MODUL PRAKTIKUM

KEAMANAN INFORMASI DAN JARINGAN

UNIVERSITAS TEKNOLOGI MATARAM

2019

Jl. Kampus Universitas Teknologi Mataram, Kekalik, Mataram

MODUL PRAKTIKUM

Daftar Isi

Cover 1
Lembar Pengesahan 2
Daftar Isi 3

Instalasi Sistem Operasi Server Linux 4
Instalasi Sistem Operasi Penestrasi 43
Management File 50
Footprinting 54
Password Management 57
Network Scanning & Enumeration 61
Denial Of Service Attack (Dos) 69
Brute Force Attack 73
Firewall (Iptables) & Blocking Nmap 77
Firewall (Iptables) & Blocking Hping3 81
Intrusion Detection System (IDS) 84
Crypthography 97

1 INSTALASI SISTEM OPERASI SERVER LINUX

A. POKOK BAHASAN

1. Melakukan instalasi sistem operasi penestrasi dan server untuk percobaan
2. Mengenal tools keamanan sistem operasi penestrasi dan server.

B. TUJUAN

setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

1. Membangun sistem komputer yang aman.
2. Mengenal kelemahan untuk sistem komputer.

C. PERALATAN

1. Sistem Operasi Linux Ubuntu Server 14.04

D. PERCOBAAN

1. Persiapan Instalasi

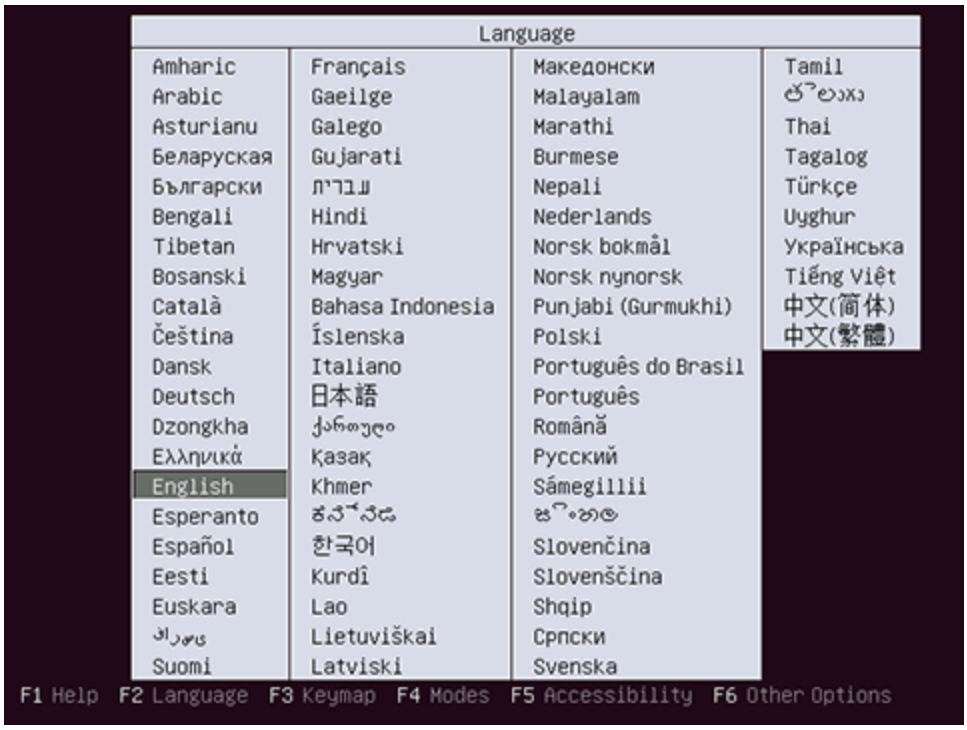
Untuk menginstall Ubuntu 14.04 Trusty Tahr versi server, diperlukan:

- Ubuntu 14.04 Trusty Tahr versi server

  Media instalasi disarankan menggunakan *CD/DVD*. Jika menggunakan *USB flash drive*, proses instalasi membutuhkan pengaturan *archive mirror country* setelah bagian pengaturan jaringan.

2. Instalasi Sistem

Lakukan *booting* komputer menggunakan media instalasi Ubuntu 14.04 Trusty Tahr versi server yang digunakan. Selanjutnya, pilih bahasa yang akan digunakan dalam proses instalasi.

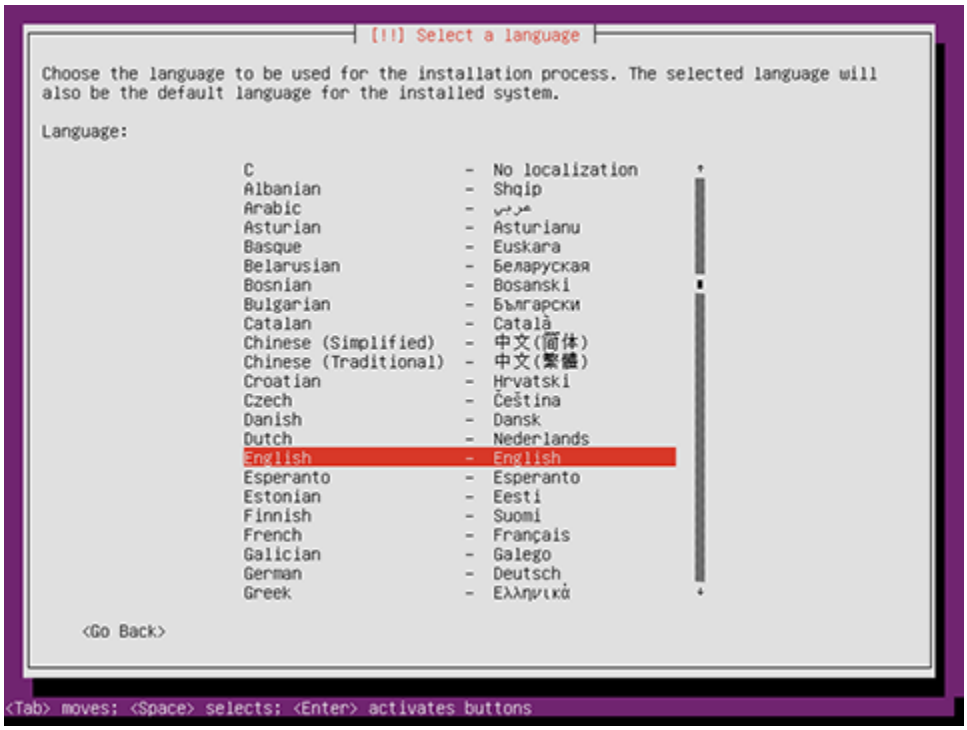


Pilih opsi *Install Ubuntu Server*.



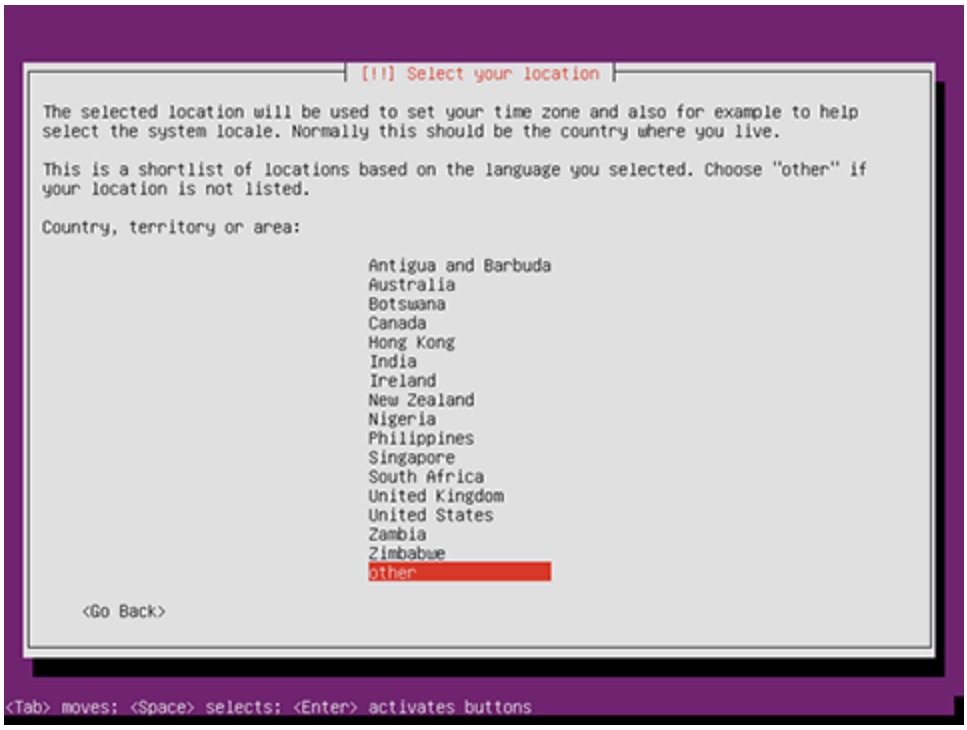
3. Pemilihan Bahasa

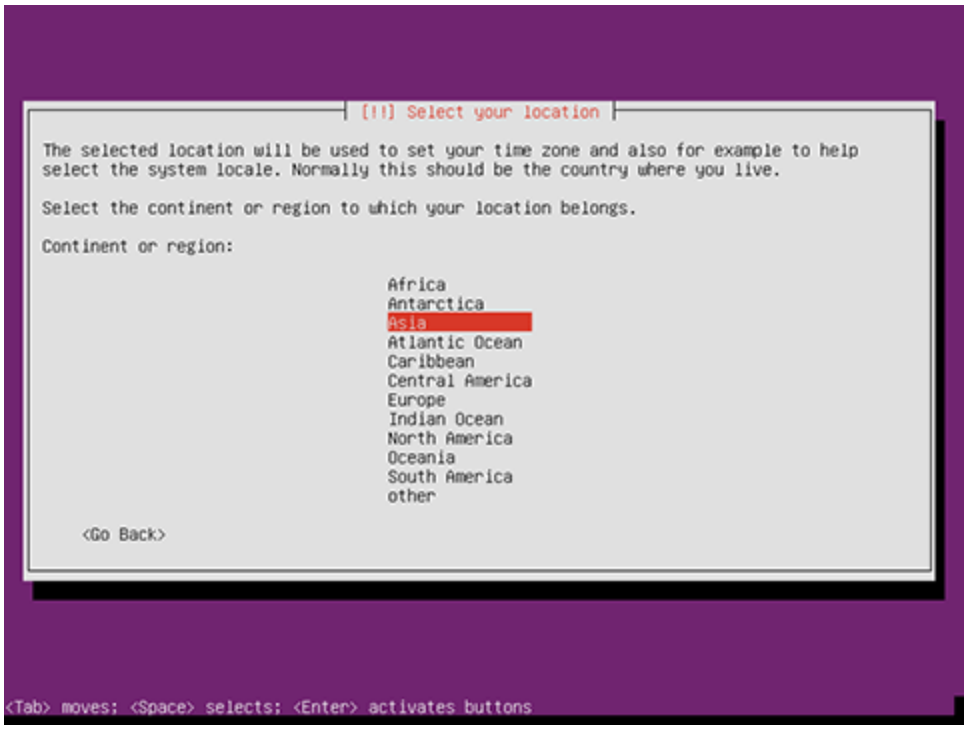
Pilih kembali bahasa yang akan digunakan dalam proses instalasi. Pilihan bahasa disini juga akan digunakan sebagai bahasa default sistem yang diinstall.

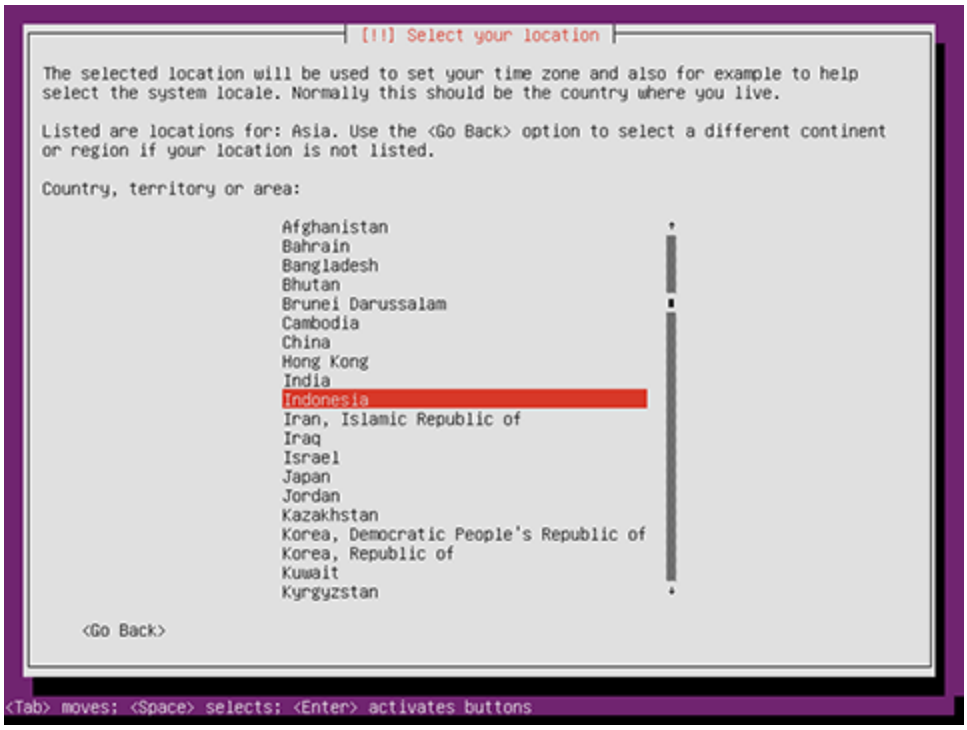


4. Penentuan Lokasi

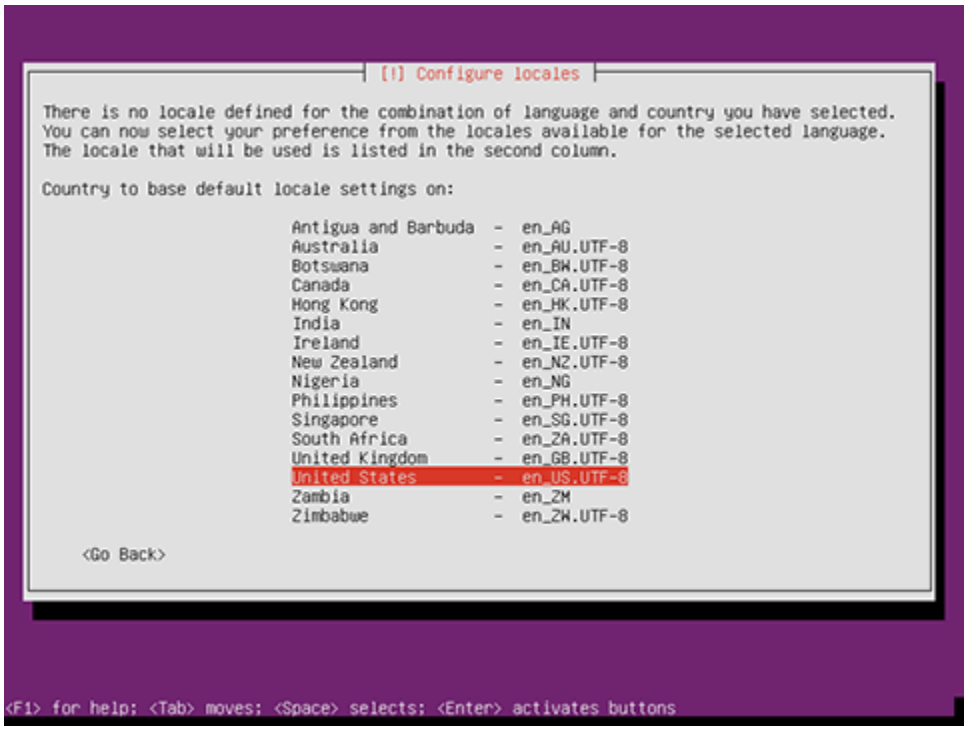
Selanjutnya, pilih lokasi.


[!!] Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.
Country, territory or area:
Antigua and Barbuda
Australia
Botswana
Canada
Hong Kong
India
Ireland
New Zealand
Nigeria
Philippines
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons


[!!] Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
Select the continent or region to which your location belongs.
Continent or region:
Africa
Antarctica
Asia
Atlantic Ocean
Caribbean
Central America
Europe
Indian Ocean
North America
Oceania
South America
other
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons



Dikarenakan kita mengkombinasikan bahasa dan lokasi yang berbeda (dalam tutorial ini *English* untuk bahasa dan *Indonesia* untuk lokasi), sementara tidak ada pengaturan standar (seperti zona waktu, format bilangan, dll) untuk kombinasi ini, proses instalasi akan meminta kita untuk memilih salah satu pengaturan standar yang tersedia. Dalam tutorial ini digunakan *en_US.UTF-8*.

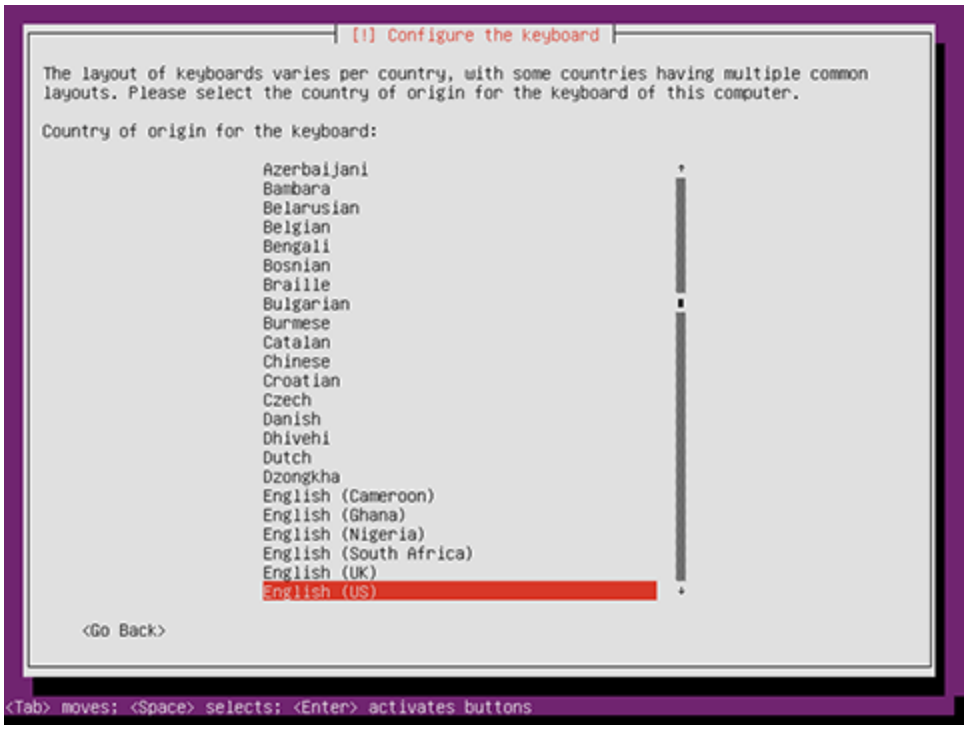


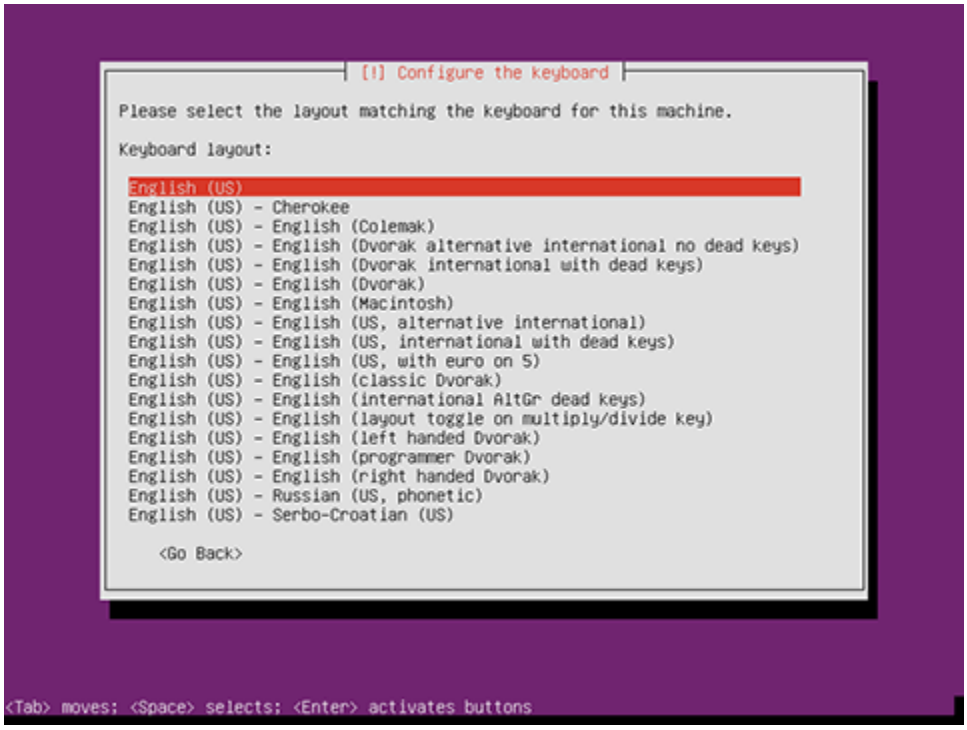
5. Penentuan *Keyboard*

Proses selanjutnya menentukan jenis layout *keyboard* yang digunakan. Klik tombol *No*, maka kita akan diminta memilih jenis layout *keyboard* dari daftar yang ada.



Secara umum, jenis layout *keyboard* yang digunakan di Indonesia adalah jenis *English (US)*.

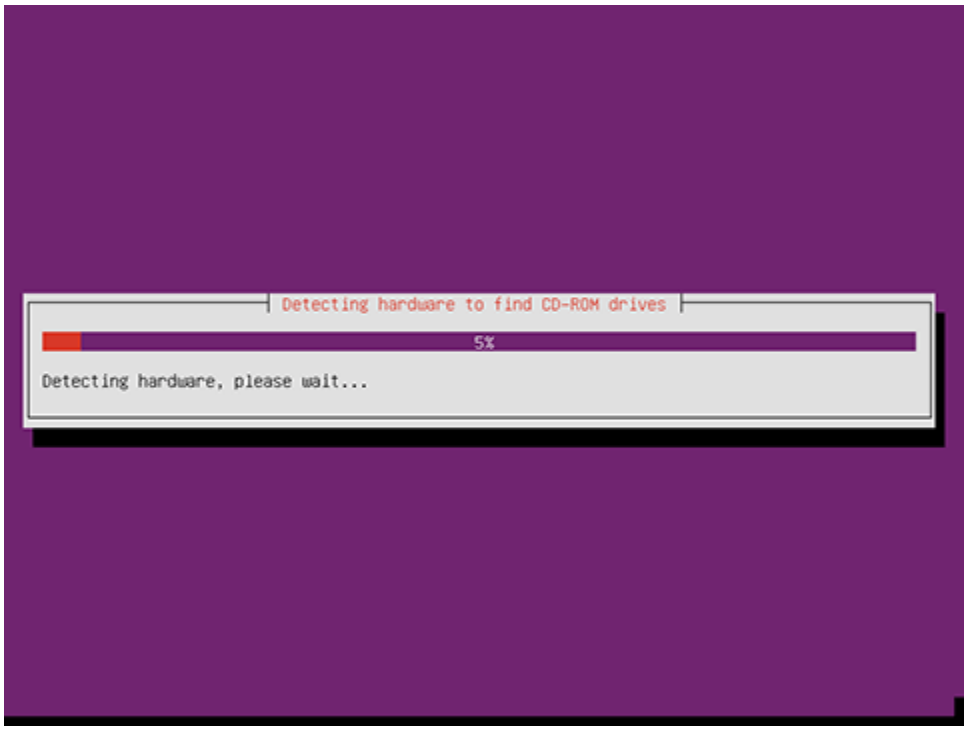


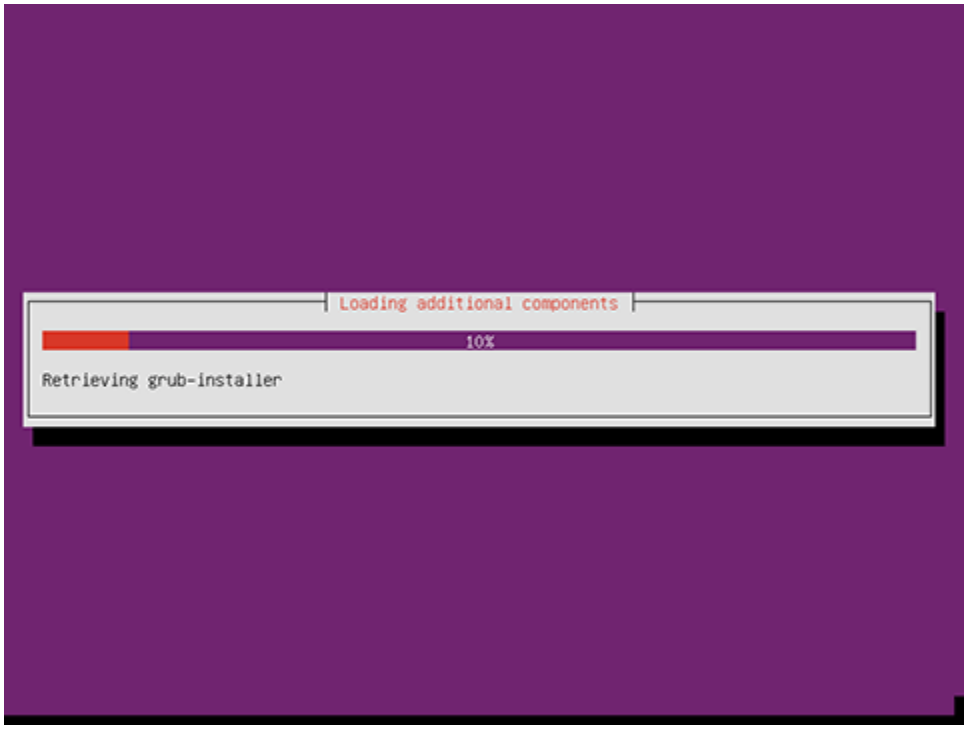


6. Pemeriksaan Media Instalasi dan Pengaturan Jaringan

Selanjutnya, proses instalasi akan memeriksa dan mengaktifkan media instalasi,

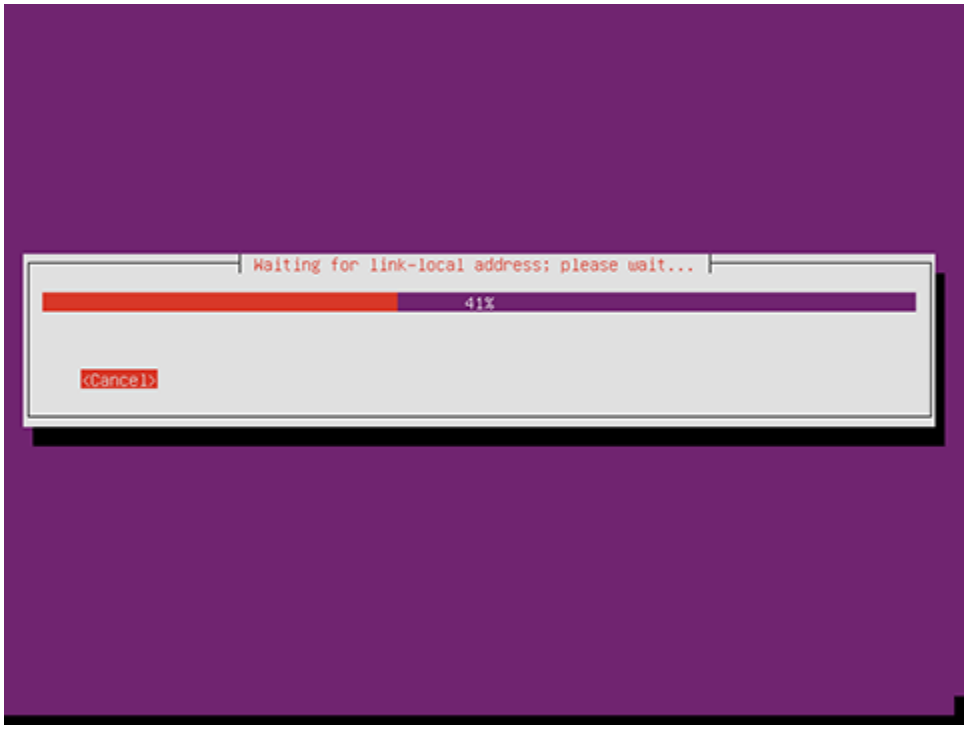
memanggil file konfigurasi awal instalasi, memanggil komponen installer dari media instalasi, memeriksa perangkat fisik jaringan komputer dan pengaturan jaringan. Dalam pengaturan jaringan, tersedia dua pilihan, yaitu Pengaturan Jaringan Otomatis atau Pengaturan Jaringan Manual.

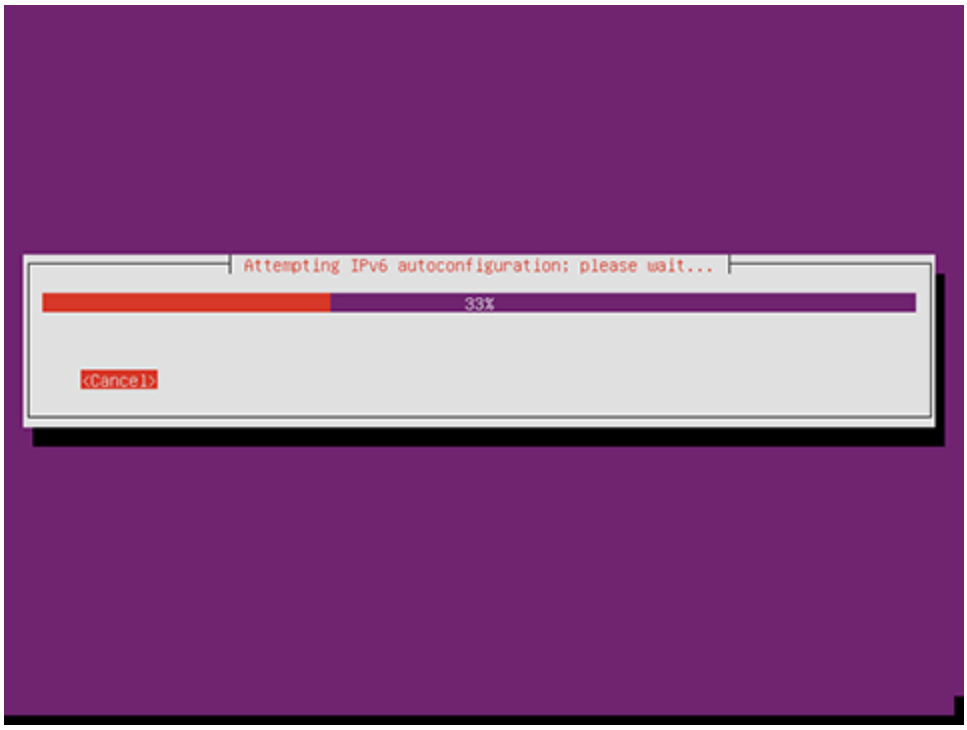


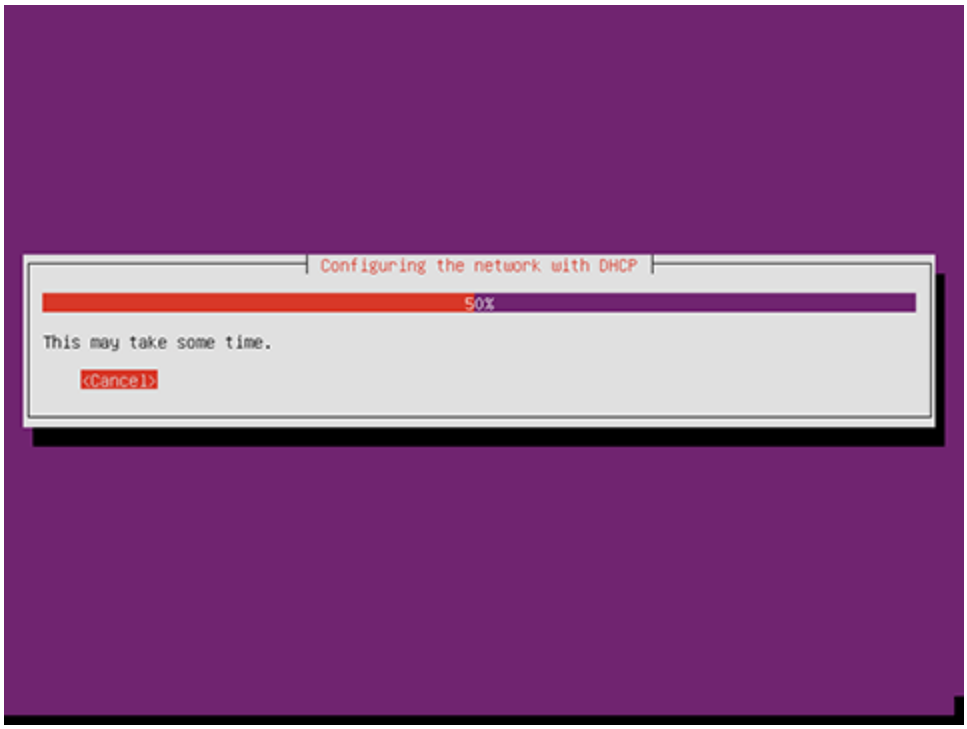


6.1. Pengaturan Jaringan Otomatis

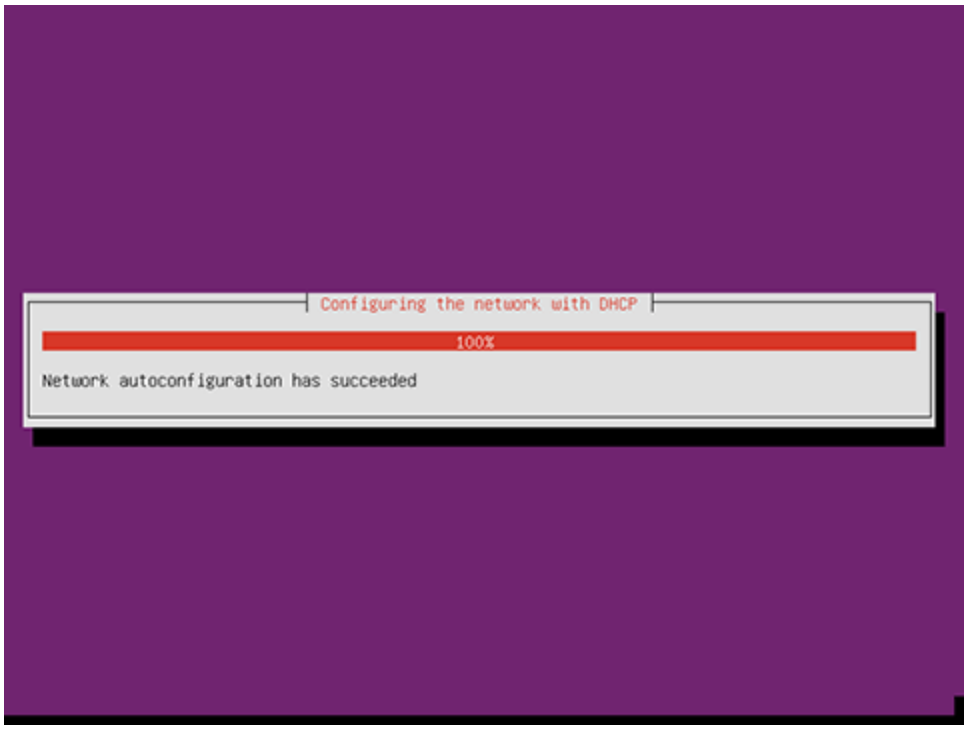
Jika komputer yang akan diinstall terhubung ke sebuah komputer atau *router* yang menyediakan layanan *DHCP server*, maka komputer akan mendapatkan alamat IP secara otomatis.





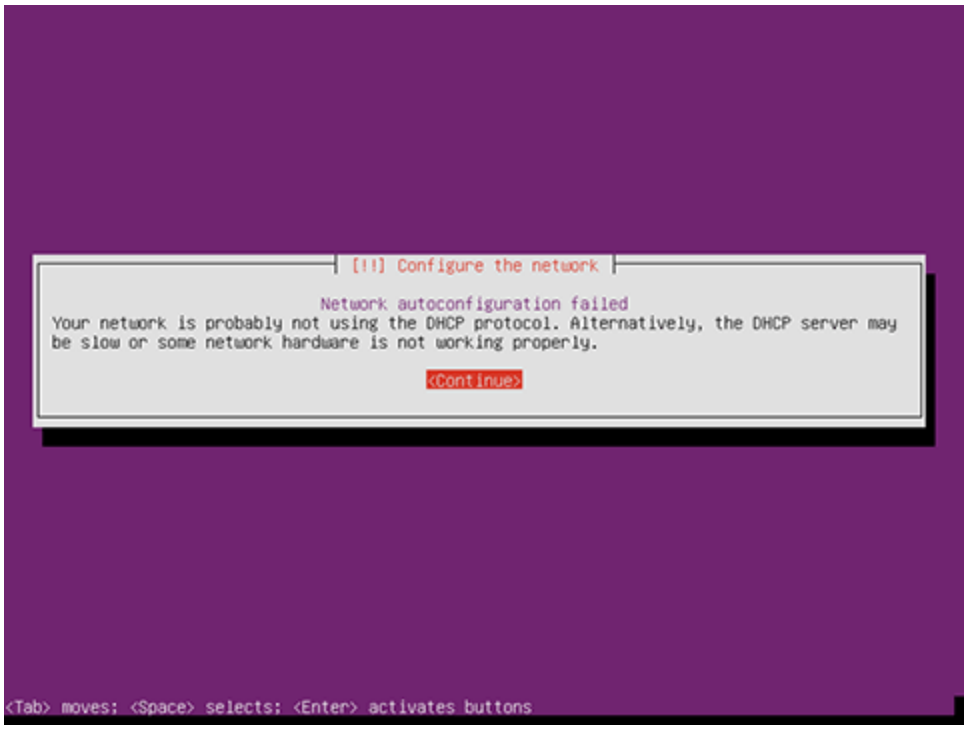


Jika pengaturan jaringan secara otomatis berhasil dilakukan, maka komputer akan mendapatkan alamat IP, *netmask* dan *gateway*.

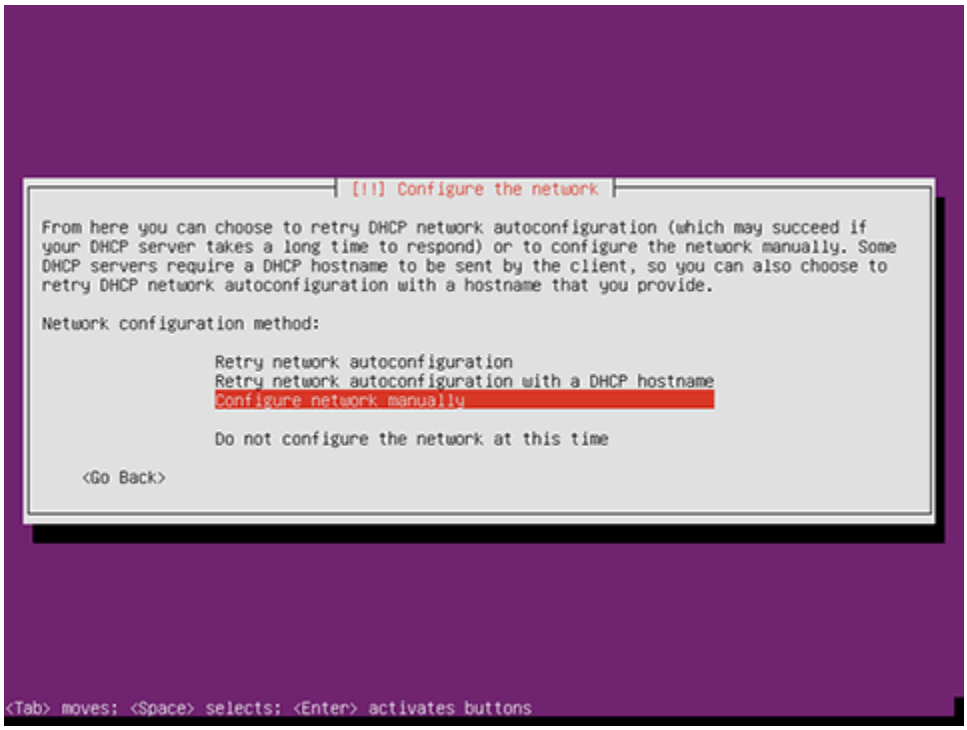


6.2. Pengaturan Jaringan Manual

Apabila komputer tidak terhubung ke sebuah *router* yang menyediakan layanan*DHCP*, maka kita akan diminta untuk melakukan pengaturan jaringan komputer secara manual, meliputi alamat *IP komputer*, *subnet mask*, alamat *IP gateway*, *name server* dan *hostname*. Klik tombol *Continue* untuk memulai pengaturan alamat IP secara manual.



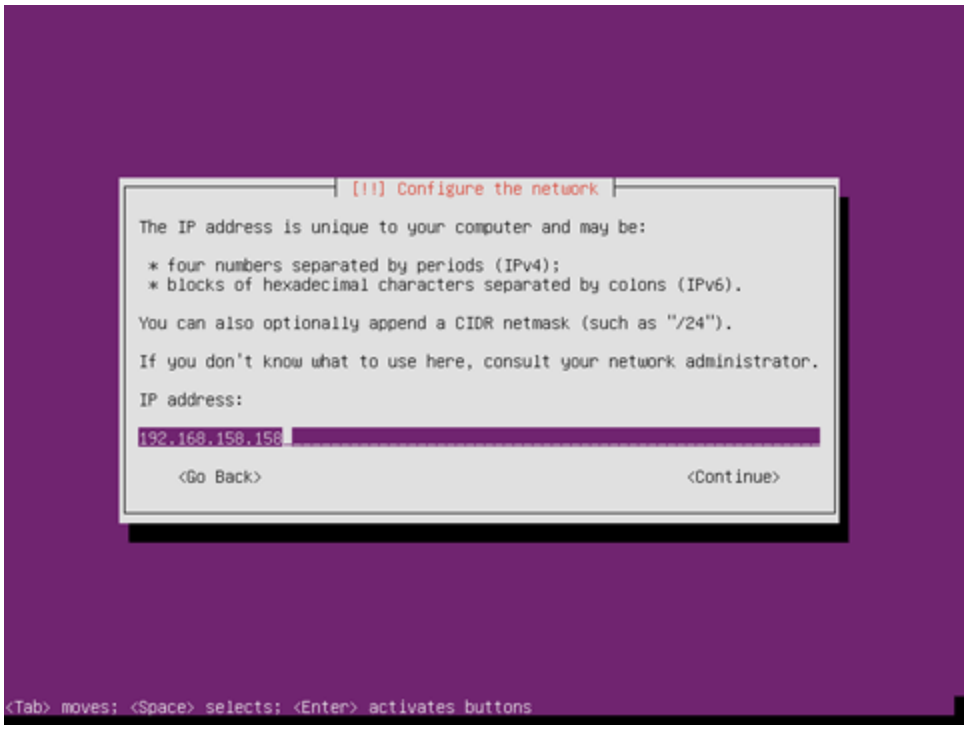
Pilih opsi *Configure network manually* untuk memulai pengaturan alamat IP secara manual.



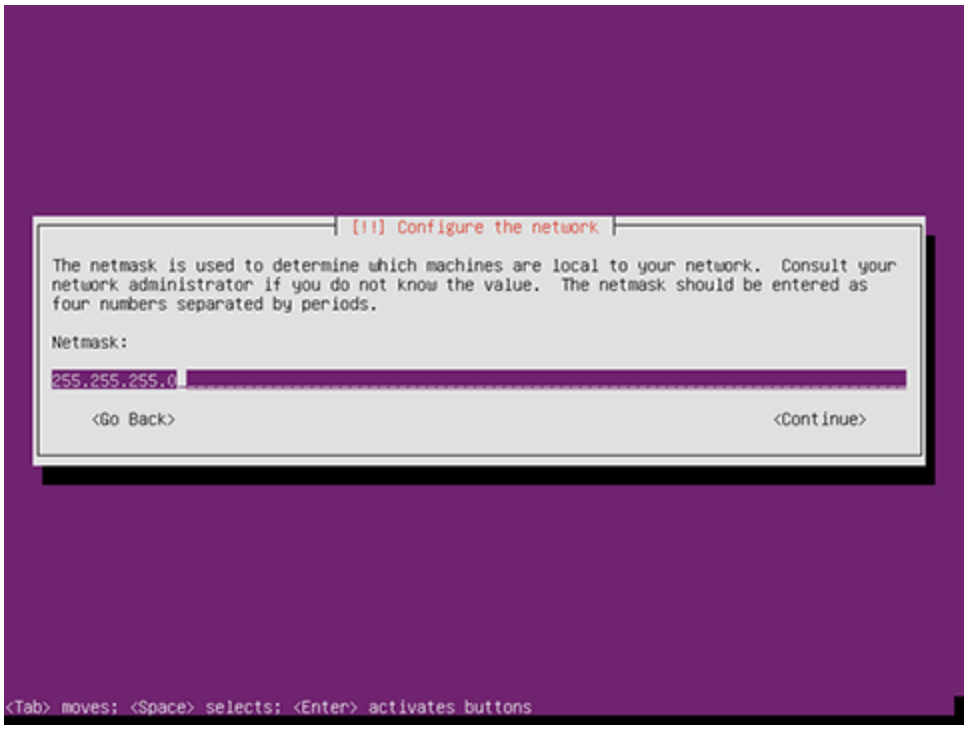
Layar selanjutnya berguna untuk pengisian alamat IP (*Internet Protocol Address*) yang akan diberikan kepada komputer.



Isian alamat IP dapat berupa IP versi 4 atau IP versi 6. Dalam tutorial ini, alamat IP yang diberikan adalah *192.168.158.158*. Selanjutnya tekan tombol *Continue*.



Layar selanjutnya untuk isian *subnet mask* yang digunakan. Secara otomatis, proses instalasi akan memberikan isian *subnet mask 255.255.255.0* (*subnet mask* default untuk IP Address kelas C). Jika diperlukan, isian tersebut dapat diganti sesuai kebutuhan. Jika tidak, tekan tombol *Continue*.

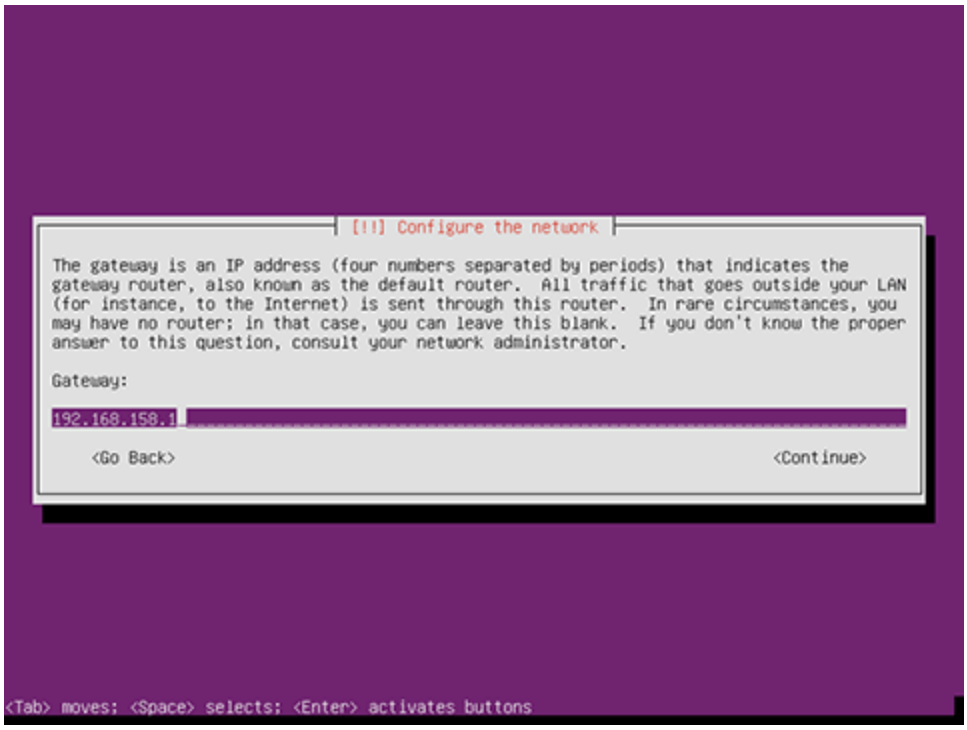


Isian selanjutnya alamat IP *gateway*. *Gateway* adalah komputer atau *router* yang bertindak sebagai "gerbang/pintu" bagi komputer lain untuk berkomunikasi ke jaringan global (Internet).

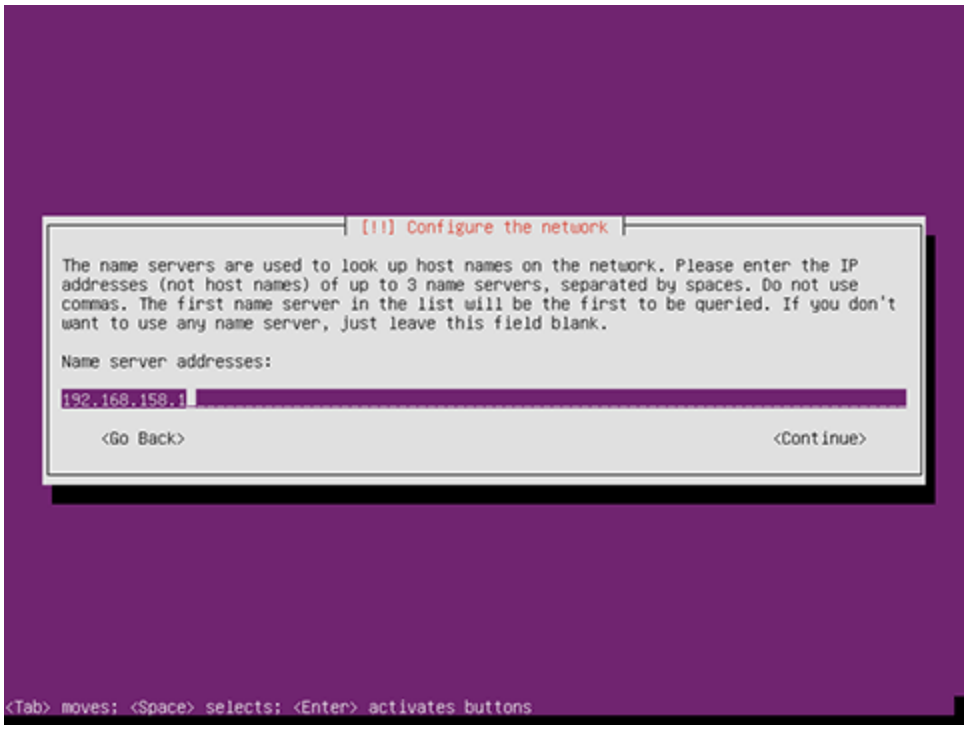
Walaupun komputer yang diinstall tidak terhubung ke jaringan global, isian alamat IP *gateway* tidak boleh kosong. Jika isian alamat IP *gateway* kosong, maka akan keluar pesan kesalahan. Tekan tombol *Continue* untuk kembali dan melengkapi isian alamat IP *gateway*.



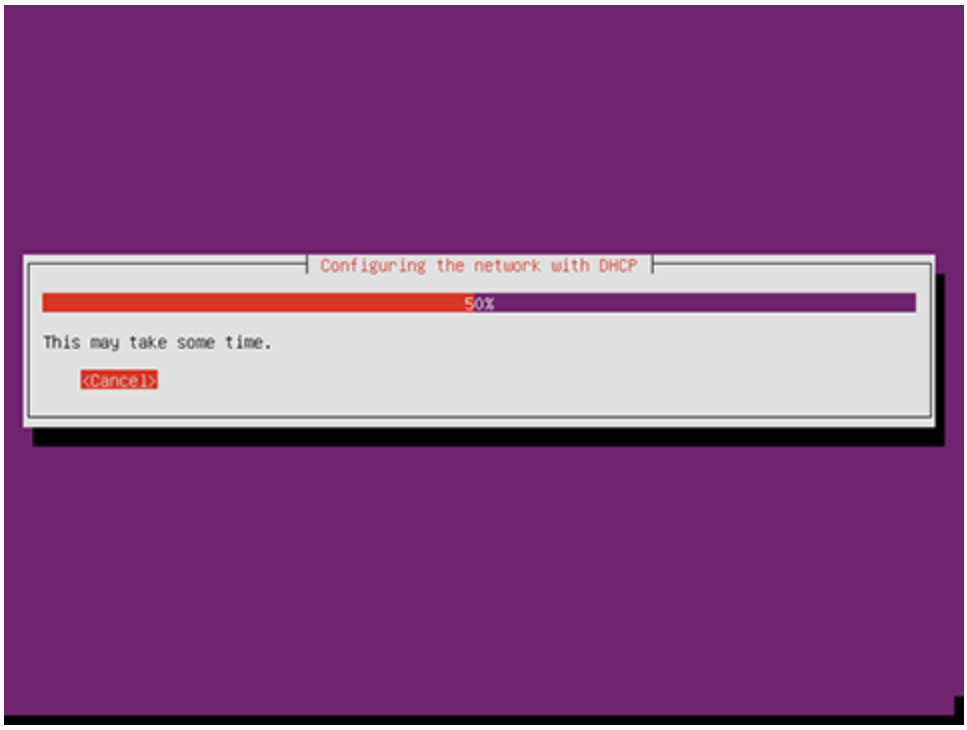
Karena itu, proses instalasi memberikan alamat IP *gateway* dengan nilai default*192.168.158.1*, dimana alamat IP *gateway* segmen ke-3 berpedoman kepada alamat IP komputer segmen ke-3 sebelumnya (*192.168.158.158*). Jika diperlukan, isian alamat IP *gateway* tersebut dapat diganti sesuai dengan kebutuhan. Jika tidak, klik tombol*Continue*.



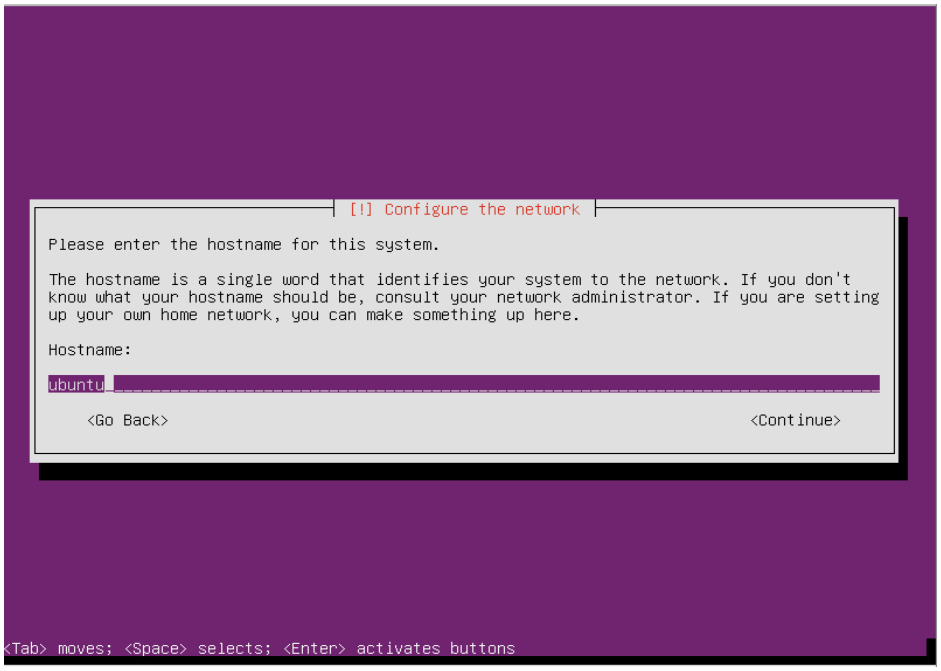
Layar selanjutnya pengisian alamat IP komputer *nameserver*. Komputer *nameserver*digunakan untuk mencari nama *host* di jaringan lokal atau jaringan global. Jika kita tidak ingin menggunakan komputer *nameserver*, isian ini dapat dikosongkan. Setelah itu, klik tombol *Continue*.



Selanjutnya, proses instalasi kembali melakukan pemeriksaan terhadap pengaturan jaringan secara manual yang telah dilakukan.

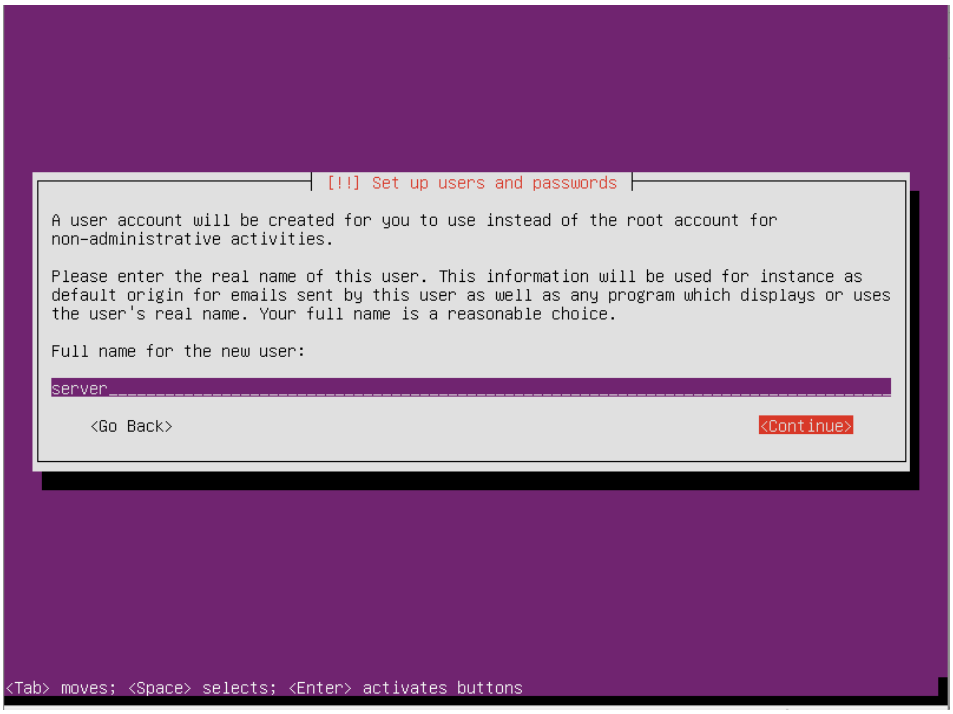


Layar selanjutnya pengaturan nama host (*hostname*). *Hostname* adalah sebuah identifikasi atau pengenal komputer dalam jaringan. *Hostname* harus dalam bentuk satu kesatuan kata, dan karakter yang diperbolehkan adalah angka dari 0-9, huruf a-z atau A-Z dan simbol minus (-).



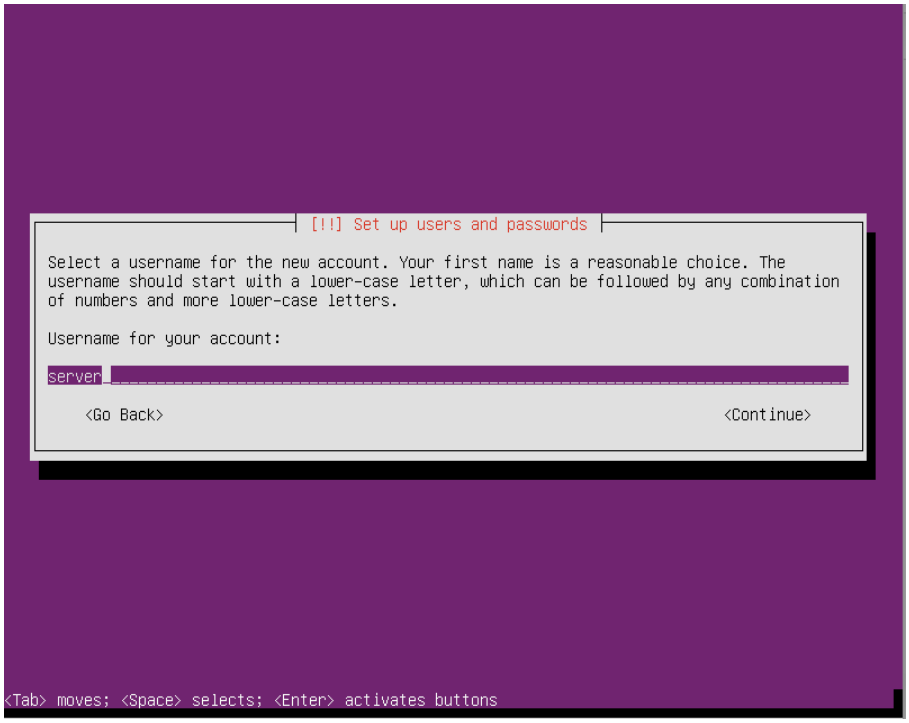
7. Pembuatan Account

Pengaturan selanjutnya berguna untuk isian nama lengkap *account* yang akan dibuat. Setelah itu, klik tombol *Continue*.

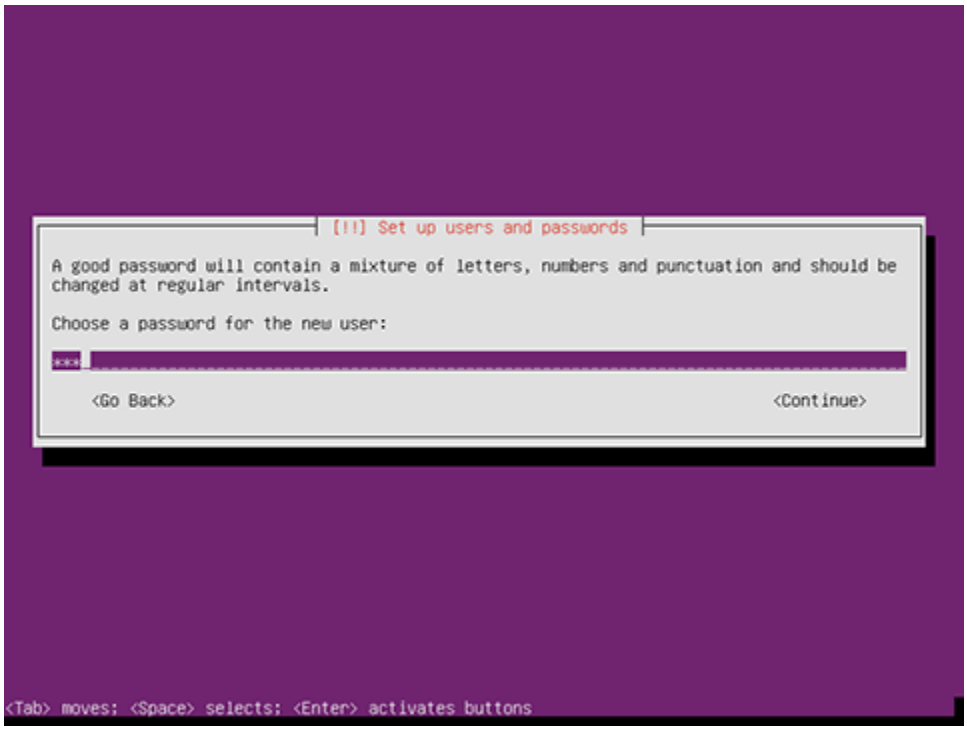


Selanjutnya, pembuatan *account* baru selain *account root*. Secara default, *account root* baru dapat digunakan setelah kita login dengan *account* yang kita buat sekarang ke dalam sistem *Ubuntu* yang diinstall.

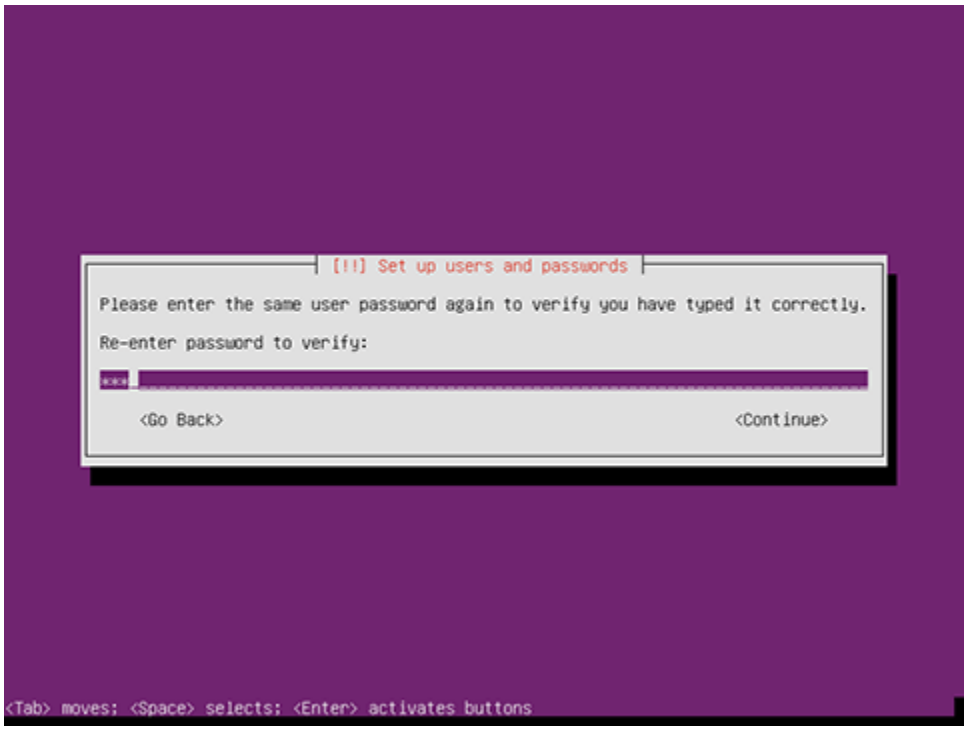
Nama *account* otomatis diambil dari kata pertama nama lengkap yang sebelumnya diisi. Jika dibutuhkan, kita dapat menggantinya. Setelah itu, klik tombol *Continue*.



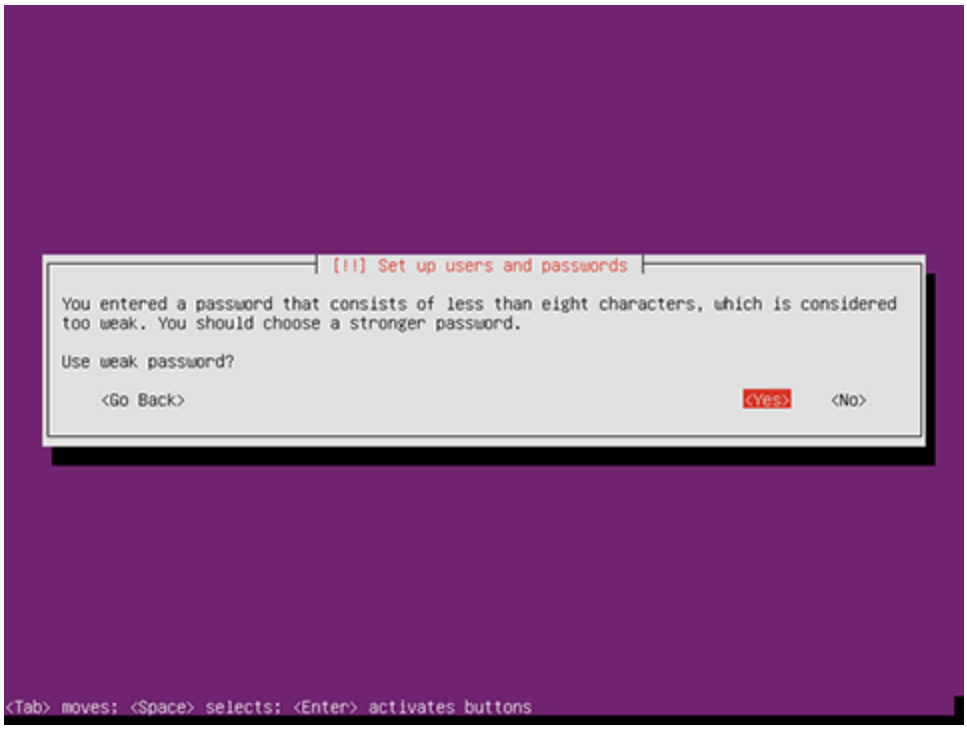
Isian kata kunci (*password*) untuk user yang baru dibuat. Setelah itu, klik tombol *Continue*.



Konfirmasi isian *password* untuk *user* yang baru dibuat. Setelah itu, klik tombol *Continue*.



Jika *password* yang kita gunakan terlalu mudah untuk ditebak, maka akan keluar pesan peringatan. Jika kita tetap ingin menggunakan password tersebut, pilih opsi *Yes*. Jika ingin merubahnya, pilih opsi *No*.

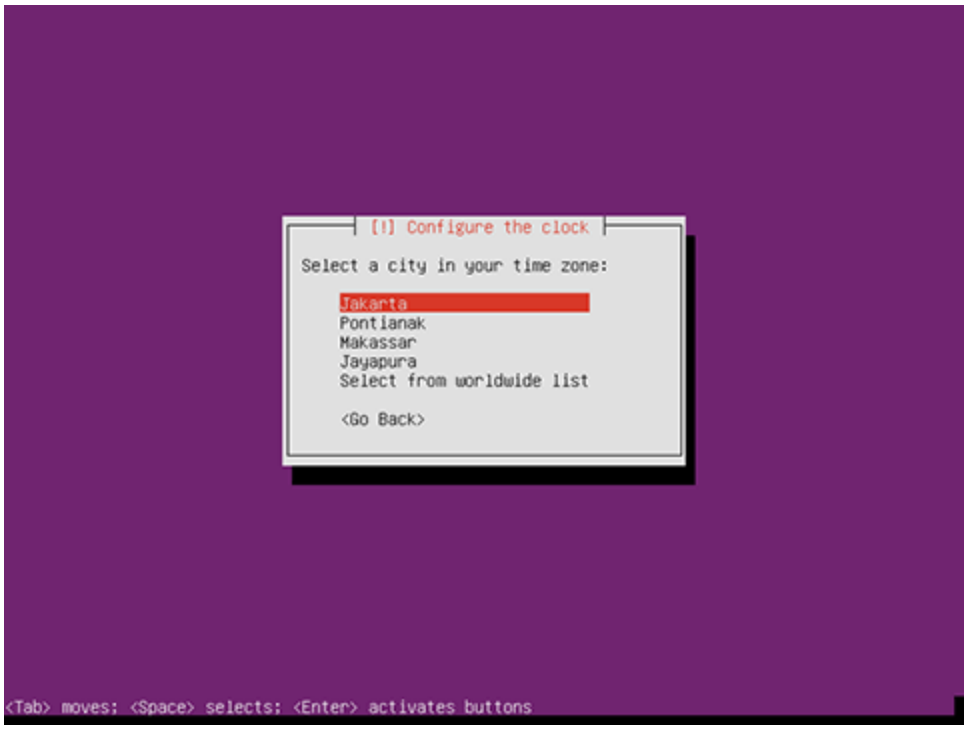


Pengaturan selanjutnya berkaitan dengan folder */home* dari *account* yang dibuat. Jika kita ingin meng-enkripsi folder */home* tersebut, pilih opsi *Yes*, jika tidak pilih opsi *No*. Enkripsi berfungsi untuk membuat teks biasa menjadi teks yang tidak bisa dibaca (*non-readable text*).



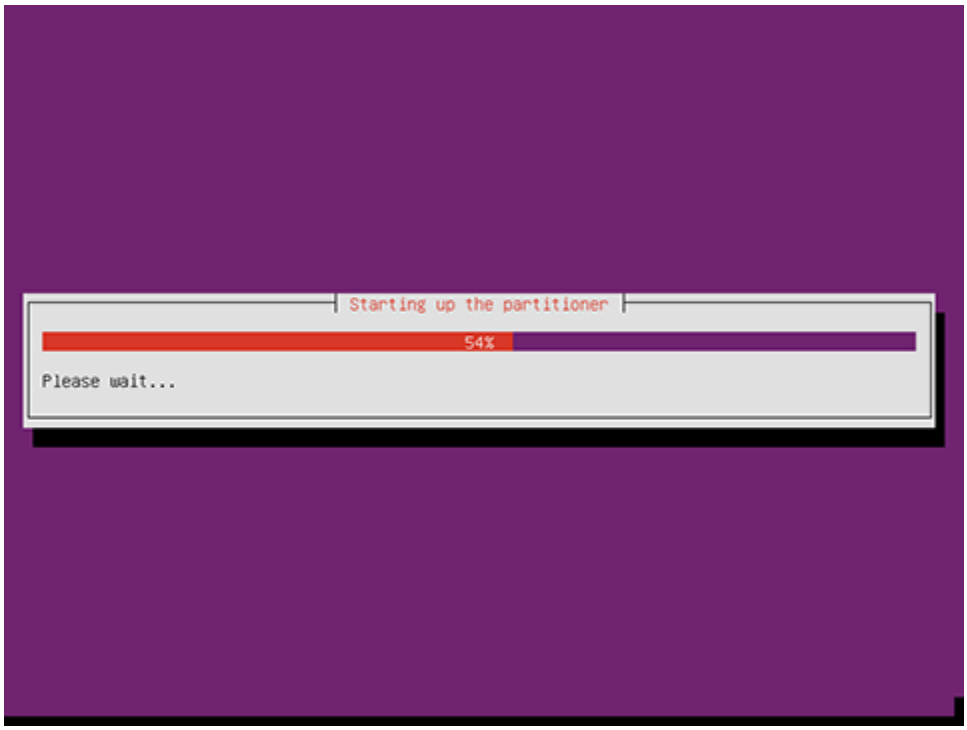
8. Pengaturan Zona Waktu

Selanjutnya pengaturan waktu (tanggal dan jam). Jika komputer terhubung ke jaringan global, maka akan muncul layar sinkronisasi (pencocokan) waktu komputer dengan waktu lokasi yang kita pilih. Jika tidak, akan muncul pilihan lokasi waktu yang akan digunakan.



9. Pembuatan Partisi *Hard Disk*

Setelah itu, proses instalasi memulai tahap pembuatan partisi *hard disk*.



Dalam pembuatan partisi *hard disk*, ada 4 (empat) pilihan yang tersedia:

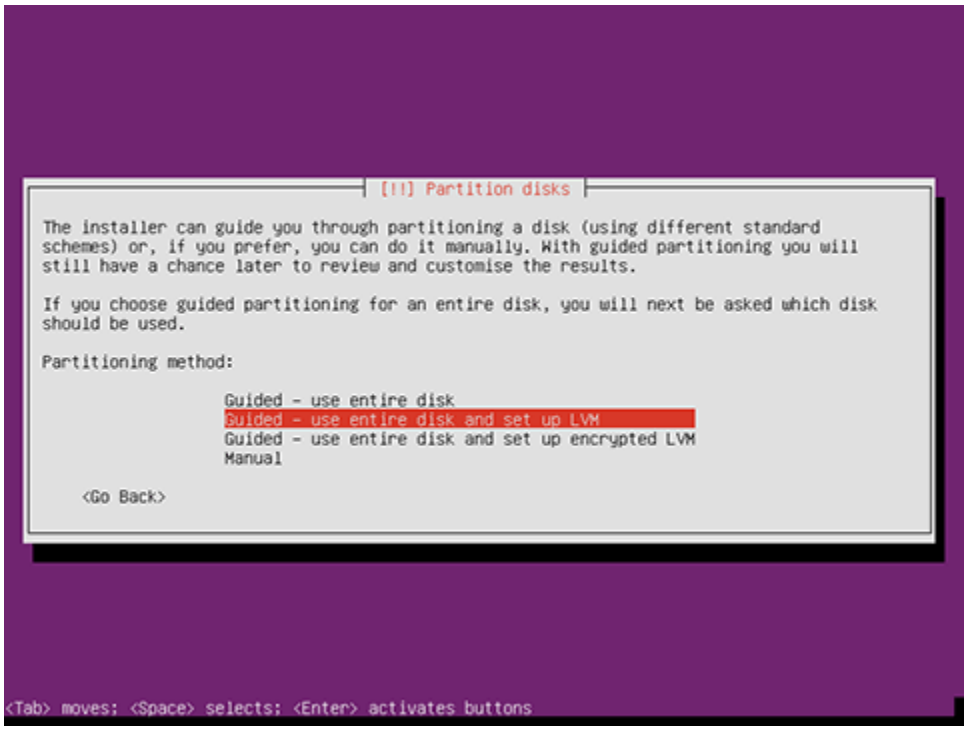
- *Guided - use entire disk*
  Pembuatan partisi *hard disk* secara otomatis dilakukan oleh sistem.

- *Guided - use entire disk and set up LVM*
  Pembuatan partisi *hard disk* secara otomatis dilakukan oleh sistem, disertai tambahan fitur LVM (*Logical Volume Manager*) yang memungkinkan kita untuk mengatur *hard disk* dalam jumlah besar atau banyak, sehingga memungkinkan kita menambah, mengganti, menyalin dan berbagi isi dari satu *hard disk* ke *hard disk* lain tanpa perlu mengganggu *service* yang sedang berjalan.

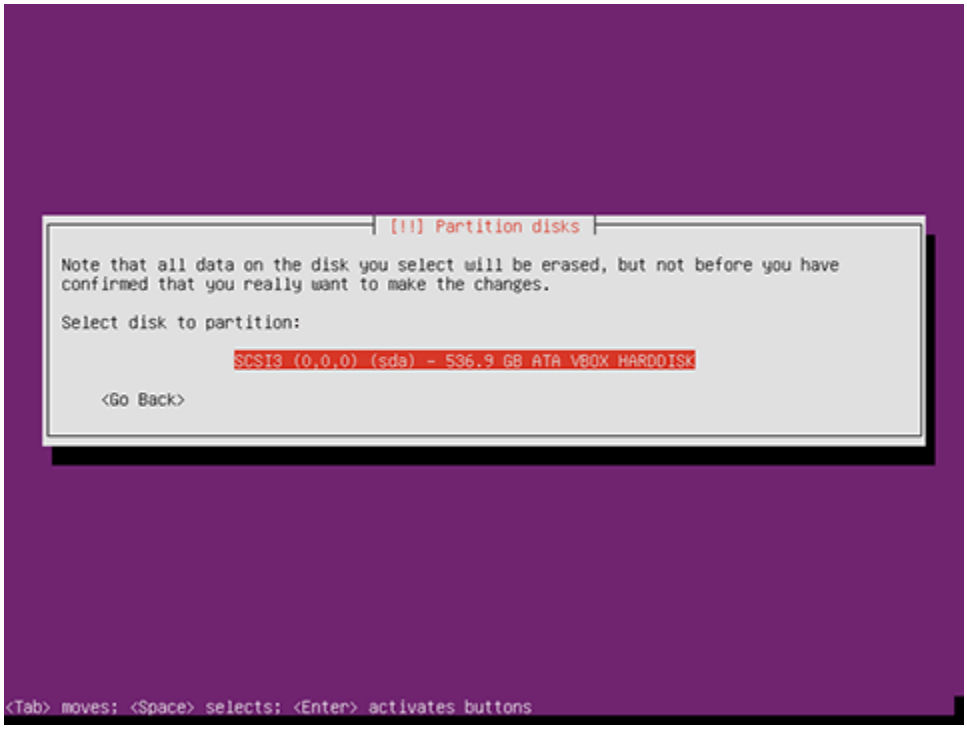
- *Guided - use entire disk and setup encrypt LVM*
  Sama dengan *Guided - use entire disk and set up LVM*, namun partisi akan dienkripsi agar tidak mudah dibaca oleh orang lain.

- *Manual*
  Pembuatan partisi *hard disk* kita lakukan sendiri.

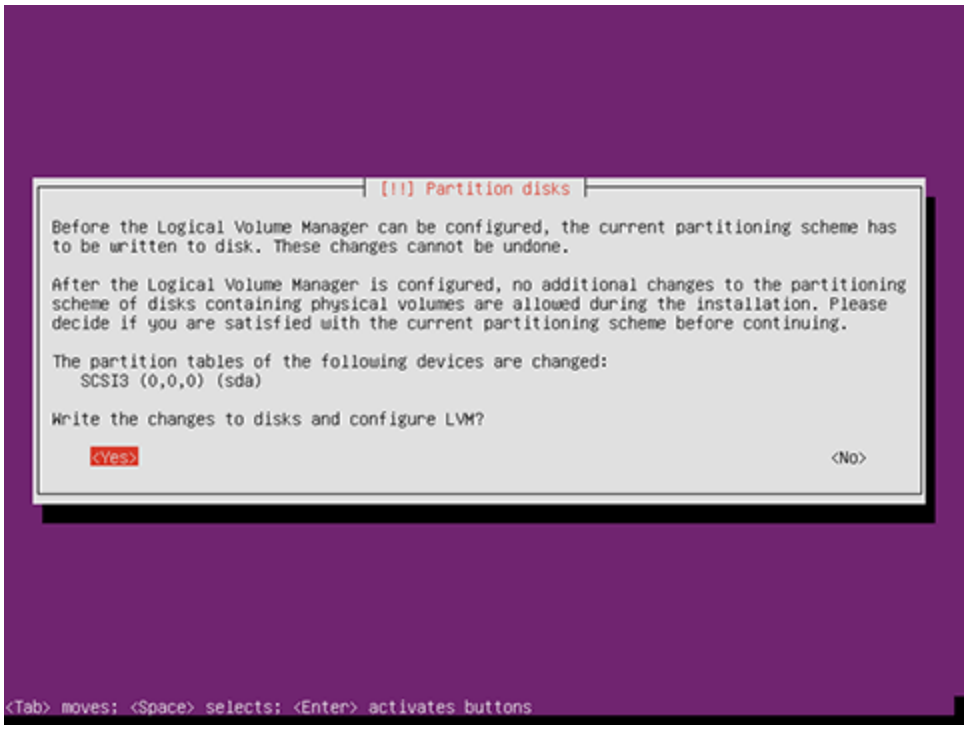
Dalam tutorial ini digunakan pilihan *Guided - use entire disk and set up LVM*. Tekan tombol *Enter* untuk melanjutkan.



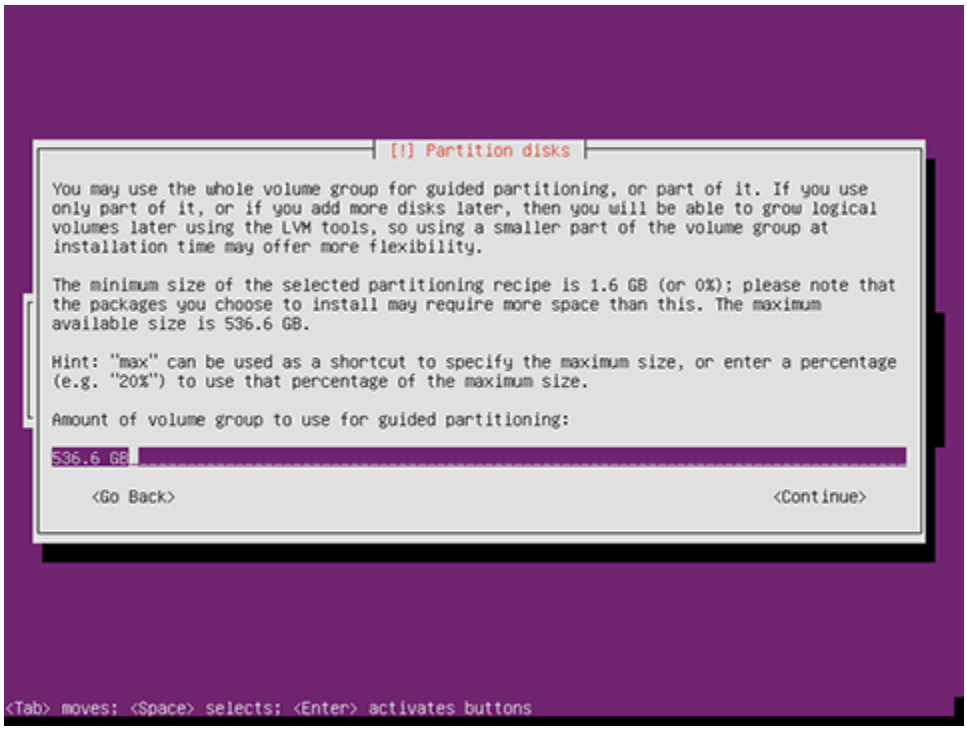
Langkah selanjutnya memilih *hard disk* yang akan dipartisi. Tekan tombol *Enter* untuk melanjutkan.



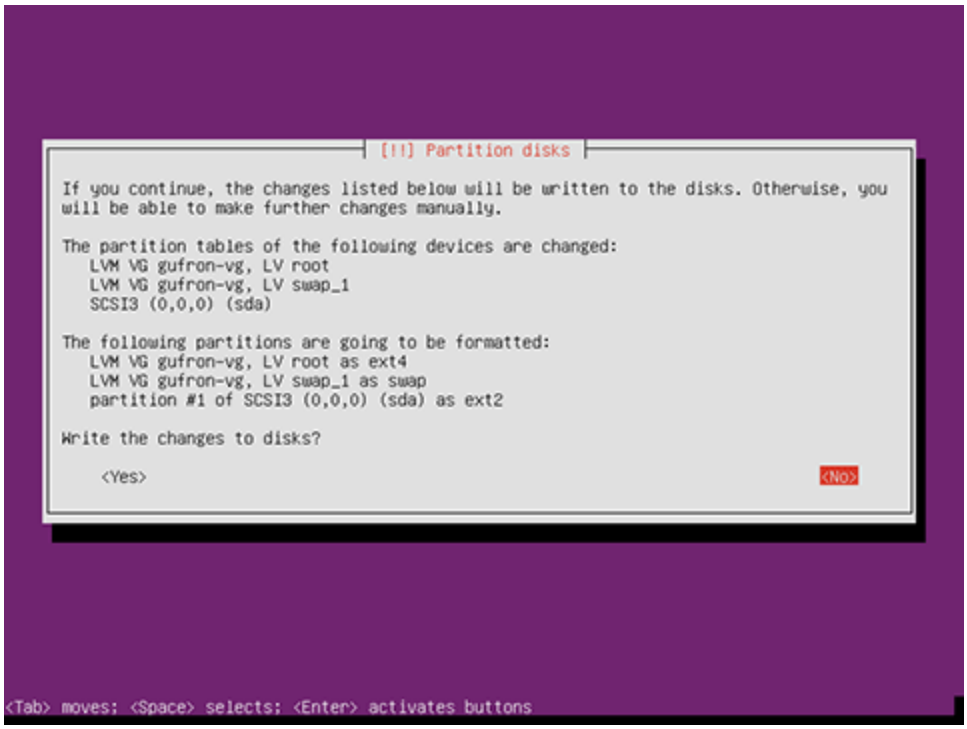
Pilih *Yes* untuk menulis tabel partisi pada *hard disk* yang dipilih dan memulai pengaturan *Logical Volume Manager*.



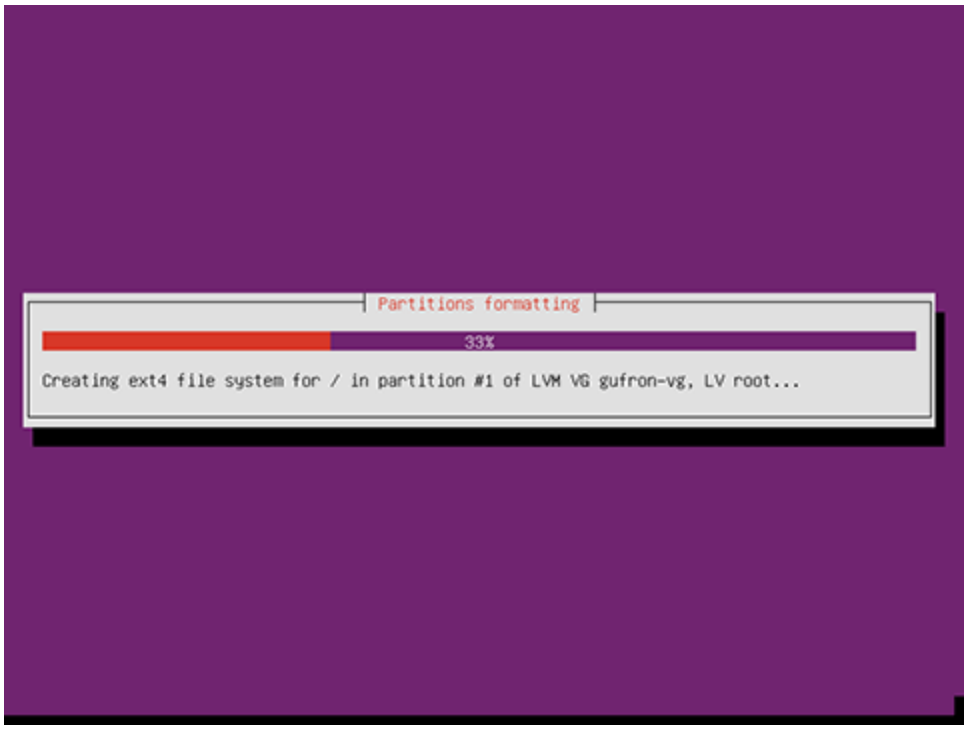
Tentukan ukuran kapasitas *hard disk* yang akan digunakan. Kemudian tekan tombol *Continue*.



Selanjutnya pemberitahuan pengaturan yang sudah ditentukan sebelumnya. Tekan tombol *No* jika ada pengaturan yang akan dirubah, atau tekan tombol *Yes* untuk memulai proses pembuatan dan format partisi.

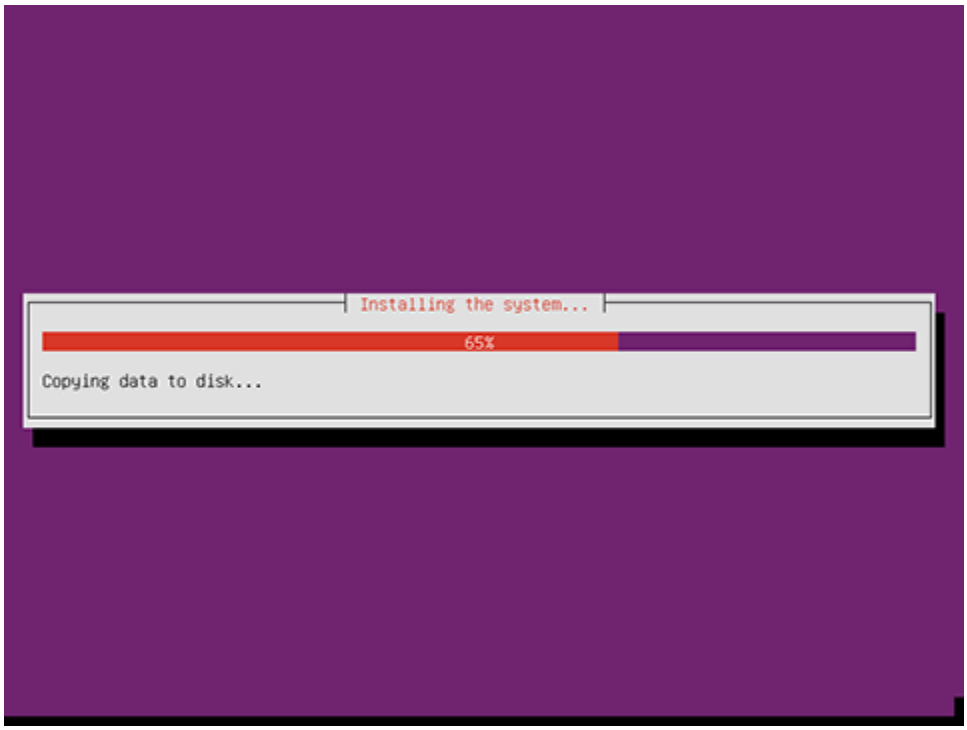


Proses format partisi dimulai.



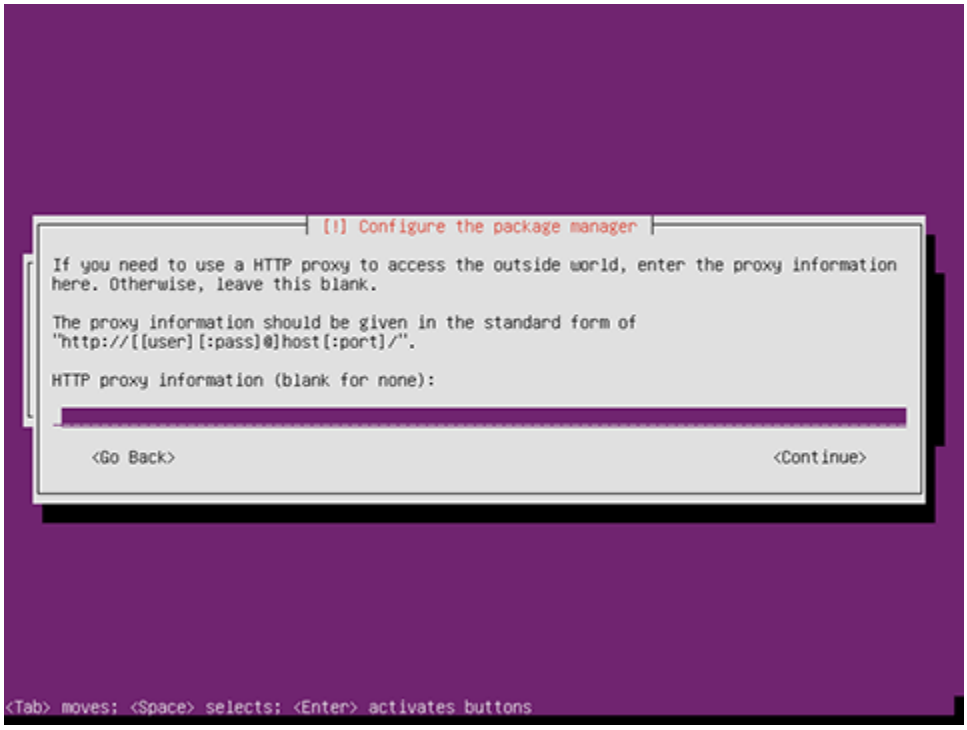
10. Instalasi Ubuntu 14.04 Trusty Tahr Versi Server

Proses instalasi Ubuntu 14.04 Trusty Tahr versi server dimulai.



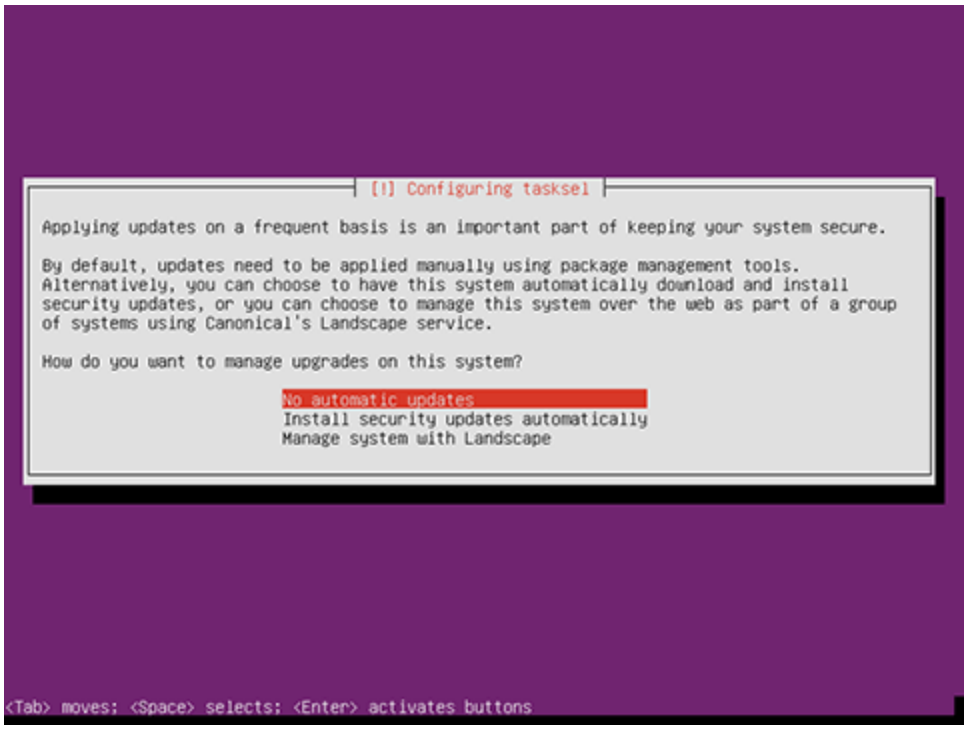
11. Pengaturan Proxy

Jika komputer yang digunakan terhubung ke jaringan global, kita dapat mengisi alamat proxy yang digunakan atau biarkan kosong jika tidak menggunakan proxy. Kemudian tekan tombol *Continue*.



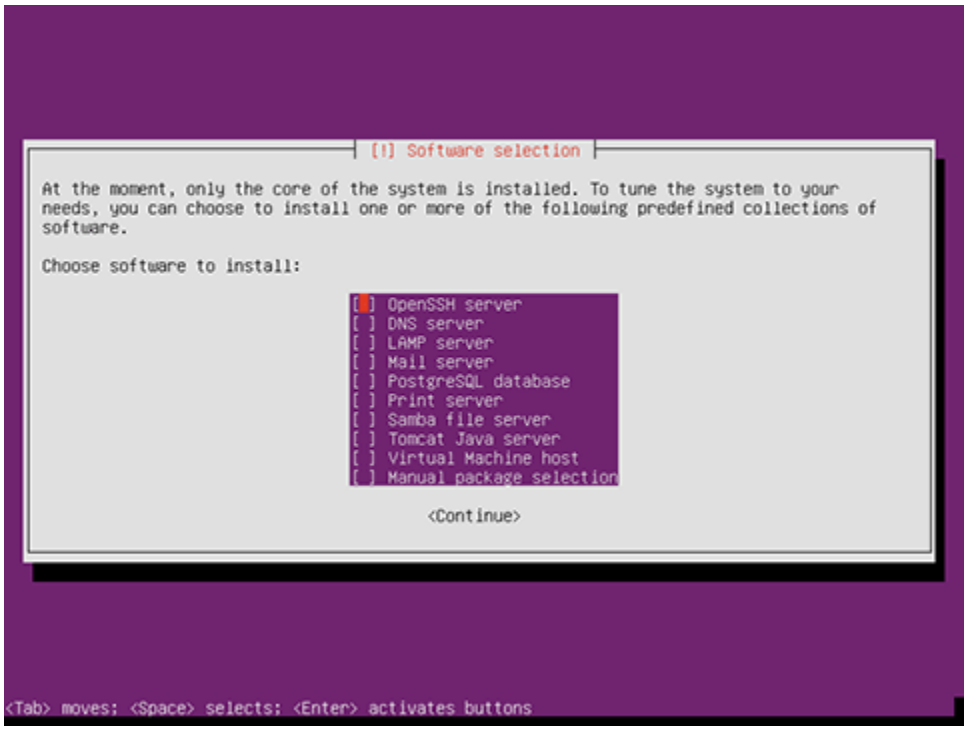
12. Pengaturan Proses Update

Selanjutnya pengaturan proses update Ubuntu 14.04 Trusty Tahr versi server yang diinstall.

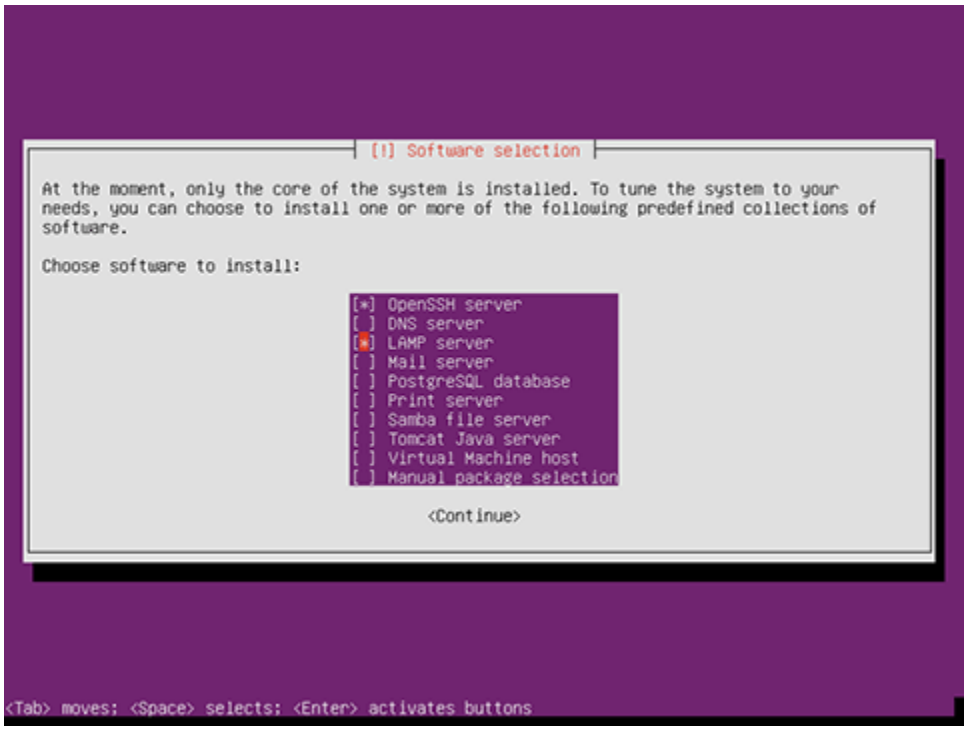


13. Pemilihan Software

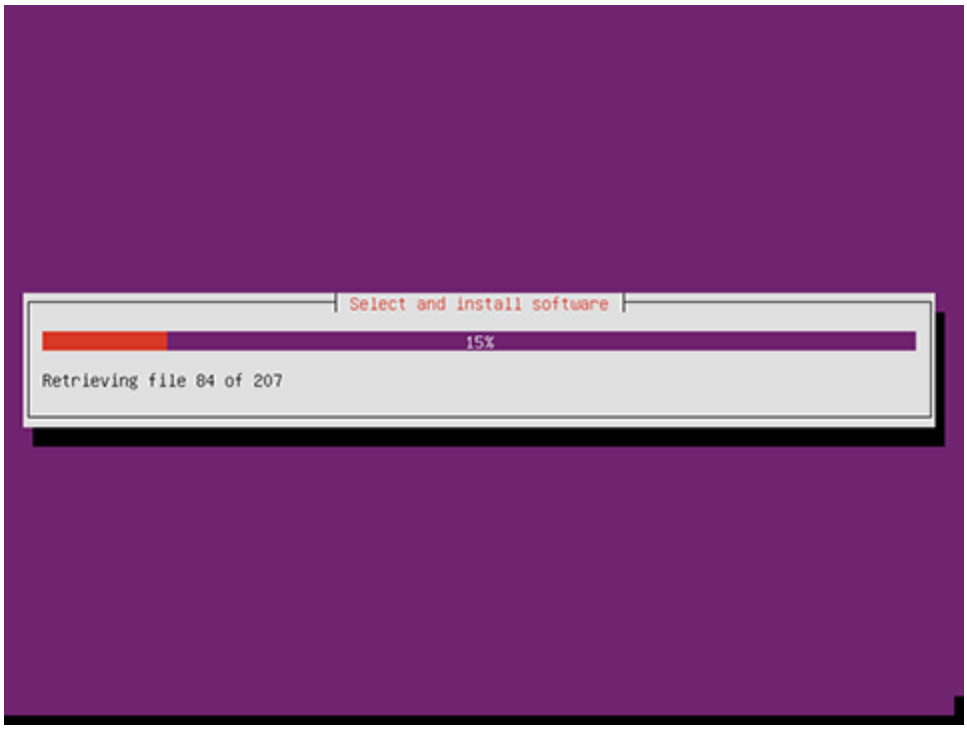
Di bagian ini kita dapat memilih *software* yang akan diinstall dengan cara menandai *software* tersebut.



Dalam tutorial ini, *software* yang akan diinstall adalah *OpenSSH server* dan *LAMP server*. *OpenSSH* atau *SSH*(*Secure Shell*) adalah protokol jaringan yang memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan untuk mengakses akun *shell*.

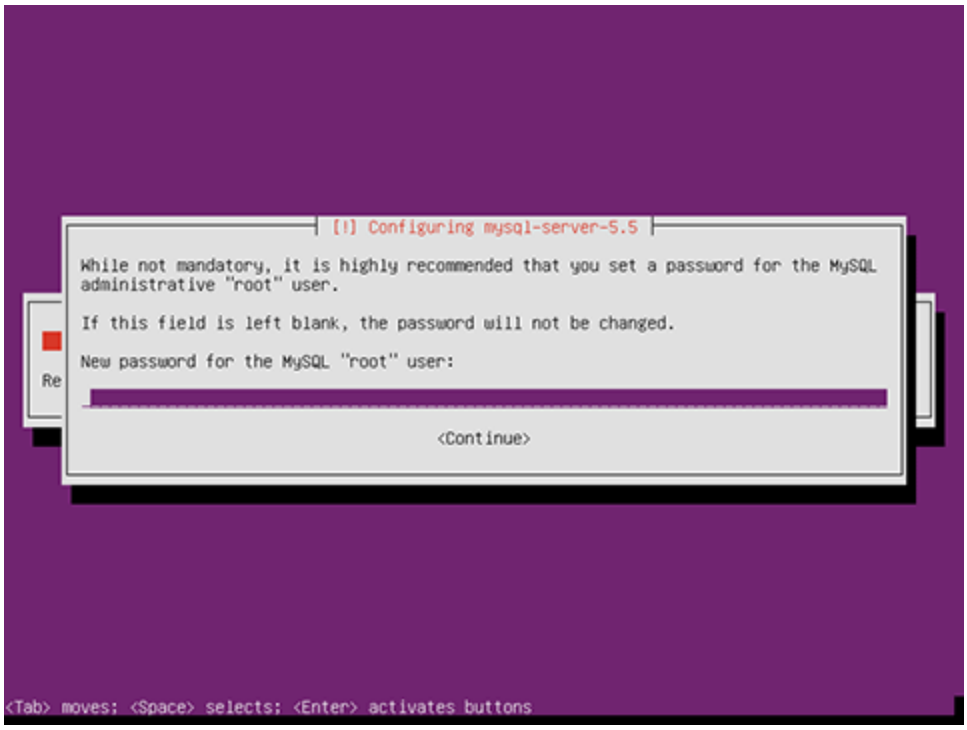


Proses instalasi *software* dimulai.

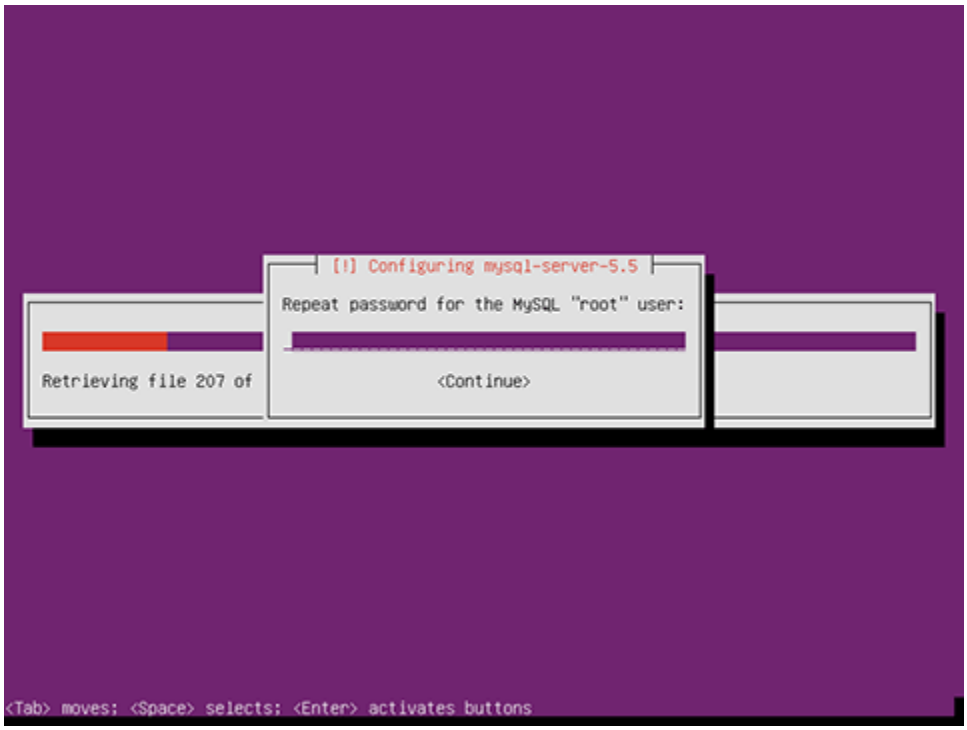


14. Pengaturan Password MySQL Server

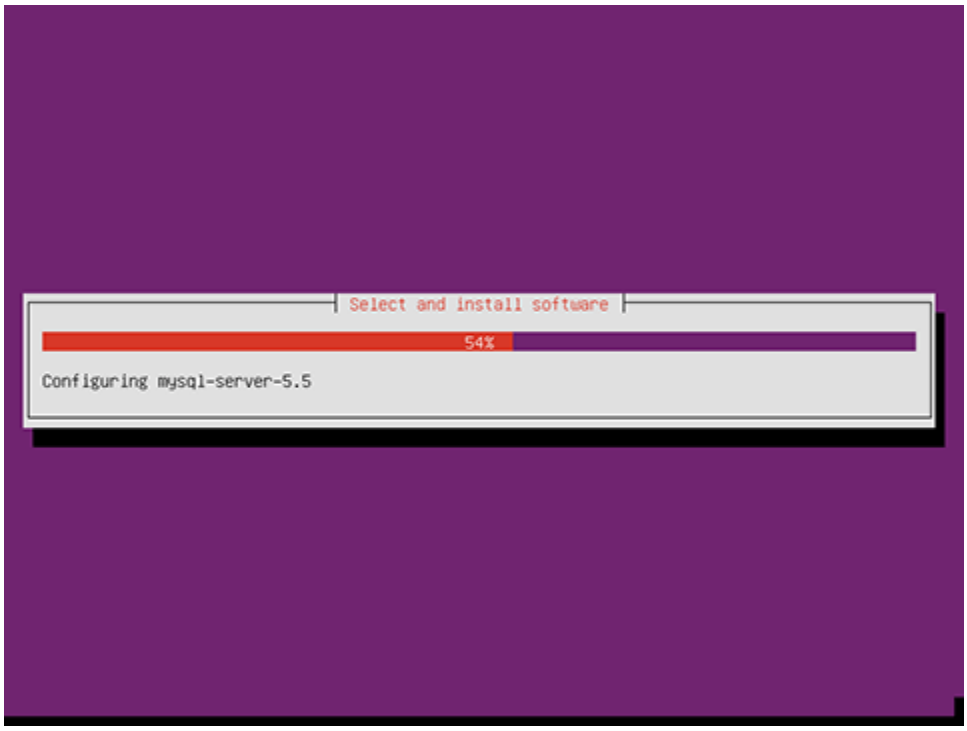
Dikarenakan kita memilih paket *LAMP server*, maka kita akan diminta untuk mengisi *password* account *root*untuk login ke *MySQL server*. Pengaturan account *root* disini berbeda dengan account *root* untuk login ke server.



Tulis kembali *password* login ke *MySQL server*.

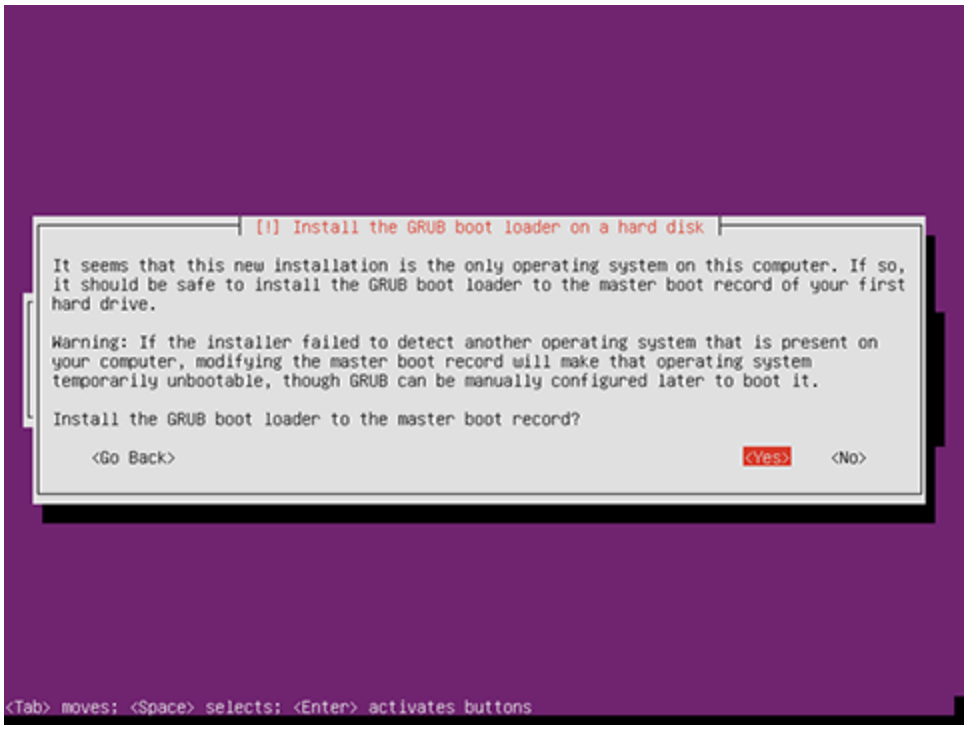


Proses instalasi dilanjutkan kembali.

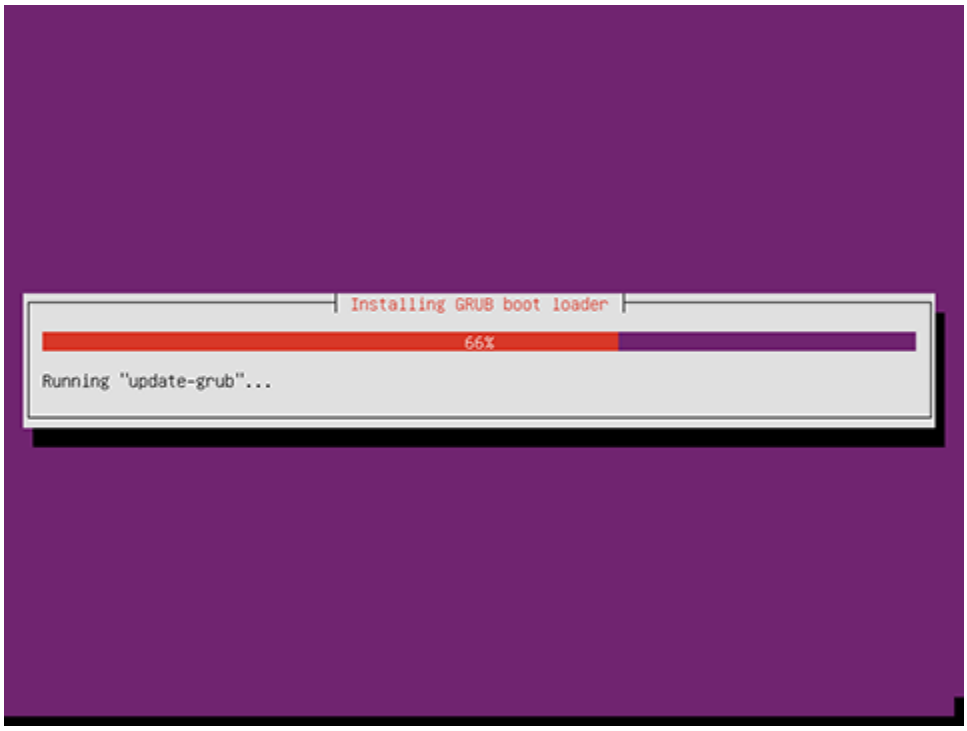


15. Penulisan GRUB Boot Loader

Pilih opsi *Yes* untuk menulis GRUB boot loader Ubuntu 14.04 Trusty Tahr versi server pada MBR (*Master Boot Record*) *hard disk*.

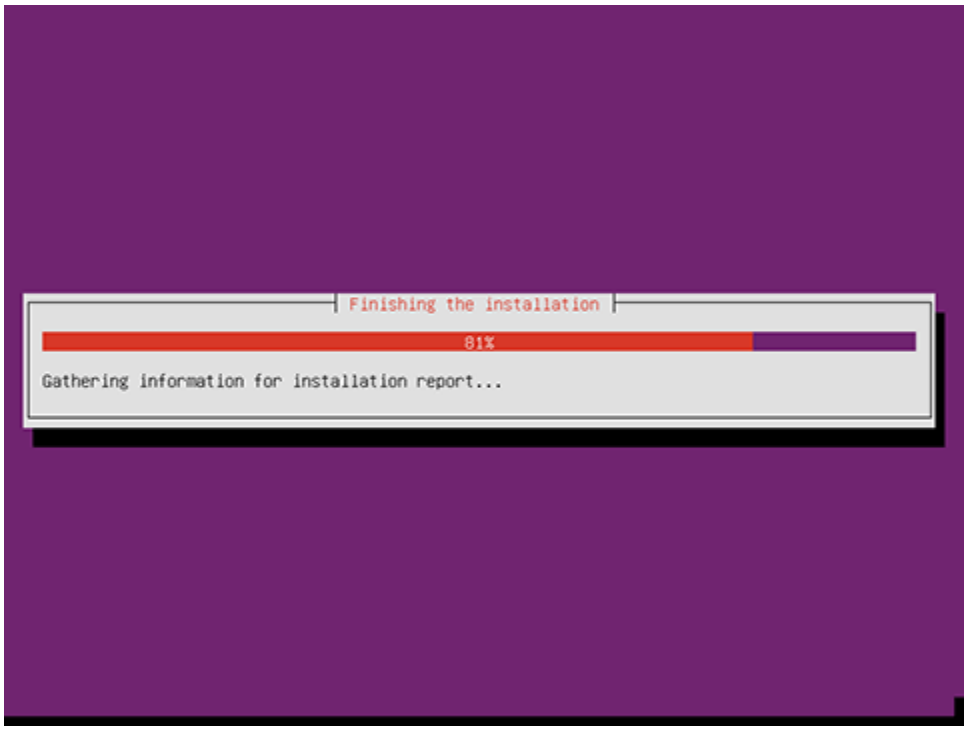


Proses penulisan *GRUB boot loader*.

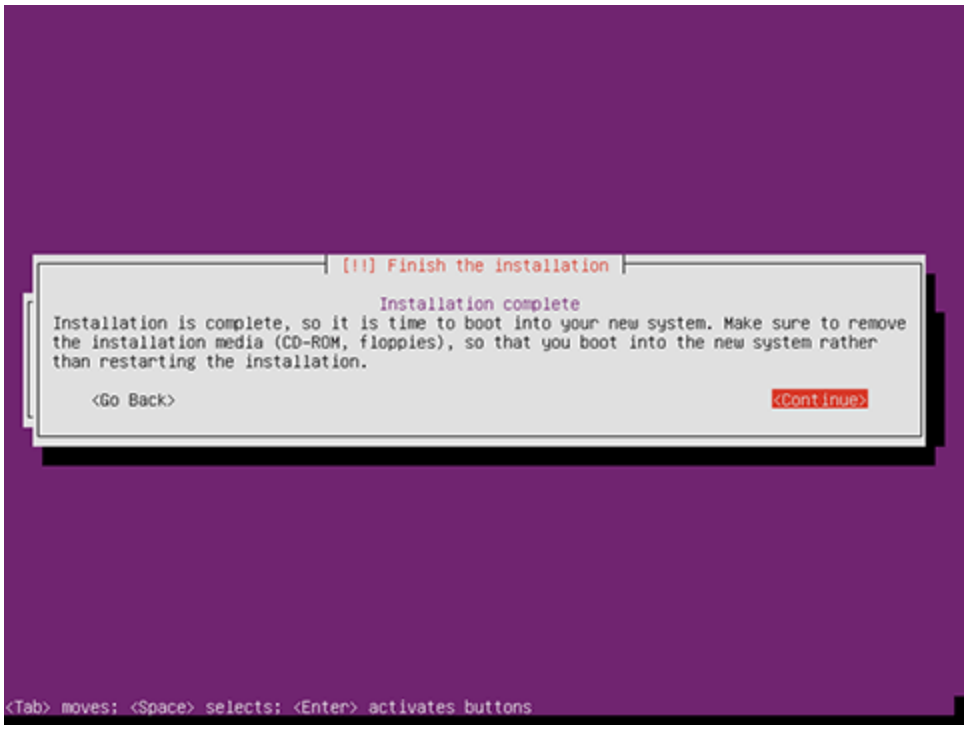


16. Penyelesaian Instalasi

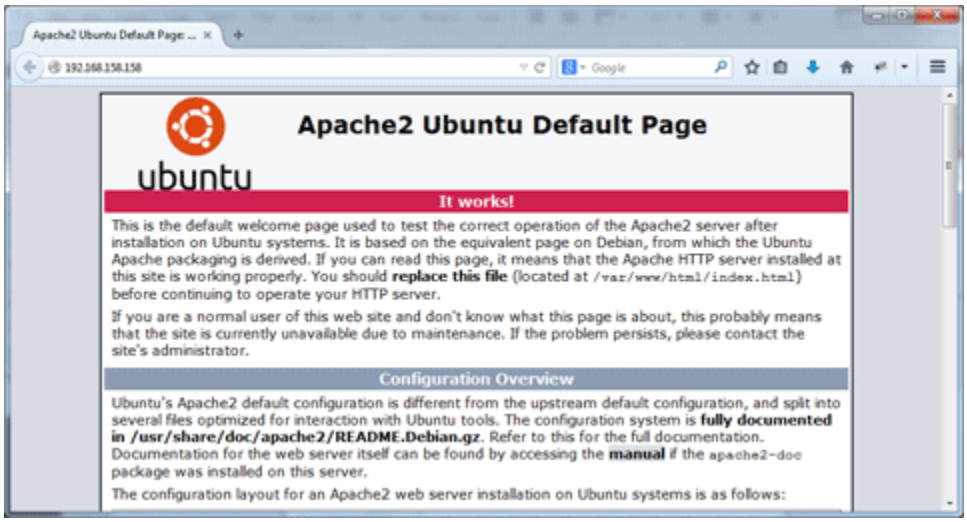
Proses akhir penyelesaian Ubuntu 14.04 Trusty Tahr versi server.



Klik tombol *Continue* untuk *booting* ulang komputer dan mulai menjalankan Ubuntu 14.04 Trusty Tahr versi server.



Jika alamat IP *http://192.168.158.158* yang merupakan alamat IP komputer web server Ubuntu 14.04 Trusty Tahr yang baru saja diinstall diakses pada browser, akan keluar:



E. TUGAS

1. Lakukan lah instalasi server seperti percobaan di atas.
2. Sebutkan dan jelaskan jenis partisi yang ada pada sistem linux seperti ext3,ext4 dan swap area.

2 INSTALASI SISTEM OPERASI PENESTRASI

A. POKOK BAHASAN

1. Melakukan instalasi sistem operasi penestrasi
2. Mengenal tools keamanan sistem operasi penestrasi.

B. TUJUAN

setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

1. Membangun sistem komputer yang aman.
2. Mengenal kelemahan untuk sistem komputer.

C. PERALATAN

1. Sistem Operasi Linux Kali

D. PERCOBAAN

1. Untuk memulai instalasi, boot dengan media instalasi yang Anda pilih. Anda akan disambut dengan Kali Linux Boot Menu. Pilih salah satu *Graphical* atau *Text-Mode*install. Dalam contoh ini, kita memilih GUI install.



2. Pilih bahasa pilihan Anda dan kemudian lokasi negara Anda. Anda juga akan diminta untuk mengkonfigurasi keyboard anda dengan keymap yang sesuai



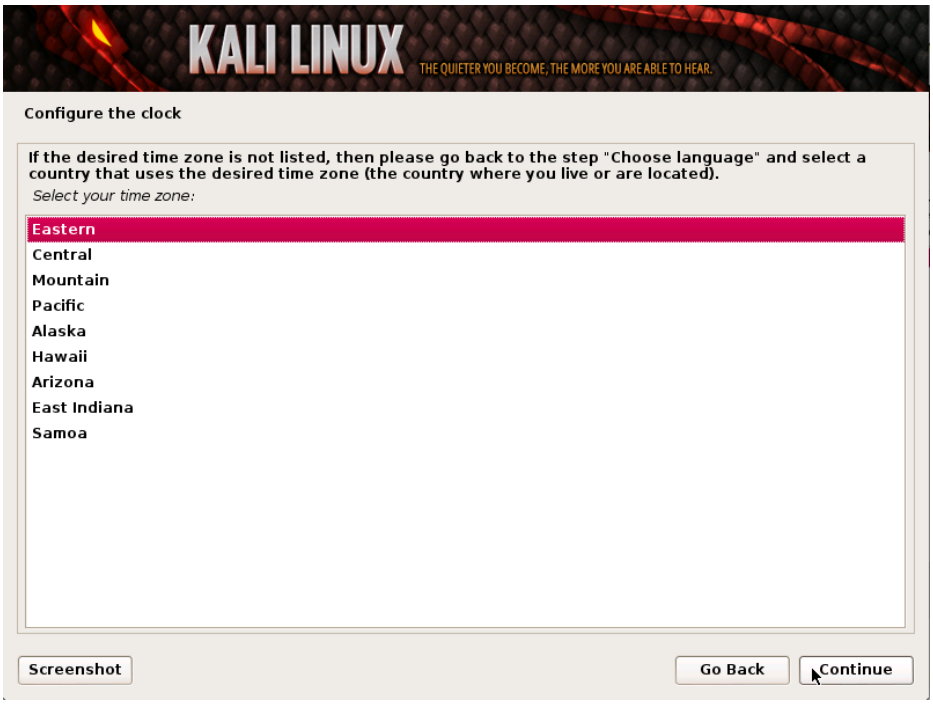
3. Installer akan mengcopy *images* ke hard disk Anda, mengecek *interface* jaringan Anda, dan kemudian meminta Anda untuk memasukkan nama host untuk sistem anda. Dalam contoh di bawah ini, kita sudah set “Kali” sebagai nama host kita.



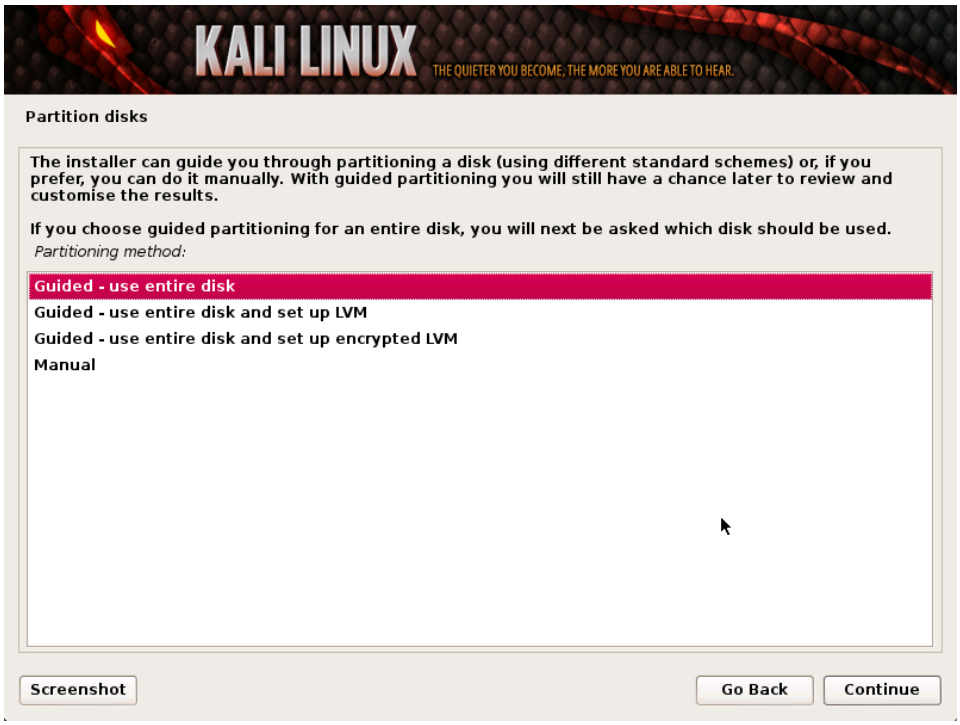
4. Masukkan password yang kuat untuk account root.



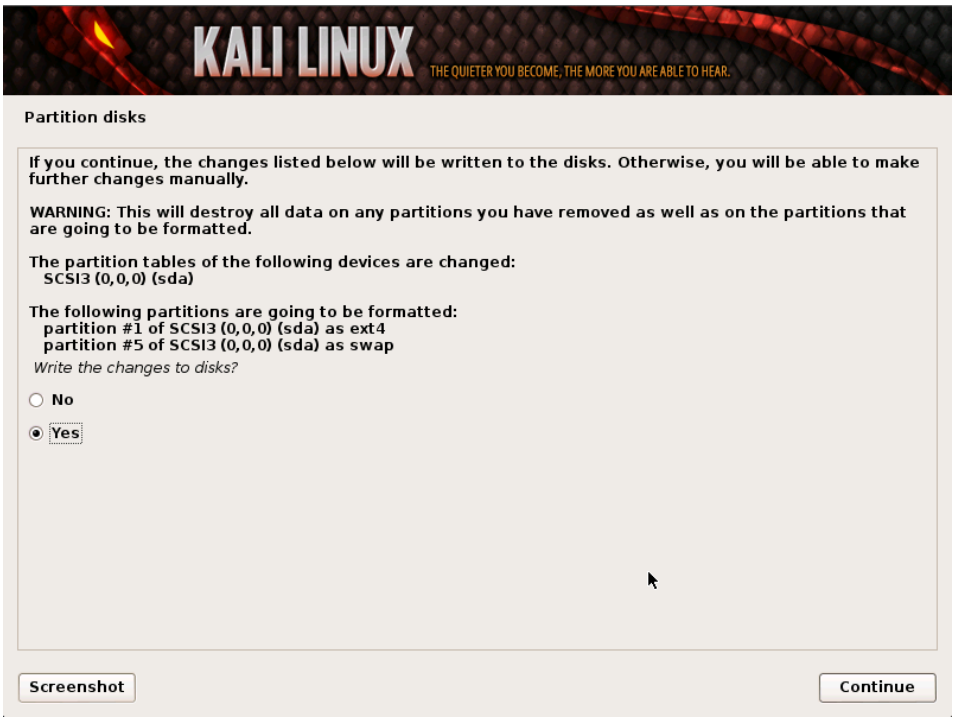
5. Selanjutnya, set zona waktu anda.



6. Installer sekarang akan menyelidiki disk Anda dan menawarkan empat pilihan. Dalam contoh ini, kita menggunakan seluruh disk pada komputer kita dan tidak mengkonfigurasi LVM (logical volume manager). Pengguna yang berpengalaman dapat menggunakan metode partisi “Manual” untuk pilihan konfigurasi yang lebih rinci.

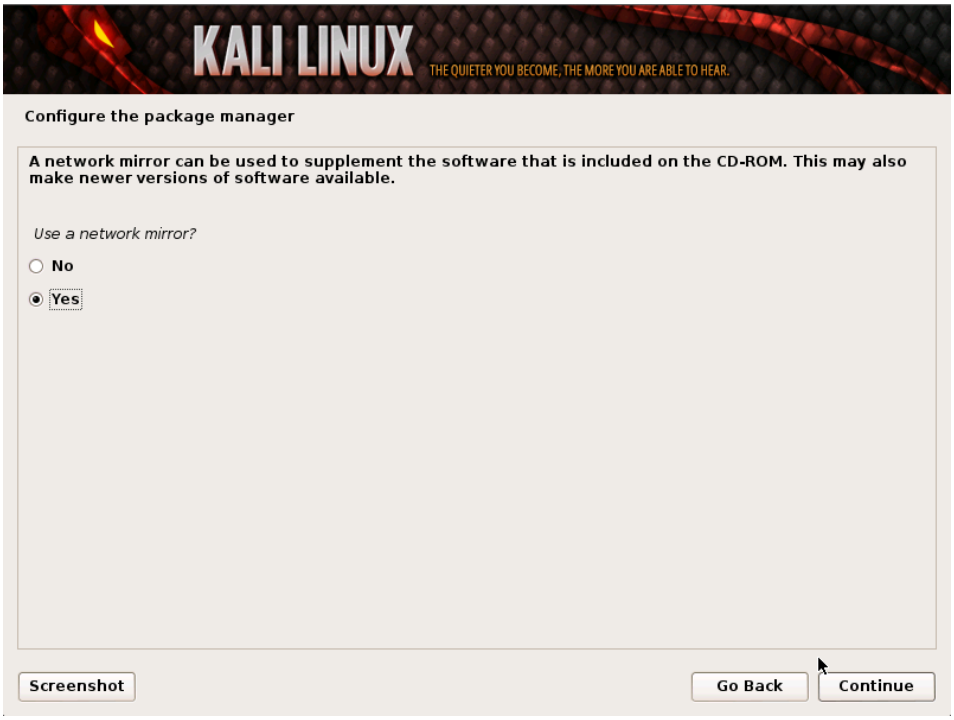


7. Selanjutnya, Anda akan memiliki satu kesempatan terakhir untuk meninjau konfigurasi disk Anda sebelum installer membuat perubahan yang tidak dapat dikembalikan. Setelah Anda klik *Continue*, installer akan melanjutkan proses nya dan hampir selesai installasinya.



8. Konfigurasi jaringan *mirror*. Kali menggunakan repositori terpusat untuk mendistribusikan aplikasi. Anda harus memasukkan informasi proxy yang tepat sesuai kebutuhan.

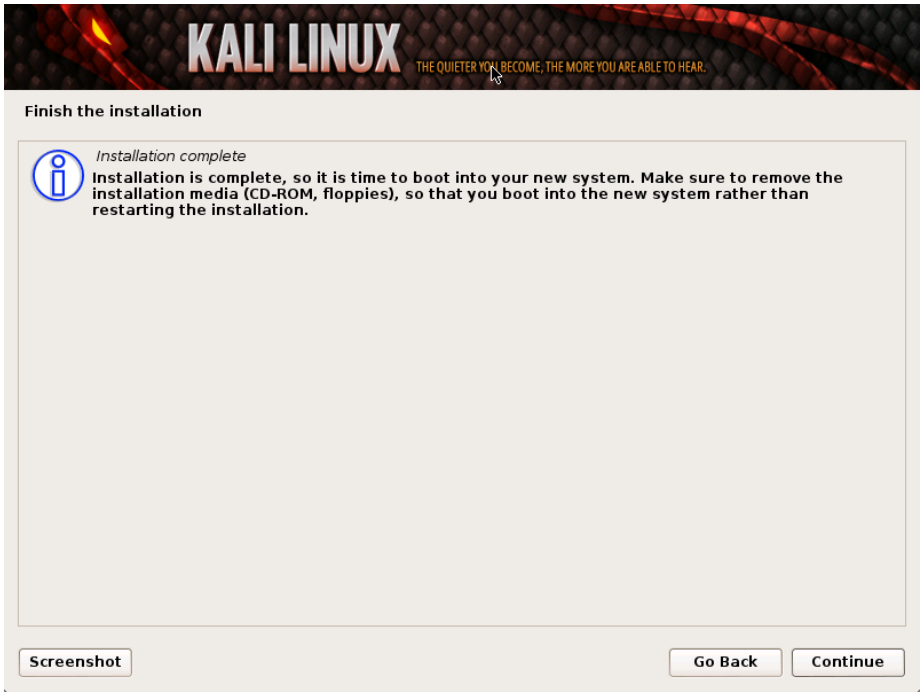
CATAT! Jika Anda pilih "NO" pada tampilan ini, Anda **TIDAK** akan dapat menginstall paket dari repositori Kali Linux.



9. Selanjutnya, install GRUB.



10. Terakhir, klik “Continue” untuk *reboot* ke installasi Kali Linux Anda yang baru.



Setelah Installasi
Sekarang Anda telah selesai menginstal Kali Linux, saatnya untuk melakukan kustomisasi sistem anda.

E. TUGAS

1. Berikan penjelasan perbedaan partisi LVM dengan encrypted LVM !

3 MANAGEMENT FILE

A. POKOK BAHASAN

1. Permission ataupun perizinan pada komputer/server berbasis Linux.
2. Perintah-perintah permission pada komputer/server.

B. TUJUAN

setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

1. Membangun sistem komputer yang aman.
2. Mengenal Permission file pada server.

C. PERALATAN

1. Sistem Operasi Linux Server

D. DASAR TEORI

Kenapa Kita perlu File Permission?

Jika kita tidak dapat mengakses beberapa file yang ada di dalah sistem Linux kita sendiri, biasanya itu karena kendala konfigurasi hak akses. Mungkin readers bertanya apa gunanya memiliki hak akses jika kita hanya pengguna tunggal di sistem Linux kita sendiri?

Untuk itu Linux di rancang untuk lingkungan multi-user (banyak pengguna). Dalam lingkungan banyak pengguna, sangat penting untuk memiliki sistem yang aman agar file di dalam sistem kita tidak di akses oleh sembarang orang.

Bahkan, jika kita hanya pengguna tunggal, Hak akses sangat di perlukan untuk menghindari kesalahan pihak luar atau kesalahan readers sendiri.|

Kepemilikan File

Setiap file di sistem Linux readers, termasuk direktori (folder), dimiliki oleh pengguna dan grup tertentu. Oleh karena itu, hak akses file di definisikan secara terpisah untuk User, Grup, dan Others (pengguna lain)

Pengertian:

- **User:** username orang yg memiliki file. Secara default, pengguna yg menciptakan file tersebut akan menjadi pemilik file tersebut.
- **Grup:** Grup User yang memiliki File tersebut. Semua pengguna yang masuk ke dalam kelompok mempunyai hak akses yang sama untuk file tersebut.
- **Others:** Pengguna yang bukan pemilik file dan tisak masuk ke dalam kelompok yang sama. Dengan kata lain jika readers menetapkan izin untuk „others“ maka orang yg tidak memiliki file atau grup inilah yang akan terkena pengaruhnya.

Hak Akses

Ada tiga jenis izin hak akses di Linux yaitu **Read, Write, Execute**

Pengertian:

- **Read:** Pada file biasa, ini berarti file dapat di buka dan di baca. Jika pada sebuah direktori, berarti readers bisa melihat isi direktori tersebut.
- **Write:** Pada file biasa, ini berarti file dapat di modifikasi (menambah, mengubah, menghapus, mengubah nama file dalam direktori).
- **Execute:** Pada file biasa, ini berarti readers bisa menjalankan file sebagai program atau shell script. Pada sebuah direktori, execute (atau biasa di sebut „search bit") memungkinkan readers untuk mengakses file dalam direktori misalnya : dengan perintah cd.

Izin Akses

Setiap obyek pada Linux harus mempunyai pemilik, yaitu nama pemakai Linux (account) yang terdaftar pada /etc/passwd. Ijin akses dibagi menjadi 3 peran yaitu :

- Pemilik (User)
- Kelompok (Group)
- Lainnya (Others)

Setiap peran dapat melakukan 3 bentuk operasi yaitu :

• Pada File

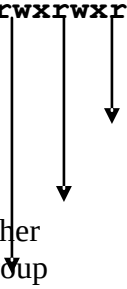
R (Read) Ijin untukmembaca
W (Write) Ijin untuk mengubah / membuat
X (Execute) Ijin untuk menjalankan program

• Pada Direktori

R (Read) Ijin untukmembaca daftar file dalam direktori
W (Write) Ijin untuk mengubah/membuat file di direktori
X (Execute) Ijin untuk masuk ke direktori (cd)

Pemilik File/Direktori dapat mengubah ijin akses sebagai berikut :

```
-rwxrwxrwx 1 student test 1639 Oct 31 20:19 file
```



other
group
user

Format untuk mengubah ijin akses

chmod [ugoa] [= + -] [rwx] File(s)
chmod [ugoa] [= + -] [rwx] Dir(s)

dimana u = user (pemilik)
g = group (kelompok)
o = others (lainnya)
a = al

Format lain dari chmod adalah menggunakan bilangan octal sebagai berikut

r	**w**	**x**		
4	**2**	**1**	**=**	**7**

E. PERCOBAAN

Bagaimana cara melihat Hak Akses di Linux ?

3. **Pertama,** kita bisa melihat hak akses dari file dengan mengetikkan perintah di terminal
   # ls –l

Hasilnya maka akan seperti ini:

```
cocoa@cocoa:~$ ls -l
total 304
-rw-------  1 root  root    1024 Sep 10 05:18 ~
drwxr-xr-x  2 cocoa cocoa   4096 Apr  2  2014 Azureus Downloads
-rw-------  1 cocoa cocoa 147467 Oct 10 11:07 bookmarks_10_10_14.html
drwxr-xr-x  2 cocoa cocoa   4096 Feb  4 07:39 Calibre Library
drwxr-xr-x  7 cocoa cocoa   4096 Feb  2 13:58 Desktop
-rw-r--r--  1 cocoa cocoa   1280 Oct  6 11:58 Diagram1.dia.autosave
drwxr-xr-x  4 cocoa cocoa   4096 Feb  4 07:49 Documents
drwx------  6 cocoa cocoa  16384 Feb  7 13:56 Downloads
drwxr-xr-x 12 cocoa cocoa   4096 Feb  7 13:32 Ebook
-rw-r--r--  1 root  root     140 Sep 29 16:29 eroor.txt
-rw-r--r--  1 cocoa cocoa  10178 Dec 26  2003 honeyd.conf.bloat
drwxr-xr-x  5 cocoa cocoa   4096 Feb  1 22:54 Images
drwxr-xr-x  2 cocoa cocoa   4096 Feb  4 07:51 Information
-rw-r-----  1 cocoa cocoa   4594 Oct  1 23:45 iptables.sh
drwxr-xr-x  5 cocoa cocoa   4096 Jan 21 10:28 Journal
-rw-r--r--  1 root  root      22 Aug  6  2014 links
drwxr-xr-x  2 cocoa cocoa   4096 Feb  4 08:05 Movie Videos
```

Apa arti outputnya?

Kolom pertama : merupakan jenis file dan perizinan yang mengikat file tersebut (perzinan meliputi perizinan User, Grup dan Others). Terdiri dari 10 karakter. Karakter pertama dari kolom pertama ini menunjukkan:

- d= directory
- -= regular file
- l= Sym bolic Link
- s= Unix Domain Socket
- p= named pipe
- c= character device file
- b= block device file

Lalu sisa 9 karakter lainnya menyatakan perizinan. Dibagi menjadi 3 grup. Tiap grup berisi 3 karakter yang mewakili : read, write dan execute. Karakter tersebut mudah diingat, diantaranya:

- r= read permission
- w= write permission
- x= execute permission
- -= no permission

Kolom kedua : menunjukkan jumlah Link (entri direktori yang merujuk ke file tersebut)
Kolom ketiga : menunjukkan pemilik file
Kolom keempat : menunjukan Grup pemilik file
Kolom kelima : menunjukkan ukuran file dalam byte
Kolom keenam, ketujuh dan kedelapan:menunjukan bulan dan tanggal terakhir di akses atau di modifikasi

Kolom kesembilan : menunjukkan nama file

Cara mengatur hak akses

Kita dapat mengatur hak akses file dengan perintah chmod. Di chmod terdapat 2 mode yang bisa di gunakan untuk konfigurasi hak akses file yaitu dengan cara simbolik dan numerik.

Cara Simbolik:

- **Pertama :** readers harus memutuskan apakah readers mengatur hak akses untuk pengguna (u), kelompok (g), pengguna lainnya (o), atau ketiganya (a).
- **Kedua :** readers bisa menambahkan izin (+), menghapus (-), atau menghapus izin sebelumnya dan menambahkan izin yang baru (=).
- **Ketiga :** tentukan perizinannya. Apakah readers mengatur izin read (r), write (w), execute (e), atau ketiganya.
- **Keempat :** readers hanya tinggal memberikan perintah untuk chmod, hak akses mana yang akan di rubah.

Mengubah Ijin akses (chmod)

pastikan dalam terminal ataupun command line interface. Lakukan perintah – perintah berikut, lakukan perbandingan pada setiap command yang telah di ketik.

```
$ touch file1 file2 file3
$ ls -l
$ chmod u+x file1
$ chmod g=w file1
$ chmod o-r file1
$ ls -l
$ chmod a=x file2
$ chmod u+x,g-r,o=w file3
$ ls -l
$ chmod 751 file1
$ chmod 624 file2
$ chmod 430 file3
$ ls -l
```

F. TUGAS

Lakukan lah perintah-perintah berikut dan lakukan perbandingan untuk setiap command.

```
$ touch file_A file_B file_C
$ ls -l
$ chmod 777 file_A
$ chmod 755 file_B
$ chmod 174 file_C
$ ls -l
$ chmod u=w file_A
$ chmod g+x file_B
$ chmod o-r file_C
```

4 FOOTPRINTING

A. POKOK BAHASAN

1. Footprinting atau mengumpulkan informasi target.
2. Perintah-perintah melakukakan footprinting pada komputer.

B. TUJUAN

setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

1. Mengenalkan pada mahasiswa tentang konsep Footprinting
2. Memahami konsep layanan whois pada layanan website
3. Mampu menganalisa kelemahan jaringan menggunakan software footprinting.

C. PERALATAN

1. Sistem Operasi Linux Penestrasi Kali

D. DASAR TEORI

Footprinting adalah segala kegiatan mengumpulkan informasi target yang akan di-hack sistemnya, sebelum melakukan penguasaan sistem sesungguhnya. Atau Footprinting, merupakan seni mencari atau mengumpulkan informasi yang berkaitan dengan target yang akan diserang. Mengapa proses footprinting ini penting? Karena menurut Certified Ethical Hacker (CEH), 90% waktu seorang hacker dan cracker dihabiskan untuk mengumpulkan informasi, sedangkan 10% untuk melakukan percobaan menguasai sistem server atau router.

Footprinting dapat dibagi 2 yaitu

1. inner footprinting dan
2. outer footprinting.

Inner footprinting adalah pencarian informasi terhadap suatu situs dimana Anda sudah berada di dalam jaringan komputer tersebut (Anda sudah berada didalam gedungnya dan menggunakan fasilitas internet gratis).

Outer Footprinting adalah pencarian informasi terhadap suatu situs dimana Anda tidak berada di dalam jaringan komputer target (Anda berada jauh dari komputer target).

E. PERCOBAAN

1. Masuk ke sistem operasi linux penestrasi.
2. Ketik pada konsole,aplikasi whois.

```
root@kali:~# whois
Usage: whois [OPTION]... OBJECT...
-l one level less specific lookup [RPSL only]
-L find all Less specific matches
-m find first level more specific matches
-M find all More specific matches
-c find the smallest match containing a mnt-irt
attribute
-x exact match [RPSL only]
```

```
-d return DNS reverse delegation objects too [RPSL only]
-i ATTR[,ATTR]... do an inverse lookup for specified ATTRibutes
-T TYPE[,TYPE]... only look for objects of TYPE
-K only primary keys are returned [RPSL only]
-r turn off recursive lookups for contact information
-R force to show local copy of the domain object even
if it contains referral
-a search all databases
-s SOURCE[,SOURCE]... search the database from SOURCE
-g SOURCE:FIRST-LAST find updates from SOURCE from serial FIRST to LAST
-t TYPE request template for object of TYPE ('all' for a
list)
-v TYPE request verbose template for object of TYPE
-q [version|sources|types] query specified server info [RPSL only]
-F fast raw output (implies -r)
-h HOST connect to server HOST
-p PORT connect to PORT
-H hide legal disclaimers
--verbose explain what is being done
--help display this help and exit
--version output version information and exit
```

Jika whois belum ada, maka lakukan instalasi whois melalui internet.

```
root@kali:~# apt-get install whois
```

3. Jalankan perintah – perintah pada whois melihat status layanan pada host target.

```
root@kali:~# whois ALAMAT_IP_TARGET
root@kali:~# whois -a ALAMAT_IP_TARGET
root@kali:~# whois -rld ALAMAT_IP_TARGET
root@kali:~# whois -c ALAMAT_IP_TARGET
```

Tulis dan jelaskan hasil perintah di atas pada laporan hasil praktikum ?

4. Ketik pada konsole, dmitry

```
root@kali:~# dmitry -h
Deepmagic Information Gathering Tool
"There be some deep magic going on"

dmitry: invalid option -- 'h'
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
-o Save output to %host.txt or to file specified by -o file
-i Perform a whois lookup on the IP address of a host
-w Perform a whois lookup on the domain name of a host
-n Retrieve Netcraft.com information on a host
-s Perform a search for possible subdomains
-e Perform a search for possible email addresses
-p Perform a TCP port scan on a host
* -f Perform a TCP port scan on a host showing output reporting filtered
ports
* -b Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
```

5. Jalankan perintah – perintah pada dmitry untuk melihat status service yang aktif di komputer.

```
root@kali:~# dmitry -n ALAMAT_IP_TARGET
```

```
root@kali:~# dmitry –iwse ALAMAT_IP_TARGET
root@kali:~# dmitry –pfb –o output.txt ALAMAT_IP_TARGET
root@kali:~# dmitry -winsepo output.txt ALAMAT_IP_TARGET
```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

6. Jalankan perintah – perintah pada tcptraceroute untuk melihat status service yang aktif di komputer.

```
root@kali:~# tcptraceroute
tcptraceroute 1.5beta7
Copyright (c) 2001-2006 Michael C. Toren <mct@toren.net>
Updates are available from http://michael.toren.net/code/tcptraceroute/

Usage: tcptraceroute [-nNFSAE] [-i <interface>] [-f <first ttl>]
[-l <packet length>] [-q <number of queries>] [-t <tos>]
[-m <max ttl>] [-pP] <source port>] [-s <source address>]
[-w <wait time>] <host> [destination port] [packet length]

root@kali:~#tcptraceroute –n ALAMAT_IP_TARGET
root@kali:~#tcptraceroute –N ALAMAT_IP_TARGET
root@kali:~#tcptraceroute –n ALAMAT_IP_TARGET –f3
root@kali:~#tcptraceroute –S ALAMAT_IP_TARGET –m25
root@kali:~#tcptraceroute –q3 –w 30 ALAMAT_IP_TARGET
root@kali:~#tcptraceroute –w5 ALAMAT_IP_TARGET
```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

F. TUGAS

1. Jalankan whois,dmitry,tcptraceroute secara online terhadap website domain berikut :
   - unsri.ac.id
   - kaskus.co.id
   - detik.com

5 PASSWORD MANAGEMENT

A. POKOK BAHASAN

1. Password Management pada komputer/server berbasis Linux.
2. Perintah-perintah untuk mengetahui password dan perlindungan pada komputer/server.

B. TUJUAN

setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

1. Mengenalkan pada mahasiswa tentang konsep dasar autentikasi password di linux
2. Memahami konsep shadow password
3. Mampu menganalisa kelemahan password dengan program password cracker yang ada

C. PERALATAN

1. Sistem Operasi Linux Penestrasi Kali

D. DASAR TEORI

Untuk dapat mengakses sistem operasi Linux digunakan mekanisme password. Pada distribusi-distribusi Linux yang lama, password tersebut disimpan dalam suatu file teks yang terletak di /etc/passwd. File ini harus dapat dibaca oleh setiap orang (world readable) agar dapat digunakan oleh program-program lain yang menggunakan mekanisme password tersebut.

Contoh isi file /etc/passwd :

```
root:..CETo68esYsA:0:0:root:/root:/bin/bash
bin:jvXHHBGCK7nkg:1:1:bin:/bin:
daemon:i1YD6CckS:2:2:daemon:/sbin:
adm:bj2NcvrnubUqU:3:4:adm:/var/adm:
rms:x9kxv932ckadsf:100:100:Richard M Stallman:/home/rms:/bin/bash
dmr:ZeoW7CaIcQmjhl:101:101:Dennis M Ritchie:/home/dmr:/bin/bash
linus:IK40Bb5NnkAHk:102:102:Linus Torvalds:/home/linus:/bin/bash
```

Keterangan :

- Field pertama : nama login
- Field kedua : password yang terenkripsi
- Field ketiga : User ID
- Field keempat : Group ID
- Field kelima : Nama sebenarnya
- Field keenam : Home directory user
- Field ketujuh : User Shell

Password login yang terdapat pada file /etc/passwd dienkripsi dengan menggunakan algoritma DES yang telah dimodifikasi. Meskipun demikian hal tersebut

tidak mengurangi kemungkinan password tersebut dibongkar (crack). Karena penyerang (attacker) dapat melakukan dictionary-based attack dengan cara :
menyalin file /etc/passwd tersebut
menjalankan program-program yang berguna untuk membongkar password, contohnya adalah John the Ripper (www.openwall.com/john/).

Untuk mengatasi permasalahan ini pada distribusi-distribusi Linux yang baru digunakan program utility shadow password yang menjadikan file /etc/passwd tidak lagi berisikan informasi password yang telah dienkripsi, informasi tersebut kini disimpan pada file /etc/shadow yang hanya dapat dibaca oleh root.

Berikut ini adalah contoh file /etc/passwd yang telah di-shadow :

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
rms:x:100:100:Richard M Stallman:/home/rms:/bin/bash
dmr:x:101:101:Dennis M Ritchie:/home/dmr:/bin/bash
linus:x:102:102:Linus Torvalds:/home/linus:/bin/bash
```

Dengan demikian, penggunaan shadow password akan mempersulit attacker untuk melakukan dictionary-based attack terhadap file password.

Selain menggunakan shadow password beberapa distribusi Linux juga menyertakan program hashing MD5 yang menjadikan password yang dimasukkan pemakai dapat berukuran panjang dan relatif mudah diingat karena berupa suatu passphrase.

Mekanisme yang telah disediakan sistem operasi tersebut di atas tidaklah bermanfaat bila pemakai tidak menggunakan password yang "baik". Berikut ini adalah beberapa kriteria yang dapat digunakan untuk membuat password yang "baik" :

1. Jangan menggunakan nama login anda dengan segala variasinya.
2. Jangan menggunakan nama pertama atau akhir anda dengan segala variasinya.
3. Jangan menggunakan nama pasangan atau anak anda.
4. Jangan menggunakan informasi lain yang mudah didapat tentang anda, seperti nomor telpon, tanggal lahir.
5. Jangan menggunakan password yang terdiri dari seluruhnya angka ataupun huruf yang sama.
6. Jangan menggunakan kata-kata yang ada di dalam kamus, atau daftar kata lainnya.
7. Jangan menggunakan password yang berukuran kurang dari enam karakter.
8. Gunakan password yang merupakan campuran antara huruf kapital dan huruf kecil.
9. Gunakan password dengan karakter-karakter non-alfabet.
10. Gunakan password yang mudah diingat, sehingga tidak perlu ditulis.
11. Gunakan password yang mudah diketikkan, tanpa perlu melihat pada keyboard.

Beberapa tool yang bisa dipakai untuk melihat strong tidaknya passwor adalah john the ripper. Kita bisa memakai utility ini untuk melihat strong tidaknya suatu pasword yang ada pada komputer.

E. PERCOBAAN

1. Masuk ke sistem operasi linux penestrasi kali
2. Masuk pada konsol untuk melihat /etc/passwd dan /etc/shadow

```
root@kali:#cat /etc/passwd
root@kali:#cat /etc/shadow
```

3. Ketik pada konsol,aplikasi john the ripper.

```
root@kali:~# john
John the Ripper password cracker, ver: 1.7.9-jumbo-7_omp [linux-x86-sse2]
Copyright (c) 1996-2012 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--config=FILE use FILE instead of john.conf or john.ini
--single[=SECTION] "single crack" mode
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
--pipe like --stdin, but bulk reads, and allows rules
--loopback[=FILE] like --wordlist, but fetch words from a .pot file
--dupe-suppression suppress all dupes in wordlist (and force preload)
--encoding=NAME input data is non-ascii (eg. UTF-8, ISO-8859-1).
For a full list of NAME use --list=encodings
--rules[=SECTION] enable word mangling rules for wordlist modes
--incremental[=MODE] "incremental" mode [using section MODE]
--markov[=OPTIONS] "Markov" mode (see doc/MARKOV)
--external=MODE external mode or word filter
--stdout[=LENGTH] just output candidate passwords [cut at LENGTH]
--restore[=NAME] restore an interrupted session [called NAME]
--session=NAME give a new session the NAME
--status[=NAME] print status of a session [called NAME]
--make-charset=FILE make a charset file. It will be overwritten
--show[=LEFT] show cracked passwords [if =LEFT, then uncracked]
--test[=TIME] run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..] load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..] load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX] load salts with[out] COUNT [to MAX] hashes
--pot=NAME pot file to use
--format=NAME force hash type NAME: afs bf bfegg bsdi crc32 crypt
des django dmd5 dominosec dragonfly3-32 dragonfly3-64
dragonfly4-32 dragonfly4-64 drupal7 dummy dynamic_n
epi episerver gost hdaa hmac-md5 hmac-sha1
hmac-sha224 hmac-sha256 hmac-sha384 hmac-sha512
hmailserver ipb2 keepass keychain krb4 krb5 lm lotus5
md4-gen md5 md5ns mediawiki mscash mscash2 mschapv2
mskrb5 mssql mssql05 mysql mysql-sha1 nethalflm netlm
netlmv2 netntlm netntlmv2 nsldap nt nt2 odf office
oracle oracle11 osc pdf phpass phps pix-md5 pkzip po
pwsafe racf rar raw-md4 raw-md5 raw-md5u raw-sha
raw-sha1 raw-sha1-linkedin raw-sha1-ng raw-sha224
raw-sha256 raw-sha384 raw-sha512 salted-sha1 sapb
sapg sha1-gen sha256crypt sha512crypt sip ssh
sybasease trip vnc wbb3 wpapsk xsha xsha512 zip
--list=WHAT list capabilities, see --list=help or doc/OPTIONS
--save-memory=LEVEL enable memory saving, at LEVEL 1..3
--mem-file-size=SIZE size threshold for wordlist preload (default 5 MB)
--nolog disables creation and writing to john.log file
--crack-status emit a status line whenever a password is cracked
--max-run-time=N gracefully exit after this many seconds
```

```
--regen-lost-salts=N regenerate lost salts (see doc/OPTIONS)
--plugin=NAME[,..] load this (these) dynamic plugin(s)
```

4. Jalankan john the ripper.

```
root@kali:~# unshadow passwd shadow > unshadowed.txt
root@kali:~# john ushadowed.txt
root@kali:~# john --show ushadowed.txt
```

Tulis dan jelaskan hasil perintah di atas pada laporan hasil praktikum ?

F. TUGAS

1. Apa kegunaan shadow password pada linux ?
2. Tampilkan password shadow pada sistem operasi anda !

```
root@bt:#cat /etc/passwd
root@bt:#cat /etc/shadow
```

6 NETWORK SCANNING & ENUMERATION

A. POKOK BAHASAN

1. Network Scanning & Enumeration pada komputer/server berbasis Linux.
2. Perintah-perintah untuk melakukan network scanning pada komputer/server.

B. TUJUAN

setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

1. Mengenalkan pada mahasiswa tentang konsep Scanner dan Probing
2. Memahami konsep layanan jaringan dan port numbering
3. Mampu menganalisa kelemahan jaringan menggunakan software scanning yang ada

C. PERALATAN

1. Sistem Operasi Linux Penestrasi Kali dan Server Linux

D. DASAR TEORI

Server tugasnya adalah melayani client dengan menyediakan service yang dibutuhkan. Server menyediakan service dengan bermacam-macam kemampuan, baik untuk lokal maupun remote. Server listening pada suatu port dan menunggu incomming connection ke port. Koneksi bisa berupa lokal maupuan remote.

Port sebenarnya suatu alamat pada stack jaringan kernel, sebagai cara dimana transport layer mengelola koneksi dan melakukan pertukaran data antar komputer. Port yang terbuka mempunyai resiko terkait dengan exploit. Perlu dikelola port mana yang perlu dibuka dan yang ditutup untuk mengurangi resiko terhadap exploit.

Ada beberapa utility yang bisa dipakai untuk melakukan diagnosa terhadap sistem service dan port kita. Utility ini melakukan scanning terhadap sistem untuk mencari port mana saja yang terbuka, ada juga sekaligus memberikan laporan kelemahan sistem jika port ini terbuka.

Port Scanner merupakan program yang didesain untuk menemukan layanan (service) apa saja yang dijalankan pada host jaringan. Untuk mendapatkan akses ke host, cracker harus mengetahui titik-titik kelemahan yang ada. Sebagai contoh, apabila cracker sudah mengetahui bahwa host menjalankan proses ftp server, ia dapat menggunakan kelemahan-kelemahan yang ada pada ftp server untuk mendapatkan akses. Dari bagian ini kita dapat mengambil kesimpulan bahwa layanan yang tidak benar-benar diperlukan sebaiknya dihilangkan untuk memperkecil resiko keamanan yang mungkin terjadi.

Type Scanning

connect scan (-sT)

Jenis scan ini konek ke port sasaran dan menyelesaikan three-way handshake (SYN,SYN/ACK, dan ACK). Scan jenis ini mudah terdeteksi oleh sistem sasaran.

-sS (TCP SYN scan)

Paling populer dan merupakan scan default nmap. SYN scan juga sukar terdeteksi, karena tidak menggunakan 3 way handshake secara lengkap, yang disebut sebagai teknik half open scanning. SYN scan juga efektif karena dapat membedakan 3 state port, yaitu open, filterd ataupun close. Teknik ini dikenal sebagai half-opening scanning karena suatu koneksi penuh TCP tidak sampai terbentuk. Sebaliknya, suatu paket SYN dikirimkan ke port sasaran. Bila SYN/ACK diterima dari port sasaran, kita dapat mengambil kesimpulan bahwa port itu berada dalam status LISTENING. Suatu RST/ACT akan dikirim oleh mesin yang melakukan scanning sehingga koneksi penuh tidak akan terbentuk. Teknik ini bersifat siluman dibandingkan TCP connect penuh, dan tidak aka tercatat pada log sistem sasaran.

TCP FIN scan (-sF)

Teknik ini mengirim suatu paket FIN ke port sasaran. Berdasarkan RFC 793, sistem sasaran akan mengirim balik suatu RST untuk setiap port yang tertutup. Teknik ini hanya dapat dipakai pada stack TCP/IP berbasis UNIX.

TCP Xmas Tree scan (-sX)

Teknik ini mengirimkan suatu paket FIN, URG, dan PUSH ke port sasaran. Berdasarkan RFC 793, sistem sasaran akan mengembalikan suatu RST untuk semua port yang tertutup.

TCP Null scan (-sN)

Teknik ini membuat off semua flag. Berdasarkan RFC 793, sistem sasaran akan mengirim balik suatu RST untuk semua port yang tertutup.

TCP ACK scan (-sA)

Teknik ini digunakan untuk memetakan set aturan firewall. Dapat membantu menentukan apakah firewall itu merupakan suatu simple packet filter yang membolehkan hanya koneksi-koneksi tertentu (koneksi dengan bit set ACK) atau suatu firewall yang menjalankan advance packet filtering.

TCP Windows scan

Teknik ini dapat mendeteksi port-port terbuka maupun terfilter/tidak terfilter pada sistem-sistem tertentu (sebagai contoh, AIX dan FreeBSD) sehubungan dengan anomali dari ukuran windows TCP yang dilaporkan.

TCP RPC scan

Teknik ini spesifik hanya pada system UNIX dan digunakan untuk mendeteksi dan mengidentifikasi port RPC (Remote Procedure Call) dan program serta normor versi yang berhubungan dengannya.

UDP scan (-sU)

Teknik ini mengirimkan suatu paket UDP ke port sasaran. Bila port sasaran memberikan respon berupa pesan (ICMP port unreachable) artinya port ini tertutup. Sebaliknya bila tidak menerima pesan di atas, kita dapat menyimpulkan bahwa port itu terbuka.Karena UDP dikenal sebagai connectionless protocol, akurasi teknik ini sangat bergantung pada banyak hal sehubungan dengan penggunaan jaringan dan system resource. Sebagai tambahan, UDP scanning merupakan proses yang amat lambat apabila anda mencoba men-scan suatu perangkat yang menjalankan packet filtering berbeban tinggi.

Beberapa Tools dan cara scanning ke sistem :

Netstat

Netstat merupakan utility yang powerfull untuk menngamati current state pada server, service apa yang listening untuk incomming connection, interface mana yang listening, siapa saja yang terhubung.

Nmap

Merupakan software scanner yang paling tua yang masih dipakai sampai sekarang.

E. PERCOBAAN

1. Masuk ke sistem operasi linux kali
2. Ketik pada konsol,aplikasi nmap.

```
root@kali:~# nmap -h
Nmap 6.40 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
-sL: List Scan - simply list targets to scan
-sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports consecutively - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
-sV: Probe open ports to determine service/version info
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
-sC: equivalent to --script=default
--script=<Lua scripts>: <Lua scripts> is a comma separated list of
directories, script-files or script-categories
```

```
--script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
--script-args-file=filename: provide NSE script args in a file
--script-trace: Show all data sent and received
--script-updatedb: Update the script database.
--script-help=<Lua scripts>: Show help about scripts.
<Lua scripts> is a comma separted list of script-files or
script-categories.
OS DETECTION:
-O: Enable OS detection
--osscan-limit: Limit OS detection to promising targets
--osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
Options which take <time> are in seconds, or append 'ms' (milliseconds),
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
-T<0-5>: Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>: Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
probe round trip time.
--max-retries <tries>: Caps number of port scan probe retransmissions.
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--log-errors: Log errors/warnings to the normal-format output file
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and
traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
```

```
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND
EXAMPLES
```

3. Jalankan perintah – perintah pada nmap melihat status service yang aktif di komputer.

```
root@kali:~# nmap -sP ALAMAT_IP_HOST
root@kali:~# nmap -sS -P0 ALAMAT_IP_HOST | grep open
root@kali:~# nmap -v -O ALAMAT_IP_HOST | grep OS
root@kali:~# nmap -sSU -P0 ALAMAT_IP_HOST | grep open
```

Tulis dan jelaskan hasil perintah di atas pada laporan hasil praktikum ?

4. Ketik pada console, netstat

```
root@kali:~# netstat --help
usage: netstat [-vWeenNcCF] [<Af>] -r netstat {-V|--version|-h|--
help}
netstat [-vWnNcaeol] [<Socket> ...]
netstat { [-vWeenNac] -i | [-cWnNe] -M | -s }

-r, --route display routing table
-i, --interfaces display interface table
-g, --groups display multicast group memberships
-s, --statistics display networking statistics (like SNMP)
-M, --masquerade display masqueraded connections

-v, --verbose be verbose
-W, --wide don't truncate IP addresses
-n, --numeric don't resolve names
--numeric-hosts don't resolve host names
--numeric-ports don't resolve port names
--numeric-users don't resolve user names
-N, --symbolic resolve hardware names
-e, --extend display other/more information
-p, --programs display PID/Program name for sockets
-c, --continuous continuous listing

-l, --listening display listening server sockets
-a, --all, --listening display all sockets (default: connected)
-o, --timers display timers
-F, --fib display Forwarding Information Base
(default)
-C, --cache display routing cache instead of FIB

<Socket>={-t|--tcp} {-u|--udp} {-w|--raw} {-x|--unix} --ax25 --ipx --
netrom
<AF>=Use '-6|-4' or '-A <af>' or '--<af>'; default: inet
List of possible address families (which support routing):
inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
x25 (CCITT X.25)
```

5. Jalankan perintah – perintah pada netstat untuk melihat status service yang aktif di komputer.

```
root@kali:~# netstat –tpane
root@kali:~# netstat –upane
```

6. Ketik pada console

```
root@kali:~# nping -h
Nping 0.6.40 ( http://nmap.org/nping )
Usage: nping [Probe mode] [Options] {target specification}

TARGET SPECIFICATION:
Targets may be specified as hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.*.1-24
PROBE MODES:
--tcp-connect : Unprivileged TCP connect probe mode.
--tcp : TCP probe mode.
--udp : UDP probe mode.
--icmp : ICMP probe mode.
--arp : ARP/RARP probe mode.
--tr, --traceroute : Traceroute mode (can only be used with
TCP/UDP/ICMP modes).
TCP CONNECT MODE:
-p, --dest-port <port spec> : Set destination port(s).
-g, --source-port <portnumber> : Try to use a custom source port.
TCP PROBE MODE:
-g, --source-port <portnumber> : Set source port.
-p, --dest-port <port spec> : Set destination port(s).
--seq <seqnumber> : Set sequence number.
--flags <flag list> : Set TCP flags (ACK,PSH,RST,SYN,FIN...)
--ack <acknumber> : Set ACK number.
--win <size> : Set window size.
--badsum : Use a random invalid checksum.
UDP PROBE MODE:
-g, --source-port <portnumber> : Set source port.
-p, --dest-port <port spec> : Set destination port(s).
--badsum : Use a random invalid checksum.
ICMP PROBE MODE:
--icmp-type <type> : ICMP type.
--icmp-code <code> : ICMP code.
--icmp-id <id> : Set identifier.
--icmp-seq <n> : Set sequence number.
--icmp-redirect-addr <addr> : Set redirect address.
--icmp-param-pointer <pnt> : Set parameter problem pointer.
--icmp-advert-lifetime <time> : Set router advertisement lifetime.
--icmp-advert-entry <IP,pref> : Add router advertisement entry.
--icmp-orig-time <timestamp> : Set originate timestamp.
--icmp-recv-time <timestamp> : Set receive timestamp.
--icmp-trans-time <timestamp> : Set transmit timestamp.
ARP/RARP PROBE MODE:
--arp-type <type> : Type: ARP, ARP-reply, RARP, RARP-reply.
--arp-sender-mac <mac> : Set sender MAC address.
--arp-sender-ip <addr> : Set sender IP address.
--arp-target-mac <mac> : Set target MAC address.
--arp-target-ip <addr> : Set target IP address.
IPv4 OPTIONS:
-S, --source-ip : Set source IP address.
--dest-ip <addr> : Set destination IP address (used as an
alternative to {target specification}
).
--tos <tos> : Set type of service field (8bits).
--id <id> : Set identification field (16 bits).
```

```
--df : Set Don't Fragment flag.
--mf : Set More Fragments flag.
--ttl <hops> : Set time to live [0-255].
--badsum-ip : Use a random invalid checksum.
--ip-options <S|R [route]|L [route]|T|U ...> : Set IP options
--ip-options <hex string> : Set IP options
--mtu <size> : Set MTU. Packets get fragmented if MTU
is
small enough.
IPv6 OPTIONS:
-6, --IPv6 : Use IP version 6.
--dest-ip : Set destination IP address (used as an
alternative to {target specification}).
--hop-limit : Set hop limit (same as IPv4 TTL).
--traffic-class <class> : : Set traffic class.
--flow <label> : Set flow label.
ETHERNET OPTIONS:
--dest-mac <mac> : Set destination mac address. (Disables
ARP resolution)
--source-mac <mac> : Set source MAC address.
--ether-type <type> : Set EtherType value.
PAYLOAD OPTIONS:
--data <hex string> : Include a custom payload.
--data-string <text> : Include a custom ASCII text.
--data-length <len> : Include len random bytes as payload.
ECHO CLIENT/SERVER:
--echo-client <passphrase> : Run Nping in client mode.
--echo-server <passphrase> : Run Nping in server mode.
--echo-port <port> : Use custom <port> to listen or connect.
--no-crypto : Disable encryption and authentication.
--once : Stop the server after one connection.
--safe-payloads : Erase application data in echoed
packets.
TIMING AND PERFORMANCE:
Options which take <time> are in seconds, or append 'ms' (milliseconds),
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m,
0.25h).
--delay <time> : Adjust delay between probes.
--rate <rate> : Send num packets per second.
MISC:
-h, --help : Display help information.
-V, --version : Display current version number.
-c, --count <n> : Stop after <n> rounds.
-e, --interface <name> : Use supplied network interface.
-H, --hide-sent : Do not display sent packets.
-N, --no-capture : Do not try to capture replies.
--privileged : Assume user is fully privileged.
--unprivileged : Assume user lacks raw socket
privileges.
--send-eth : Send packets at the raw Ethernet layer.
--send-ip : Send packets using raw IP sockets.
--bpf-filter <filter spec> : Specify custom BPF filter.
OUTPUT:
-v : Increment verbosity level by one.
-v[level] : Set verbosity level. E.g: -v4
-d : Increment debugging level by one.
-d[level] : Set debugging level. E.g: -d3
-q : Decrease verbosity level by one.
-q[N] : Decrease verbosity level N times
--quiet : Set verbosity and debug level to
minimum.
--debug : Set verbosity and debug to the max
level.
```

```
EXAMPLES:
nping scanme.nmap.org
nping --tcp -p 80 --flags rst --ttl 2 192.168.1.1
nping --icmp --icmp-type time --delay 500ms 192.168.254.254
nping --echo-server "public" -e wlan0 -vvv
nping --echo-client "public" echo.nmap.org --tcp -p1-1024 --flags ack

SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

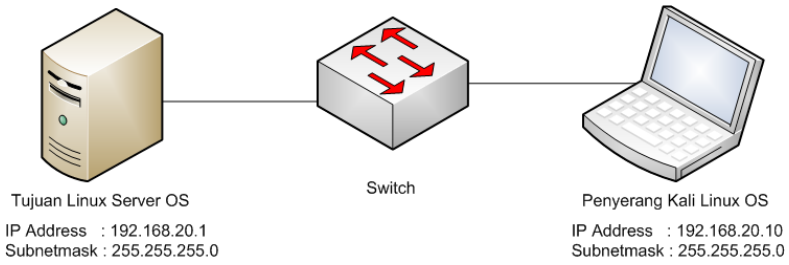
7. Jalankan perintah – perintah pada nping untuk melihat status service yang dikomputer.

```
root@kali:~# nping ALAMAT_IP_HOST
```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

F. TUGAS

1. Buatlah skenario topologi offline sebagai berikut :



Jadikan server ubuntu linux sebagai target dan system operasi kali linux sebagai penyerang.

2. Lakukan penestrasi dengan menggunakan tools nmap,nping dari penyerang ke server.adapun command yang di lakukakan sebagai berikut :

```
root@kali:~# nmap -v -A ALAMAT_IP_HOST
root@kali:~# nping ALAMAT_IP_HOST
```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

7 DENIAL of SERVICE ATTACK (DoS)

A. POKOK BAHASAN

1. Denial of Service pada komputer/server berbasis Linux.
2. Perintah-perintah tools DoS pada komputer/server.

B. TUJUAN

setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

1. Mengenalkan pada mahasiswa tentang konsep Denial of Service
2. Mahasiswa mampu menangani masalah DoS

C. PERALATAN

1. Sistem Operasi Linux Penestrasi Kali dan Server Linux

D. DASAR TEORI

Denial of Service adalah aktifitas menghambat kerja sebuah layanan (servis) atau mematikan-nya, sehingga user yang berhak/berkepentingan tidak dapat menggunakan layanan tersebut. Dampak akhir dari aktifitas ini menjurus kepada tehambatnya aktifitas korban yang dapat berakibat sangat fatal (dalam kasus tertentu).

Pada dasarnya Denial of Service merupakan serangan yang sulit diatasi, hal ini disebabkan oleh resiko layanan publik dimana admin akan berada pada kondisi yang membingungkan antara layanan dan kenyamanan terhadap keamanan. Seperti yang kita tahu, keyamanan berbanding terbalik dengan keamanan. Maka resiko yang mungkin timbul selalu mengikuti hukum ini.

Beberapa aktifitas DoS adalah:

1. Aktifitas 'flooding' terhadap suatu server.
2. Memutuskan koneksi antara 2 mesin.
3. Mencegah korban untuk dapat menggunakan layanan.
4. Merusak sistem agar korban tidak dapat menggunakan layanan

Beberapa tipe-tipe serangan DoS.

SYN-Flooding

SYN-Flooding merupakan network Denial ofService yang memanfaatkan 'loophole' pada saat koneksi TCP/IP terbentuk. Kernel Linux terbaru (2.0.30 dan yang lebih
baru) telah mempunyai option konfigurasi untuk mencegah Denial of Service dengan mencegahmenolak cracker untuk mengakses sistem.

Pentium 'FOOF' Bug

Merupakan serangan Denial of Service terhadap prosessor Pentium yang menyebabkan sistem menjadi reboot. Hal ini tidak bergantung terhadap jenis sistem

operasi yang digunakan tetapi lebih spesifik lagi terhadap prosessor yang digunakan yaitu pentium.

Ping Flooding

Ping Flooding adalah brute force Denial of Service sederhana. Jika serangan dilakukan oleh penyerang dengan bandwidth yang lebih baik dari korban, maka mesin korban tidak dapat mengirimkan paket data ke dalam jaringan (network). Hal ini terjadi karena mesin korban di banjiri (flood) oleh peket-paket ICMP. Varian dari serangan ini disebut "smurfing"

Pencegahan DoS

Selalu Up 2 Date.

Seperti contoh serangan diatas, SYN Flooding sangat efektif untuk membekukan Linux kernel 2.0.*. Dalam hal ini Linux kernel 2.0.30 keatas cukup handal untuk mengatasi serangan tersebut dikarenakan versi 2.0.30 memiliki option untuk menolak cracker untuk mengakses system.

Ikuti perkembangan security

Hal ini sangat efektif dalam mencegah pengerusakan sistem secara ilegal. Banyak admin malas untuk mengikuti issue-issue terbaru perkembangan dunia security. Dampak yang paling buruk, sistem cracker yang 'rajin', 'ulet' dan 'terlatih' akan sangat mudah untuk memasuki sistem dan merusak - tidak tertutup kemungkinan untuk melakukan Denial of Service -.

E. PERCOBAAN

1. Masuk ke sistem operasi linux kali
2. Ketik pada console.

```
root@kali:~# hping3 -h
usage: hping3 host [options]
-h --help show this help
-v --version show version
-c --count packet count
-i --interval wait (uX for X microseconds, for example -i u1000)
--fast alias for -i u10000 (10 packets for second)
--faster alias for -i u1000 (100 packets for second)
--flood sent packets as fast as possible. Don't show replies.
-n --numeric numeric output
-q --quiet quiet
-I --interface interface name (otherwise default routing interface)
-V --verbose verbose mode
-D --debug debugging info
-z --bind bind ctrl+z to ttl (default to dst port)
-Z --unbind unbind ctrl+z
--beep beep for every matching packet received
Mode
default mode TCP
-0 --rawip RAW IP mode
-1 --icmp ICMP mode
-2 --udp UDP mode
-8 --scan SCAN mode.
Example: hping --scan 1-30,70-90 -S www.target.host
-9 --listen listen mode
IP
-a --spoof spoof source address
```

```
--rand-dest random destionation address mode. see the man.
--rand-source random source address mode. see the man.
-t --ttl ttl (default 64)
-N --id id (default random)
-W --winid use win* id byte ordering
-r --rel relativize id field (to estimate host traffic)
-f --frag split packets in more frag. (may pass weak acl)
-x --morefrag set more fragments flag
-y --dontfrag set don't fragment flag
-g --fragoff set the fragment offset
-m --mtu set virtual mtu, implies --frag if packet size > mtu
-o --tos type of service (default 0x00), try --tos help
-G --rroute includes RECORD_ROUTE option and display the route buffer
--lsrr loose source routing and record route
--ssrr strict source routing and record route
-H --ipproto set the IP protocol field, only in RAW IP mode
ICMP
-C --icmptype icmp type (default echo request)
-K --icmpcode icmp code (default 0)
--force-icmp send all icmp types (default send only supported types)
--icmp-gw set gateway address for ICMP redirect (default 0.0.0.0)
--icmp-ts Alias for --icmp --icmptype 13 (ICMP timestamp)
--icmp-addr Alias for --icmp --icmptype 17 (ICMP address subnet mask)
--icmp-help display help for others icmp options
UDP/TCP
-s --baseport base source port (default random)
-p --destport [+][+]<port> destination port(default 0) ctrl+z inc/dec
-k --keep keep still source port
-w --win winsize (default 64)
-O --tcpoff set fake tcp data offset (instead of tcphdrlen / 4)
-Q --seqnum shows only tcp sequence number
-b --badcksum (try to) send packets with a bad IP checksum
many systems will fix the IP checksum sending the packet
so you'll get bad UDP/TCP checksum instead.
-M --setseq set TCP sequence number
-L --setack set TCP ack
-F --fin set FIN flag
-S --syn set SYN flag
-R --rst set RST flag
-P --push set PUSH flag
-A --ack set ACK flag
-U --urg set URG flag
-X --xmas set X unused flag (0x40)
-Y --ymas set Y unused flag (0x80)
--tcpexitcode use last tcp->th_flags as exit code
--tcp-mss enable the TCP MSS option with the given value
--tcp-timestamp enable the TCP timestamp option to guess the HZ/uptime
Common
-d --data data size (default is 0)
-E --file data from file
-e --sign add 'signature'
-j --dump dump packets in hex
-J --print dump printable characters
-B --safe enable 'safe' protocol
-u --end tell you when --file reached EOF and prevent rewind
-T --traceroute traceroute mode (implies --bind and --ttl 1)
--tr-stop Exit when receive the first not ICMP in traceroute mode
--tr-keep-ttl Keep the source TTL fixed, useful to monitor just one hop
--tr-no-rtt Don't calculate/show RTT information in traceroute mode
ARS packet description (new, unstable)
--apd-send Send the packet described with APD (see docs/APD.txt)
```

3. Jalankan perintah – perintah pada hping3 dan nping untuk melihat status service yang dikomputer.
   - Simple SYN flood

     ```
     root@kali:~# hping3 -S --flood -V www.alamattarget.com
     ```

   - Simple SYN flood with spoofed IP

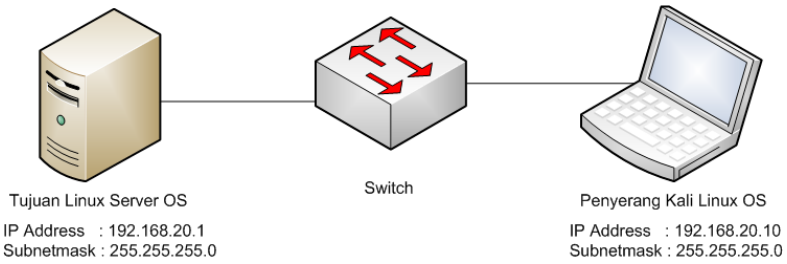
```
root@kali:~# hping3 -S -P -U --flood -V --rand-source www.alamattarget.com
```

   - TCP connect flood

     ```
     root@kali:~# nping --tcp-connect -rate=90000 -c 900000 -q www.target.com
     ```

F. TUGAS

1. Buatlah skenario topologi offline sebagai berikut :



   Jadikan server ubuntu linux sebagai target dan system operasi kali linux sebagai penyerang.

2. Lakukan penestrasi dengan menggunakan tools nmap,nping dari penyerang ke server.adapun command yang di lakukakan sebagai berikut :

```
root@kali:~# hping3 -S --flood -V 192.168.20.1
root@kali:~# hping3 -S -P -U --flood -V --rand-source 192.168.20.1
root@kali:~# nping --tcp-connect -rate=90000 -c 900000 -q 192.168.20.1
```

   Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

3. Lakukan monitoring dengan menggunakan tools tcpdump dari terhadap server.adapun command yang di lakukakan sebagai berikut :

   Sebelum melakukan melakukan instalasi tcpdump pada server dengan menggunakan jaringan internet.

```
root@server:~# apt-get install tcpdump
root@server:~# tcpdump -i eth0
```

   Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

8 BRUTE FORCE ATTACK

A. POKOK BAHASAN

1. Brute Force pada komputer/server berbasis Linux.
2. Perintah-perintah tools Brute Force pada komputer/server.

B. TUJUAN

setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

1. Mengenalkan pada mahasiswa konsep tentang Brute Force
2. Mahasiswa mampu menangani masalah Brute Force

C. PERALATAN

1. Sistem Operasi Linux Penestrasi Kali dan Server Linux

D. DASAR TEORI

Serangan brute-force adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin. Pendekatan ini pada awalnya merujuk pada sebuah program komputer yang mengandalkan kekuatan pemrosesan komputer dibandingkan kecerdasan manusia.

Sebagai contoh, untuk menyelesaikan sebuah persamaan kuadrat seperti $x^2+7x-44=0$, di mana x adalah sebuah integer, dengan menggunakan teknik serangan brute force, penggunanya hanya dituntut untuk membuat program yang mencoba semua nilai integer yang mungkin untuk persamaan tersebut hingga nilai x sebagai jawabannya muncul. Istilah brute force sendiri dipopulerkan oleh Kenneth Thompson, dengan mottonya: "When in doubt, use brute-force" (jika ragu, gunakan brute-force). Secara sederhana, menebak password dengan mencoba semua kombinasi karakter yang mungkin. Brute force attack digunakan untuk menjebol akses ke suatu host (server/workstation/network) atau kepada data yang terenkripsi.

Metode ini dipakai para cracker untuk mendapatkan account secara tidak sah, dan sangat berguna untuk memecahkan enkripsi.

Enkripsi macam apapun, seperti Blowfish, AES, DES, Triple DES dsb secara teoritis dapat dipecahkan dengan brute-force attack. Pemakaian password sembarangan, memakai password yang cuma sepanjang 3 karakter, menggunakan kata kunci yang mudah ditebak, menggunakan password yang sama, menggunakan nama, memakai nomor telepon, sudah pasti sangat tidak aman. Namun brute force attack bisa saja memakan waktu bahkan sampai berbulan-bulan atau tahun bergantung dari bagaimana rumit passwordnya.

Brute Force attack tidak serumit dan low-tech seperti algoritma hacking yang berkembang sekarang. Seorang penyerang hanya cukup menebak anama dan kombinasi password sampai dia menemukan yang cocok. Mungkin terlihat bahwa brute force attack atau dictionary attack tidak mungkin berhasil. Namun yang mengejutkan, kemungkinan berhasil brute force attack menjadi membaik ketika site yang ingin diretasi tidak dikonfigurasikan dengan baik. Beberapa faktor yang menjadi

keuntungan seorang hacker, bisanya disebabkan oleh kemalasan manusia itu sendiri, Hal-hal yang perlu diperhatikan dalam menggunakan metode brute force attack :
a. Asumsikan bahwa password diketik dalam huruf kecil (lower case).

Pada kasus ini, waktu yang dibutuhkan akan cenderung sama tetapi jika password mengandung huruf kapital (upper case) cara ini tidak akan berhasil.
b. Coba semua kemungkinan. Tujuh karakter lower case membutuhkan sekitar 4 jam untuk berhasil mendapatkan password tetapi jika dicoba semua kemungkinan kombinasi antara karakter upper case dan lower case akan membutuhkan waktu sekitar 23 hari.
c. Metode ketiga adalah trade-off. Hanya kombinasi-kombinasi yang mungkin yang dimasukkan dalam pencarian, sebagai contoh “password”, “PASSWORD” dan “Password”. Kombinasi rumit seperti “pAssWOrD” tidak dimasukkan dalam proses.

Dalam kasus ini, lambatnya proses dapat tertangani tetapi ada kemungkinan password tidak ditemukan.

E. PERCOBAAN

1. Masuk ke sistem operasi linux kali
2. Ketik pada console.

```
root@kali:~# hydra -h
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes
only

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr]
[-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT]
[-x MIN:MAX:CHARSET] [-SuvV46] [service://server[:PORT][/OPT]]

Options:
-R restore a previous aborted/crashed session
-S perform an SSL connect
-s PORT if the service is on a different default port, define it here
-l LOGIN or -L FILE login with LOGIN name, or load several logins from
FILE
-p PASS or -P FILE try password PASS, or load several passwords from
FILE
-x MIN:MAX:CHARSET password bruteforce generation, type "-x -h" to get
help
-e nsr try "n" null password, "s" login as pass and/or "r" reversed
login
-u loop around users, not passwords (effective! implied with -x)
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to be attacked in parallel, one entry per line
-o FILE write found login/password pairs to FILE instead of stdout
-f / -F exit when a login/pass pair is found (-M: -f per host, -F
global)
-t TASKS run TASKS number of connects in parallel (per host, default: 16)
-w / -W TIME waittime for responses (32s) / between connects per thread
-4 / -6 prefer IPv4 (default) or IPv6 addresses
-v / -V / -d verbose mode / show login+pass for each attempt / debug mode
-U service module usage details
server the target server (use either this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module
help)

Supported services: asterisk afp cisco cisco-enable cvs firebird ftp ftps
http[s]-{head|get} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq
```

```
    imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] mssql mysql ncp nntp
    oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres rdp rexec
    rlogin rsh s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn
    teamspeak telnet[s] vmauthd vnc xmpp

    Hydra is a tool to guess/crack valid login/password pairs - usage only
    allowed
    for legal purposes. This tool is licensed under AGPL v3.0.
    The newest version is always available at http://www.thc.org/thc-hydra
    These services were not compiled in: sapr3 oracle.

    Use HYDRA_PROXY_HTTP or HYDRA_PROXY - and if needed HYDRA_PROXY_AUTH -
    environment for a proxy setup.
    E.g.: % export HYDRA_PROXY=socks5://127.0.0.1:9150 (or socks4:// or
    connect://)
    % export HYDRA_PROXY_HTTP=http://proxy:8080
    % export HYDRA_PROXY_AUTH=user:pass

    Examples:
    hydra -l user -P passlist.txt ftp://192.168.0.1
    hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
    hydra -C defaults.txt -6 pop3s://[fe80::2c:31ff:fe12:ac11]:143/TLS:DIGEST-
    MD5

    ------------------------------------------------------------------------

root@kali:~# pw-inspector
PW-Inspector v0.2 (c) 2005 by van Hauser / THC vh@thc.org [http://www.thc.org]

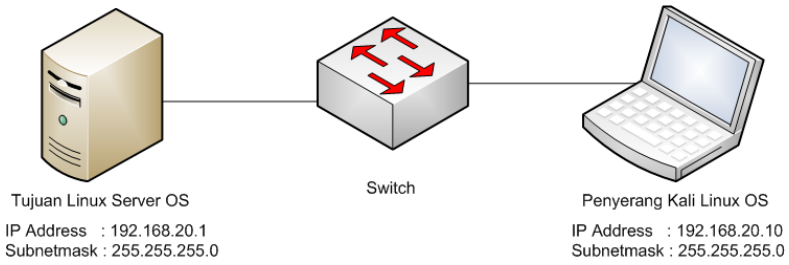
Syntax: pw-inspector [-i FILE] [-o FILE] [-m MINLEN] [-M MAXLEN] [-c MINSETS] -
l -u -n -p -s

Options:
-i FILE file to read passwords from (default: stdin)
-o FILE file to write valid passwords to (default: stdout)
-m MINLEN minimum length of a valid password
-M MAXLEN maximum length of a valid password
-c MINSETS the minimum number of sets required (default: all given)
Sets:
-l lowcase characters (a,b,c,d, etc.)
-u upcase characters (A,B,C,D, etc.)
-n numbers (1,2,3,4, etc.)
-p printable characters (which are not -l/-n/-p, e.g. $,!,/,(,*,
etc.)
-s special characters - all others not withint the sets above

PW-Inspector reads passwords in and prints those which meet the requirements.
The return code is the number of valid passwords found, 0 if none was found.
Use for security: check passwords, if 0 is returned, reject password choice.
Use for hacking: trim your dictionary file to the pw requirements of the
target.
Usage only allowed for legal purposes.
```

F. TUGAS

1. Buatlah skenario topologi offline sebagai berikut :



   Jadikan server ubuntu linux sebagai target dan system operasi kali linux sebagai penyerang.

2. Lakukan penestrasi dengan menggunakan tools hydra dari penyerang ke server.adapun command yang di lakukakan sebagai berikut :

```
root@kali:~# hydra -l root -P /usr/share/wordlists/metasploit/unix_passwords.txt -t 6
ssh://192.168.20.1
```

   Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

3. Lakukan penestrasi dengan menggunakan tools hydra dari penyerang ke server.adapun command yang di lakukakan sebagai berikut :

```
root@kali:~# pw-inspector -i /usr/share/wordlists/nmap.lst -o /root/passes.txt -m 6 -M 10
root@kali:~# wc -l /usr/share/wordlists/nmap.lst
5086 /usr/share/wordlists/nmap.lst
root@kali:~# wc -l /root/passes.txt
4490 /root/passes.txt
```

   Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

9 FIREWALL (IPTABLES) & BLOCKING NMAP

A. POKOK BAHASAN

1. Blocking Nmap pada komputer/server berbasis Linux dengan Iptables.
2. Perintah-perintah iptables pada komputer/server dan serangan dari penyerang.

B. TUJUAN

setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

1. Mengenalkan pada mahasiswa tentang konsep dasar firewall
2. Mahasiswa mampu mengimplementasikan proses filtering firewall menggunakan aplikasi iptables.

C. PERALATAN

1. Sistem Operasi Linux Penestrasi Kali dan Server Linux

D. DASAR TEORI

Firewall adalah sistem atau sekelompok sistemyang menetapkan kebijakan kendali akses antara dua jaringan. Secara prinsip, firewall dapat dianggap sebagai sepasang mekanisme : yang pertama memblok lalu lintas, yang kedua mengijinkan lalu lintas jaringan. Firewall dapat digunakan untuk melindungi jaringan anda dari serangan jaringan oleh pihak luar, namun firewall tidak dapat melindungi dari serangan yang tidak melalui firewall dan serangan dari seseorang yang berada di dalam jaringan anda, serta firewall tidak dapat melindungi anda dari program-program aplikasi yang ditulis dengan buruk.

Secara umum, firewall biasanya menjalankan fungsi:

- Analisa dan filter paket
  Data yang dikomunikasikan lewat protokol di internet, dibagi atas paket-paket. Firewall dapat menganalisa paket ini, kemudian memperlakukannya sesuai kondisitertentu. Misal, jika ada paket a maka akan dilakukan b. Untuk filter paket, dapat dilakukan di Linux tanpa program tambahan.
- Bloking isi dan protocol
  Firewall dapat melakukan bloking terhadap isi paket, misalnya berisi applet Jave, ActiveX,VBScript, Cookie.
- Autentikasi koneksi dan enkripsi
  Firewall umumnya memiliki kemampuan untuk menjalankan enkripsi dalam autentikasi identitas user, integritas dari satu session, dan melapisi transfer data dari intipan pihak lain. Enkripsi yang dimaksud termasuk DES, TripleDES, SSL, IPSEC, SHA, MD5, BlowFish, IDEA dan sebagainya.

Secara konseptual, terdapat dua macam firewall yaitu :

- Network level
  Firewall network level mendasarkan keputusan mereka pada alamat sumber, alamat tujuan dan port yang terdapat dalam setiap paket IP. Network level firewall sangat cepat dan sangat transparan bagi pemakai. Application level firewall biasanya adalah host yang berjalan sebagai proxy server, yang tidak mengijinkan lalu lintas antar jaringan, dan melakukan logging dan auditing lalu lintas yang melaluinya.
- Application level.
  Application level firewall menyediakan laporan audit yang lebih rinci dan cenderung lebih memaksakan model keamanan yang lebih konservatif daripada network level firewall. Firewall ini bisa dikatakan sebagai jembatan. Application-Proxy Firewall biasanya berupa program khusus, misal squid.

Firewall IPTables packet filtering memiliki tiga aturan (policy), yaitu:

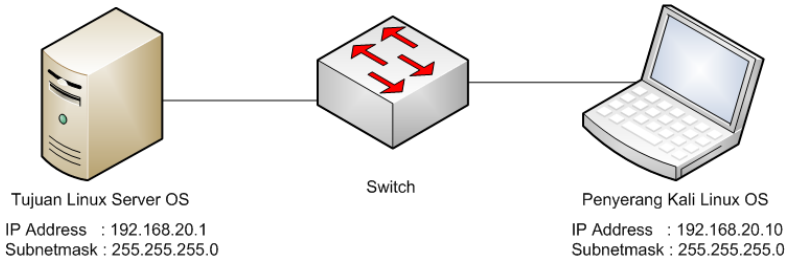
a. INPUT
   Mengatur paket data yang memasuki firewall dari arah intranet maupun internet. kita bisa mengelola komputer mana saja yang bisa mengakses firewall. misal: hanya komputer IP 192.168.1.100 yang bisa SSH ke firewall dan yang lain tidak boleh.
b. OUTPUT
   Mengatur paket data yang keluar dari firewall ke arah intranet maupun internet. Biasanya output tidak diset, karena bisa membatasi kemampuan firewall itu sendiri.
c. FORWARD
   Mengatur paket data yang melintasi firewall dari arah internet ke intranet maupun sebaliknya. Policy forward paling banyak dipakai saat ini untuk mengatur koneksi internet berdasarkan port, mac address dan alamat IP.

Selain aturan (policy) firewall iptables juga mempunyai parameter yang disebut dengan TARGET, yaitu status yang menentukkan koneksi di iptables diizinkan lewat atau tidak. TARGET ada tiga macam yaitu:

a. ACCEPT
   Akses diterima dan diizinkan melewati firewall
b. REJECT
   Akses ditolak, koneksi dari komputer klien yang melewati firewall langsung terputus, biasanya terdapat pesan "Connection Refused". Target Reject tidak menghabiskan bandwidth internet karena akses langsung ditolak, hal ini berbeda dengan DROP.
c. DROP
   Akses diterima tetapi paket data langsung dibuang oleh kernel, sehingga pengguna tidak mengetahui kalau koneksinya dibatasi oleh firewall, pengguna melihat seakan - akan server yang dihubungi mengalami permasalahan teknis. Pada koneksi internet yang sibuk dengan trafik tinggi Target Drop sebaiknya jangan digunakan.

E. PERCOBAAN

1. Buatlah skenario topologi offline sebagai berikut :



Jadikan server ubuntu linux sebagai target dan system operasi kali linux sebagai penyerang.

2. Lakukan penestrasi dengan menggunakan tools nmap dari penyerang sedangkan dari server menggunakan iptables. Adapun command yang di lakukakan sebagai berikut :
   - Null Scan
     Pada system operasi kali linux,penyerang melakukan serangan ke server.

     ```
     root@kali:~# nmap –sN 192.168.20.1
     ```

     Untuk penyegahan terhadap Null scan pada server

     ```
     root@server:~# iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
     ```

     Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

   - Xmas scan
     Pada system operasi kali linux,penyerang melakukan serangan ke server.

     ```
     root@kali:~# nmap –sX 192.168.20.1
     ```

     Untuk penyegahan terhadap Xmas scan pada server

     ```
     root@server:~# iptables -A INPUT -p tcp --tcp-flags ALL FIN,PSH,URG -m
     limit --limit 3/m --limit-burst 5 -j LOG --log-prefix "Firewall> XMAS
     scan "
     ```

     Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

   - FIN Scan
     Pada system operasi kali linux,penyerang melakukan serangan ke server.

     ```
     root@kali:~# nmap –sF 192.168.20.1
     ```

     Untuk penyegahan terhadap FIN scan pada server

     ```
     root@server:~# iptables -A INPUT -p tcp --tcp-flags ALL FIN -m limit --
     limit 3/m --limit-burst 5 -j LOG --log-prefix "Firewall> FIN scan "
     ```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

- ACK Scan
  Pada system operasi kali linux,penyerang melakukan serangan ke server.

```
root@kali:~# nmap –sA 192.168.20.1
```

Untuk penyegahan terhadap ACK scan pada server

```
root@server:~# iptables -A INPUT -p tcp ! --syn -m state --state NEW
-m comment --comment "Drop TCP connection not starting by SYN" -j DROP
```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

- SYN Scan dan TCP connect Scan
  Pada system operasi kali linux,penyerang melakukan serangan ke server.

```
root@kali:~# nmap –sT 192.168.20.1
```

Untuk penyegahan terhadap SYN dan TCP scan pada server

```
root@server:~# iptables -A INPUT -p tcp -m multiport --dports 23,79 --
tcp-flags ALL SYN -m limit --limit 3/m --limit-burst 5 -j LOG --log-
prefix "Firewall>SYN scan trap:"
```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

- UDP Scan
  Pada system operasi kali linux,penyerang melakukan serangan ke server.

```
root@kali:~# nmap –sU 192.168.20.1
```

Untuk penyegahan terhadap UDP scan pada server

```
root@server:~# iptables -A INPUT -p udp -m limit --limit 6/h --limit-
burst 1 -m length --length 0:28 -j LOG --log-prefix "Firewall>0 length
udp "
```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

F. TUGAS

1. Lakukan monitoring dengan menggunakan tools tcpdump dari terhadap server.adapun command yang di lakukakan sebagai berikut :

```
root@server:~# tcpdump –i eth0
```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

10 FIREWALL (IPTABLES) & BLOCKING HPING3

A. POKOK BAHASAN

1. Blocking Hping3 pada komputer/server berbasis Linux dengan Iptables.
2. Perintah-perintah iptables pada komputer/server dan serangan dari penyerang.

B. TUJUAN

setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

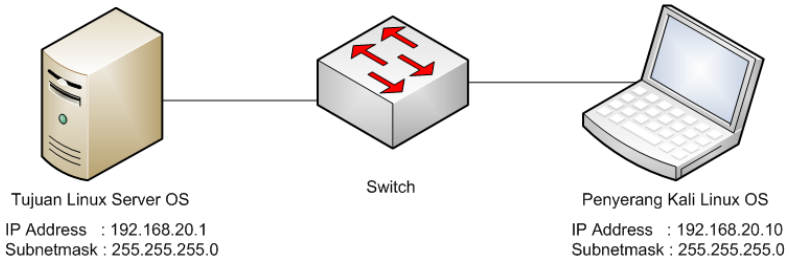
1. Mengenalkan pada mahasiswa tentang konsep dasar firewall
2. Mahasiswa mampu mengimplementasikan proses filtering firewall menggunakan aplikasi iptables.

C. PERALATAN

1. Sistem Operasi Linux Penestrasi Kali dan Server Linux

D. PERCOBAAN

1. Buatlah skenario topologi offline sebagai berikut :



Jadikan server ubuntu linux sebagai target dan system operasi kali linux sebagai penyerang.

2. Lakukan penestrasi dengan menggunakan tools hping3 dari penyerang sedangkan dari server menggunakan iptables. Adapun command yang di lakukakan sebagai berikut :
   - ICMP Flood

     Pada system operasi kali linux,penyerang melakukan serangan ke server.

```
root@kali:~# hping3 -q -n -a 10.0.0.1 --id 0 --icmp -d 56 --flood
192.168.20.1
```

     Untuk penyegahan terhadap ICMP Flood pada server

```
# Create chain dedicated to ICMP flood

root@server:~# iptables -N thyl-icmp-flood
```

```
# Jump to that chain when ICMP detected

root@server:~# iptables -A INPUT -p icmp -j thyl-icmp-flood
# Get out of chain if packet rate for the same IP is below 4 per second
with a burst of 8 per second

root@server:~# iptables -A thyl-icmp-flood -m limit --limit 4/s --
limit-burst 8 -m comment --comment "Limit ICMP rate" -j RETURN

# Log as flood when rate is higher

root@server:~# iptables -A thyl-icmp-flood -m limit --limit 6/h --
limit-burst 1 -j LOG --log-prefix "Firewall>Probable icmp flood "

# Blacklist IP for 3 minutes

root@server:~# iptables -A thyl-icmp-flood -m recent --name
blacklist_180 --set -m comment --comment "Blacklist source IP" -j DROP
```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

- UDP Flood
  Pada system operasi kali linux,penyerang melakukan serangan ke server.

```
root@kali:~# hping3 -q -n -a 10.0.0.1 --udp -s 53 --keep -p 68 --
flood 192.168.20.1
```

  Untuk penyegahan terhadap UDP Flood pada server

```
# # Create chain for UDP flood

root@server:~# iptables -N thyl-udp-flood

# Jump to chain if UDP

root@server:~# iptables -A INPUT -p udp -j thyl-udp-flood

# Limit UDP rate to 10/sec with burst at 20 (sometimes it is not
enough, if you know a better average rate, let me know!)

root@server:~# iptables -A thyl-udp-flood -m limit --limit 10/s --
limit-burst 20 -m comment --comment "Limit UDP rate" -j RETURN

# Log

root@server:~# iptables -A thyl-udp-flood -m limit --limit 6/h --limit-
burst 1 -j LOG --log-prefix "Firewall>Probable udp flood "

# 3 minutes ban for flooders

root@server:~# iptables -A thyl-udp-flood -m recent --name
blacklist_180 --set -m comment --comment "Blacklist source IP" -j DROP
```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

- SYN Flood
  Pada system operasi kali linux,penyerang melakukan serangan ke server.

```
root@kali:~# hping3 -q -n -a 10.0.0.1 -S -s 53 --keep -p 22 --flood
```

```
192.168.20.1
```

Untuk penyegahan terhadap SYN Flood pada server

```
# Create syn-flood chain

root@server:~# iptables -N thyl-syn-flood

# Jump into syn-flood chain when a syn packet is detected

root@server:~# iptables -A INPUT -p tcp --syn -j thyl-syn-flood

# Limit packet rate to 2 per second with a 6 per second burst

root@server:~# iptables -A thyl-syn-flood -m limit --limit 2/s --limit-
burst 6 -m comment --comment "Limit TCP SYN rate" -j RETURN

# Log flooders

root@server:~# iptables -A thyl-syn-flood -m limit --limit 6/h --limit-
burst 1 -j LOG --log prefix "Firewall>Probable syn flood "

# Ban flooders for 3 minutes
root@server:~# iptables -A thyl-syn-flood -m recent --name blacklist_180
--set -m comment --comment "Blacklist source IP" -j DROP
```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

E. TUGAS

1. Lakukan monitoring dengan menggunakan tools tcpdump dari terhadap server.adapun command yang di lakukakan sebagai berikut :

```
root@server:~# tcpdump –i eth0
```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

11 INTRUSION DETECTION SYSTEM (IDS)

A. POKOK BAHASAN

1. IDS menggunakan snort pada komputer/server berbasis Linux.
2. Perintah-perintah snort dan rules pada komputer/server.

B. TUJUAN

setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

1. Mengenalkan pada mahasiswa tentang konsep IDS di linux
2. Mahasiswa memahami konsep IDS : Snort yang ada di linux
3. Mahasiswa mampu melakukan konfigurasi dan analisa terhadap aplikasi snort

C. PERALATAN

1. Sistem Operasi Linux Penestrasi Kali dan Server Linux

D. DASAR TEORI

Deteksi Penyusupan (Intrusion Detection)

Deteksi penyusupan adalah aktivitas untuk mendeteksi penyusupan secara cepat dengan menggunakan program khusus yang otomatis. Program yang dipergunakan biasanya disebut sebagai Intrusion Detection System (IDS).

Tipe dasar dari IDS adalah:

- Rule-based systems - berdasarkan atas database dari tanda penyusupan atau serangan yang telah dikenal. Jika IDS mencatat lalulintas yang sesuai dengan database yang ada, maka langsung dikategorikan sebagai penyusupan.
- Adaptive systems - mempergunakan metode yang lebih canggih. Tidak hanya berdasarkan database yang ada, tapi juga membuka kemungkinan untuk mendeteksi terhadap bentuk bentuk penyusupan yang baru.

Bentuk yang sering dipergunakan untuk komputer secara umum adalah rule-based systems.

Pendekatan yang dipergunakan dalam rule-based systems ada dua, yakni pendekatan pencegahan (preemptory) dan pendekatan reaksi (reactionary). Perbedaannya hanya masalah waktu saja. Pendekatan pencegahan, program pendeteksi penyusupan akan memperhatikan semua lalu lintas jaringan. Jika ditemukan paket yang mencurigakan, maka program akan melakukan tindakan yang perlu. Pendekatan reaksi, program pendeteksi penyusupan hanya mengamati file log. Jika ditemukan paket yang mencurigakan, program juga akan melakukan tindakan yang perlu.

Snort

Mengoperasikan Snort

Tiga (3) buah mode, yaitu

1. **Sniffer mode**, untuk melihat paket yang lewat di jaringan.

2. **Packet logger mode**, untuk mencatat semua paket yang lewat di jaringan untuk di analisa di kemudian hari.
3. **Intrusion Detection mode**, pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini di perlukan setup dari berbagai rules / aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.

Sniffer Mode

Untuk menjalankan snort pada sniffer mode tidaklah sukar, beberapa contoh perintah-nya terdapat di bawah ini,

```
#snort –v
#snort –vd
#snort –vde
#snort –v –d –e
```

dengan menambahkan beberapa switch –v, -d, -e akan menghasilkan beberapa keluaran yang berbeda, yaitu

-v, untuk melihat header TCP/IP paket yang lewat.

-d, untuk melihat isi paket.

-e, untuk melihat header link layer paket seperti ethernet header.

Packet Logger Mode

Tentunya cukup melelahkan untuk melihat paket yang lewat sedemikian cepat di layar terutama jika kita menggunakan ethernet berkecepatan 100Mbps, layar anda akan scrolling dengan cepat sekali susah untuk melihat paket yang di inginkan. Cara paling sederhana untuk mengatasi hal ini adalah menyimpan dulu semua paket yang lewat ke sebuah file untuk di lihat kemudian, sambil santai. Beberapa perintah yang mungkin dapat digunakan untuk mencatat paket yang ada adalah

```
./snort –dev –l ./log
./snort –dev –l ./log –h 192.168.0.0/24
./snort –dev –l ./log –b
```

perintah yang paling penting untuk me-log paket yang lewat adalah

-l ./log

yang menentukan bahwa paket yang lewat akan di log / di catat ke file ./log. Beberapa perintah tambahan dapat digunakan seperti –h 192.168.0.0/24 yang menunjukan bahwa yang di catat hanya packet dari host mana saja, dan –b yang memberitahukan agar file yang di log dalam format binary, bukan ASCII.

Untuk membaca file log dapat dilakukan dengan menjalankan snort dengan di tambahkan perintah –r nama file log-nya, seperti,

```
./snort –dv –r packet.log
./snort –dvr packet.log icmp
```

Intrusion Detection Mode

Mode operasi snort yang paling rumit adalah sebagai pendeteksi penyusup (intrusion detection) di jaringan yang kita gunakan. Ciri khas mode operasi untuk pendeteksi penyusup adaah dengan menambahkan perintah ke snort untuk membaca file konfigurasi –c nama-file-konfigurasi.conf. Isi file konfigurasi ini lumayan banyak, tapi sebagian besar telah di set secara baik dalam contoh snort.conf yang dibawa oleh source snort.

Beberapa contoh perintah untuk mengaktifkan snort untuk melakukan pendeteksian penyusup, seperti

```
./snort –dev –l ./log –h 192.168.0.0/24 –c snort.conf
./snort –d –h 192.168.0.0/24 –l ./log –c snort.conf
```

Untuk melakukan deteksi penyusup secara prinsip snort harus melakukan logging paket yang lewat dapat menggunakan perintah –l nama-file-logging, atau membiarkan snort menggunakan default file logging-nya di directory /var/log/snort. Kemudian menganalisa catatan / logging paket yang ada sesuai dengan isi perintah snort.conf.

Ada beberapa tambahan perintah yang akan membuat proses deteksi menjadi lebih effisien, mekanisme pemberitahuan alert di Linux dapat di set dengan perintah –A sebagai berikut,

-A fast, mode alert yang cepat berisi waktu, berita, IP & port tujuan.
-A full, mode alert dengan informasi lengkap.
-A unsock, mode alert ke unix socket.
-A none, mematikan mode alert.

Untuk mengirimkan alert ke syslog UNIX kita bisa menambahkan switch –s, seperti tampak pada beberapa contoh di bawah ini.

```
./snort –c snort.conf –l ./log –s –h 192.168.0.0/24
./snort –c snort.conf –s –h 192.168.0.0/24
```

Untuk mengirimkan alert binary ke workstation windows, dapat digunakan perintah di bawah ini,

```
./snort –c snort.conf –b –M WORKSTATIONS
```

Agar snort beroperasi secara langsung setiap kali workstation / server di boot, kita dapat menambahkan ke file /etc/rc.d/rc.local perintah di bawah ini

```
/usr/local/bin/snort –d –h 192.168.0.0/24 –c /root/snort/snort.conf –A full –s –D

atau
/usr/local/bin/snort –d –c /root/snort/snort.conf –A full –s –D
```

dimana –D adalah switch yang menset agar snort bekerja sebagai Daemon (bekerja dibelakang layar).

E. PERCOBAAN

1. Lakukan instalasi snort pada server linux:

   ```
   root@server:~# apt-get install snort
   ```

   Masukkan range network yang akan dianalisa :
   Address range for the local network :

   ```
   192.168.20.0/24
   ```

2. Manjalankan snort
   a. Bekerjalah dengan teman anda, salah satu menjalankan snort yang satunya menjalankan aplikasi yang lain.
   b. Jalankan perintah ping dari komputer lain ke komputer snort, buka terminal

yang lain dan jalankan nmap.

c. Jalankan snort dengan menggunakan mode sniffer

```
root@server:~# snort –v
root@server:~# snort –vd
root@server:~# snort –vde
root@server:~# snort –v –d –e
```

Ket : Running in packet dump mode
Jelaskan perbedaan hasil dari option di atas.

d. Untuk mempermudah pembacaan masukkan hasil snort ke dalam file, jalankan perintah berikut :

```
root@server:~# snort –dev –i eth0 –L /var/log/snort/snort.log
```

Ket : Running in packet logging mode

Akan menghasilkan sebuah file di folder /var/log/snort, lihat dengan perintah :

```
root@server:~# ls /var/log/snort
```

e. Untuk membaca file snort (misal : snort.log.1234) berikan option –r pada snort

```
root@server:~# snort -dev -r /var/log/snort/snort.log.1234
```

f. Jalankan perintah ping dan nmap dari komputer lain ke komputer snort.

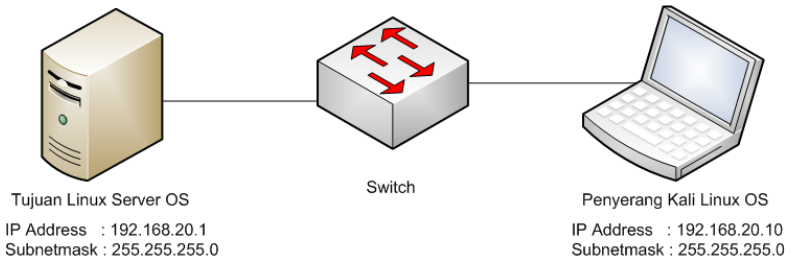
3. Menjalankan snort dengan mode NIDS (Network Intrusion Detection System)

a. Opsi e, dihilangkan karena kita tidak perlu mengetahui link layer MAC. Opsi v dihilangkan juga

```
root@server:~# snort -d -h 192.168.20.0/24 -l /var/log/snort -c
/etc/snort/snort.conf
```

Ket : Running in IDS mode

b. Sekarang coba jalankan scanning dari komputer lain dengan nmap menuju komputer yang anda pasangi snort. Terlebih dulu jalankan snort dengan mode NIDS, kemudia lakukan scanning dengan perintah :




```
root@server:~# snort -d -h 192.168.20.0/24 host <no_ip_snort> -l
/var/log/snort –c /etc/snort/snort.conf

root@kali:~# #nmap -sS -v <no_ip_snort>
```

c. Lihatlah apakah scan anda terekam oleh snort. Jika iya, copy paste hasil snort pada bagian scanning SYN. Untuk melihat, gunakan perintah :

```
root@server:~# snort –dev –r <nama-log-file> | more
```

Apakah scanning ini ditandai sebagai alert ? Coba lihat di /var/log/snort, gunakan perintah :

```
root@server:~# vim /var/log/snort/alert
```

F. TUGAS

1. Lakukan monitoring dengan menggunakan tools tcpdump dari terhadap server.adapun command yang di lakukakan sebagai berikut :

```
root@server:~# tcpdump –i eth0
```

Tulis dan jelaskan hasil perintah - perintah di atas pada laporan hasil praktikum?

12 CRYPTHOGRAPHY

A. POKOK BAHASAN

1. Enkripsi dan Dekripsi Kriptografi Klasik (Caesar Cipher,RC4).
2. Pemrograman Enkripsi dan Dekripsi.

B. TUJUAN

setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

1. Mengenalkan pada mahasiswa tentang konsep cryptography
2. Mahasiswa mampu membuat program enkripsi Caesar dan RC4
3. Mahasiswa mampu membuat program dekripsi Caesar dan RC4

C. PERALATAN

1. Sistem Operasi Linux Penestrasi Kali

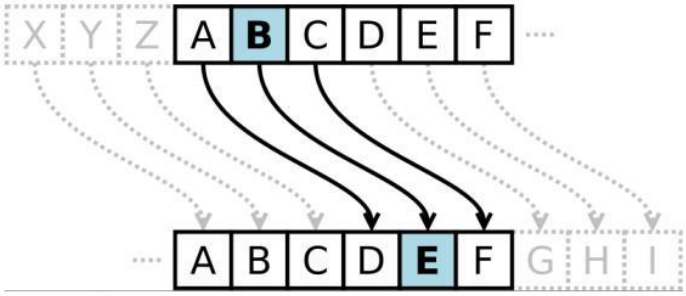
D. DASAR TEORI

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Terdapat 2 jenis kriptografi dipandang dari masanya :

1. Kriptografi klasik : Caesar cipher, Affine cipher, Vigenere cipher dll.
2. Kriptografi modern, terbagi 2 yaitu :
   a. Kriptografi simetrik : RC4, DES, AES, IDEA
   b. Kriptografi asimetrik : RSA, DSA, El gama

Kriptografi Klasik (Caesar)

Pada Caesar cipher, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu 3). Susunan alphabet setelah digeser sejauh 3 huruf membentuk sebuah table substitusi sebagai berikut :



Gambar 1. Kriptografi Caesar

Kriptografi Simetrik

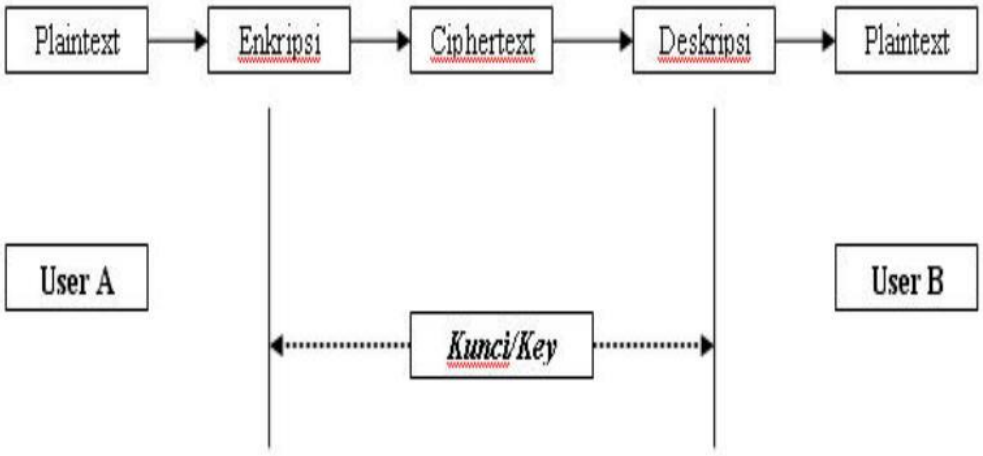
Kriptografi simetrik atau dikenal pula sebagai kriptografi kunci rahasia, merupakan kriptografi yang menggunakan kunci yang sama baik untuk proses enkripsi maupun dekripsi. Secara metematis dapat dinyatakan bahwa :

E = d = k.....(4)
Ek(m) = c.....(5)
Dk(c) = m.....(6)

Dalam algoritma simetri, kunci yang digunakan dalam proses enkripsi dan dekripsiadalah sama atau pada prinsipnya identik. Kunci ini pun bisa diturunkan dari kunci lainnya. Oleh karena itu sistem ini sering disebut secret-key ciphersystem.

Agar komunikasi tetap aman, kunci yang menggunakan teknik enkripsi ini harus betul-betul dirahasiakan.

Kriptografi simetrik sangat menekankan pada kerahasiaan kunci yang digunakan untuk proses enkripsi dan dekripsi. Oleh karena itulah kriptografi ini dinamakan pula sebagai kriptografi kunci rahasia. Gambaran proses sederhana enkripsidengan algoritma simetri:



Gambar 2. Blok Diagram algoritma Simetri

Algoritma RC4

RC4 merupakan merupakan salah satu jenis stream cipher, yaitu memproses unit atau input data pada satu saat. Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah input data tertentu sebelum diproses, atau menambahkan byte tambahan untuk mengenkrip. Metode enkripsi RC4 sangat cepat kurang lebih 10 kali lebih cepat dari DES.

RC4 merupakan stream cipher yang didesain oleh Rivest untuk RSA Data Security(sekarang RSA Security) pada 1987. RC4 menggunakan panjang variabel kunci dari 1 s.d 256 byte untuk menginisialisasi statetabel. State tabledigunakan untuk pengurutan menghasilkan byte pseudo-randomyang kemudian menjadi stream pseudo-random. Setelah di-XOR dengan plaintextsehingga didapatkan ciphertext. Tiap elemen pada state tabledi swapsedikitnya sekali. Kunci RC4 sering dibatasi sampai 40 bit, tetapi dimungkinkan untuk mengunakan kunci 128 bit. RC4 memiliki kemampuan penggunaan

kunci antara 1 sampai 2048 bit.

Panjang kunci merupakan faktor utama dalam sekuritas data. RC4 dapat memiliki kunci sampai dengan 128 bit. Protokol keamanan SSL (Secure Socket Layer) pada Netscape Navigatormenggunakan algoritma RC4 40-bit untuk enkripsi simetrisnya.

Algoritma RC4 memiliki dua fase, setup kunci dan pengenkripsian. Setup untuk kunci adalah fase pertama dan yang paling sulit dalam algoritma ini. Dalam setup S-bit kunci (S merupakan panjang dari kunci), kunci enkripsi digunakan untuk menghasilkan variabel enkripsi yang menggunakan dua buah array, state dan kunci, dan sejumlah-S hasil dari operasi penggabungan. Operasi penggabungan ini terdiri dari pemindahan (swapping) byte, operasi modulo, dan rumus lain. Operasi modulo merupakan proses yang menghasilkan nilai sisa dari satu pembagian. Sebagai contoh, 11 dibagi 4 adalah 2 dengan sisa pembagian 3, begitu juga jika tujuh modulo empat maka akan dihasilkan nilai tiga.

Variabel enkripsidihasikan dari setup kunci dimana kunci akan di XOR-kan dengan plain textuntuk menghasilkan teks yang sudah terenkripsi. XOR merupakan

E. PERCOBAAN

1. Masuk ke sistem operasi linux kali
2. Jalankan service apache :

```
root@server:~# /etc/init.d/apache2 restart
```

   a. Buatlah Kriptograsi Klasik (Caesar Cipher) dengan menggunakan script php di dalam direktori /var/www/ Pembuatan Form Masukkan php. Buat file untuk masukan plainteks dan key (berupa bilangan), beri nama file : awal.php

```
<html>
<head>
<title>FORM UNTUK ENKRIPSI</title>
</head>
<body>
<form action="enkcaesar.php" method="get">
Plainteks : <input type="text" name="kata"> <br>
Key : <input type="text" name="key" maxlength="2"> <br>
<input type="submit" value="kirim">
<input type="reset" value="ulangi">
</form>
</body>
</html>
```

   b. Proses Enkripsi dengan Caesar Algorithm. Buat file untuk melakukan proses enkripsi, beri nama file : enkcaesar.php

```
<?php
$kalimat = $_GET["kata"];

$key = $_GET["key"];
for($i=0;$i<strlen($kalimat);$i++)
{
       $kode[$i]=ord($kalimat[$i]); //rubah ASCII ke desimal
       $b[$i]=($kode[$i] + $key ) % 256; //proses enkripsi
```

```
$c[$i]=chr($b[$i]); //rubah desimal ke ASCII
}
echo "kalimat ASLI : ";
for($i=0;$i<strlen($kalimat);$i++)
{
echo $kalimat[$i];
}
echo "<br>";
echo "hasil enkripsi =";
$hsl = '';
for ($i=0;$i<strlen($kalimat);$i++)
{
       echo $c[$i];
       $hsl = $hsl . $c[$i];
}
echo "<br>";
//simpan data di file
$fp = fopen ("enkripsi.txt","w");
fputs ($fp,$hsl);
fclose($fp);
?>
```

c. Test Proses Enkripsi
Buka web browser dari PC Client dan akseslah file php dari PC Kali Linux **http://<no_ip_pc >/awal.php** . kemudian Catat hasil enkripsi diatas.

d. Pembuatan Form untuk proses dekripsi
Buat file untuk masukan key (berupa bilangan), agar bisa menghasilkan kembali plainteks maka key harus sama dengan proses enkripsi, beri nama file: akhir.php di PC Kali Linux

```
<html>
<head>
       <title>Form untuk Dekripsi</title>
</head>
<body>
<form action="dekCaesar.php" method="get">
Key : <input type="text" name="key" maxlength="2"> <br>
<input type="submit" value="kirim">
<input type="reset" value="ulangi">
</form>
</body>
</html>
```

e. Proses Dekripsi dengan Caesar Algorithm
Buat file untuk melakukan proses dekripsi, beri nama file : dekCaesar.php di PC Kali Linux

```
<?php
$key = $_GET["key"];
$nmfile = "enkripsi.txt";
$fp = fopen($nmfile,"r"); // buka file hasil enkripsi
$isi = fread($fp,filesize($nmfile));
for($i=0;$i<strlen($isi);$i++)
{
       $kode[$i]=ord($isi[$i]); // rubah ASII ke desimal
```

```
        $b[$i]=($kode[$i] - $key ) % 256; // proses dekripsi Caesar
        $c[$i]=chr($b[$i]); //rubah desimal ke ASCII
}
echo "kalimat ciphertext : ";
for($i=0;$i<strlen($isi);$i++)
{
        echo $isi[$i];
}
echo "<br>";
echo "hasil dekripsi =";
for ($i=0;$i<strlen($isi);$i++)
{
        echo $c[$i];
}
echo "<br>";
?>
```

f. Test Proses Dekripsi
   Buka web browser dari PC Client dan akseslah file php dari PC Kali Linux **http://<no_ip_pc>/akhir.php**

3. Kriptografi Modern (Simetrik RC4)
   a. Pembuatan Form Masukan PHP. Gunakan kembali file di poin 2.a, beri nama yang berbeda : awalrc4.php. Buat di direktori /var/www/ PC Kali, dan rubah hanya baris berikut :

```
...
<form action="penkripsi.php" method="get">
Plainteks : <input type="text" name="kata"> <br>
Key : <input type="text" name="kcenkripsi" maxlength="16"> <br>
...
```

   NB : untuk kunci, dimasukkan kata tanpa spasi sebanyak 16 karakter.

   b. Proses Pembentukan Kunci Enkripsi dengan RC4 Algorithm. Buat file untuk memproses setupkey dan enkripsi RC4, beri nama file penkripsi.php Kemdian buatlah program untuk setupkey :

```
function setupkey() //proses pengacakan kunci di SBox
{
echo "<br>";
$kce = $_GET["kcenkripsi"];
echo "Kunci enkripsi = $kce";
echo "<br>";
        for($i=0;$i<strlen($kce);$i++)
        {
                $key[$i]=ord($kce[$i]); //rubah ASCII ke desimal
        }
global $m;
$m=array();
// buat encrpyt
for($i=0;$i<256;$i++){
$m[$i] = $i;
}
$j = $k = 0;
for($i=0;$i<256;$i++)
{
$a = $m[$i];
$j = ($j + $m[$i] + $key[$k]) % 256;
```

```
$m[$i] = $m[$j];
$m[$j] = $a;
$k++;
if($k>15)
{
$k=0;
}
}
} //akhir function
```

c. Proses Enkripsi Algoritma RC4. Tambahkan program untuk enkripsi RC4 dibawah fungsi setupkey

```
function crypt2($inp)
{
global $m;
$x=0;$y=0;
$bb='';
$x = ($x+1) % 256;
$a = $m[$x];
$y = ($y+$a) % 256;
$m[$x] = $b = $m[$y];
$m[$y] = $a;
//proses XOR antara plaintext dengan kunci
//dengan $inp sebagai plaintext
//dan $m sebagai kunci
$bb= ($inp^$m[($a+$b) % 256]) % 256;
return $bb;
}
```

d. Tampilkan kalimat asli dan hasil enkripsi RC4
$kalimat = $_GET["kata"];

```
setupkey();
for($i=0;$i<strlen($kalimat);$i++)
{
	$kode[$i]=ord($kalimat[$i]); //rubah ASCII ke desimal
	$b[$i]=crypt2($kode[$i]); //proses enkripsi RC4
	$c[$i]=chr($b[$i]); //rubah desimal ke ASCII
}
echo "kalimat ASLI : ";
for($i=0;$i<strlen($kalimat);$i++)
{
	echo $kalimat[$i];
}
echo "<br>";
echo "hasil enkripsi =";
$hsl = '';
for ($i=0;$i<strlen($kalimat);$i++)
{
	echo $c[$i];
	$hsl = $hsl . $c[$i];
}
echo "<br>";
//simpan data di file
$fp = fopen ("enkripsirc4.txt","w");
fputs ($fp,$hsl);
fclose($fp);
```

e. Tes Proses Enkripsi. Buka web browser dari PC Client dan akseslah file php dari PC Kali Linux http://<no_ip_pc>/awalrc4.php
f. Catat hasil enkripsi diatas.

g. Pembuatan Form untuk proses dekripsi. Gunakan kembali file di 2.d. dan rubah beberapa baris berikut : Buat file untuk masukan key (berupa bilangan), agar bisa menghasilkan kembali plainteks maka key harus sama dengan proses enkripsi, beri nama file: akhirrc4.phpdi PC

```
…
<form action="pdekripsi.php" method="get">
Key : <input type="text" name="kcdekripsi" maxlength="16"> <br>
...
```

NB : agar bisa menghasilkan kembali plainteks maka key harus sama dengan proses enkripsi.

h. Proses Pembentukan Kunci Dekripsi dengan RC4 Algorithm. Buat file untuk memproses setupkey dan enkripsi RC4, beri nama file pdekripsi.php
i. Buat program untuk setupkey (proses ini sama dengan proses pembentukan kunci untuk enkripsi) :

```
function setupkey()
{
$kcd = $_GET["kcdekripsi"];
echo "Kunci Dekripsi = $kcd";
echo "<br>";
       for($i=0;$i<strlen($kcd);$i++)
       {
              $key[$i]=ord($kcd[$i]); //rubah ASCII ke desimal
       }
global $mm;
$mm=array();
// buat decrpyt
$mm=array();
for($i=0;$i<256;$i++)
$mm[$i] = $i;
$j = $k = 0;
for($i=0;$i<256;$i++)
{
$a = $mm[$i];
$j = ($j + $a + $key[$k]) % 256;
$mm[$i] = $mm[$j];
$mm[$j] = $a;
$k++;
if($k>15)
{
$k=0;
}
}
} //akhir function
```

j. Proses Dekripsi Algoritma RC4. Tambahkan program untuk dekripsi RC4 dibawah fungsi setupkey :

```
function decrypt2($inp)
{
global $mm;
$xx=0;$yy=0;
$bb='';
$xx = ($xx+1) % 256;
$a = $mm[$xx];
$yy = ($yy+$a) % 256;
$mm[$xx] = $b = $mm[$yy];
$mm[$yy] = $a;
//proses XOR antara ciphertext dengan kunci
//dengan $inp sebagai ciphertext
//dan $m sebagai kunci
$bb = ($inp^$mm[($a+$b) % 256]) % 256;
return $bb;
}
```

k. Tampilkan hasil dekripsi RC4

```
setupkey();
$nmfile = "enkripsirc4.txt";
//ambil data dari file enkripsirc4.txt
$fp = fopen($nmfile,"r");
$isi = fread($fp,filesize($nmfile));
echo "Ciphertext : $isi"."<br>";
for($i=0;$i<strlen($isi);$i++)
{
$b[$i]=ord($isi[$i]); // rubah ASCII ke desimal
$d[$i]=decrypt2($b[$i]); // proses dekripsi RC4
$s[$i]=chr($d[$i]); // rubah desimal ke ASCII
}
echo "hasil dekripsi = ";
for ($i=0;$i<strlen($isi);$i++)
{
echo $s[$i];
}
echo "<br>";
```

l. Tes Proses Dekripsi.Buka web browser dari PC Client dan akseslah file php dari PC Server http://<no_ip_pc>/akhirrc4.php

m. Catat hasil dekripsi diatas.