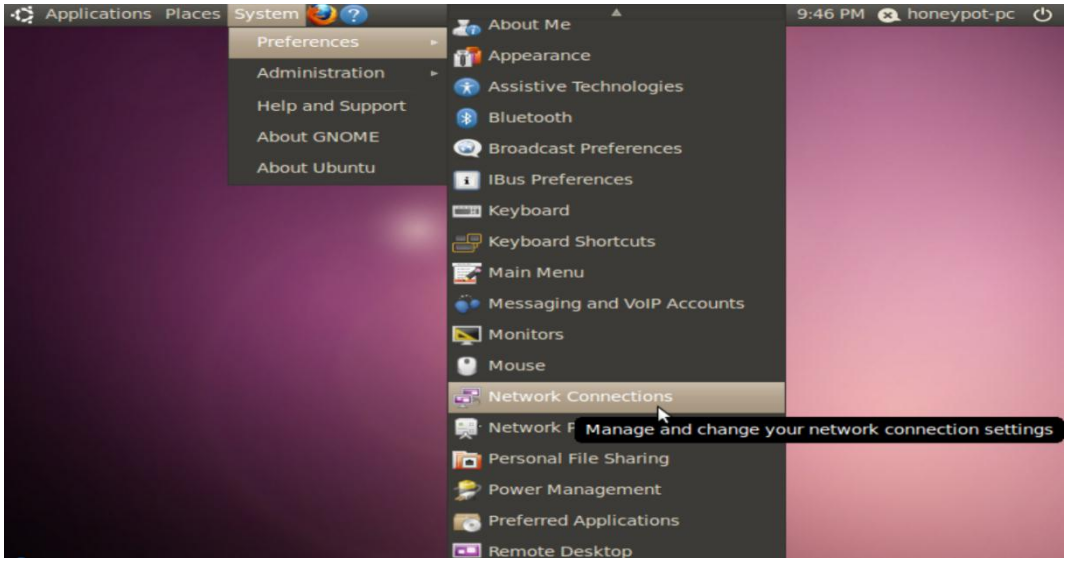


Gambar 4.13 Tes ping pc IPS terhadap pc server

4.3 Konfigurasi IP Address PC *Honeypot*

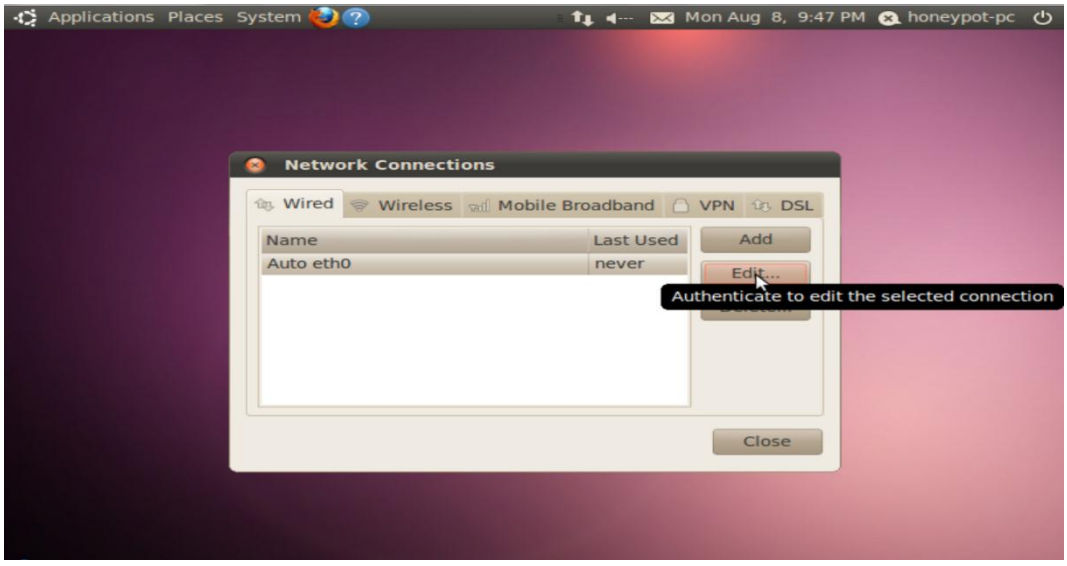
Berikut ini adalah tahapan-tahapan konfigurasi untuk pengalamatan ip address komputer atau pc IPS :

1. Masuk ke *Network Connections* untuk memasukan alamat ip pc yang terdapat pada *system* > *preferences* > *network connection* seperti yang dapat dilihat pada gambar 4.14.



Gambar 4.14 Network connection pc honeypot

2. Pilih *auto eth0* sebagai koneksi *Ethernet* atau jaringan yang akan digunakan kemudian klik edit untuk mengubah alamat ip seperti yang dapat dilihat pada gambar 4.15.



Gambar 4.15 Edit alamat ip pada pc honeypot

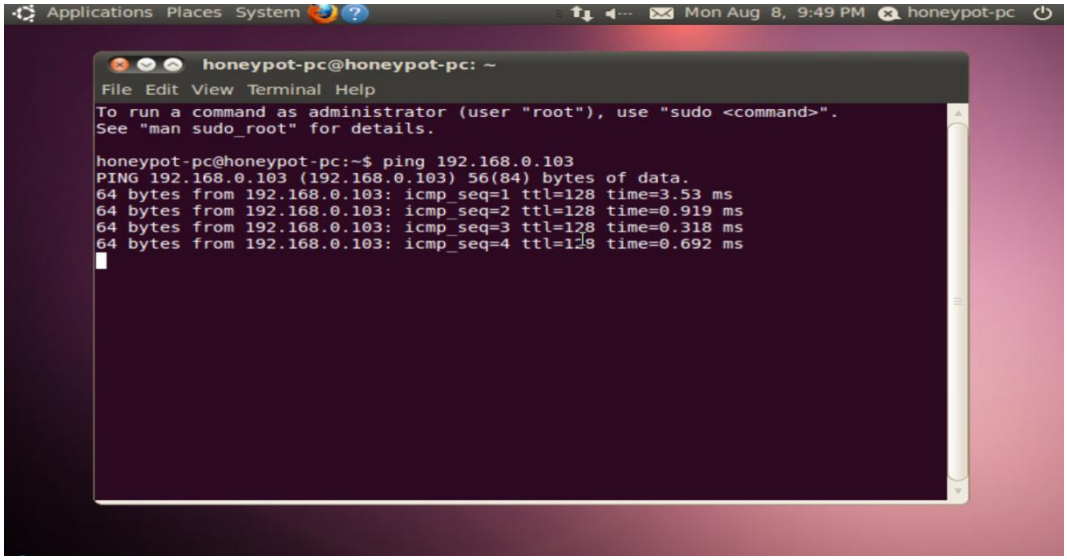
3. Kemudian pilih IPv4 *Setting*, kemudian pilih *manual* pada bagian *method* agar pengalamatan ip dilakukan secara manual. Setelah itu masukan alamat ip

yang akan digunakan yaitu 192.168.0.102 dan *netmask* 255.255.255.0 karena menggunakan ip kelas C kemudian klik *apply* seperti yang dapat dilihat pada gambar 4.16.



Gambar 4.16 Masukan alamat ip yang akan digunakan pc honeypot

4. Setelah alamat ip diubah saatnya melakukan tes ping pada pc *server* yang beralamatkan 192.168.0.103 dengan cara membuka terminal kemudian ketik "*ping 192.168.0.103*" seperti yang dapat dilihat pada gambar 4.17.

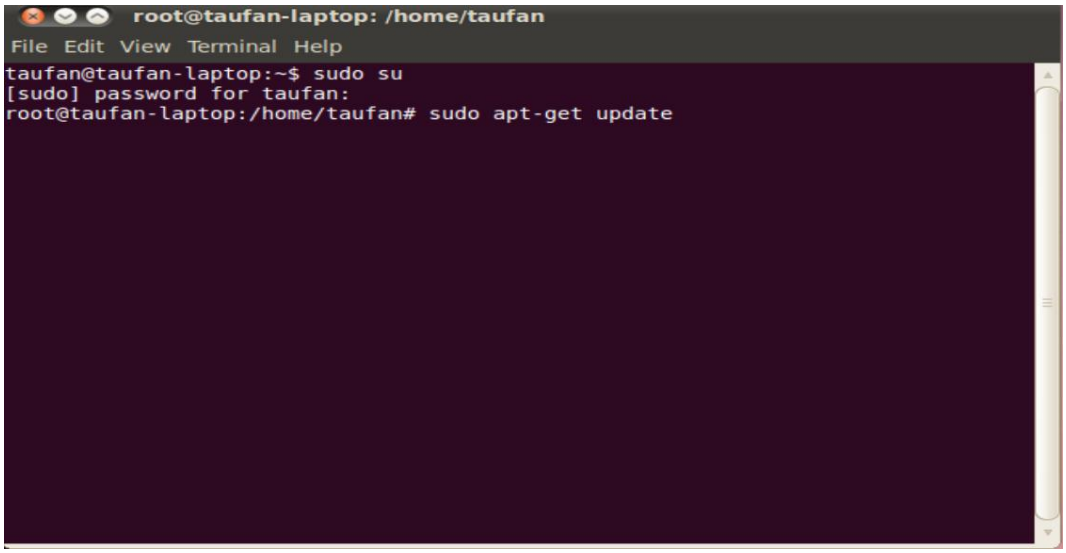


Gambar 4.17 Tes ping pc honeypot terhadap pc server

4.4 Instalasi dan Konfigurasi PSAD

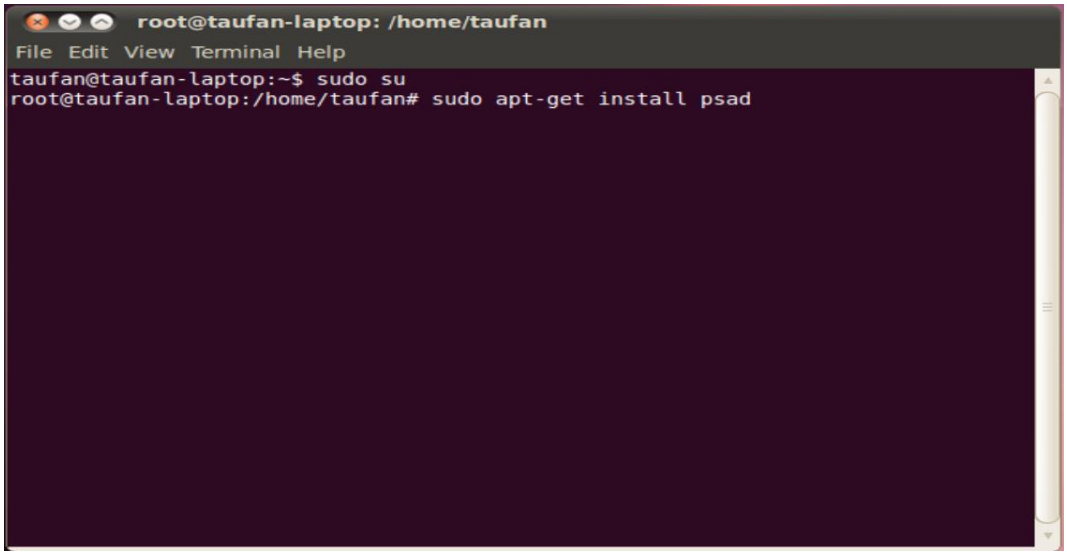
Berikut ini adalah tahapan-tahapan dari konfigurasi PSAD untuk PC atau komputer IPS yaitu sebagai berikut :

1. Pertama-tama masuk terminal, kemudian login sebagai *super user* dan lakukan *update repository* dengan mengetik "sudo apt-get update" seperti yang terlihat pada gambar 4.18.



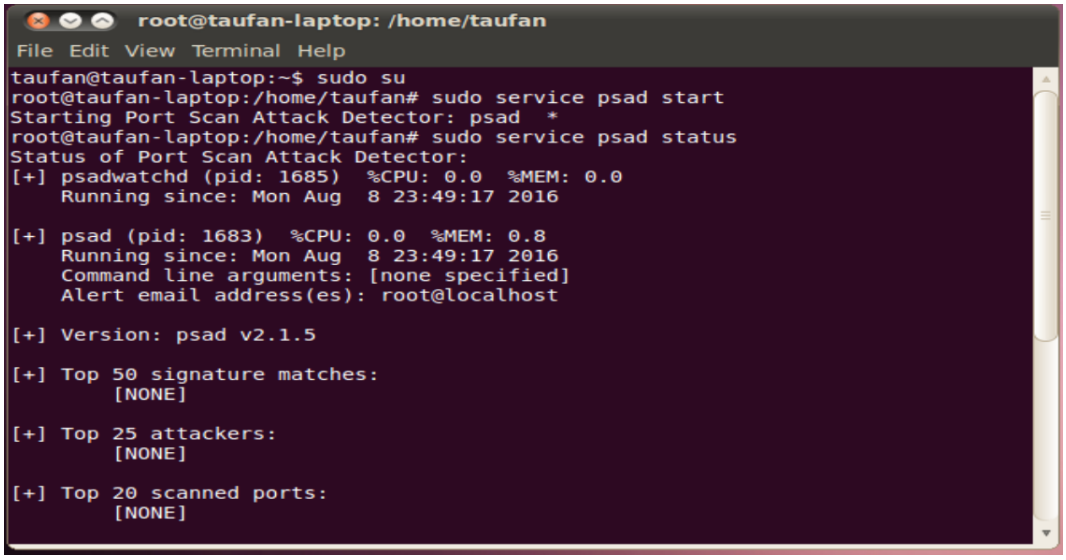
Gambar 4.18 Login SU dan update repository

2. Setelah melakukan *update repository*, selanjutnya adalah menginstal psad yang dapat dilakukan dengan mengetik "sudo apt-get install psad" atau dapat mengunduh filenya dari alamat http://www.cipherdyne.org/psad/download/ seperti yang dapat dilihat pada gambar 4.19.



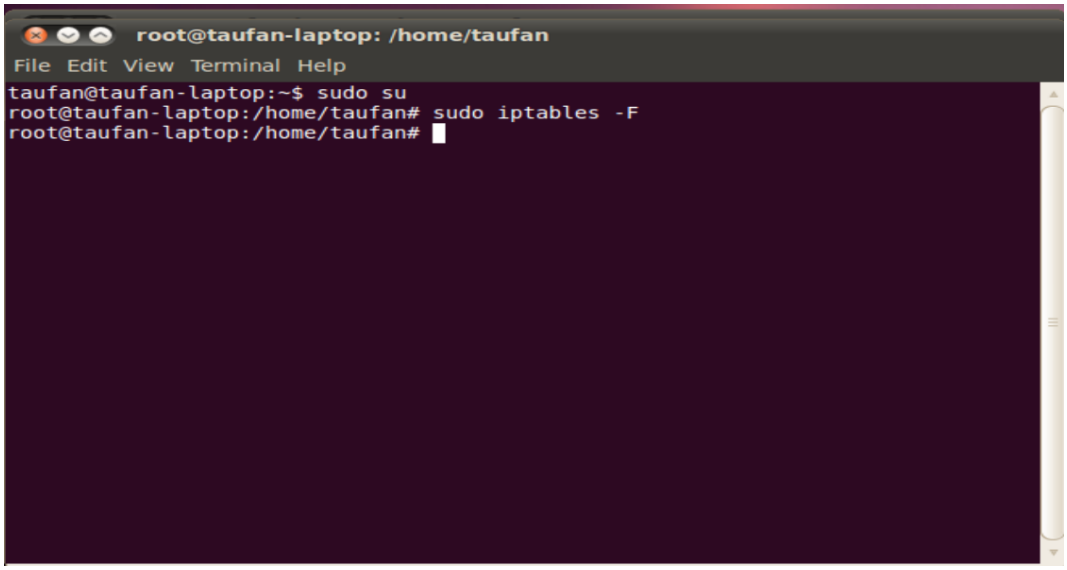
Gambar 4.19 Instalasi PSAD

3. Setelah PSAD selesai terpasang, nyalakan fitur PSAD dengan perintah "sudo service psad start". Kemudian lihat status PSAD dengan perintah "sudo service psad status" seperti yang dapat dilihat pada gambar 4.20.



Gambar 4.20 Perintah start dan status psad

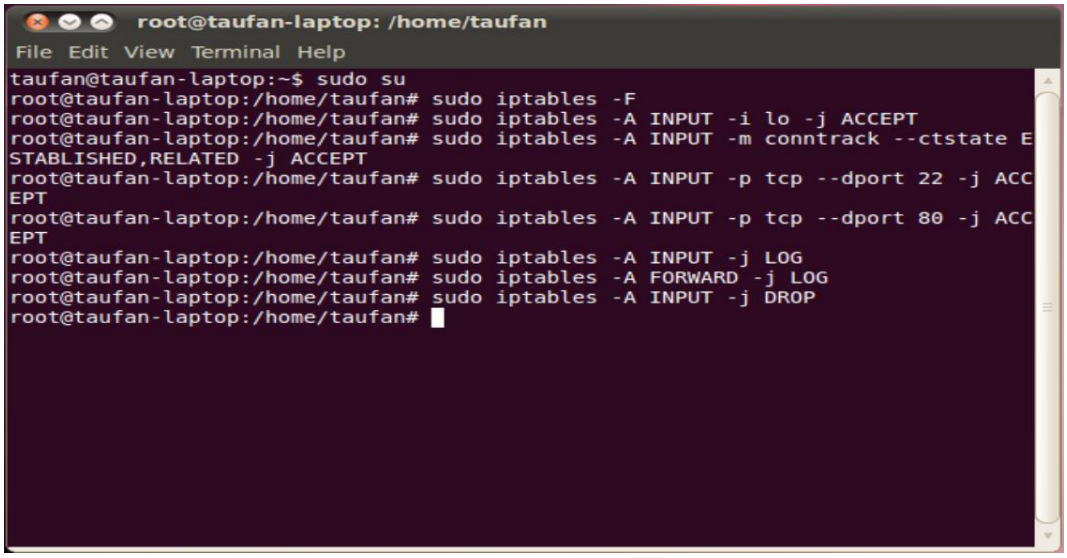
4. Selanjutnya adalah konfigurasi *iptables* atau *firewall*, sebelum melakukan konfigurasi *iptables* sebaiknya melakukan *flush iptables* dahulu agat list *iptables* data diisi dari kosong dengan mengetikan perintah "sudo iptables –F" seperti yang dapat dilihat pada gambar 4.21.



Gambar 4.21 Flush iptables

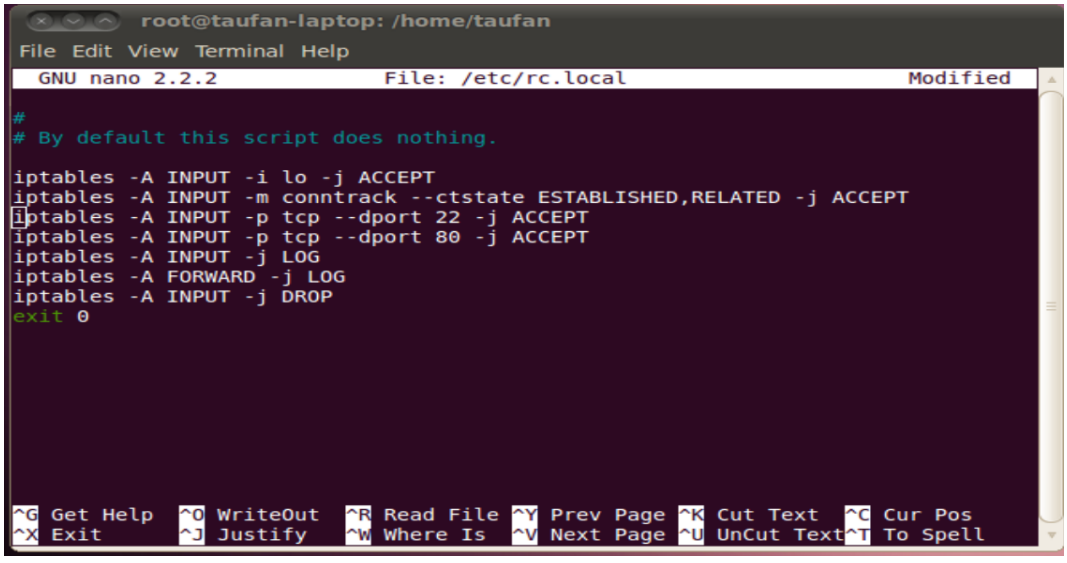
5. Setelah melakukan *flush iptables* selanjutnya akan masukan *rules-rules iptables* yang akan digunakan, adapun beberapa *rules* yang akan digunakan yaitu diantaranya:
   a. Sudo iptables –A INPUT –i lo –j ACCEPT
   b. Sudo iptables –A INPUT –m conntrack –ctstate ESTABLISHED,RELATED –j ACCEPT
   c. Sudo iptables –A INPUT –p tcp --dport 22 –j ACCEPT
   d. Sudo iptables –A INPUT –p tcp --dport 80 –j ACCEPT
   e. Sudo iptables –A INPUT –j LOG
   f. Sudo iptables –A FORWARD –j LOG
   g. Sudo iptables –A INPUT –j DROP

   Hasil dari perintah yang dimasukan dapat dilihat pada gambar 4.22 dibawah.



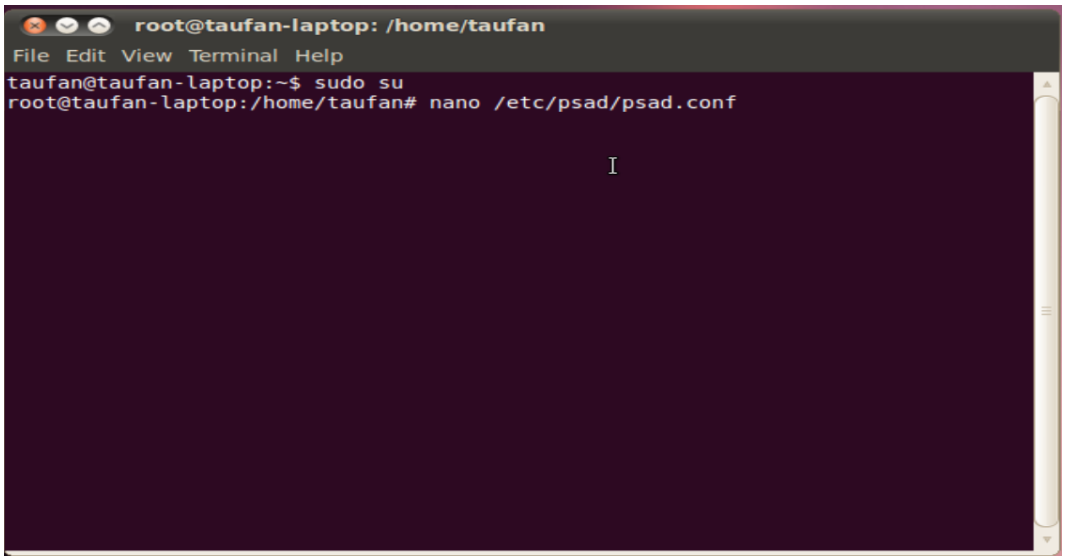
Gambar 4.22 Rules-rules iptables

6. Setelah *rules-rules iptables* terpasang, agar *rules* tidak hilang yang disebabkan apabila pc tersebut melakukan *restart* maka *rules iptables* pun akan me-*reset* ke kondisi awal. Oleh sebab itu dilakukan penyimpanan *rules-rules iptables* yang dapat dilakukan dengan memasukan kembali *rules-rules* tersebut pada file rc.local dengan melakukan perintah "nano /etc/rc.local", kemudian masukan *rules* yang digunakan dan save seperti yang dapat dilihat pada gambar 4.23



Gambar 4.23 Penyimpanan rules iptables

7. Setelah *rules-rules* tersebut disimpan, selanjutnya melakukan konfigurasi pengaturan PSAD yang dapat di ubah pada file psad.conf yang dapat dibuka melalui terminal dengan perintah "nano /etc/psad/psad.conf" seperti yang dapat dilihat pada gambar 4.24.

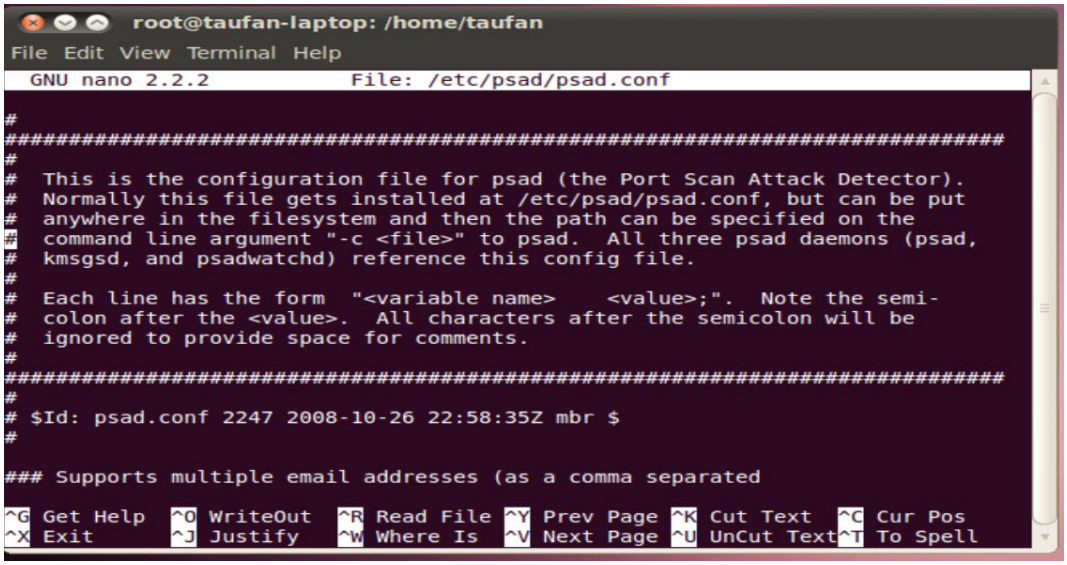


Gambar 4.24 Perintah konfig PSAD

8. Setelah masuk pada file konfigurasi psad ada beberapa setingan yang harus dirubah dari setelan *default*nya diantaranya :

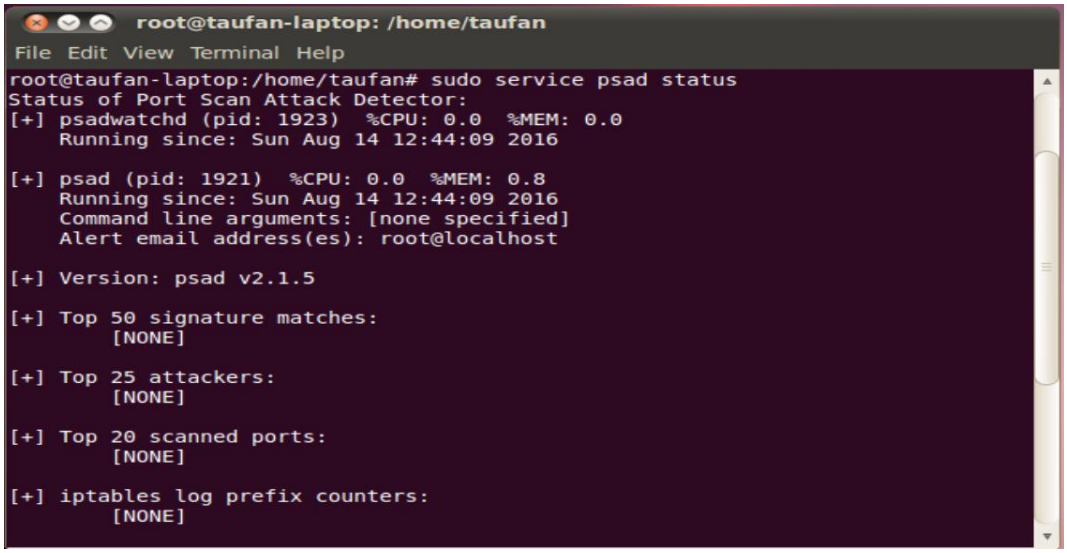
a.	EMAIL_ADDRESSES	root@localhost;
b.	HOSTNAME	IPS-pc;
c.	PORT_RANGE_SCAN_THRESHOLD	1;
d.	ENABLE_PERSISTENCE	Y;
e.	IPT_SYSLOG_FILE	/var/log/syslog;
f.	MIN_DANGER_LEVEL	2;
g.	IMPORT_OLD_SCANS	Y;
h.	ENABLE_DSHIELD_ALERTS	N;
i.	ENABLE_AUTO_IDS	Y;
j.	AUTO_IDS_DANGER_LEVEL	2;
k.	AUTO_BLOCK_TIMEOUT	3600;
l.	IPTABLES_BLOCK_METHOD	Y;

Berikut adalah tampilan dari file konfigurasi PSAD yang dapat dilihat pada gambar 4.25.



Gambar 4.25 Tampilan file konfig PSAD

9. Setelah konfigurasi PSAD dilakukan tahap selanjutnya adalah melakukan *update signature* PSAD yang dapat dilakukan dengan memasukan perintah "sudo psad –-sig-update".
10. Setelah *update signature* selesai, maka harus dilakukan *restart* pada servis PSAD dengan memasukan perintah "sudo service psad restart" dan setelah itu untuk dapat melihat status PSAD sudah berjalan dan terjadi apasaja dengan perintah "sudo service psad status" seperti yang dapat dilihat pada gambar 4.26.

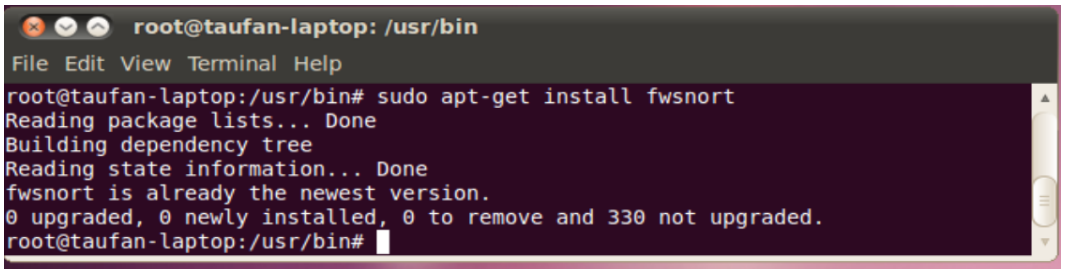


Gambar 4.26 Tampilan status PSAD

4.5 Instalasi dan Konfigurasi *Fwsnort*

Berikut ini adalah tahapan-tahapan dari konfigurasi *Fwsnort* untuk PC atau komputer IPS yaitu sebagai berikut :

1. Masuk terminal kemudian install *fwsnort* dengan memasukan perintah “sudo apt-get install fwsnort” seperti yang dapat dilihat pada gambar 4.27.

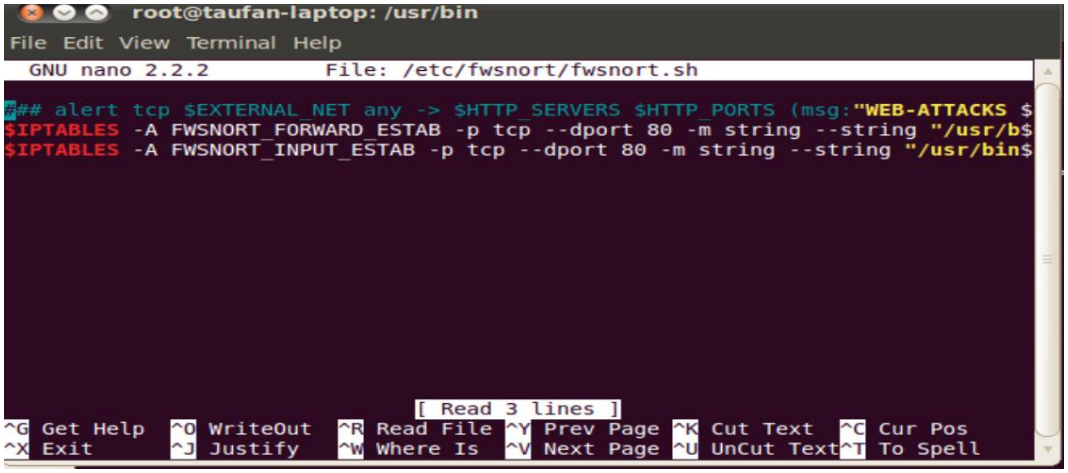


Gambar 4.27 Perintah instalasi fwsnort

2. Setelah itu lakukan *update snort rules* dengan perintah “sudo fwsnort –-update rules”
3. Selanjutnya masukan *script rules iptable* pada *fwsnort* yaitu :
   a. $IPTABLES -A FWSNORT_FORWARD_ESTAB -p tcp --dport 80 -m string --string "/usr/bin/gcc" --algo bm -m comment --comment "sid:1341; msg:WEB-ATTACKS /usr/bin/gcc command attempt; classtype:web-application-attack; rev:5; FWS:1.0.2;" -j LOG --log-ip-options --log-tcp-options --log-prefix "[5] SID1341 ESTAB "

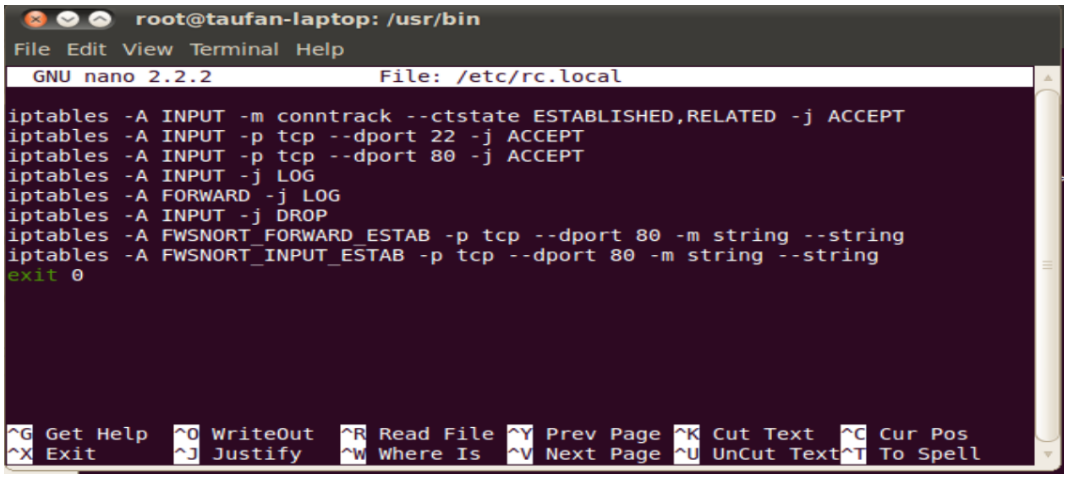
b. $IPTABLES -A FWSNORT_INPUT_ESTAB -p tcp --dport 80 -m string --string "/usr/bin/gcc" --algo bm -m comment --comment "sid:1341; msg:WEB-ATTACKS /usr/bin/gcc command attempt; classtype:web-application-attack; rev:5; FWS:1.0.2;" -j LOG --log-ip-options --log-tcp-options --log-prefix "[5] SID1341 ESTAB "

Masukan rules tersebut pada file konfig *fwsnort* dengan perintah "sudo nano /etc/fwsnort/fwsnort.sh" seperti yang dapat dilihat pada gambar 4.28.



Gambar 4.28 Rules iptables fwsnort

4. Setelah itu masukan juga *rules iptables* tersebut pada file rc.local dengan perintah "sudo nano /etc/rc.local" seperti pada gambar 4.29.

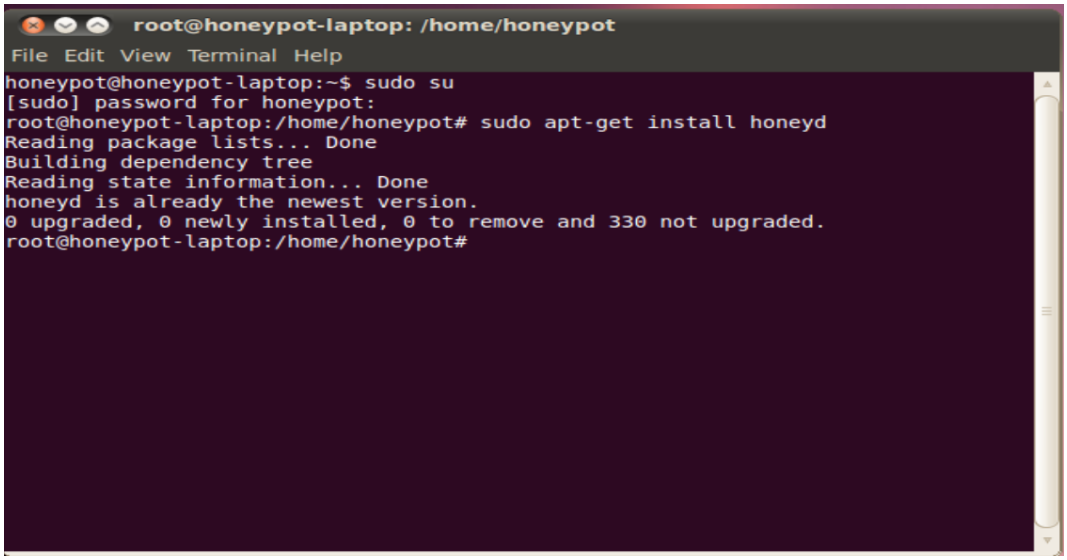
5. 

Gambar 4.29 Iptables fwsnort pada rc.local

4.6 Instalasi dan Konfigurasi *HoneyD*

Berikut ini adalah tahapan-tahapan dari konfigurasi *HoneyD* untuk PC atau komputer *honeypot* yaitu sebagai berikut :

1. Unduh dahulu file instalasi honeyd dengan memasukan perintah " sudo apt-get install honeyd" seperti yang dapat dilihat pada gambar 4.30.



Gambar 4.30 Instalasi honeyd

2. Setelah instalasi berhasil, selanjutnya buat file konfigurasi untuk honeyd dengan nama file "honeyd.conf" yang berisikan konfigurasi-konfigurasi sebagai berikut yang dapat dilihat pada table 4.1. :

Table 4.1 Konfigurasi honeyd

Crate default #set default default tcp action block Set default default udp action block Set default default icmp action block Create linux Set linux personality "Linux 2.2.14" #set linux default tcp action reset Add linux tcp port 21 open Add linux tcp port 25 open Create linux2 Set linux2 personality "Linux 2.2.14" #set linux2 default tcp action reset Add linux2 tcp port 21 open

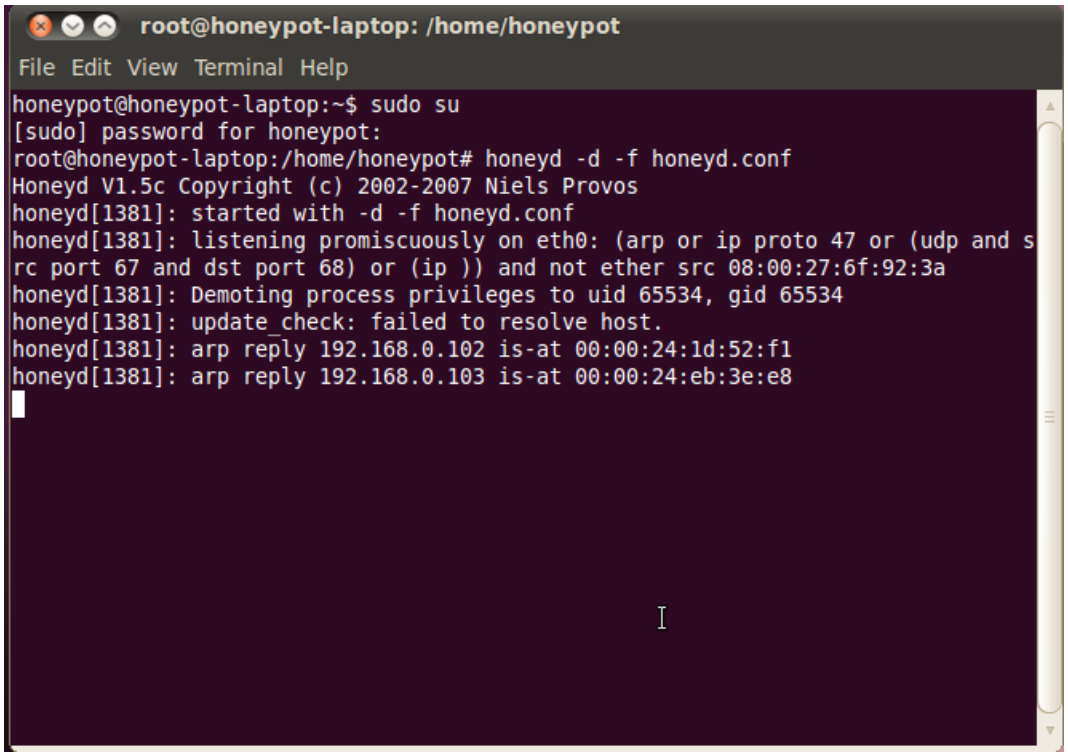
```
Add linux2 tcp port 25 open

Create linux2
Set linux2 personality “Linux 2.2.14”
#set linux2 default tcp action reset
Add linux2 tcp port 21 open
Add linux2 tcp port 25 open

Set linux Ethernet “00:00:24:ab:8c:12”
Dhcp linux on eth0
Set linux2 Ethernet “00:00:24:ab:8c:13”
Dhcp linux on eth0
Set linux3 Ethernet “00:00:24:ab;8c:14”

Bind 192.168.0.103 linux
Bind 192.168.0.102 linux2
Bind 192.168.0.104 linux3
```

3. Setelah konfigurasi dimasukan, selanjutnya lakukan tes apakah honeyd sudah dapat berjalan atau belum dengan memasukan perintah “sudo honeyd –d –f honeyd.conf”. Hasil perintah persebut dapat dilihat pada gambar 4.31.



Gambar 4.31 Status kinerja honeyd

4.7 Skenario Pengujian

Pada pengujian akan dilakukan beberapa skenario pengujian atau tes pada sistem yang telah dibangun yang terdiri dari beberapa pengujian penetrasi pada sistem diantaranya adalah :

1. Pengujian *scanning* Nmap atau zenmap.
2. Pengujian serangan DoS atau DDoS menggunakan Hping3 dan Torshammer.
3. Pengujian melakukan serangan Sql*injection.*

4.8 Pengujian Pada Sistem Keamanan IPS dan *Honeypot*

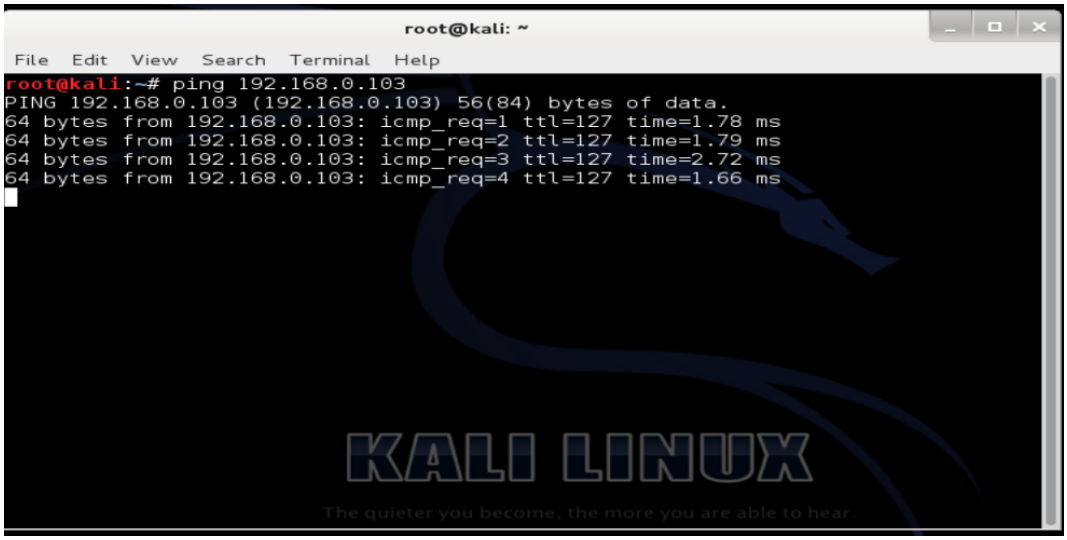
Sebelum pengujian dilakukan pastikan pada sistem IPS bahwa ip komputer untuk melakukan simulasi serangan tidak masuk dalam list blokir dan sebelum melakukan skenario pengujian serangan selanjutnya, pada komputer IPS harus dilakukan dahulu *flush* ip yang di blokir agar komputer penyerang dapat melakukan kembali pengujian serangan. Alamat untuk dilakukan pengujian adalah sebagai berikut :

Table 4.2 Alamat pc pengujian

Alamat IP	Keterangan
192.168.0.103	PC *Server*
192.168.0.102	PC IPS
192.168.0.104	PC *Honeypot*
192.168.1.123	PC Penyerang

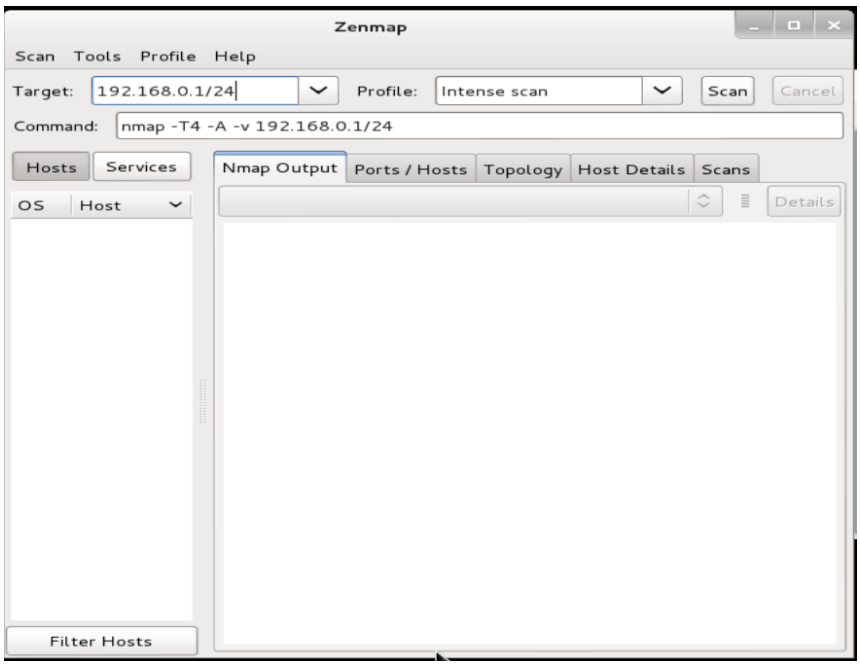
4.8.1 Pengujian *Port Scanning* Pada Sistem Keamanan

Pada pengujian *port scanning* ini akan menggunakan *tools* nmap atau zenmap yang terdapat pada sistem operasi kali linux. Untuk memulai pengujian coba dahulu melakukan ping dari pc penyerang menuju pc *server* apakah sudah terkoneksi atau belum seperti yang dapat dilihat pada gambar 4.32.



Gambar 4.32 koneksi pc penyerang pada server

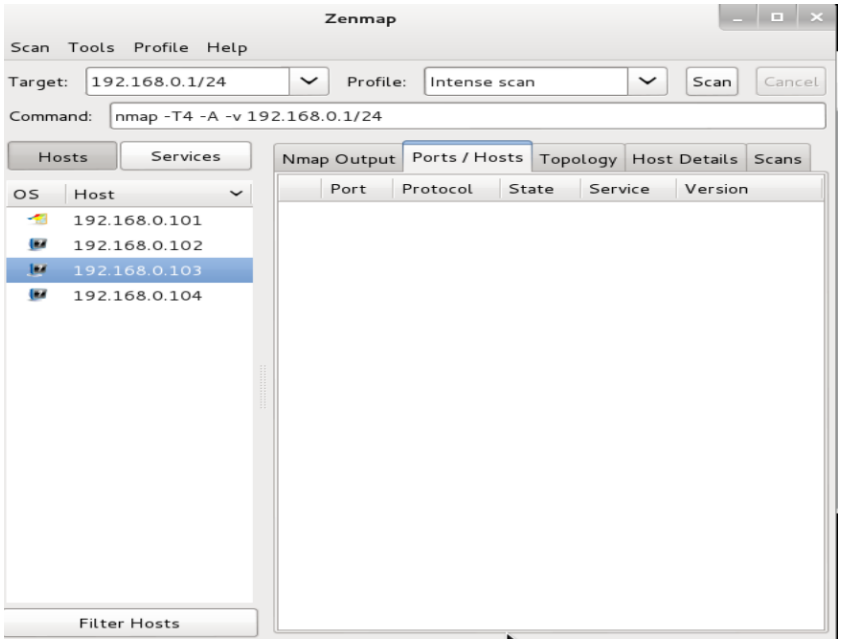
Setelah terkoneksi maka tahap selanjutnya adalah melakukan *scanning* pada *server* menggunakan zenmap dengan memasukan alamat ip 192.168.0.1/24 pada *tools* zenmap, dimana ip pc *server* terdapat pada subnet *class* ip tersebut seperti pada gambar 4.33.



Gambar 4.33 Tahap awal port scanning

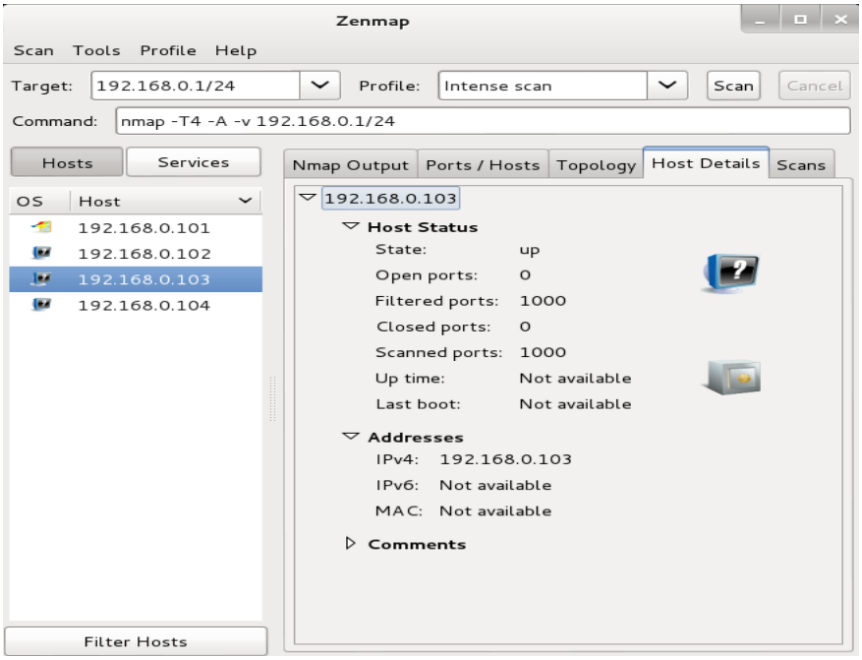
Setelah ip dimasukan maka akan dilakukan *intense scan*, dimana zenmap akan melakukan *scan* pada setiap alamat ip pada subnet tersebut yang sedang aktif

atau terkoneksi pada jaringan. Hasil dari *scanning* zenmap dapat dilihat pada gambar 4.34.



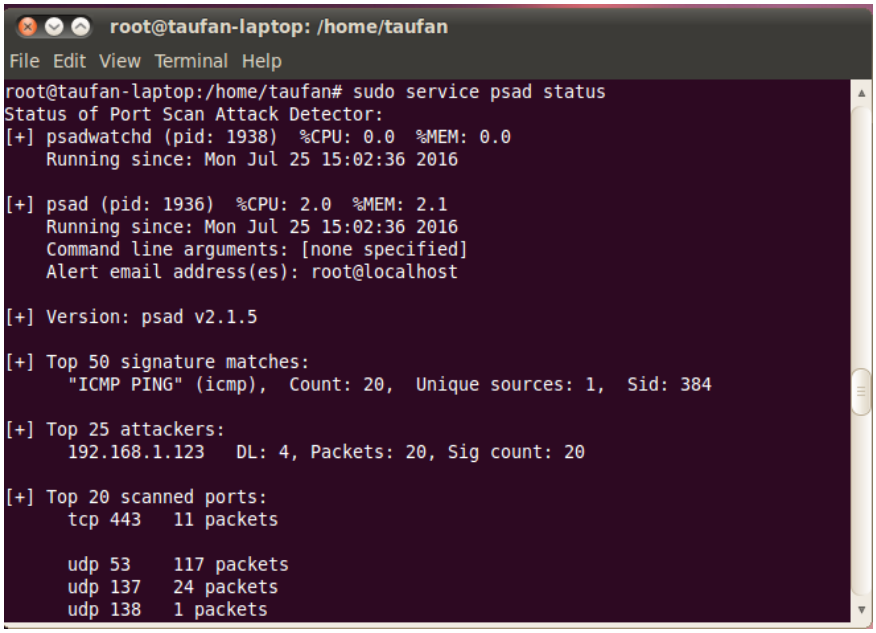
Gambar 4.34 Hasil port scanning

Pada gambar 4.34 terlihat hasil *scanning* pada pc *server* terlihat namun pada daftar *port* yang terbuka tidak akan tampil dikarenakan sudah dilakukan blokir oleh pc IPS dan pada bagian *host details* pun tidak akan tampil karena sudah terblokir juga koneksi jaringan pada pc penyerang seperti pada gambar 4.35.



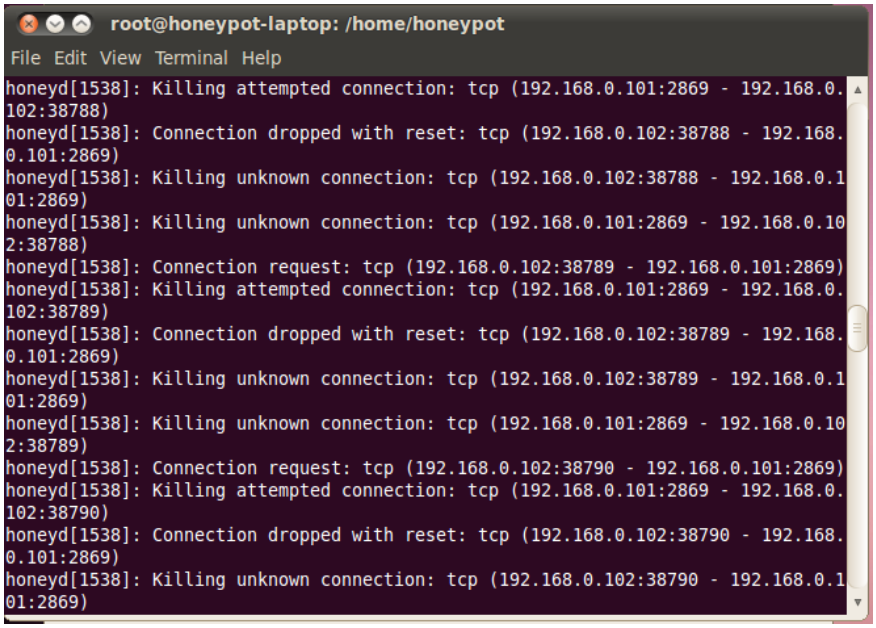
Gambar 4.35 Hasil scanning host detail

Dan pada pc ips pun terdapat *log* dan status ip penyerang yang mencoba melakukan *scanning* pada pc *server* seperti yang dapat dilihat pada gambar 4.36.



Gambar 4.36 Status PSAD port scanning

Dan pada pc *honeypot* terdapat log dimana terdapat koneksi yang mencoba untuk memasuki setiap alamat ip aktif pada jaringan seperti yang terlihat pada gambar 4.37.

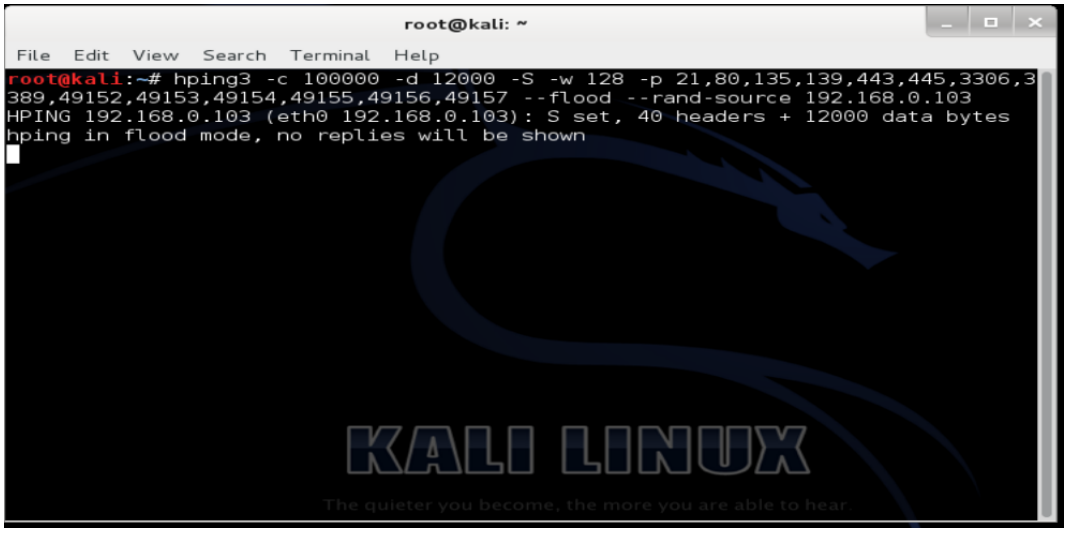


Gambar 4.37 Aktifitas honeyd pada port scanning

Hasil dari pengujian ini dapat disimpulkan bahwa ketika penyerang ingin mencoba untuk melakukan *scanning port* pada *server*, PSAD akan mendeteksi dan dengan bantuan iptables dapat memblokir usaha tersebut, dan honeypot akan mendeteksi juga usaha tersebut dan akan berusaha mengecoh penyerang dengan informasi palsu apabila sistem IPS tidak dapat menanganinya.

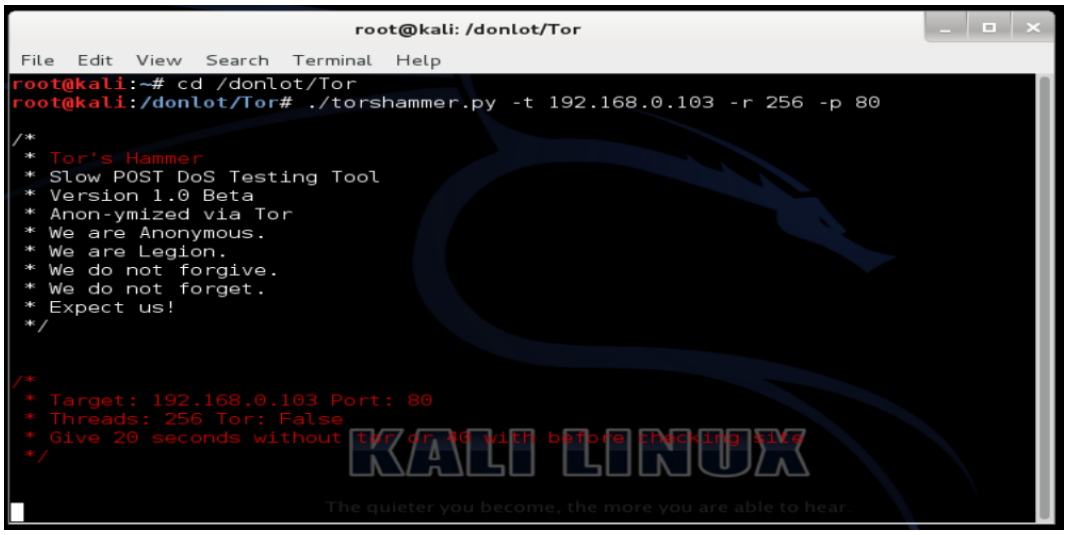
4.8.2 Pengujian *DoS* atau *DDoS* Pada Sistem Keamanan

Pada pengujian DoS atau DDoS akan menggunakan *tools* Hping3 dan *torshammer*. Sebelum melakukan pengujian lakukan dahulu *flush* pada ip pc penyerang agar dapat melakukan pengujian selanjutnya. Untuk pengujian ini pertama-tama buka aplikasi hping3 yang sudah terinstal pada pc penyerang dan lakukan serangan pada pc server dengan perintah “hping3 –c 100000 –d 12000 –S –w 128 –p 21,80,135,139,443,445,3306,3389,49152,49153,49154,49155,49156,49157 –-flood –-rand-source 192.168.0.103 ” seperti yang terlihat pada gambar 4.38.



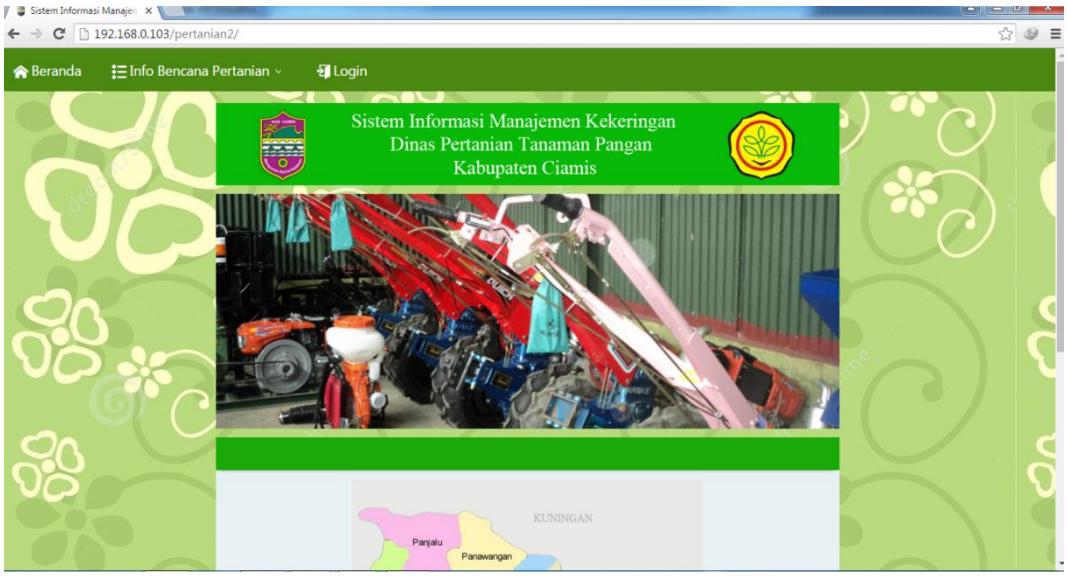
Gambar 4.38 Serangan hping3 pada server

Dan pada *tools Torshammer* akan menyerang menggunakan perintah "./torshammer.pt –t 192.168.0.103 –r 256 –p 80" seperti yang terlihat pada gambar 4.39.



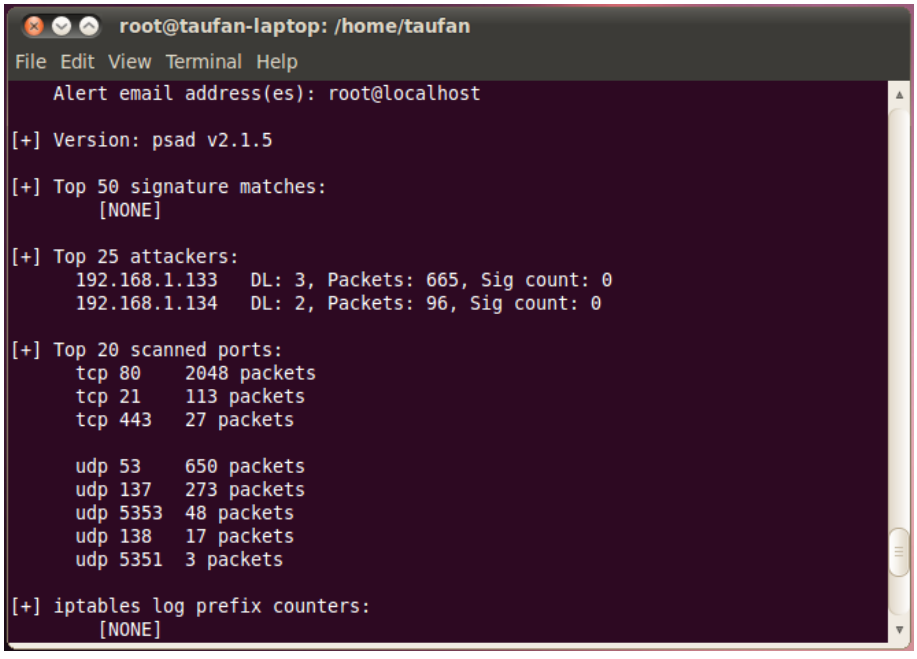
Gambar 4.39 Serangan torshammer pada server

Setelah serangan dilancarkan maka akan dicoba mengakses *website* yang terdapat pada pc *server*, apakah *website* masih bisa di akses atau tidak. Pada pc lain akan di coba membuka *website* yang terdapat pada *server* dan hasilnya *website* tersebut dapat dibuka seperti yang terlihat pada gambar 4.40



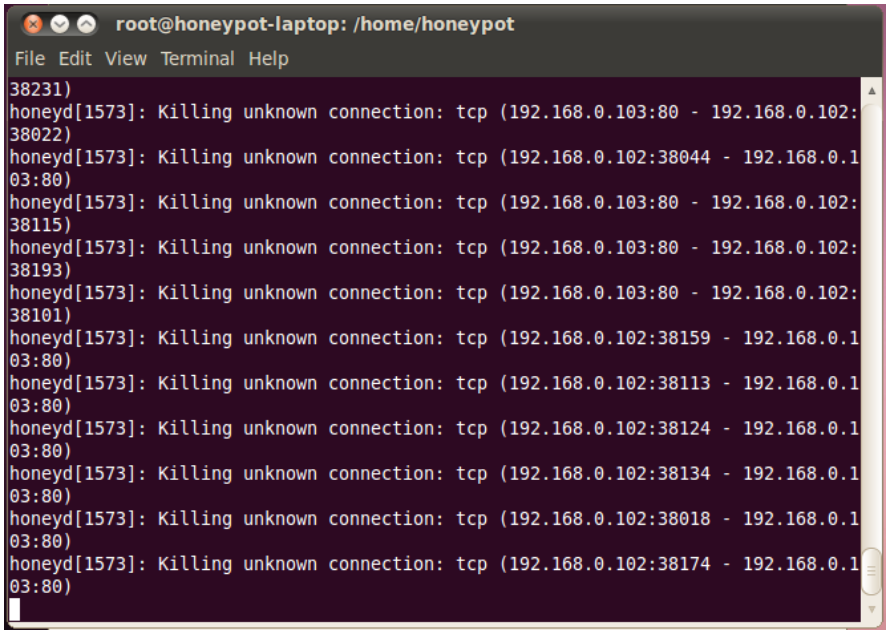
Gambar 4.40 Akses website pengujian DoS

Sedangkan pada pc IPS terekam data serangan yang terjadi pada pc *server* seperti yang dapat dilihat pada gambar 4.41.



Gambar 4.41 Status PSAD pengujian DoS

Dan pada pc *honeypot* terlihat aktifitas jaringan pada alamat server, dimana terjadi pemutusan koneksi pada alamat ip server karena adanya usaha penyerangan seperti yang terlihat pada gambar 4.42

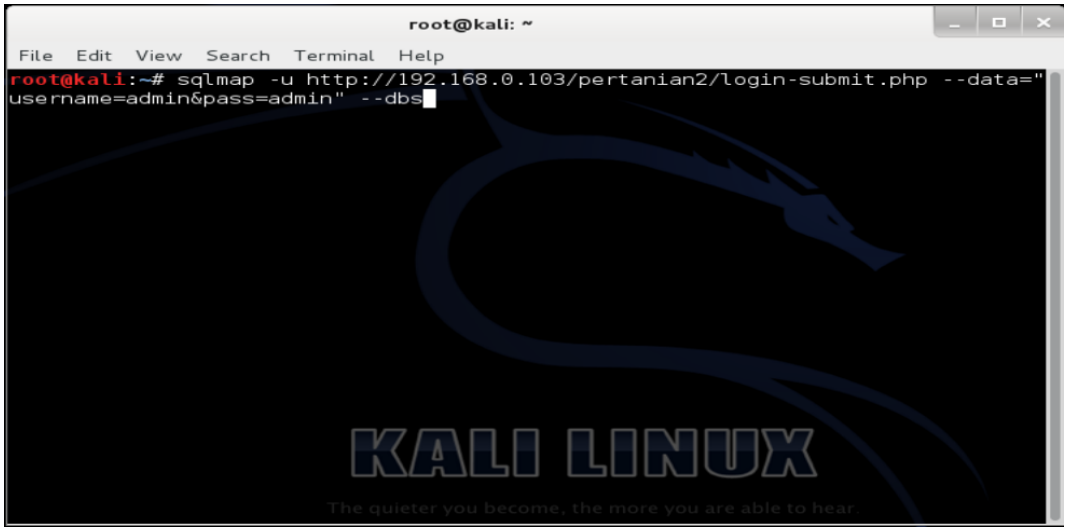


Gambar 4.42 Aktifitas honeyd pengujian DoS

Dari hasil pengujian DoS atau DDoS dapat disimpulkan sistem keamanan IPS akan memblokir penyerang karena berusaha mengirimkan paket yang cukup besar secara terus menerus, karena pada konfigurasi PSAD terdapat *danger level* dimana bila ada suatu alamat ip yang mencoba mengirimkan paket yang besar dia akan menolak koneksi jaringan tersebut dan memblokirnya.

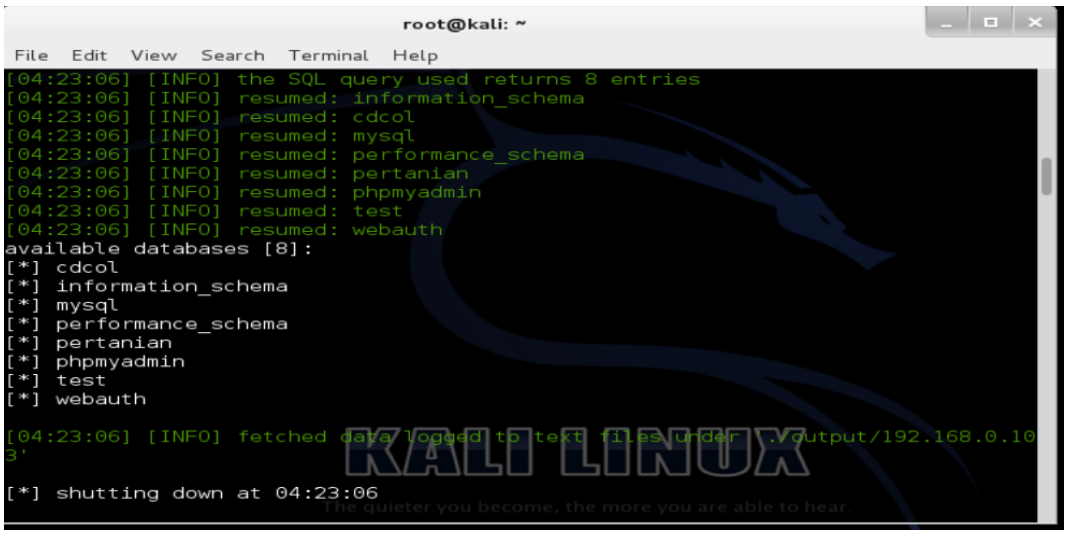
4.8.3 Pengujian Sql*injection* Pada Sistem Keamanan

Pada pengujian ini akan dilakukan sql*injection* menggunakan *tools* sqlmap yang sudah terdapat pada sistem operasi kali linux. Untuk tahap awal pengujian ini akan dilakukan dahulu *scanning database* pada pc *server* dengan memasukan perintah "sqlmap –u http://192.168.0.103/pertanian2/login-submit.php --data="username=admin&pass=admin" --dbs" pada sqlmap seperti yang dapat dilihat pada gambar 4.43.



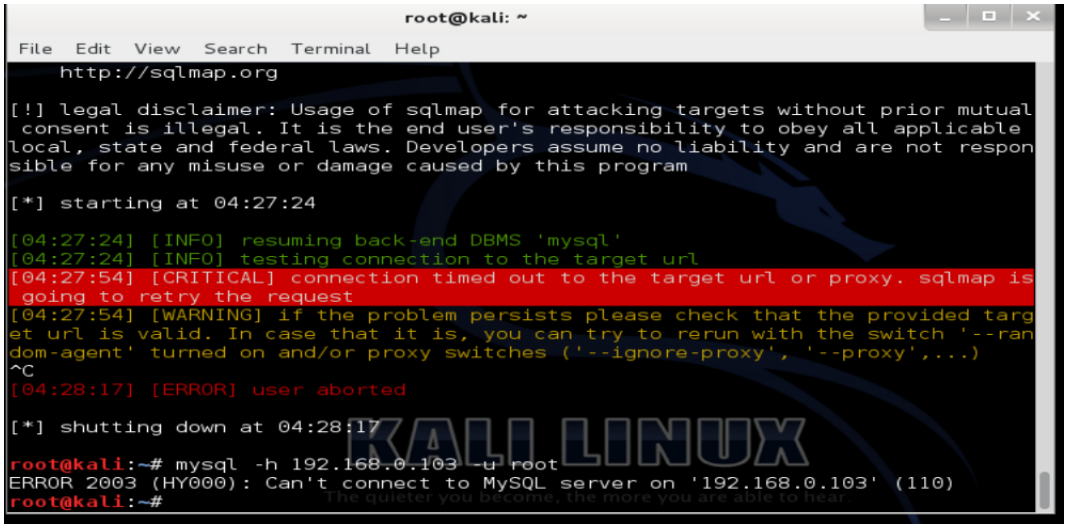
Gambar 4.43 Perintah scan database pengujian sqlinjection

Pada percobaan *scanning database*, peyerang masih dapat memperoleh data pada server seperti yang dapat dilihat pada gambar 4.44.



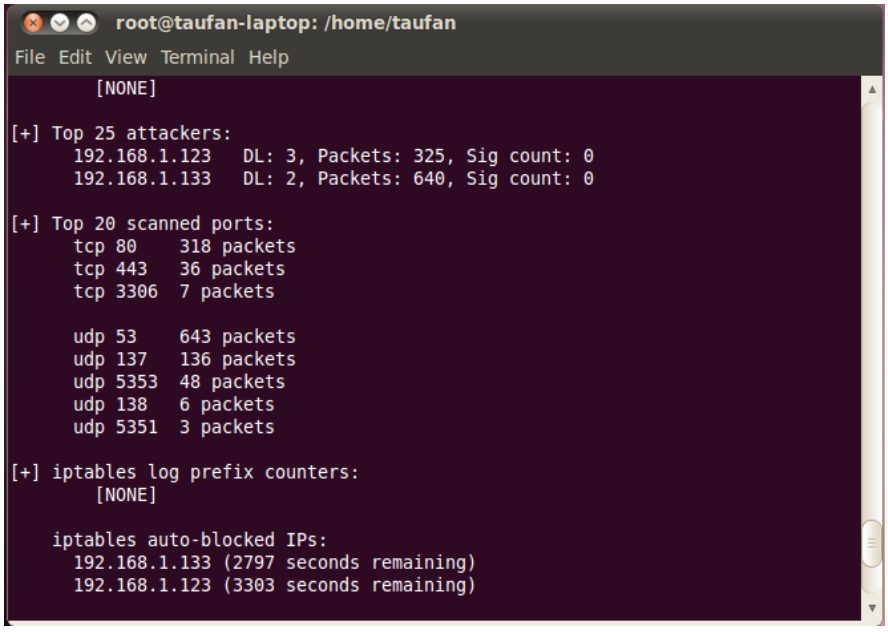
Gambar 4.44 Hasil scan database pengujian sqlinjection

Namun ketika akan melakukan koneksi pada mysql pada pc *server*, ternyata penyerasng sudah tidak dapat melakukan koneksi karena koneksi pc penyerang sudah terputus dari *server* karena diduga terdapat indikasi-indikasi mencurigakan yang ditangkap pc IPS seperti yang terlihat pada gambar 4.45



Gambar 4.45 Hasil koneksi mysql pengujian sqlinjection

Dan berikut ini adalah tampilan status pada PSAD yang terdapat pada pc IPS yang dapat dilihat pada gambar 4.46.



Gambar 4.46 Status PSAD pengujian sqlinjection

Dari hasil pengujian sql*injection* dapat disimpulkan, ternyata *honeypot* tidak dapat mengatasi serangan tersebut dan PSAD masih dapat mendeteksi usaha penyerangan dan memasukannya dalam list blokir.

4.9 Kesimpulan Hasil Pengujian pada Sistem keamanan IPS dan *Honeypot*

Dari hasil pengujian yang dilakukan, ternyata sistem keamanan IPS menggunakan PSAD cukup membantu dalam mengamankan jaringan karena mampu untuk memblokir lalulintas data penyerang dan menyimpan *log* serangan yang dapat digunakan oleh admin untuk dipelajari.

Sedangkan dari sisi kinerja *Honyepot* sudah dapat membantu dengan mengecoh penyerang apabila tidak tertangani oleh IPS, namun masih terdapat kekurangannya yaitu *honeyd* sering memblokir ip address yang mengakses ke *server* dan bukan penyerang karena masih terdapat konfigurasi yang belum cocok.