PENGEMBANGAN SISTEM OPERASI LINUX UNTUK KEAMANAN JARINGAN

Di ajukan untuk melengkapi tugas dan memenuhi syarat-syarat guna memperoleh gelar Sarjana Komputer STMIK U'Budiyah Indonesia

Oleh

Nama : Milzam. A

Nim : 09111024

PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

STMIK U'BUDIYAH INDONESIA

BANDA ACEH

2014

PENGEMBANGAN SISTEM OPERASI LINUX UNTUK KEAMANAN JARINGAN

SKRIPSI/KARYA TULIS ILMIAH

Di ajukan untuk melengkapi tugas dan memenuhi syarat-syarat guna memperoleh gelar Sarjana Komputer STMIK U'Budiyah Indonesia

Oleh
Nama : Milzam .A
Nim : 09111024

Banda Aceh, 21 Februari 2014
Menyetujui

Penguji I	Penguji II
Sayed Fakhrurrazi, M.Kom	**Muslim, S.Si., M.InfoTech**
Ka. Prodi S-1 Teknik Informatika,	Pembimbing,
Fathiah, ST., M.Eng	**Fathiah, ST., M.Eng**

Mengetahui,
Ka. STMIK U'Budiyah Indonesia

Agus Ariyanto SE., M.Si

LEMBAR PENGESAHAN SIDANG

PENGEMBANGAN SISTEM OPERASI LINUX UNTUK KEAMANAN JARINGAN

Tugas Akhir/KTI oleh *(Milzam .A)* ini telah dipertahankan didepan dewan penguji pada hari jumat *(21 Februari 2014)*

Dewan Penguji:

1. Ketua **Fathiah, ST., M.Eng**

2. Anggota **Sayed Fakhrurrazi, M.Kom**

3. Anggota **Muslim, S.Si., M.InfoTech**

HALAMAN MOTTO

Barang siapa menghendaki kehidupan sekarang (duniawi), maka Kami segerakan baginya di dunia itu apa yang kami kehendaki bagi orang yang kami kehendaki dan Kami tentukan baginya neraka jahannam; ia akan memasukinya dalam keadaan tercela dan terusir.

Dan barangsiapa yang menghendaki kehidupan akhirat dan berusaha ke arah itu dengan sungguh-sungguh sedang ia adalah mukmin, maka mereka itu adalah orang-orang yang usahanya dibalasi dengan baik.

[QS Al-isro:18-19]

More U feel Stupid.More clever U're Now.

[y3d1ps E-C-H-O]

Talk is cheap, show me the code!

[Linus Torvalds]

Jika Sukses di rumuskan, maka rumus sukses = X + Y + Z

dengan X = bekerja,Y = bermain dan Z = tutup mulutmu.

[Albert Einsten]

Every man's work, whether it be literature or music or pictures or architecture or 'hacking' or anything else, is always a portrait of himself

[Samuel Butler]

The more i put my spirit the more i lose my limits

[Tamara Geraldine]

Ketika aku lahir, aku menangis dan orang orang mentertawakan ku. Aku ingin ketika meninggal, aku tertawa dan orang-orang menangis.

[Lord Boden Powell]

HALAMAN PERNYATAAN

Saya menyatakan bahwa skripsi yang saya susun, sebagai syarat memperoleh gelar sarjana merupakan hasil karya tulis saya sendiri. Adapun bagian-bagian tertentu dalam penulisan skripsi ini yang saya kutip dari hasil karya orang lain telah dituliskan sumbernya secara jelas sesuai dengan norma, kaidah, dan etika penulisan ilmiah. Saya bersedia menerima sanksi pencabutan gelar akademik yang saya peroleh dan sanksi-sanksi lainnya sesuai dengan peraturan yang berlaku, apabila dikemudian hari ditemukan adanya plagiat dalam skripsi ini.

Banda Aceh,21 Februari 2014

Yang Membuat Pernyataan,

Milzam .A

NIM : 09111024

KATA PENGANTAR

Bismillahirrahmaanirrahim

Assalamu'alaikum Wr.Wb

Alhamdulillahi rabbil'aalamiin, segala puji syukur penulis panjatkan kehadirat Allah SWT, atas limpahan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul **"PENGEMBANGAN SISTEM OPERASI LINUX UNTUK KEAMANAN JARINGAN".**

Penulis menyadari bahwa sejak awal selesainya penulisan skripsi ini tidak lepas dari bantuan, dorongan dan bimbingan berbagai pihak. Oleh karena itu dalam kesempatan ini penulis menyampaikan penghargaan dan ucapan terima kasih kepada :

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya serta izin-Nya demi kelancaran penyelesaian laporan akhir.
2. Kedua orang tua beserta keluarga tercinta yang telah memberikan dukungan moril, material, dan spiritual.
3. Bapak Agus Ariyanto, SE., M.Si selaku Ketua STMIK U'budiyah Indonesia.
4. Ibu Fathiah, ST., M.eng selaku Ketua Prodi Teknik Informatika STMIK U'budiyah Indonesia dan juga sebagai dosen pembimbing yang telah meluangkan waktu untuk membimbing dan mengarahkan penulis.

5. Bapak dan Ibu dosen, selaku dewan penguji pada saat seminar proposal yang telah banyak memberikan kritik dan saran sehingga menjadi bahan perbaikan bagi penulis untuk melanjutkan Skripsi ini.
6. Teman - teman seperjuangan S-1 Teknik Informatika angkatan 2009.
7. Semua pihak yang telah banyak membantu saya dari saudara, sahabat, dan lainnya.

Penulis menyadari bahwa Tugas Akhir ini masih jauh dari kesempurnaan, baik dari segi isi dan bahasanya. Hal ini disebabkan karena keterbatasan ilmu pengetahuan yang Penulis miliki. Oleh karena itu Penulis sangat mengharapkan saran-saran dan kritik yang membangun dan bermanfaat dari semua pihak.

Hanya kepada Allah SWT Penulis berserah diri atas jerih payah dan bantuan dari berbagai pihak. Semoga Allah memberikan balasan yang setimpal. Akhir kata penulis mengharapkan agar Tugas Akhir ini dapat bermanfaat bagi penulis dan pembacanya. InsyaAllah Sang Khaliq selalu memberikan dan meridhoi hidup kita semua. Amin Ya Rabbal ‘Alamin.

Banda Aceh, 21 Januari 2014

Penulis

ABSTRAK

Penelitian ini bertujuan untuk membuat distribusi Linux yang memfokuskan diri pada desktop yang ringan serta ditujukan untuk menjadi sebuah lingkungan belajar dan pengembangan kemampuan pada lingkungan keamanan jaringan yang dapat dimanfaatkan mahasiswa/mahasiswi kampus STMIK U'budiyah Indonesia.

Distribusi ini dikembangkan dengan metode remastering dari Distro Linux Mint Isadora sebagai base system. Distribusi ini diberi nama Fullboster-OS. Yang di kembangkan mulai dari tahap kompilasi source code program, membuat file script dan konfigurasi sampai pada tahap pembuatan Live CD dan Installer.

Hasil dari penelitian ini berupa Live CD dan installer sehingga bisa di jalankan tanpa harus menginstalnya atau pun bisa langsung di pasangkan ke hardisk dan di dalam distro ini berisi tool untuk lingkungan belajar mengenai sistem keamanan jaringan. Tool Utama yang disertakan didalamnya adalah etherap, wireshark, ethercape, nmap, dll.

Kata Kunci : Distribusi, Distro, Linux, Open Source

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar Belakang

Belakangan ini kondisi dunia jaringan komputer di indonesia sangat mengawatirkan mulai dari adanya penyebaran *virus* melalui *internet* yang mudah menyebar melalui komputer ke komputer maupun penyebaran melalui perangkat *mobile* canggih yang sedang *booming* di negara kita yaitu *smartphone*. Tidak hanya itu beberapa waktu yang lalu sempat juga kita mengalami gangguan *cyber crime* yang di lancarkan oleh pihak australia demi mengambil keuntungan dari indonesia, seperti pencurian data, penyadapan suara, berkas-berkas yang dianggap penting, *website deface* sampai melakukan *Denials Of Service* ke beberapa server jaringan di indonesia dan aksi *Cracking* lainnya.

Aksi-aksi seperti diatas sudah tidak asing lagi kita dengar di negara kita ini, karena sudah terlalu sering terjadi, sebenarnya banyak cara untuk mengantisipasi hal-hal yang tidak diinginkan seperti itu, mulai dari memperbaiki *bug* (celah keamanan) pada aplikasi dan jaringan, memasang *firewall* atau bahkan membackup data-data penting yang mudah diserang seperti *database*.

Dari keterangan-keterangan diatas penulis sangat tertarik untuk membuat salah satu distribusi *linux pentest (penetration testing)* yang digunakan untuk melindungi data dan keamanan jaringan sehingga penulis mengambil judul ***"Pengembangan Sistem Operasi Linux untuk Keamanan"*** untuk dijadikan bahan penelitian yang nantinya memiliki tujuan utama untuk melindungi akses jaringan komputer pada STMIK U'budiyah Indonesia dan juga sebagai wadah

serta tempat untuk belajar mengenai sistem keamanan jaringan, sehingga nantinya juga diharapkan akan menghasilkan para *hacker-hacker* muda potensial yang akan membangun lingkungan kampus pada khususnnya dan lingkungan teknologi Indonesia pada umumnya.

Dengan melakukan penggabungan antara *Linux* dan Jaringan ini nantinya juga diharapkan berdampak positif bagi *industry software* di indonesia dengan melahirkan sistem keamanan pada jaringan, dan juga sistem ini nantinya akan bersifat ”*Free Software/Open source Software”* sehingga mudah untuk dikembangkan kembali.

1.2 Rumusan Masalah

Rumusan masalah pada tugas akhir ini akan lebih terfokus pada pembuatan sebuah distribusi *linux* yang mampu :

1. Menjaga keamanan data dan jaringan pada computer.
2. Menggabungkan metode *pentest* kedalam *Linux* agar mahasiswa/mahasiswi STMIK U’budiyah Indonesia mampu memahami dan mempelajari serta mengaplikasikan semua perangkat lunak *open source* yang sudah terinstal didalam distribusi *Linux* ini dengan baik.

1.3 Batasan Masalah

Pada penelitian ini, permasalahan akan sangat dibatasi seperti berikut :

1. Membangun sistem yang hanya berjalan pada komputer arsitektur x86.
2. Membangun sistem dengan aplikasi utama yang nantinya bisa digunakan untuk belajar keamanan jaringan seperti *Wireshark, Etherape, Ethercape, Nmap, Trojan, Tracer*, dll

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk membuat sebuah distribusi *Linux* seperti dibawah ini :

1. Distribusi yang memfokuskan diri pada sistem dan aplikasi berbasis *desktop*.
2. Sistem ditujukan pada mahasiswa/mahasiswa yang memfokuskan diri untuk mendalami sistem jaringan komputer beserta keamanannya.

1.5 Sistematika Penulisan

Dalam penulisannya, penelitian ini dibagi menjadi 5 bab. Sistematika penulisan bab dan gambaran isi masing-masingnya adalah sebagai berikut :

BAB I membahas latar belakang penelitian yang akan dilakukan, rumusan masalah, sampai dengan batasan masalah, serta tujuan penilitian dan sistematika penulisan.

BAB II membahas mengenai konsep dasar jaringan, dasar keamanan jaringan, pembagian *hacker* dan *cracker*, pengertian sistem operasi *linux*, distribusi dan *tool-tool* yang dipakai untuk membuat distribusi *Linux* ini.

BAB III membahas tentang jadwal penelitian, tempat penelitan, prosedur yang digunakan seperti jenis dan pengamatan penelitian.

BAB IV membahas tentang proses pembuatan distribusi *Linux,* konfigurasi sistem, instalasi program sampai pada tahap melakukan *remaster* pada distribusi *Linux* agar bisa di instal kedalam komputer.

BAB V merupakan bab terakhir berisi kesimpulan dan saran yang diperoleh dari pembuatan sistem tersebut.

BAB II

TINJAUAN PUSTAKA

2.1 Konsep Dasar Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Adapun tujuan dari jaringan komputer yang dimaksud adalah:

1. Jaringan komputer yaitu hubungan antara beberapa komputer untuk saling berbagi pakai.
2. Membagi sumber daya contohnya berbagi pemakaian *printer*, *internet*, *folder*, *desktop.*
3. Komunikasi: contohnya surat elektronik, *instant messaging*, *chatting.*
4. Akses informasi: contohnya *web browsing* .

Teknologi jaringan komputer mengalami perkembangan yang pesat, hal ini terlihat pada era tahun 80-an. Jaringan komputer masih merupakan teka-teki yang ingin dijawab oleh kalangan akademisi, dan pada tahun 1988 jaringan komputer mulai digunakan di universitas-universitas, perusahaan-perusahaan, sekarang memasuki era milenium ini terutama *world wide internet* atau sekarang lebih dikenal dengan singkatn WWW telah menjadi realitas sehari-hari jutaan manusia di muka bumi ini.

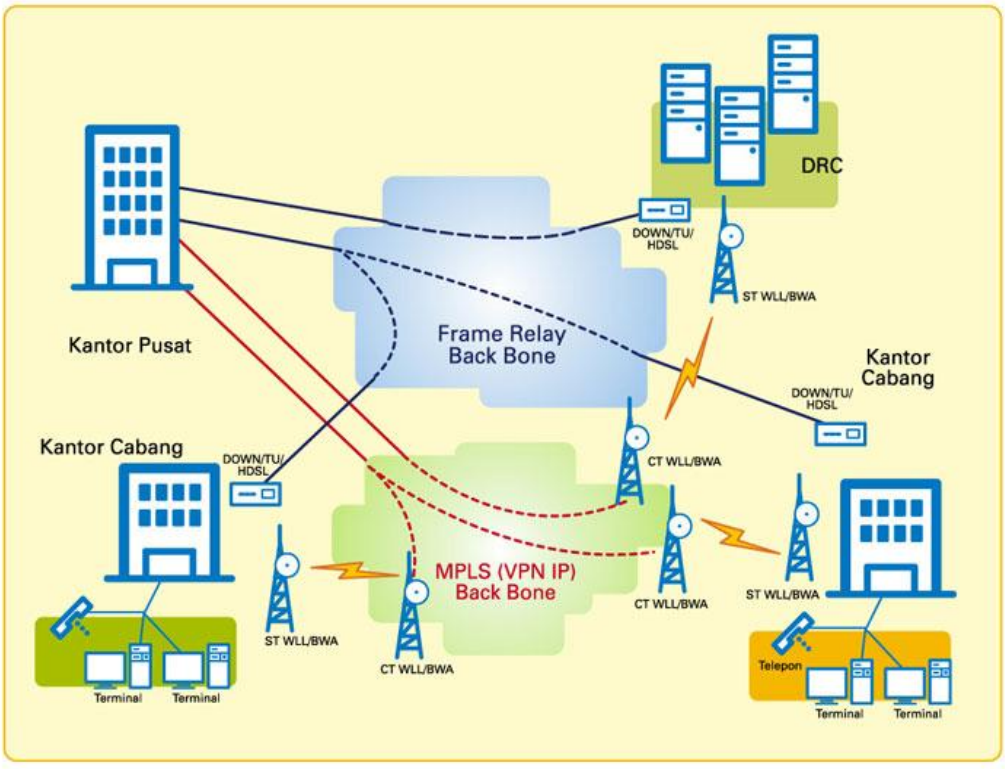
Selain itu, perangkat keras dan perangkat lunak jaringan telah benar-benar berubah, di awal perkembangannya hampir seluruh jaringan dibangun dari kabel *koaxial*, kini banyak telah diantaranya dibangun dari serat optik *(fyber optics)* atau komunikasi tanpa kabel.

Dari sinilah kemudian muncul sebuah konsep yang dikenal dengan nama TSS *(Time Sharing System),* yakni bentuk pertama kali jaringan komputer. Aplikasi pada konsep TSS yaitu beberapa komputer *terminal* terhubung secara seri ke sebuah *host* komputer. Selanjutnya konsep ini berkembang menjadi konsep *Distributed Processing* (proses dan sistem distribusi) yang mampu melayani *host* komputer secara paralel. Kemudian berkembang sebuah teknologi LAN *(Local Area Network),* jaringan raksasa yang di kenal dengan WAN (*Wide Area Network)* hingga internet *(global).*

Di bawah ini adalah beberapa jenis-jenis jaringan pada komputer yang sering digunakan dalam kehidupan sehari – hari diantaranya adalah:

1. LAN (*Local Area Network*) kerupakan jaringan milik pribadi dengan jangkauan satu gedung atau beberapa KM saja untuk dapat memakai bersama sumber daya dan saling bertukar informasi dan memiliki konsep yang sama dengan LAN namun bedanya hanya penambahan *web server* pada servernya. *Intranet* bersifat tertutup dan keamanannya terjaga (hanya digunakan oleh kalangan sendiri).
2. MAN (*Metropolitan Area Network*) merupakan kumpulan LAN dengan jangkauan lebih besar yaitu satu kota. MAN dapat mencakup kantor- kantor atau perusahaan yang letaknya berdekatan. Dapat dimanfaatkan untuk keperluan pribadi atau umum dan mampu menunjang data, suara, bahkan TV kabel.

3. WAN (*Wide Area Network*) merupakan jaringan komputer dengan jangkauan daerah yang luas yaitu antar negara bahkan benua. Sifatnya tertutup dengan menggunakan jasa *provider* tertentu sebagai media penghubungnya.
4. *Internet* merupakan kumpulan jaringan yang terkoneksi yang dapat diakses oleh siapapun, kapanpun, dan dimanapun. Sifatnya sangat terbuka dan keamannya kurang terjamin.
5. *Wireless* (jaringan tanpa kabel) merupakan jaringan komunikasi yang dilakukan tanpa kabel yang mampu memberikan kecepatan akses lebih cepat dibanding jaringan dengan kabel, contohnya : teknologi *infrared, bluetooth, modem*, dll.



Gambar 2.1 Jaringan Internet saling terhubung satu dengan yang lainnya (Purbo, Onno W. 1992)

2.2 Keamanan Komputer

Keamanan jaringan adalah menjaga agar *resource* digunakan sebagaimana mestinya oleh pemakai yang berhak. Keamanan jaringan komputer sendiri sering dipandang sebagai hasil dari beberapa faktor. Faktor ini bervariasi tergantung pada bahan dasar, tetapi secara normal setidaknya beberapa hal dibawah ini diikutsertakan :

1. *Confidentiality* (kerahasiaan).
2. *Integrity* (integritas).
3. *Availability* (ketersediaan).

Keamanan Jaringan juga memiliki factor-faktor yang membuat suatu jaringan beresiko untuk kehilangan data. Beberapa faktor penyebab resiko dalam Jaringan Komputer adalah sebagai berikut :

1. Kelemahan manusia (*human error*)
2. Kelemahan perangkat keras
3. Kelemahan sistem operasi jaringan
4. Kelemahan sistem jaringan komunikasi

Ada beberapa ancaman di jaringan yang harus diwaspadai sesuai dengan bentuk serangan yang dilakukan diantaranya adalah :

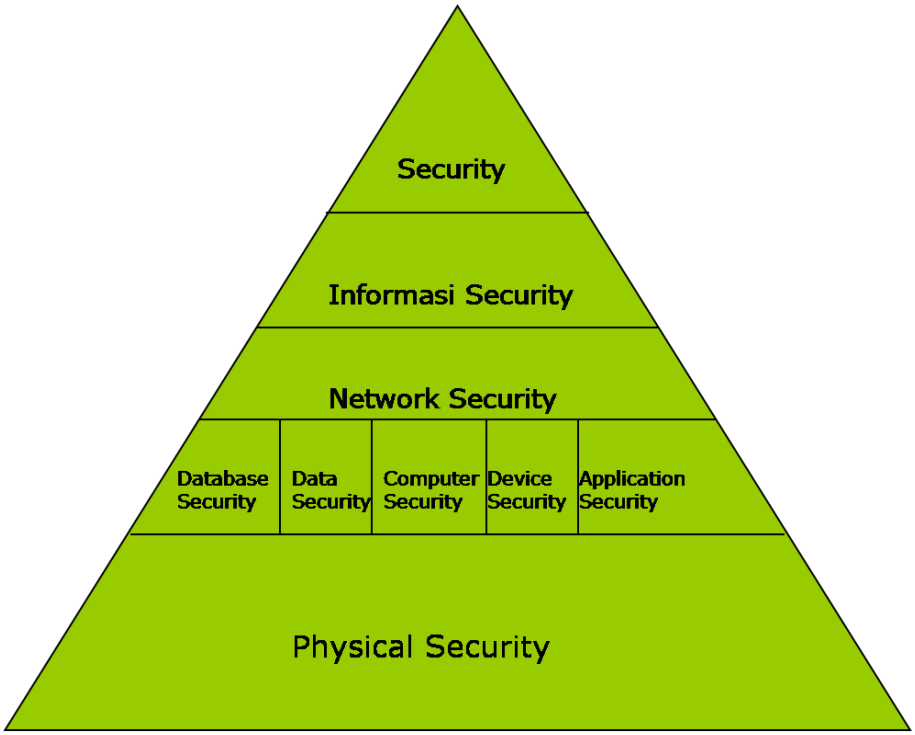
1. Fisik
    a. Pencurian perangkat keras komputer atau perangkat jaringan
    b. Kerusakan pada komputer dan perangkat komunikasi jaringan
    c. Wiretapping
    d. Bencana alam

2. Logik

   a. Kerusakan pada sistem operasi atau aplikasi

   b. Virus

   c. Sniffing



Gambar 2.1 Security Methodelogy (Tanembaum, Andrews.1996)

2.3 Hacker

Salah satu ancaman keamanan jaringan adalah *Hacker*. Istilah *Hacker* muncul pada awal tahun 1960-an diantara para anggota organisasi mahasiswa *Tech Model Railroad Club* di laboratorium kecerdasan *Artifisial Massachusetts Institute of Technology* (MIT). Kelompok mahasiswa tersebut merupakan salah satu perintis perkembangan teknologi komputer dan mereka beroperasi dengan sejumlah komputer *mainframe*. Kata *hacker* pertama kali muncul dengan arti

positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik dari yang telah dirancang bersama. Kemudian pada tahun 1983, analogi *hacker* semakin berkembang untuk menyebut seseorang yang memiliki obsesi untuk memahami dan menguasai sistem komputer. Pasalnya, pada tahun tersebut untuk pertama kalinya FBI menangkap kelompok kriminal komputer *The 414s* yang berbasis di Milwaukee AS. *The 414*s merupakan kode area lokal mereka. Kelompok yang kemudian disebut hacker tersebut dinyatakan bersalah atas pembobolan 60 buah komputer, dari komputer milik pusat kanker *Memorial Sloan-Kettering* hingga komputer milik laboratorium National Los Alamos. Salah seorang dari antara pelaku tersebut mendapatkan kekebalan karena testimonialnya, sedangkan 5 pelaku lainnya mendapatkan hukuman masa percobaan.

Kemudian pada perkembangan selanjutnya muncul kelompok lain yang menyebut-nyebut diri *hacker*, padahal bukan. Mereka ini (terutama para pria dewasa) yang mendapat kepuasan lewat membobol komputer dan mengakali telepon (*phreaking*). *Hacker* sejati menyebut orang-orang ini *'Cracker'* dan tidak suka bergaul dengan mereka. *Hacker* sejati memandang *Cracker* sebagai orang malas, tidak bertanggung jawab, dan tidak terlalu cerdas. *Hacker* sejati tidak setuju jika dikatakan bahwa dengan menerobos keamanan seseorang telah menjadi *hacker*.

Para *hacker* mengadakan pertemuan setiap setahun sekali yaitu diadakan setiap pertengahan bulan Juli di Las Vegas. Ajang pertemuan *hacker* terbesar di dunia tersebut dinamakan *Def Con*. Acara *Def Con* tersebut lebih kepada ajang pertukaran informasi dan teknologi yang berkaitan dengan aktivitas hacking.

Kesimpulan yang didapat dari perbedaan seorang *Hacker* dan *Cracker* diatas adalah :

1. *Hacker* adalah sebutan untuk orang atau sekelompok orang yang memberikan sumbangan bermanfaat untuk dunia jaringan dan sistem operasi, membuat program bantuan untuk dunia jaringan dan komputer. *Hacker* juga bisa di kategorikan perkerjaan yang dilakukan untuk mencari kelemahan suatu *system* dan memberikan ide atau pendapat yang bisa memperbaiki kelemahan *system* yang di temukannya. Contoh *Hacker* terkenal yang sudah banyak membantu perkembangan teknologi adalah Kevin Mitnick, Adrian, Linus Torvald, John Draper, Mark Abene, Robert Moris, Richard Stallman, dan masih banyak lagi yang lainnya. Selain itu di indonesia tidak kalah hebatnya sebagai negara yang termasuk kedalam negara yang paling sering menggunakan internet ada beberapa kelompok hacker dan perorangan yang perlu kita ketahui sebagai inspirasi dunia teknologi di tanah air, diantaranya adalah Onno W.Purbo, Jim Geovendi, Dani Firmansyah, I Made Wiryana, dan ada juga komunitas seperti Kecoak Electronik, Jasakom, Xcode, Echo, KPLI-Aceh, Ophrack3rz dll.
2. *Cracker* adalah sebutan untuk mereka yang masuk ke sistem orang lain dan *cracker* lebih bersifat destruktif, biasanya di jaringan komputer, mem-*bypass*

password atau lisensi program komputer, secara sengaja melawan keamanan komputer, men-*deface* (merubah halaman muka web) milik orang lain bahkan hingga men-*delete* data orang lain, mencuri data. Beberapa *Cracke*r berbahaya di dunia yang perlu diketahui diantaranya adalah Gary McKinnon, Joseph Jonathan James, George Hotz, Adrian Lamo, David Smith, Michael Calce, Robbert Tappan Moris, Vladimir Levin, dan Organisasi Black Hat yang paling terkenal saat ini adalah anggota *Cracker* Anonymous, yang masih dalam pencarian FBI.

2.3.1 Penggolongan Hacker

Di dalam dunia komputer dan internet, *hacker* atau *hacking* bukan istilah yang asing lagi. Tujuan mereka adalah meretas data, informasi atau sistem keamanan bahkan hingga dapat mengendalikannya. Dalam susunannya, ternyata *Hacker* dibagi menjadi kedalam beberapa golongan yaitu :

1. *Script Kiddies*

Golongan ini adalah golongan pemula atau *newbie* yang melakukan *hacking* terhadap *website* atau sistem lain dengan menggunakan *software* atau program khusus yang sudah diciptakan oleh para *hacker* terdahulu dan berpengalaman.

Script Kiddies hanya menggunakan program- program tersebut tanpa perlu mencoba menciptakan program baru. Secara relatif, mereka hanya mengerti konsep dasar *hacking* saja. Rata- rata para *Script Kiddies* melakukan aksinya dengan dasar iseng dan tidak melakukannya untuk alasan tertentu. Boleh dibilang hanya sebagai pencarian jati diri atau masih belajar di dunia *hacking*.

2. Hacker Group

Hacker Group ini adalah kumpulan orang juga para *Script Kiddies* yang bersatu dengan membuat sebuah komunitas untuk tujuan tertentu. Mereka akan merasa kuat apabila kekuatan, pengalaman dan kemampuan yang mereka miliki digabungkan dalam satu kelompok.

Mayoritas orang-orang dalam *Hacker Group* ini beraksi dengan tujuan tertentu dan selain untuk mencari popularitas, mereka juga mencari keuntungan. Dalam *Hacker Group* ini dapat digolongkan dalam beberapa kategori seperti *Defacer*, *Cracker*, *Carder* dan *Exploiter* seperi grup yang banyak kita jumpai di *facebook* dll.

3. Hacktivist

Hacktivist adalah sekumpulan orang yang mempunyai visi dan misi sama. Mereka rata- rata mempunyai keahlian, kemampuan dan pengalaman yang tinggi. Kelompok satu ini menggelar aksinya dengan tujuan politis dan sosial. Salah satu contoh *hacktivist* terkenal dengan sebutan *Anonymous* yang juga mempunyai cabang- cabang di setiap negara.

4. Black Hat Professionals

Kelompok ini adalah kelompok yang mahir dalam hal *coding*. Kelompok ini susah dihancurkan atau juga ditemui secara mudah. Mereka akan terus tumbuh dan berkembang. Rata-rata kelompok satu ini merupakan musuh para pemerintah dan pebisnis.

5. Organized Criminal Gangs

Kelompok satu ini bisa dikatakan kelompok yang sangat berbahaya karena mereka secara langsung berada di bawah geng kriminal. Orang- orang dalam kategori ini merupakan orang-orang pilihan yang mempunyai keahlian di atas rata-rata. Mereka beraksi secara halus sehingga pihak kepolisian pun akan sulit untuk mendeteksi bahkan menangkapnya.

6. Nation States

Kelompok satu ini boleh dibilang lebih terorganisasi dan terselubung. Dalam aksinya mereka mengincar data-data infrastruktur penting seperti milik pemerintah, publik, finansial dan militer. Salah satu contohnya adalah munculnya *virus flame* yang berhasil menginfeksi ribuan komputer di daerah Timur Tengah pada pertengahan tahun 2012 lalu.

7. The Automated Tool

Orang-orang yang masuk dalam kategori ini adalah para pencipta virus berbahaya yang dapat menginfeksi jutaan *website* atau juga perangkat di komputer. Kelompok ini juga dibagi atas kategori dengan dasar tingkat pengalaman dan kemampuan yang tinggi.

2.3.2 Jenis Jenis Serangan *Cyber (Hacking)*

Secara umum, keamanan komputer *(computer security)* memiliki banyak makna, karena dapat dilihat dari berbagai sisi. Menurut Garfinkel dan Spafford, suatu komputer dapat dikatakan aman jika bisa diandalkan dan perangkat lunaknya bekerja sesuai dengan yang diharapkan oleh pengguna. Secara garis besar, keamanan komputer mencakup empat hal mendasar, yaitu keamanan secara

fisik *(physical security),* keamanan akses *(access security),* keamanan data *(data security),* dan keamanan jaringan *(network security).*

Dari klasifikasi yang telah dijelaskan di atas, dapat disebutkan beberapa jenis serangan yang dilakukan melalui dunia maya, antara lain:

1. Session Hijacking

Session Hijacking adalah aksi pengambilan kendali *session* milik *user* lain setelah sebelumnya "pembajak" berhasil memperoleh *autentifikasi ID session* yang biasanya tersimpan dalam *cookies*. *Session hijacking* menggunakan metode *captured, brute forced* atau *reserve enggineered* guna memperoleh *ID session*, yang untuk selanjutnya memegang kendali atas *session* yang dimiliki oleh *user* lain tersebut selama session berlangsung.

HTTP merupakan protokol yang *stateless,* sehingga perancang aplikasi mengembangkan suatu cara untuk menelusuri suatu *state* diantara *user-user* yang memiliki koneksi secara *multipl*e. Aplikasi menggunakan *session* untuk menyimpan parameter-parameter yang relevan terhadap *user. Session* akan terus ada pada server selama user masih aktif/terkoneksi. *Session* akan otomatis dihapus jika *user logout* atau melampaui batas waktu koneksi. Karena sifatnya ini, session dapat dimanfaatkan oleh seorang *hacker* untuk melakukan *session hijacking.*

Istilah sesi pembajakan (*session hijacking*) umumnya digunakan untuk menggambarkan proses sebuah koneksi TCP yang diambil alih oleh sebuah rangkaian serangan yang sudah dapat diprediksi sebelumnya. Pada serangan seperti itu, penyerang memperoleh kendali melalui koneksi TCP yang sudah ada.

Bila diterapkan pada keamanan aplikasi web, *session hijacking* mengacu pada pengambil alihan sebuah *session* aplikasi web.

2. Spoofing

Spoofing adalah teknik yang digunakan untuk memperoleh akses yang tidak sah kesuatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah *host* yang dapat dipercaya seperti memalsukan identitas, IP, dan DNS, hal ini biasanya dilakukan oleh seorang *hacker/cracker.*

3. SQL Injection

Injeksi SQL atau SQL *Injection* memiliki makna dan arti yaitu sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi. Celah ini terjadi ketika masukan pengguna tidak disaring secara benar dari karakter-karakter pelolos bentukan *string* yang diimbuhkan dalam pernyataan SQL atau masukan pengguna tidak bertipe kuat dan karenanya dijalankan tidak sesuai harapan. Ini sebenarnya adalah sebuah contoh dari sebuah kategori celah keamanan yang lebih umum yang dapat terjadi setiap kali sebuah bahasa pemrograman atau skrip diimbuhkan di dalam bahasa yang lain.

SQL *injection* adalah jenis aksi *hacking* pada keamanan komputer di mana seorang penyerang bisa mendapatkan akses ke basis data di dalam sistem. SQL *injection* yaitu serangan yang mirip dengan serangan XSS dalam bahwa penyerang memanfaatkan aplikasi vektor dan juga dengan *common* dalam

serangan XSS. Contohnya seperti kejadian pada aplikasi website kampus dengan alamat *www.stmikubudiyah.ac.id* yang berhasil diretas oleh seorang hacker dengan inisial *kait00kid* pada tahun 2011 dan 2012.

4. Malicious Software

Malicous Software atau sering disebut dengan *malware* merupakan program yang disusupkan ke dalam sebuah sistem dengan tujuan untuk melakukan berbagai macam aktivitas yang dapat merugikan korban. Tingkat kerugian tersebut bermacam-macam, mulai dari sekedar memperlambat kinerja sistem hingga merusak dan menghancurkan data yang berada dalam sistem tersebut seperti *virus*, *worm* dan *trojan* pada komputer.

5. Denial Of Service (DOS)

Denial of Service (DOS) adalah sebuah jenis serangan yang dapat dilakukan siapa saja di *internet*, yang memiliki tujuan melakukan pencegahan terhadap para *user* yang berwenang untuk melakukan akses kepada komputer, atau jaringan tertentu. Serangan DOS menargetkan *bandwidth* dan koneksi sebuah jaringan untuk dapat mencapai misinya. Pada serangan terhadap *bandwidth*, sang penyerang melakukan pembajiran “lalu-lintas” data dalam suatu jaringan, dengan menggunakan “perangkat” yang sudah tersedia pada jaringan itu sendiri, sehingga membuat *user* yang sudah terkoneksi didalam nya mengalami hilang koneksi. Di sisi lain, jenis serangan terhadap aktifitas koneksi, adalah dengan sedemikian rupa banyaknya, meminta koneksi langsung terhadap *server* ataupun *router* yang

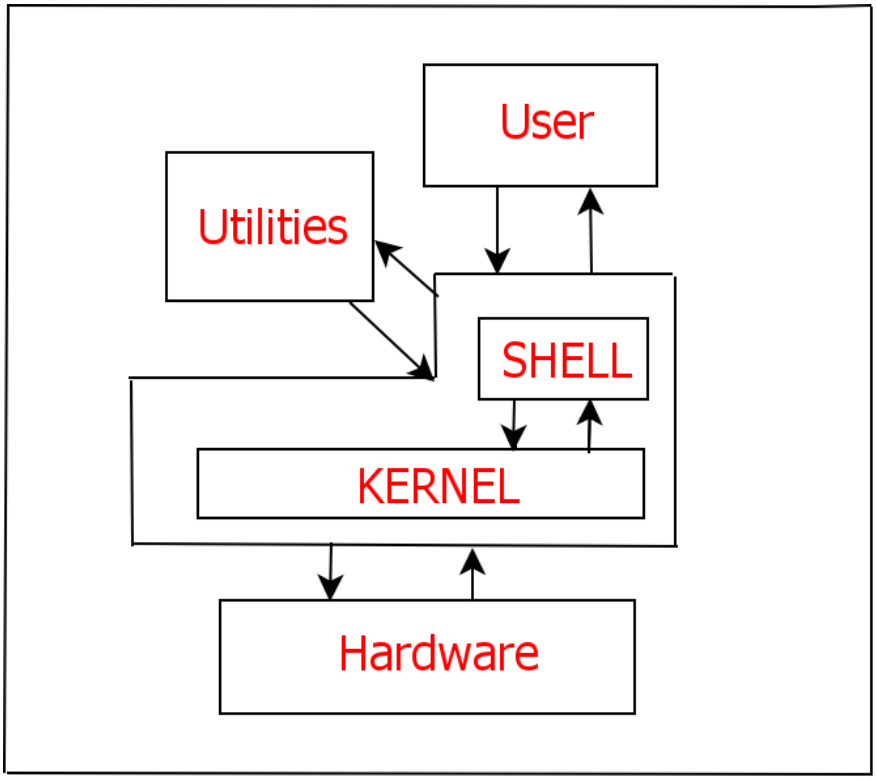
bersangkutan, sehingga membuat operasi sistem menjadi tidak memiliki "*spot* koneksi" lagi untuk *user* lain, dan membuat *user-user* tersebut tidak dapat terkoneksi ke *server* itu.

2.4 Sistem Operasi

Sistem operasi komputer merupakan sumber daya yang menghubungkan antara *user* atau pengguna dari komputer dengan perangkat keras komputer dan menyediakan layanan *(system calls*) kepemakai sehingga mempermudah penggunaan serta pemanfaatan sumber daya sistem komputer.

Untuk mengenal sistem operasi komputer dengan baik kita harus mengetahui fungsi dasar dari perangkat keras, program aplikasi, sistem operasi sendiri dan juga para pengguna komputer. Fungsi perangkat keras sendiri sebagai masukan, keluaran dan juga menjadi alokasi memori. Sedangkan sistem operasi berfungsi sebagai penghubung antara program aplikasi dan perangkat keras komputer.

Sementara program aplikasi menentukan bagaimana cara sumber daya sistem dapat digunakan untuk menyelesaikan permasalahan komputer dari *user* seperti *assembler, loader, linker, compiler*. Dan *user* atau pengguna adalah orang, mesin atau bisa juga komputer lain yang mengunakan sistem tersebut.



Gambar 2.3 Diagram Sistem Operasi (Tanembaum, Andrews.1996)

Untuk mengenal sistem operasi komputer kita harus mengerti tentang definisi *Resource allocator*, program *control* dan juga kernel sebagai berikut :

1. *Resource allocator* adalah sistem operasi yang mengatur dan mengalokasikan sumber daya-sumber daya dari sistem komputer.
2. Program *control* adalah sistem operasi yang melakukan *control* atau eksekusi dari sebuah program *user* dan operasi *input* maupun *output.*
3. *Kernel* merupakan suatu program yang berjalan sepanjang waktu (selain program aplikasi).

Ada beberapa macam bentuk sistem operasi yang sering di gunakan, diantaranya adalah sebagai berikut :

1. *Batch system* yaitu perintah yang dilakukan dalam satu rangkaian yang seterusnya akan di eksekusi secara berurutan. *System* ini ada pada generasi kedua yang berfungsi FMS *(Fortarn Monitoring System)* dan IBSYS.
2. *Multiprogramming*, beberapa tugas yang disimpan dalam memori dalam satu waktu. Pada *system multiprogramming* sistem operasi harus menyediakan mekanisme untuk *managemen* memori , penjadwalan dan juga *managemen disk.*
3. *Time sharing* adalah metode dimana memperbolehkan banyak pengguna untuk mengunakan komputer secara interaktif atau dapat melakukan *prosesing* dalam satu komputer. *Time sharing* atau *multitasking* adalah pengembangan dari *system multiprogram*.
4. Paralel (*multiprocessor)* merupakan metode yang menggunakan lebih dari satu CPU yang mempunyai hubungan yang erat. *System* ini juga disebut dengan *multiprosesor,* juga sering digunakan adalah model *symmetric multiprosesing* di mana setiap *procesor* menjalankan sistem operasi yang identik.
5. Terdistribusi Merupakan tren *system computer* saat ini yang mendistribusikan komputasi di antara beberapa *prosesor.*
6. *Cluster* Sistem terklaster *(clustered system*) adalah pengembangan dari sistem terdistribusi. Sistem ini mempunyai kehandalan sistem yang tinggi seperti pada sistem terdistribusi. Sistem terklaster dapat berupa model *asymmetric clustering* dimana satu sumber menjalankan aplikasi sementara server lainnya standby. Model lainnya adalah *symmetric clustering* dimana semua *host* menjalankan aplikasi.

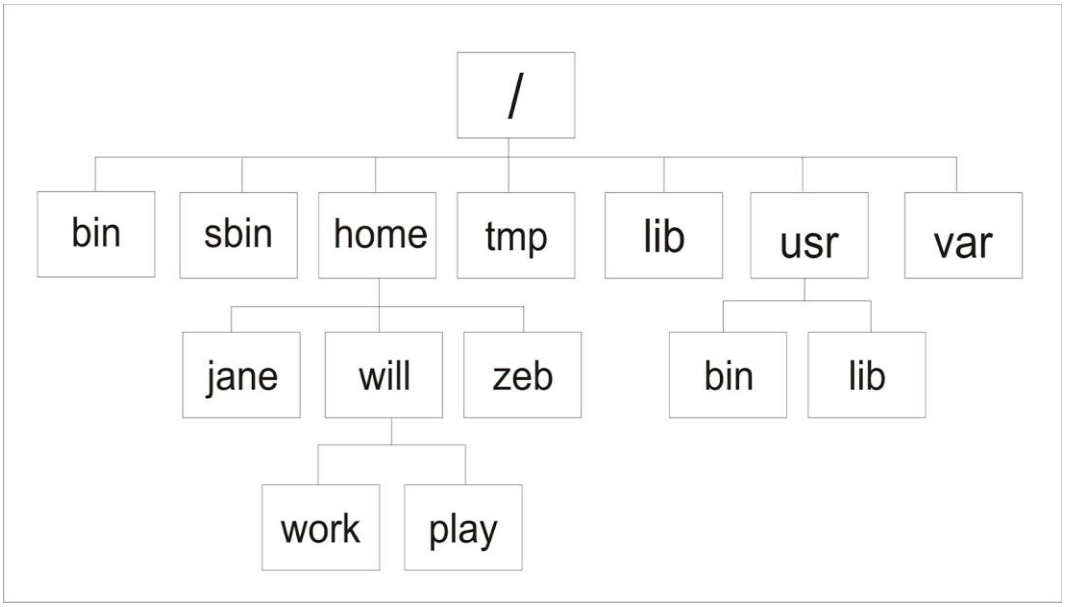
7. *Real time System*, *real-time* mempunyai dua bentuk yaitu *hard real-time* dan *soft real-time*. *Hard real-time* seringkali digunakan sebagai alat pengontrol aplikasi yang *dedicated* dan mempunyai batasan waktu yang tepat dan didefinisikan dengan baik. Sedangkan *soft real-time* mempunyai sedikit batasan waktu yang keras dan tidak mendukung penjadwalan dengan menggunkan batasan akhir.
8. *Handheld* sekitar tahun 1990-an dikembangkan sistem yang lebih kecil dari mikrokompuer yang disebut dengan sistem *handheld* dalam bentuk *personal digital assistants* (PDA). Contohnya seperti gadget sartphone android, backberry, windows phone, iphone, nokia, meego, dll.

2.5 GNU/LINUX

GNU/Linux adalah sebuah sistem operasi yang diciptakan oleh *Linus Benedict Torvalds* seorang *hacker* sekaligus mahasiswa Universitas Helsinki Finlandia di tahun 1991. Proyek GNU ini diluncurkan pada tahun 1984 untuk mengembangkan sebuah sistem operasi lengkap mirip UNIX berbasis perangkat lunak bebas: yaitu sistem GNU (GNU merupakan akronim berulang dari "*GNU's Not Unix";* GNU dilafalkan dengan "*genyu*"). Varian dari sistem operasi GNU, yang menggunakan *kernel Linux,* dewasa ini telah digunakan secara meluas. Walau pun sistem ini sering dirujuk sebagai "*Linux*", sebetulnya lebih tepat jika disebut sistem GNU/*Linux*. Ada salah satu fitur atau kemampuan yang sangat menarik dari GNU/*Linux* yang belum ada pada sistem operasi populer lainnya, yaitu menjalankan sistem operasi dan aplikasi lengkap tanpa menginstalnya di

hard disk. Dengan cara ini dengan mudah kita dapat menggunakan GNU/*Linux* di komputer orang lain karena tak perlu menginstalnya (tak perlu mengutak-atik *hard disk* dan partisinya).

Sejarah sistem operasi *Linux* berkaitan erat dengan proyek GNU, proyek program bebas *freeware* terkenal diketuai oleh Richard Stallman. Proyek GNU diawali pada tahun 1983 untuk membuat sistem operasi seperti Unix lengkap, *kompiler, utiliti* aplikasi, *utiliti* pembuatan dan seterusnya diciptakan sepenuhnya dengan perangkat lunak bebas. Pada tahun 1991, pada saat versi pertama kerangka *Linux* ditulis, proyek GNU telah menghasilkan hampir semua komponen sistem ini kecuali *kernel*. Torvalds dan pembuat *kernel* seperti *Linux* menyesuaikan *kernel* mereka supaya dapat berfungsi dengan komponen GNU, dan seterusnya mengeluarkan sistem operasi yang cukup berfungsi. Oleh karena itu, *Linux* melengkapi ruang terakhir dalam rancangan GNU.



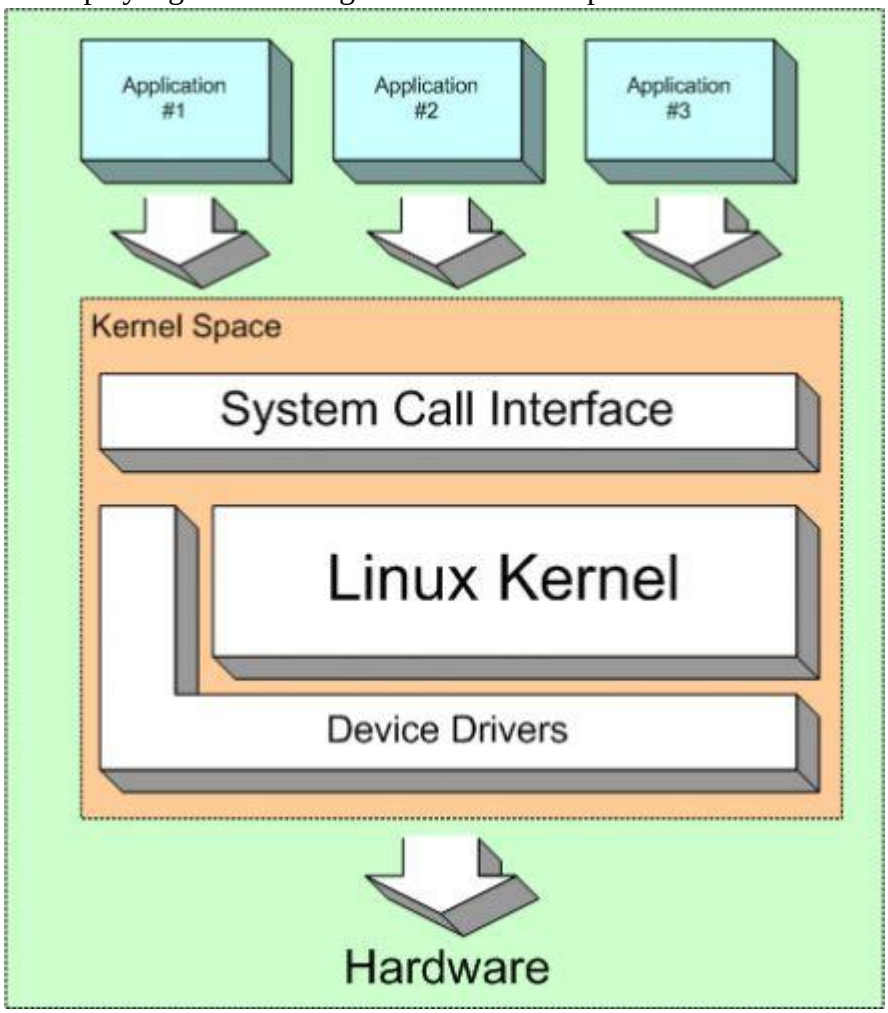
Gambar 2.4 Struktur directory Linux

2.5.1 Kernel

Kernel adalah suatu perangkat lunak yang menjadi bagian utama dari sebuah sistem operasi. Tugasnya melayani bermacam program aplikasi untuk mengakses perangkat keras komputer secara aman. Istilah *Linux* sebetulnya hanya mengacu pada *kernel* dari suatu sistem operasi. *Kernel* adalah jembatan antara *hardware* dan aplikasi-aplikasi yg menterjemahkan bahasa *software* sehingga mampu dimengerti dan diproses oleh *hardware* sesuai dengan permintaan. Karena akses terhadap perangkat keras terbatas, sedangkan ada lebih dari satu program yang harus dilayani dalam waktu yang bersamaan, maka *kernel* juga bertugas untuk mengatur kapan dan berapa lama suatu program dapat menggunakan satu bagian perangkat keras tersebut. Hal tersebut dinamakan sebagai *multiplexing.* Akses kepada perangkat keras secara langsung merupakan masalah yang *kompleks*, oleh karena itu kernel biasanya mengimplementasikan sekumpulan abstraksi *hardware*. Abstraksi-abstraksi tersebut merupakan sebuah cara untuk menyembunyikan *kompleksitas*, dan memungkinkan akses kepada perangkat keras menjadi mudah dan seragam. Sehingga abstraksi pada akhirnya memudahkan pekerjaan *programer.*

Sebuah *kernel* sistem operasi tidak harus ada dan dibutuhkan untuk menjalankan sebuah komputer. Program dapat langsung dijalankan secara langsung di dalam sebuah mesin (contohnya adalah CMOS *Setup*) sehingga para pembuat program tersebut membuat program tanpa adanya dukungan dari sistem operasi atau *hardware abstraction*. Cara kerja seperti ini, adalah cara kerja yang digunakan pada zaman awal-awal dikembangkannya komputer (pada sekitar tahun

1950). Kerugian dari diterapkannya metode ini adalah pengguna harus melakukan *reset* ulang komputer tersebut dan memuatkan program lainnya untuk berpindah program, dari satu program ke program lainnya. Selanjutnya, para pembuat program tersebut membuat beberapa komponen program yang sengaja ditinggalkan di dalam komputer, seperti halnya *loader* atau *debugger*, atau dimuat dari dalam ROM *(Read-Only Memory)*. Seiring dengan perkembangan zaman komputer yang mengalami akselerasi yang signifikan, metode ini selanjutnya membentuk apa yang disebut dengan *kernel* sistem operasi.



Gambar 2.5 Diagram Kernel Linux

Selanjutnya, para arsitek sistem operasi mengembangkan *kernel* sistem operasi yang pada akhirnya terbagi menjadi empat bagian yang secara desain berbeda, sebagai berikut:

1. *Monolithic kernel* mengintegrasikan banyak fungsi di dalam *kernel* dan menyediakan lapisan abstraksi perangkat keras secara penuh terhadap perangkat keras yang berada di bawah sistem operasi.
2. *Microkernel* menyediakan sedikit saja dari abstraksi perangkat keras dan menggunakan aplikasi yang berjalan di atasnya yang disebut dengan server untuk melakukan beberapa *fungsionalitas* lainnya.
3. *Hybrid kernel* adalah pendekatan desain *microkernel* yang dimodifikasi. Pada *hybrid kernel,* terdapat beberapa tambahan kode di dalam ruangan *kernel* untuk meningkatkan performanya.
4. *Exokernel* menyediakan *hardware abstraction* secara minimal, sehingga program dapat mengakses *hardware* secara langsung. Dalam pendekatan *desain exokernel, library* yang dimiliki oleh sistem operasi dapat melakukan abstraksi yang mirip dengan abstraksi yang dilakukan dalam desain *monolithic kernel.*

2.5.2 Shell

Shell adalah program yang dapat membaca intruksi-intruksi yang di inputkan dan mengartikan kontrol *statement* agar dapat diproses sesuai dengan perintah yang di inginkan dan juga dapat di artikan sebagai jembatan yang menhubungkan antara *user* dengan *kernel* atau biasanya disebut dengan inti dari sistem operasi

Ada beberapa macam *shel* yang bisa dipakai pada *linux* sebagai perintah yang dapat menjalankan fungsi kernel, diantaranya adalah :

1. *Bourne Shell* (sh $) yaitu *shell* yang paling tua atau *primitive* dan kurang memiliki perintah *control.*
2. *C- Shell* (csh %), dikembangkan di Berkeley, paling populer dan interaktif.
3. *Jsh* yaitu versi baru dari *Bourne Shell*, hanya ada di *system* V *release* 4.*Korn*.
4. *Shell* (ksh) merupakan *shell* yang *compatible* dengan *Bourne Shell*, tapi juga memiliki kemampuan *C- Shell.*
5. *Bourne Again Shell* yaitu *shell* yang tidak standard dikembangkan oleh *Free Software Fondation*
6. *Tcsh* merupakan *Extended csh* (versi terbaru dari *C- Shell*).

2.5.3 Distribusi Linux (Distro)

Distro Linux merupakan singkatan dari distribusi *Linux*, yaitu sebuah sebutan untuk sistem operasi komputer yang mirip Unix. Dimana *kernel* yang digunakan adalah *kernel Linux*, bukan *kernel* Unix. Istilah *Linux* sendiri digunakan untuk menyatakan bahwa sistem operasi ini di-ilhami dari sistem operasi Unix yang telah lebih dulu populer. *Linux* merupakan singkatan dari *Like* Unix.

Pada saat ini, telah banyak beredar distro-distro *Linux* di pasaran. Distribusi *Linux* bisa berupa perangkat lunak bebas digunakan dan dikembangkan *(open source),* dan bisa juga berupa perangkat lunak komersial seperti *Red Hat Enterprise, SuSE,* dan lain-lain. Banyaknya distro *Linux* yang beredar di pasaran

saat ini banyak disebabkan oleh sifat sistem operasi *Linux* yang kebanyakan bersifat perangkat lunak bebas untuk digunakan dan dikembangkan *(open source).* Karena dalam penelitian ini penulis ingin membuat sebuah distribusi *linux* yang dapat digunakan untuk lingkungan keamanan jaringan komputer, berikut referensi dari berbagai distro linux yang sudah lama mengikuti perjalanan di dunia keamanan komputer atau lebih dikenal dengan sebutan *pentest.*

1. *Kali Linux*

Kali Linux adalah distribusi berlandasan distribusi *Debian* GNU/*Linux* untuk tujuan *forensik digital* dan di gunakan untuk pengujian penetrasi, yang dipelihara dan didanai oleh *Offensive Security*. *Kali* juga dikembangkan oleh *Offensive Security* sebagai penerus *BackTrack Linux*. *Kali* menyediakan pengguna dengan mudah akses terhadap koleksi yang besar dan komprehensif untuk alat yang berhubungan dengan keamanan, termasuk *port scanner* untuk *password cracker.*

2. *Backtrack*

Backtrack merupakan salah satu distro linux untuk penetrasi dan *audit* yang paling banyak digunakan saat ini di seluruh dunia. *Backtrack* awalnya adalah *Whoppix, IWHAX*, and *Auditor* kemudian di gabungkan menjadi satu *live linux* CD dimana terintegrasi lebih dari 300 *security tools* didalamnya. Tak Heran *Backtrack* 4 *pre release* di *download* lebih dari 4 juta. Versi terakhir *backtrack 5r3* di *release* bulan agustus 2013

3. *Samurai Web Testing Framework*

Distro *linux* ini memang di khususkan untuk *web testing*. Didalamnya terdapat banyak *open source tool* pilihan untuk *web testing*. Seperti dikutip di *official* webnya, *Web testing framework* menyediakan *tool-tool* untuk *web test* dalam 4 tahap.

Dimulai dengan tahap *reconnaissance,* distro ini menyediakan *tool* semacam *fierce domain scanner* dan *maltego*. Untuk *mapping* tersedia *tool* semacam *WebScarab* dan *ratproxy.* tahap *Discovery* bisa menggunakan tool *w3af* dan *burp*. Dan terakhir exploitasi tersedia tool *BeEF, AJAXShell* dan lainya. versi terakhirnya adalah *samurai-0.9.9.*

4. *NetSecL*

NetSecL adalah *distro linux* berbasis *OpenSuse* untuk penetrasi jaringan *Computer desktop* maupun *server*. Versi terakhir *NetsecL 3.2* dengan fitur XFCE memberikan performance yang handal, *compatibility* dengan *OpenSuse 11.4* dan *kernel 2.6.32.8*. Bagi anda yang biasa dengan lingkungan *OpenSuse NetSecl* bisa menjadi pilihan untuk melakukan *pentest system*.

5. *The Live Hacking* DVD

Live DVD *hacking* adalah distro *linux* baru dengan base *Ubuntu* yang berisi *tool-tool* untuk *ethical hacking*, *pentest,* dan *countermeasure*. Didalamnya terdapat *tool-tool* untuk DNS, *reconnaissance*, *foot-printing* (mengumpulkan informasi komputer target), *password cracking*, *network sniffing*, *spoofing* dan *wireless utilities*.

6. *SANS Investigate Forensic Toolkit (SIFT) Workstation*

Yang tertarik di dunia *Forensic* komputer. *International team of forensic expert Sans Faculty* telah membuat distro *linux* yang di khususnya untuk bidang ini. Distro *linux* ini telah di *release* ke *public* dan bisa digunakan oleh setiap orang yang tertarik untuk 'menangkap *intruder'*. *Toolkit* yang disediakan sudah sesuai dengan perkembangan *modern forensic tool.*

7. *Operator*

Satu lagi *Distro* turunan *Debian* untuk penestrasi jaringan. *Distro* yang mirip dengan *knoppix* yang *bootable* dari CD dan *running* di RAM ini dilengkapi juga dengan *forensic* dan *recovery tool*. *Operato*r berisi banyak *open source network security tool* untuk penetrasi *computer* dan server jaringan.

BAB III

METODELOGI PENELITIAN

3.1 Jadwal Penelitian

Penelitian ini dilaksanakan pada minggu pertama bulan Januari 2014 sampai dengan minggu keempat bulan juni 2014, mulai dari tahap pengumpulan data, menganalisa, merancang, membuat sistem, melakukan testing sampai tahap akhir yaitu melakukan dokumentasi pada setiap jadwal kegiatan yang telah di lakukan, agar pembuatan sistem ini nantinya dapat terstruktur dengan bagus. selengkapnya dapat dilihat seperti pada tabel jadwal penelitian berikut ini.

NO	KEGIATAN	Waktu Pelaksanaan					
		Januari	Februari	Maret	April	Mei	Juni
1	Pengumpulan Data						
2	Analisa Data						
3	Perancangan Sistem						
4	Pembuatan Program						
5	Test Program						
6	Evaluasi Program						
7	Perbaikan Program						
8	Implementasi Program						
9	Dokumentasi						

Tabel 3.1 Jadwal Penelitian

3.2 Lokasi Penelitian

Untuk membuat semua penelitian ini penulis melakukan penelitian di Kampus STMIK U'budiyah Indonesia, dan juga meliputi beberapa tempat yang

sering penulis datangi yaitu Laboratorium multimedia dan komputer STMIK U'budiyah Indonesia, Kelas jaringan komputer dan keamanan jaringan komputer, serta yang paling berperan penting adalah pustaka STMIK U'budiyah Indonesia, tempat dimana penulis mengambil beberapa referensi untuk membantu semua penelitian ini.

3.3 Alat dan Bahan Penelitian

Sesuai dengan judul yang penulis ambil yaitu tentang pengembangan sistem operasi *Linux* yang akan berjalan pada lingkungan keamanan jaringan, disini penulis melakukan beberapa percobaan sehingga diketahui spesifikasi minimum untuk menginstal sistem yang telah penulis buat, selain itu dalam pembuatan sistem ini penulis juga memakai satu unit komputer pribadi berikut rincian nya seperti di bawah ini.

Spesifikasi minimum komputer untuk menginstal *Distribusi Linux* keamanan jaringan yaitu :

1. *Prosesor* X86 : Pentium IV setara atau lebih baik.
2. *Harddisk* : 10 GB atau diatasnya.
3. *Memory* : 256 MB atau diatasnya.
4. VGA : VGA *graphics card* dengan resolusi 640x480 *pixels.*
5. *Media* Optik : CD-RW 1 Unit.

Pada Skripsi ini perangkat keras yang penulis gunakan antara lain :

1. *Mainboard* : *Inspiron* 1440.
2. *Prosesor* : *Intel Core*™2 Duo.

3. *Memory* : DDR I GB.
4. *Harddisk* : *Seagate Barracuda* ATA IV 320 *Gbytes.*
5. *Media* Optik : CD-RW DELL 48x24x52x IDE.
6. VGA *Cad* : *Mobile Intel*® 45 *Express Chipset Family*
7. *Sound Card* : *OnBoard.*
8. *Wireless* : *Broadcom* B43
9. *Monitor* : *Generic PnP Monitor*
10. *Mouse* : PS/2 *Logitech* 3 tombol.
11. *Keyboard* : PS/2 *generic.*
12. *Adaptor* : 100-240v
13. Speaker Aktif : 1 Unit

Adapun perangkat lunak utama dan pendukung yang diperlukan yang digunakan untuk membuat sistem ini adalah :

1. Sistem operasi induk yaitu *Distro Linux Mint Isadora* yang merupakan *distro* induk dalam pembuatan sistem operasi ini, nantinya sistem operasi *Linux Mint* ini akan di instal langsung kedalam komputer yang di gunakan untuk penelitian.
2. Menggunakan *kernel* **2.6.39** diharapkan mampu mendukung perangkat keras terbaru dan kinerja terbaik saat ini.
3. *Remastersys* adalah program pendukung untuk me-*remaster* ulang sistem *mint* menjadi sistem operasi yang baru menjadi sistem operasi yang dimaksud dalam penelitian ini yaitu sistem yang berfungsi untuk keamanan jaringan.
4. Lingkungan yang akan digunakan untuk pembuatan *distro Linux* ini meliputi sebagai berikut :

a. *X-Window System* merupakan tampilan grafis pada sistem operasi *Linux* yang akan membantu *kernel* menghubungkan sistem operasi dengan perangkat keras.
b. *Gnome Shell (Gnome Shel Desktop Environtment)* menggunakan versi 3.10. *Gnome Shell* adalah perkembangan dari *Gnome Panel* yang merupakan lingkungan *desktop* dan antarmuka grafik pengguna yang berjalan di atas sistem operasi. *GNOME Shell* secara keseluruhan terdiri dari perangkat lunak bebas dan gratis. *GNOME Shell* merupakan proyek internasional untuk menciptakan kerangka, aplikasi perangkat lunak untuk *desktop*, dan juga untuk mengatur peluncuran, penanganan *file* dan manajemen tugas jendela (*window*).
c. *Plymouth,* adalah tampilan *boot splash* pada saat memulai sistem operasi *Linux*, pada penelitian ini *Plymouth* ini akan penulis buat sendiri melalui konfigurasi *script* bahasa pemograman python.
d. Editor, dukungan terhadap teks *editor* minimal seperti *terminal* dan *gedit.*
e. *Internet,* beberapa paket dalam modus grafis yang digunakan untuk berinteraksi saat menggunakan internet seperti *Google Chrome* dan *Firefox.*
f. *Lingkungan keamanan komputer,* Lingkungan inilah yang menjadi *point* penting pada pengembangan *distribusi* ini nantiya, Lingkungan keamanan jaringan yang dimaksud merupakan rangkaian aplikasi untuk membantu mengamankan jaringan yang nantinya fasilitas tersebut sudah bisa dipakai dengan instan tanpa harus melakukan konfigurasi yang rumit lagi, contoh

aplikasinya seperti *nmap, ethercape, wireshark* dan masih banyak yang lainnya..

g. *Konfigurasi Server* seperti *mail server, windows file server, DNS name server, Network server* yang tak dapat dipisahkan yaitu layanan untuk bertukar informasi.
h. *Administrasi Tools,* layanan ini digunakan untuk administrasi dan konfigurasi seperti perangkat *wireless, print, keyboard*, bahasa, waktu atau juga suara.
i. *System Tools,* alat bantu untuk mempermudah penggunaan sistem.

3.4 Jenis Penelitian

Pada Penelitian ini penulis mengambil jenis penelitian yang berupa *Development Research* yang merupakan penelitian pengembangan yang mampu menghasilkan atau mengembangkan suatu produk, bahan media, alat atau strategi pembelajaran guna meningkatkan pembelajaran. Penelitian pengembangan bukan untuk menguji teori tetapi mengembangkan dan menguji keefektifitas model dalam hal ini berupa *Linux* yang akan dijadikan sebagai metode belajar baru khususnya di kampus STMIK U'budiyah Indonesia.

3.5 Pengamatan Penelitian

Dalam Penelitian ini juga penulis melakukan pengamatan dari berbagai aspek seperti bertanya, berkomunikasi atau langsung berpartisipasi dengan objek pengamatan, dan standar pengamatan dalam penelitian ini dapat disimpulkan sebagai berikut :

1. Melayani tujuan penelitian yang telah dirumuskan.
2. Direncanakan secara sistematik.
3. Dihubungkan dengan dalil-dalil yang lebih umum ketimbang dipaparkan semata-mata sebagai refleksi atas seperangkat rasa ingin tahu.
4. Dapat diuji kebenarannya (*validity*) dan keterandalannya (*reliability*).

BAB IV

PEMBAHASAN

4.1 Tahap Implementasi Umum

Linux keamanan jaringan dibangun diatas *Distro Linux Mint Isadora* dengan komputer berkecepatan *corei3 64-bit* dan RAM 2GB serta *harddisk* 350GB. Untuk membangun sistem ini ada beberapa konfigurasi yang diperlukan yaitu *development package* seperti *autoconf, automake, kernel header*, serta *remastersys*. Berikut tahap-tahap untuk membangun sistem ini dijelaskan lebih rinci seperti dibawah.

4.1.1 Mengenal *Linux Mint*

Bagi para pengguna komputer yang notabenenya adalah pemula, sistem operasi *Linux* masih menjadi sistem operasi "kelas dua" dan masih jarang digunakan. *Linux* adalah sistem operasi yang bersifat *free* (bebas) dan *open source* atau sering disebut dengan kode sumber terbuka. Sistem operasi besutan *Linus Torvalds* ini sudah terlanjur dicap sebagai sistem operasi yang sulit digunakan dan hanya cocok digunakan oleh seorang *power user.*

Tetapi hal semacam inilah yang coba ditepis oleh *Linux Mint*, salah satu *distro Linux* yang popularitasnya telah mengalahkan *Ubuntu Linux* di *chart distrowatch*. *Ubuntu Linux* sendiri turun popularitasnya sejak mengadopsi tampilan *desktop* yang disebut *"Unity"* sehingga banyak pengguna *Linux* yang beralih ke *Linux Mint (linuxmint.com, 2014)*

Linux Mint adalah salah satu sistem operasi *Linux* yang masih keturunan dari *Ubuntu. Linux Mint* mulai dikembangkan pada tahun 2006 berdasarkan

sistem operasi *Ubuntu Linux*. Salah satu ciri khas *Linux Mint* adalah selalu menggunakan nama wanita sebagai kode nama sebuah rilis, sebut saja *Linux Mint Gloria, Julia, Felicia, Isadora, Lisa* dan yang lainnya.

Kelebihan *Linux Mint* dibandingkan dengan Distro *Linux* lain adalah kemudahan penggunaan, bahkan oleh seorang pengguna komputer awam pun akan dengan mudah beradaptasi dengan *Linux Mint*. *Linux Mint* juga membawa fitur *Mint4Win* yang memungkinkan *Linux Mint* diinstal didalam *Windows* sebagai sebuah perangkat lunak biasa. Berbeda dengan *Ubuntu, Linux Mint* hadir dengan dukungan *playback file* multimedia dan *flash player*, hal ini tidak terdapat di *Ubuntu Linux*. *Distro Linux Mint* ini cocok bagi pengguna yang sekedar ingin mencoba sistem operasi *Linux* atau migrasi dari sistem operasi lain seperti *Windows.*

Dengan melihat kesederhanaan dari *Distro Linux mint* inilah penulis berinsiatif untuk melanjutkan arah pengembangan *distro* yang tadi hanya sederhana menjadi sebuah *distro* yang mampu mengimplementasikan berbagai bentuk serangan atau pertahanan serta memberikan kontribusi bermanfaat dalam lingkungan keamanan jaringan.

Dari sumber *page hit rangking* yang sangat populer yaitu situs ***distrowacth.com*** terhitung diakses pada 6 bulan terakhir, *Linux mint* menempati rangking urutan pertama seperti pada gambar 4.1 dibawah ini yang menunjukkan *Distro Linux Mint* yaitu distro yang mengusung slogan *"Linux Mint From Freedom came elegance,* sudah mencapai 4103 pemakai terdaftar yang melakukan *vote* pada situs tersebut.

Page Hit Ranking

Data span:

Last 6 months

Refresh

Rank	Distribution	H.P.D*
1	Mint	4103▼
2	Ubuntu	2202▼
3	Fedora	1688▲
4	Mageia	1424▲
5	Debian	1394▼
6	openSUSE	1373▼
7	Arch	1188▲
8	CentOS	1052▼
9	Puppy	909–

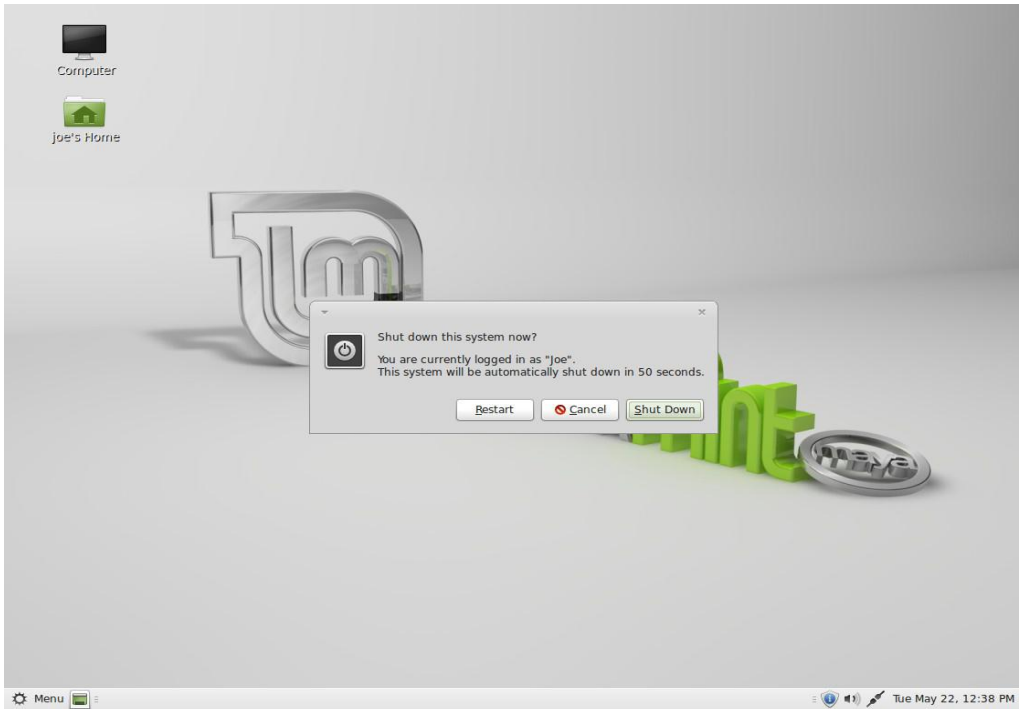
Gambar 4.1 Page Hit Rangking Linux disitus distrowacth.com

Gambar 4.2 Logo Linux Mint

4.1.2 Instalasi *Linux Mint*

Untuk melakukan instalasi *Linux Mint* ada beberapa perangkat yang harus disiapkan yaitu ISO *Linux* dan juga DVD/USB. Disini penulis men-*download* langsung ISO *Linux Mint* pada situs resmi yang telah disiapkan oleh *developer*-nya yaitu ***http://www.linuxmint.com/rel_isadora.php***. Disini penulis me-*ekstrak* ISO *Linux* kedalam USB untuk tahapan instalasi nya seperti dibawah ini.

1. Tempatkan USB ke dalam *port* dan hidupkan ulang komputer.
2. *Setting booting* komputer menggunakan USB melalui pengaturan *bios.*
3. Kemudian komputer membaca *file* ISO yang terdapat pada USB, dari layar pertama pilih pilihan *default "Start Linux Mint"* dan tekan *enter,* setelah beberapa saat *sistem live* telah siap dipakasi melaui *mode Live* CD.
4. Klik ganda pada *icon* "*Install Linux Mint*" yang terletak pada *desktop*, Selanjutnya pilih bahasa, disini penulis memilih bahasa inggris dan tekan klik *"Forward".*
5. Kemudian akan muncul konfigurasi waktu dan jenis *keyboard* serta pengaturan *user* tekan *forward* ikuti intruksinya dan tunggu beberapa saat sampai *Linux Mint* berhasil di instal kedalam komputer.
6. Setelah proses instalasi berhasil, komputer akan melakukan *reboot* untuk memastikan *Linux Mint* berhasil atau tidaknya dipasang, apabila berhasil langsung masuk ke *mode desktop,* sehingga terlihat *desktop Linux Mint* seperti gambar 4.3 dibawah ini.



Gambar 4.3 Desktop Linux Mint

4.1.3 Konfigurasi dan Persiapan Paket Instalasi

Repository adalah tempat penyimpanan arsip-arsip *file software*, dimana pengguna dapat mengambilnya untuk digunakan. Penggunanya adalah ketika *user* ingin menginstal satu *software* maka sistem akan mencari *software* tersebut pada *repository*, jika ketemu maka sistem akan langsung melakukan penginstalan secara otomatis, dan tentunya membutuhkan koneksi *internet* yang stabil.

Repository Linux diatur kedalam 4 area komponen, dan masing masing komponen memiliki fungsi untuk mengatur kestabilitas *repository*, berikut penjelasannya:

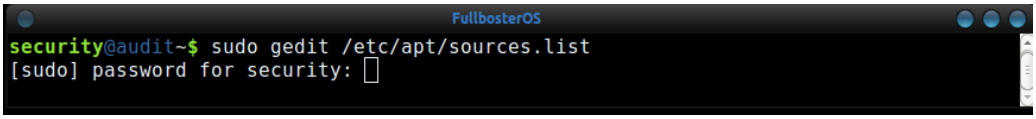
1. *Main*, adalah *software* yang didukung secara resmi.
2. *Restricted*, adalah *software* yang didukung tapi tidak sepenuhnya dalam *free license.*

3. *Universe*, adalah *software* yang dikelola oleh komunitas (bukan *software* yang didukung dengan resmi)
4. *Multiverse*, adalah *software* yang berbayar.

Sebelum mengubah sistem dan menambahkan serta mengurangi paket, ada beberapa hal yang harus di lakukan. Untuk melakukan penginstalan *software* penulis menggunakan *repository* yang didapatkan secara *online*, sebenarnya bisa juga menggunakan media DVD yang berisi *repository security network*, namun penulis lebih memilih menggunduh secara *online* karena *software* yang di terakan biasa nya lebih terbaru dibandingkan menggunakan *media offline* (DVD). Untuk memperlancar dan mempercepat proses pengunduhan penulis mengubah letak *repository* standar ke *repository* yang banyak digunakan untuk mengambil *software* keamanan jaringan.

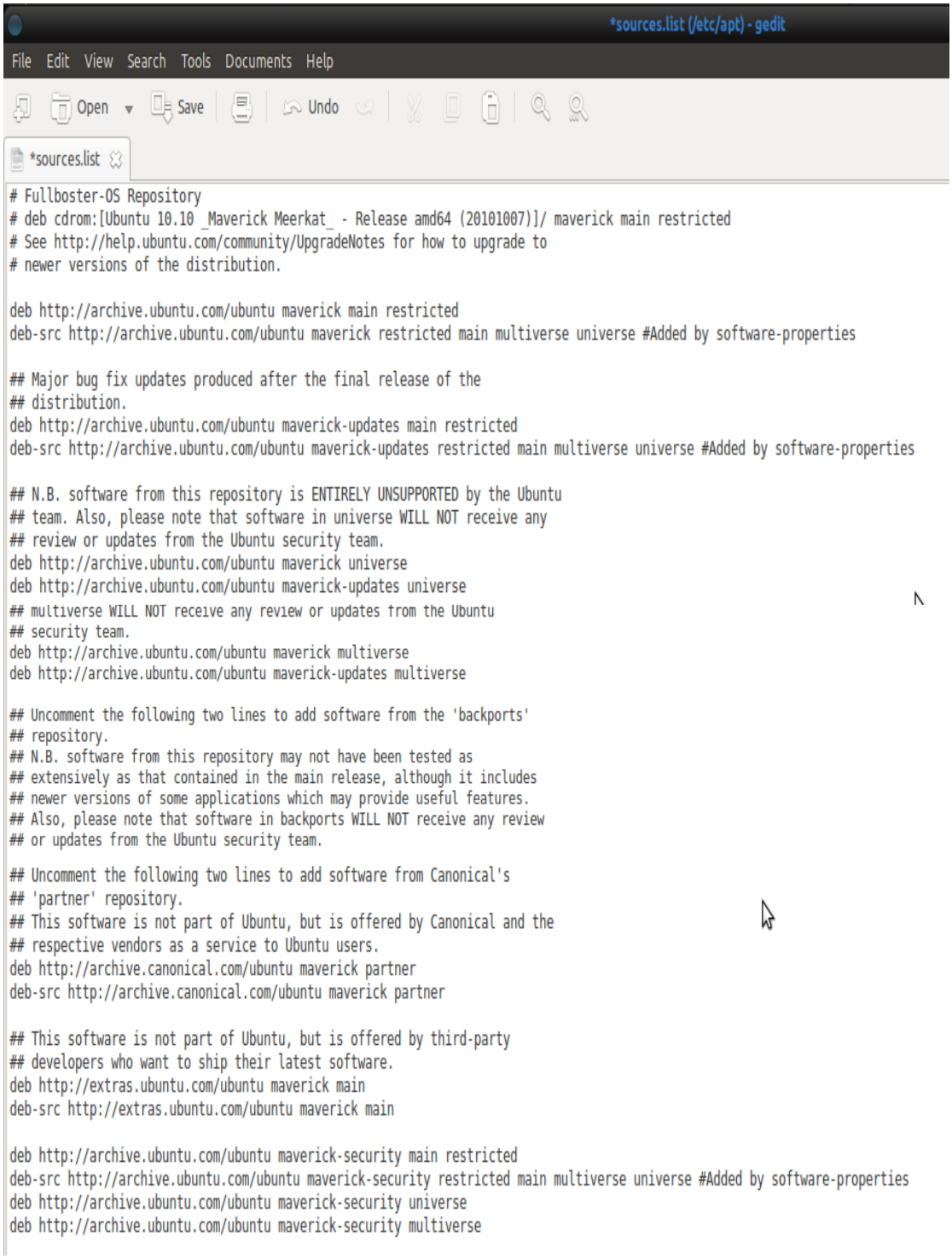
Di bawah ini adalah langkah-langkah yang penulis lakukan untuk merubah *repository* melalui *terminal* :

1. Menjalankan perintah dibawah ini pada terminal:



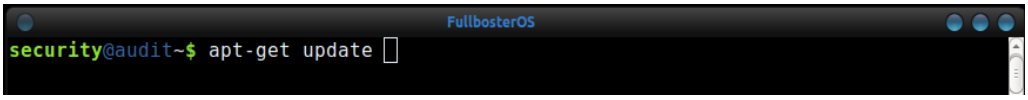
Gambar 4.4 Menggunakan Repository Online

2. Masukkan *password root*, kemudian hapus seluruh baris pada *file* tersebut dan mengganti dengan baris-baris pada server *repository* yang akan digunakan seperti terlihat pada gambar 4.5 berikut ini.



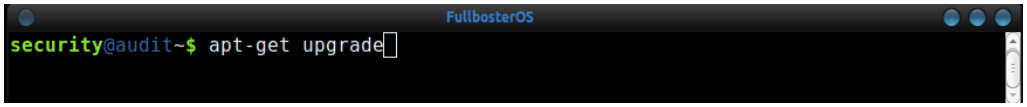
Gambar 4.5 Source Repository yang akan digunakan

3. Kemudian *update repository* sistem melalui *terminal*, dengan menjalankan perintah:



Gambar 4.6 Update Repository

4. Setelah selesai melakukan *update* melalui *repository*, kemudian masukkan perintah dibawah untuk meng-*upgrade* sistem yang sudah di-*update* dan tunggu sampai proses *upgrade* selesai.

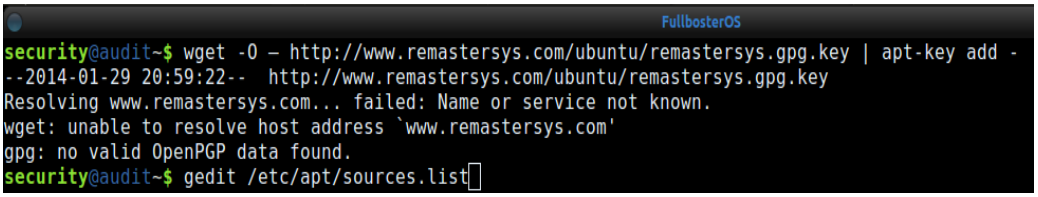


Gambar 4.7 Upgrade Repository

4.1.4 Instalasi Perangkat Lunak Pendukung Utama

Remastersys sebenarnya adalah *utilitas* yang digunakan untuk melakukan fungsi *back-up* sistem menjadi sebuah *Live*-CD/DVD. Aplikasi ini juga biasa digunakan oleh pengguna sistem operasi *Linux Mint* atau turunan *Debian* untuk membuat *Distro* sendiri sehingga sesuai dengan keinginannya atau bisa digunakan untuk dibagikan kepada orang lain yang koneksi *internet*-nya terbatas. Aplikasi ini secara *default* tidak terdapat pada paket *repository* resmi *Linux Mint.* Untuk itu sebelum menginstalnya terlebih dahulu harus menambahkan daftar *repository*. melalui *terminal* masukan perintah sebagai berikut :

1. ***$ sudo –s*** kemudian masukkan *password root* agar masuk kehalaman *super user*.
2. Kemudian masukkan perintah berikut untuk menyertakan *list repository remastersys* melalui *repository ubuntu.*



Gambar 4.8 Menambahkan Repository Remastersys

3. Tambahkan perintah ini pada baris paling bawah *repository* yang digunakan.

Gambar 4.9 Source Repository Remastersys

4. Setelah ditambahkan ke *source.list*, *save* dan *close* aplikasi editor *gedit* yang digunakan.
5. Langkah terakhir adalah men-*download* dan menginstal *remastersys* nya, berikut perintahnya :

Gambar 4.10 Update dan Install Repository

Tunggu proses instal *remastersys* di *Linux Mint* sampai selesai, jika sudah selesai aplikasi *remastersys* akan secara otomatis akan diletakkan pada panel aplikasi sistem.

Application > System Tools > Administration> Remastersys

4.2 File Konfigurasi *Global*

4.2.1 Konfigurasi *X-window*

Sistem *X-window* adalah penyedia grafik pada sistem atau aplikasi yang berjalan di atas *Linux*. Dari *statement* sederhana itu, kita dapat menyelidiki ke dalam pokok yang *kompleks. Linux* menyediakan banyak aneka pilihan *fleksibilitas* yang kita inginkan.

X-window dengan sistem API nya banyak menciptakan program grafis yang berjalan diatas *Linux*. Kita akan menemukan bagaimana cara menyusun dan menghubungkan, dengan dukungan API yang tersedia.

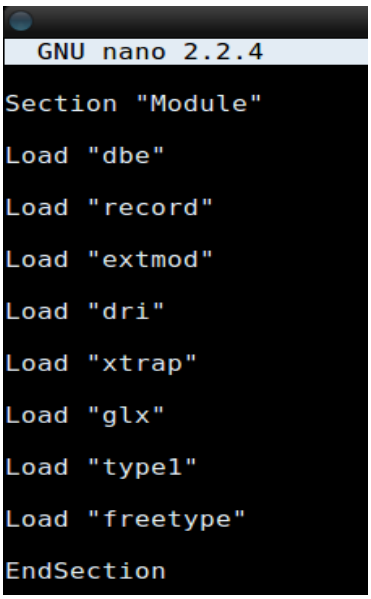
Sejak awal perkembangannya sistem (unix) operasi banyak mengalami revisi atau perbaruan karena unix tidak pernah mempunyai sistem grafik *(X-window)* yang distandarisasikan, sebagai contoh *Sun workstations* hanya berjalan di *Sunview*, *Hewlett-Packard workstations* juga hanya berjalan di *HPWindows*, hal ini tidak bisa luput dari penciptaan unix pertama kali, dimana unix pertama kali dikembangkan di *Bell Lab* dengan para *development* dari *Global Computer Network*, dan waktu itu unix hanya dikembangkan dilingkungan para akademik/team riset di bidang pendidikan saja.

Teknologi *X-window* memulai berkembang sebagai proyek yang didukung oleh berbagai penjual/*vendors unix*, seperti *IBM* dengan peralatan khususnya *digital*, yang mana mengarah pada menyediakan suatu sistem *X-window*, selain itu para *vendor unix* tersebut banyak yang memberikan *source* programnya *(Source Code)* untuk dikembangkan oleh komunitas lainnya, hal inilah yang menciptakan serta mendorong ke arah banyaknya implementasi hampir di tiap-tiap sistem mereka.

Konfigurasi utama *X-window* ada pada *file Xserver* yang terletak pada *direktory* ***/etc/X11/xorg.conf*** yang merupakan *file* konfigurasi utama untuk *X-window* sistem di *Linux.* *X-window* nantinya menjadi dasar untuk *Window-Manager* atau *desktop* serta aplikasi GUI yang berjalan diatasnya. Berikut ini adalah isi dari file konfigurasi beserta penjelasannya.

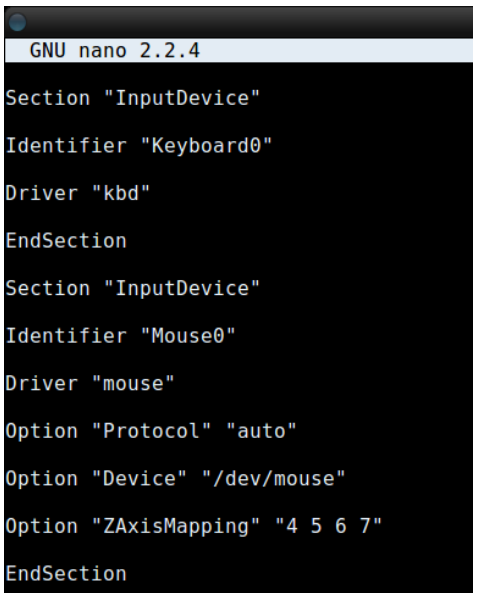
Gambar 4.11 Section file font dan module Xserver

Section file di atas digunakan untuk menentukan *file-file font* dan *file module* yang dibutuhkan oleh *Xserver.*



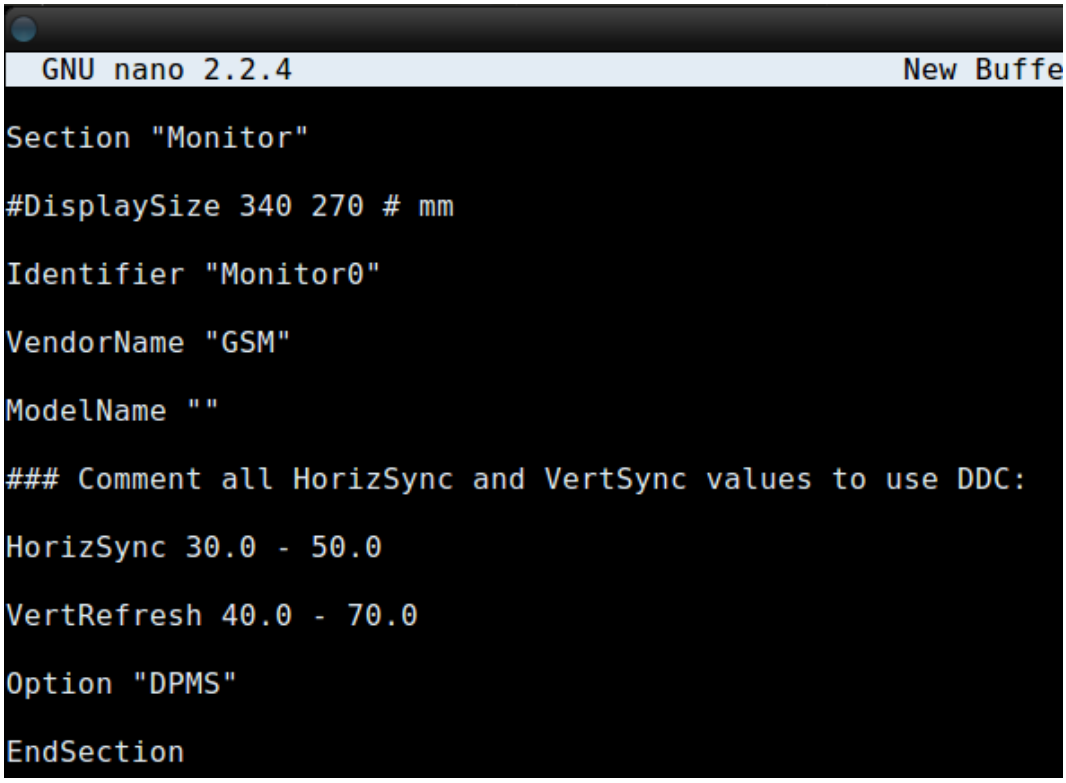
Gambar 4.12 Section Load pada Xserver

Section module menentukan *modul X-window* apa yang nantinya akan di *load* secara *default* saat *Xserver* di jalankan.



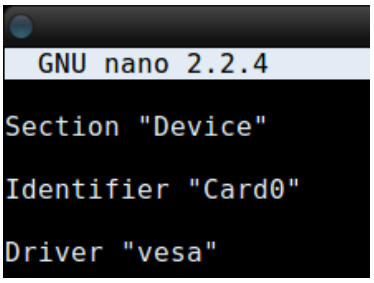
Gambar 4.13 Section file pengatur keyboard dan mouse

Section input device diatas untuk mengatur *keyboard* dan *mouse* yang ada di sistem. Karena sistem ini diharapkan akan bekerja di berbagai konfigurasi komputer yang berbeda maka protokol yang dipilih disini adalah *auto*.



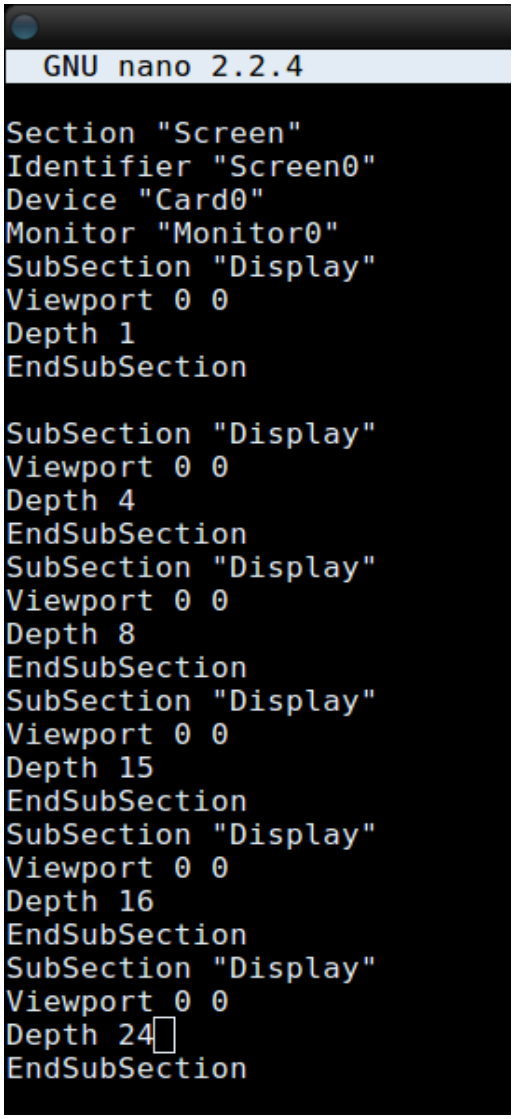
Gambar 4.14 Section monitor pada Xserver

Section monitor, bagian ini menentukan *horizontal sync* 30-50 dan *vertical refresh monitor* 40-70. Konfigurasi ini juga merupakan konfigurasi *default* dimana *monitor* pada umumnya berjalan normal pada konfigurasi diatas.



Gambar 4.15 Penggunaan Driver Generic pada Xserver

Menentukan jenis kartu grafis yang dipakai oleh sistem. Luasnya kartu grafis yang tersedia bisa membuat sistem tidak bisa dijalankan pada modus grafis. Oleh karena itu untuk VGA *card* pun menggunakan *driver generic* yaitu *vesa*.

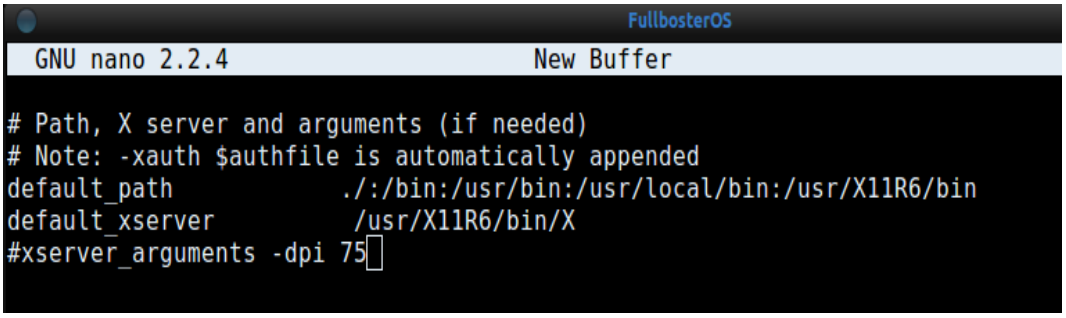


Gambar 4.16 Konfigurasi Resolusi dan kedalaman warna

Bagian ini menjelaskan konfigurasi resolusi dan kedalaman warna yang bisa ditampilkan. Kedalaman warna pada sistem ini *maximal* adalah 32 *bit*. Walaupun sebenarnya ada *monitor* yang mempunyai kemampuan diatas itu, namun konfigurasi disini dibatasi sampai kedalam 32 *bit* agar sistem ini cukup aman dipakai pada konfigurasi dan kemampuan *monitor* yang berbeda-beda.

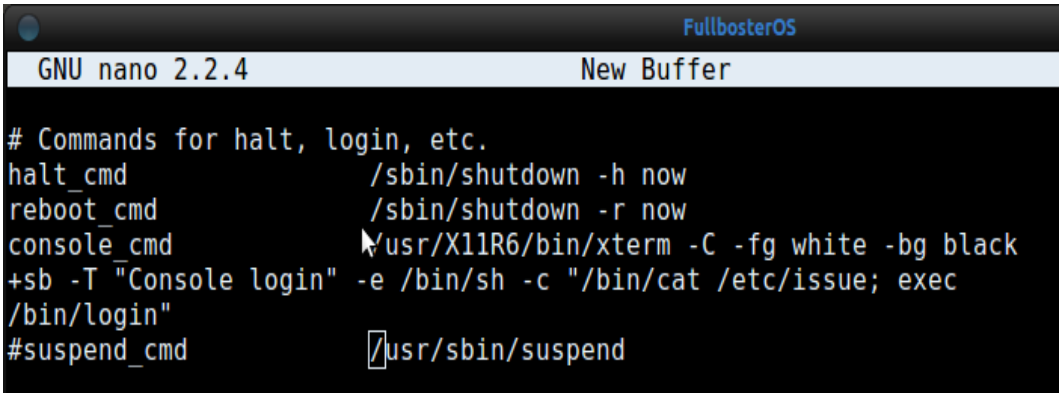
4.2.2 Konfigurasi *Login Manager* dan *Desktop*

Distro ini menggunakan GDM sebagai *login manager*-nya dan *nautilus* serta *gnome* sebagai *desktop*-nya. Berikut ada beberapa *File* konfigurasi yang digunakan oleh GDM *login manager*. Untuk memperpendek pembahasan sebagian besar komentar pada file ini dihilangkan.



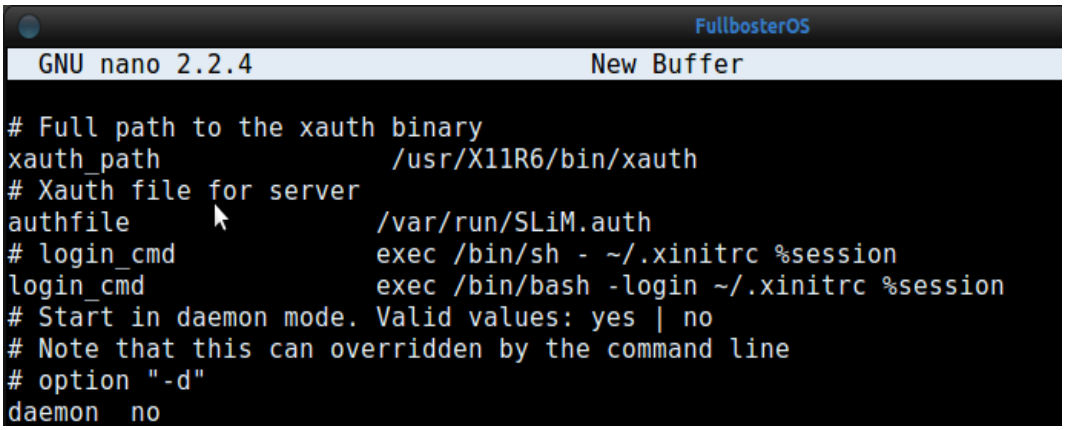
Gambar 4.17 Path Default Xserver

Perintah diatas menunjukkan letak *path default* untuk *Xserve*r dan *file-file* lain yang dibutuhkan saat menjalankan *mode GUI*.



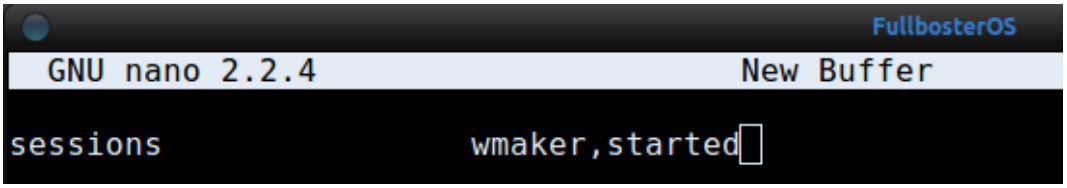
Gambar 4.18 Perintah Reboot dan Shutdown sistem

Pada gambar 4.18 diatas terdapat perintah yang akan digunakan untuk me-*reboot* dan men-*shutdown* sistem.



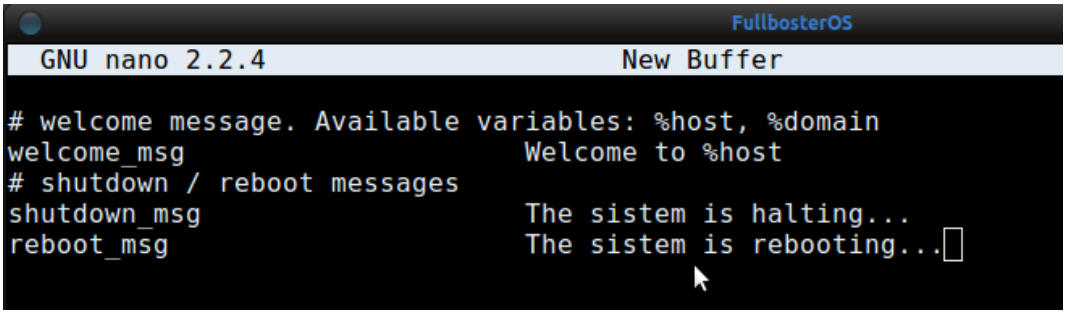
Gambar 4.19 Perintah GDM manager

Pada gambar diatas terdapat beberapa perintah yang menjalankan fungsi *GDM manager* dan sistem ini tidak dijalankan sebagai *deamon*, namun dijalankan sebagai aplikasi biasa.



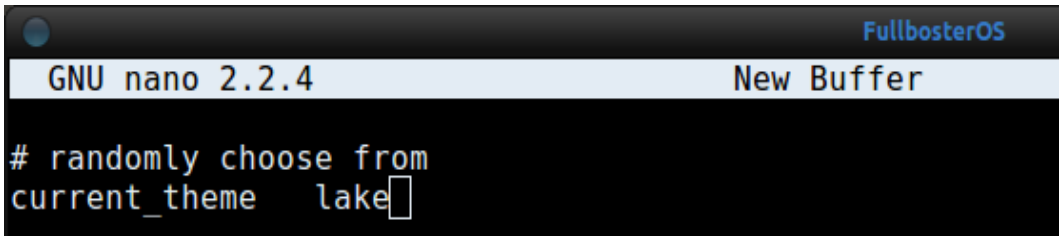
Gambar 4.20 wmaker, started fungsional

Fungsi dari perintah di atas adalah memfasilitasi sistem ini untuk menyediakan dua *window-manager* yang berbeda, yang pertama *nautilus* dan yang kedua adalah *gnome.*



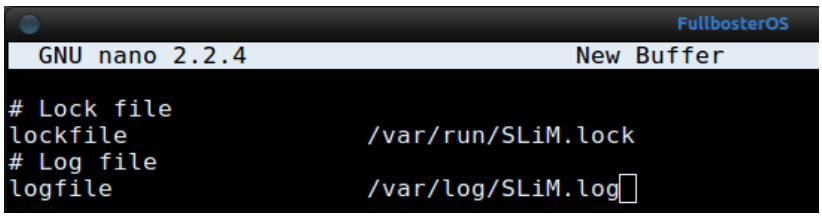
Gambar 4.21 Message sistem

Pesan pada gambar 4.21 adalah pesan yang nantinya muncul saat sistem di-*reboot* ataupun di-*shutdown*.



Gambar 4.22 Tema yang akan digunakan GDM

Konfigurasi diatas berfungsi untuk menerapkan tema pada GDM, dan *theme* GDM yang dipakai disini adalah l*ake.*



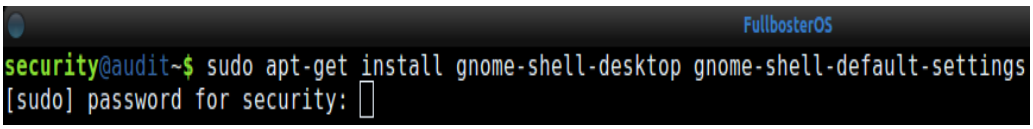
Gambar 4.23 Letak file lock dan log

Kode pada gambar 4.23 diatas menentukan letak dimana *file lock* dan *log* nantinya disimpan.

4.2.3 Pemasangan *Gnome-Shell*

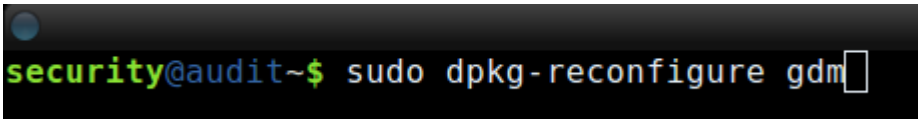
Gnome-Shell merupakan bentuk sederhana dari teknologi *Gnome3* yang sekarang banyak di pakai pada distriusi *Linux* seperti *Ubuntu, BlankOn, Fedora, Open Suse* dan lain-lain. Tetapi dalam pengembangan distribusi ini, penulis menetapkan *Gnome-Shell* sebagai bentuk antar muka dari sistem operasi ini, mulai dari bentuk GDM, *desktop*, tema sampai dengan *icon* aplikasinya. Berikut cara pemasangan *Gnome-Shell.*

1. Buka *terminal* kemudian masuk ke bentuk *super user*, dan ketikkan perintah:



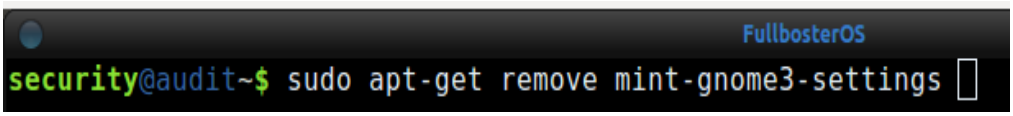
Gambar 4.24 Installasi gnome-shell

2. Kemudian setelah pemasangan di atas selesai, konfigurasi GDM dari *Gnome-Shell* yang sudah terinstal dengan mengetikkan perintah di bawah, tunggu hingga selesai.



Gambar 4.25 Konfigurasi ulang GDM

3. Setelah kedua tahap di atas selesai, sekarang saatnya menghapus *setting*-an *Gnome 3* yang terpasang di *Linux Mint* dengan mengetikkan perintah:

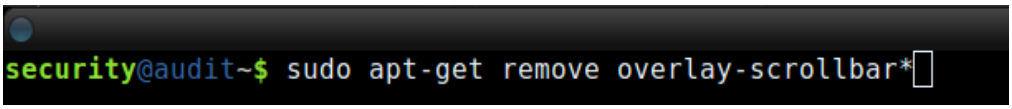


Gambar 4.26 Menghapus setting-an Gnome3

4. Dan kemudian melakukan penginstalan paket-paket yang tersedia pada *Gnome-Shell* dengan menjalankan perintah ini :

Gambar 4.27 Instalasi paket gnome-shell

Setelah proses ini berhasil, jalankan pula perintah di bawah agar *seting*-an awal *Gnome3* di *Linux Mint* terhapus dan menjadikan *Gnome-Shell* sebagai tampilan *default* pada distribusi *Linux* keamanan jaringan yang dibuat.



Gambar 4.28 Menghapus settingan gnome3 pada linux mint

5. Proses selesai dan kemudian *restart* komputer.

4.2.4 Instalasi Aplikasi Keamanan Jaringan

Pengembangan distribusi ini bertujuan sebagai *distro* yang mampu melakukan penetrasi terhadap jaringan komputer sebagai lingkungan utamanya. Oleh karena itu *distro* ini akan menyertakan kurang lebih 300 aplikasi keamanan jaringan yang harus dimanfaatkan sebaik mungkin oleh para pengguna, berikut beberapa lingkungan aplikasi yang penulis sertakan didalam distro ini.

4.2.4.1 Penetration Testing (Pentest)

Lingkungan ini adalah lingkungan utama yang disertakan yang bertujuan menjadi sistem *forensic* terhadap jaringan, baik itu untuk melakukan penetrasi, *troubleshooting, scanning port* jaringan dll, berikut ruang lingkup aplikasinya.

1. *Information Gathering*, lingkungan yang berisi *toolkits* pencari informasi akses jaringan komputer yang dipakai, baik itu jaringan yang dipakai oleh penyerang maupun yang lainnya, aplikasi yang akan disertakan adalah sebagai berikut.

No	*Information Gathering*	Keterangan
1	*All*	*All*
2	*Archive*	Aplikasi *backup* data
3	*DNS*	Aplikasi pencari DNS *server*
4	*Route*	Routing terhadap jaringan
5	*Search Enginer*	Mesin pencari
6	*SMTP*	Protokol *e-mail*
7	*SNMP*	Protokol jaringan

Tabel 4.1 Aplikasi Information Gathering

2. *Network Mapping* adalah teknik pemetaan jaringan yang menggunakan konektivitas fisik jaringan *internet,* betikut beberapa aplikasi yang akan di ikut sertakan.

No	***Network Mapping***	**Keterangan**
1	*All*	All
2	*Identify Live Host*	Pengidentifikasi *hosting* jaringan
3	*OS Fingerprinting*	Pengidentifikasi sidik jari
4	*Port Scanning*	Pencarian *port*
5	*Service Fingerprinting*	Perbaikan *port* sidik jari
6	*VPN*	Jaringan *private*

Tabel 4.2 Aplikasi Network Mapping

3. *Vulnerability Identification* bertujuan untuk mengetahui daftar rincian *vulnerability* (kelemahan) sistem IT *money* bank yang dapat di *eksploitasi.*

No	***Vulnerability Identification***	**Keterangan**
1	*All*	All
2	*Cisco*	Jaringan Cisco
3	*Database Analysis*	Analisa database
4	*Fuzzer*	Aplikasi web testing
5	*Open VAS4*	Open V4S4
6	*Web Analysis*	Aplikasi analisa web

Tabel 4.3 Aplikasi Vulnerability Identification

4. *Penetration* bertujuan untuk menentukan dan mengetahui serangan-serangan yang bisa terjadi terhadap kerentanan yang ada pada sistem, mengetahui dampak bisnis yang diakibatkan dari hasil *ekploitas*i yang dilakukan oleh penyerang.

No	***Penetration***	**Keterangan**
1	*BeEF*	Aplikasi penetrasi jaringan
2	*Exploitdb*	Penetrasi terhadap *database*
3	*Fast Track*	Penetrasi jaringan *peer to peer*
4	*Inguma*	Penetrasi sistem MacOS
5	*Metasploit*	Penetrasi kedalam komputer
6	*Origami*	Penetrasi *Origami*
7	*SAP Penetration Testing*	SAP *testing* aplikasi
8	*SET - Social Engineer*	Penetrasi dengan metode sosial
9	*Piranha*	Penetrasi ke server jaringan

Tabel 4.4 Aplikasi Penetration

5. *Privilege eskalasi* adalah tindakan meng-*eksploitasi bug*, desain yang rusak atau konfigurasi pengawasan dalam sebuah sistem operasi, berikut aplikasinya.

No	***Privilege Escalation***	**Keterangan**
1	*Offline Password Attack*	Penyerangan jaringan *offline*
2	*Online Password Attack*	Penyerangan jaringan *online*
3	*Sniffers*	Penyadapan data
4	*Spoofing*	Pemantau paket data

Tabel 4.5 Aplikasi Privilege Escalation

6. *Maintenance* adalah segala kegiatan yang bertujuan untuk menjaga peralatan dalam kondisi terbaik.

No	***Mantain Acces***	**Keterangan**
1	*Backdoor and Rootkits*	Pintu belakang sistem dan sistem robot
2	*Tunneling*	Pemantau tunneling sistem jaringan

Tabel 4.6 Aplikasi Mantain Access

7. *Radio Network Analysis* adalah penganalisa akses jaringan pada radio tentang kelemahan dan pencegahan.

No	***Radio Network Analysis***	**Keterangan**
1	*80211*	Penetrasi frekuensi radio
2	*Bluetooth*	Penetrasi perangkat bluetooth
3	*RFID*	Penetrasi perangkat infra red
4	*VOIP analysys*	Analisa jaringan VOIP

Tabel 4.7 Aplikasi Radio Network Analysis

8. *Digital Forensic* bertujuan mengidentifikasi, mengoleksi, menganalisa dan menguji bukti–bukti digital jaringan komputer, berikut aplikasi yang akan di sertakan untuk membantu proses *digital forensic.*

No	***Digital Forensic***	***Keterangan***
1	*All*	All
2	*Anti Forensic*	Pertahanan *forensic*
3	*File Carding*	Identifikasi teknik *carding*
4	*Forensic Analysis*	Analisa *forensik*
5	*Image Acquiring*	Pemecahan kode gambar
6	*Malware Analysis*	Analisa program jahat
7	*Network Forensic*	Jaringan *forensic*
8	*PDF Analysis*	Analisa PDF
9	*Steganography*	Pemecahan kode
10	*Hashing Tools*	Pemecahan *password*
11	*Digital Forensic Framework*	Pendukung *digital dorensic*

Tabel 4.8 Aplikasi Digital Forensik

9. *Security network,* Pada bagian ini merupakan kumpulan beberapa aplikasi *security network* lainnya.

No	***Secutiry network***	**Keterangan**
1	*Reverse Engineeing*	Pengumpulan data penetrasi
2	*Source Code Audit*	Pemecahan kode sumber
3	*Strees Testing*	Penetrasi tingkat lanjut
4	*Miscellaneous*	Trojan, virus dan worm

Tabel 4.9 Aplikasi lain keamanan jaringan

4.2.4.2 Service

Berikutnya adalah lingkungan *service*, lingkungan ini berfungsi mempersiapkan sebuah server lokal berupa *localhost* yang berisikan *database testing* untuk memperbaiki *bug* (kelemahan) pada sebuah sistem, dengan bantuan *service* bisa dengan mudah melakukan penelitian, baik itu untuk memecahkan *database*, *password* dan lain-lain, berikut beberapa aplikasi yang disertakan selain berguna untuk membantu pemecahan masalah keaman jaringan, beberapa aplikasinya seperti apache, myqsl dapat berfungsi juga dalam bahasa program.

No	***Service***	**Keterangan**
1	*Apache*	Aplikasi *Web Server*
2	*Mysql*	*Database Mysql*
3	*OpenV4S4*	*Audit database*
4	*PortgeSQL*	*Database PortgeSQL*
5	*PyFlag*	Server jaringan *forensik*
6	*SSH*	Protokol Jaringan
7	*TFTP*	File *Transfer Protocol*
8	*Xplico*	Protokol POP dan SMTP

Tabel 4.10 Paket aplikasi service

4.3 Konfigurasi *Module* Pada Sistem

Module adalah paket yang berhubungan langsung dengan fungsi *kernel*, yaitu melakukan pemanggilan terhadap perangkat keras, pemanggilan *kernel header*, pemanggilan fungsi instalasi dan lain-lain. Didalam sistem ini penulis menyertakan beberapa *module* yang penting dalam sebuah distribusi sehingga dengan inisiatif ini penulis bertujuan agar nantinya sistem dapat berjalan stabil pada perangkat keras yang mengalami masalah pada *module* yang bersifat *vendor* tertutup, berikut beberapa konfigurasi *module* yang akan disertakan.

4.3.1 Instalasi *Module Driver Wireless*

Beberapa perangkat lunak *wireless* yang dipasang pada komputer terkadang ada yang tidak mendukung sistem operasi *linux*, itu merupakan kendala terbesar bagi para pengguna *Linux* pada umumnya, karena sistem operasi *Linux* seakan mati tanpa ada nya koneksi. Untuk mengantisipasi hal tersebut, penulis memasangkan beberapa *module driver wireless* didalam distribusi ini, sehingga nantinya distribusi ini tidak bermasalah lagi dengan koneksi jaringan dengan *wireless*. Untuk melakukan pemasangan *module* di bawah ini penulis juga memerlukan perangkat jaringan LAN untuk meng-*update source* yang akan di tanamkan pada sistem. Berikut beberapa *module wireless* yang akan di pasang pada sistem operasi ini, mulai dari *Broadcom, Atheros, Realtek* dan Lain Lain.

1. Penginstalan paket *build-essential debhelper, module assistant, quilt* dan *wireless tool,* dengan mengetikkan perintah di bawah ini pada jendela terminal:

Gambar 4.29 Penginstalan paket module wireless

2. Setelah proses instalasi berhasil, kemudian *download source* paket *driver wireless* pada *repository debian linux.*

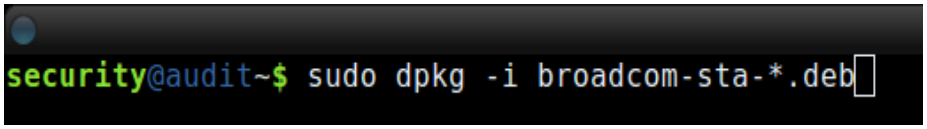
   a. Source Module Broadcom :

   Jalankan perintah di bawah ini pada terminal :

   1) *Download Source* paket dan *driver Broadcom*

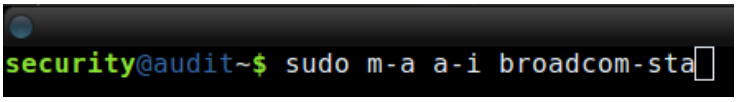
http://ftp.us.debian.org/debian/pool/non-free/b/broadcom-sta/broadcom-sta-source_5.60.48.36-2_all.deb
http://ftp.us.debian.org/debian/pool/non-free/b/broadcom-sta/broadcom-sta-common_5.60.48.36-2_all.deb

2) Instal paket *Broadcom* yang sudah di *download*



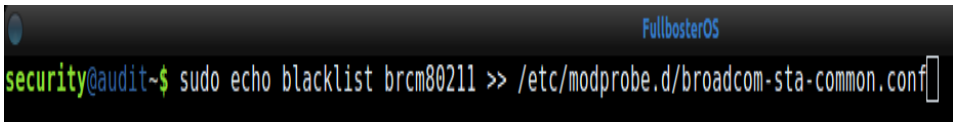
Gambar 4.30 Instalasi Broadcom

3) Instal *module-assistant driver Broadcom*



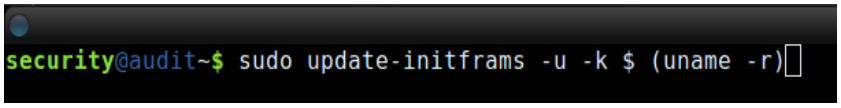
Gambar 4.31 Instal module driver

4) *Blacklist modul* brcm80211, hal ini untuk mencegah hal yg saling bertentangan untuk pendukung perangkat



Gambar 4.32 Blacklist module

5) *Rebuild initial ramdisk* pada sistem

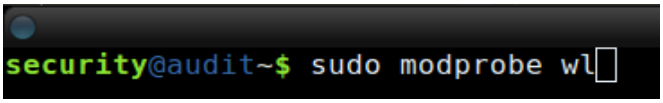


Gambar 4.33 Rebuid initial ramdisk

6) *Unload module-module* yang konflik

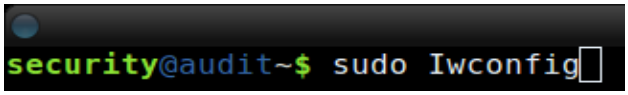
Gambar 4.34 Unload module

7) *Unload module* wl



Gambar 4.35 Unload module wl

8) Periksa ketersediaan interface, kemudian reboot.



Gambar 4.36 Pengecekan terakhir

b. Source Module Realtek dan Atheros

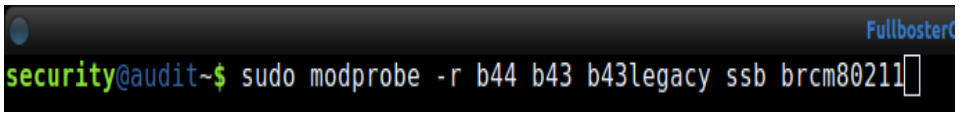
1) Tambahkan Perintah di bawah ini pada *source list* sistem.

```
# Debian Wheezy (testing)
deb http://ftp.us.debian.org/debian wheezy main contrib non-free
```

2) Buka *Terminal Update* dan *Install module Realtek* dan *Atheros*

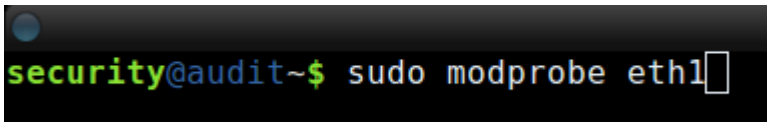
Gambar 4.37 Install Module

3) *Unload module modul* yang konflik



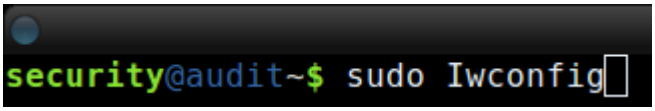
Gambar 4.38 Unload module konflik

4) *Load module* eth1



Gambar 4.39 Load module

5) Periksa ketersediaan *interface*



Gambar 4.40 Cek Interface wireless

3. Setelah semua *Module driver wireless* berhasil di instal kemudian segera lakukan *reboo*t pada komputer dan periksa kembali fungsi dari *driver wireless* yang telah di Instal.

4.3.2 Instalasi *Module Driver* VGA

Driver VGA sangat berpengaruh sekali pada proses jalannya sistem operasi, beberapa Distribusi *Linux* seperti *Ubuntu, BlankOn, Fedora, Debian, Slack* atau yang lainnya tidak menyertakan *Driver* VGA pada paket sistem operasinya, terkadang para pengguna *linux* sering sekali menginstal manual VGA milik komputernya yang sudah terpasang sistem *Linux.* Pada kasus ini, distribusi ini memberikan solusi pada saat pemakaian, yaitu nantinya para pengguna tidak perlu repot-repot lagi untuk memasang *driver* VGA nya, karena pada penelitian ini penulis menyertakan pemasangan *module driver* VGA komputer pada sistem operasi ini, dengan alasan kenyamanan saat pemakaian.

Berikut beberapa VGA yang sudah di pasangkan pada distribusi *Linux* keamanan jaringan seperti dibawah ini.

1. ATI Driver

a. Penulis men-*download source driver* ATI terlebih dahulu di situs resmi http://support.amd.com/us/gpudownload/linux/101/Pages/radeon_linux.aspx

b. Kemudian langsung melakukan pemasangan *source* program dengan mengetikkan perintah pada terminal : ***$ sudo update-pciids***

c. Kemudian setelah proses selesai lakukan penginstalan pada *source driver* ATI dengan mengetikkan perintah :

```
$ sudo chmod +x ati-driver-installer-10-1x86.x86
$ sudo sh ati-driver-installer-10-1x86.x86_64.run
```

d. Setelah proses di atas selesai maka *module driver* ini sudah berhasil terinstal kemudian tinggal mengaktifkan *driver* ATI agar jalan secara otomatis saat penginstalan sistem dengan mengetikkan perintah :

```
$ sudo jockey-text -e xorg:fglrx
```

2. Nvidia

Nvidia merupakan *driver* VGA yang sangat bermasalah dengan sistem operasi *Linux*, dengan banyaknya tipe *driver* ini yang tidak mendukung sistem operasi *open source* seperti *linux* membuat para pengguna komputer dengan VGA jenis Nvidia kalang kabut. Tetapi dengan sifat *open source* yang menanamkan sistem gotong royong pada pengembangan aplikasinya sekarang sudah bisa kita rasakan driver Nvidia yang secara mudah terinstal pada sistem *linux* tentunya semua ini dikembangkan oleh komunitas pengguna *linux*, namun tetap masih banyak juga distribusi *linux* yang tidak menyertakan jenis *driver* ini pada sistemnya. Disini penulis juga telah memasukkan *driver* Nvidia agar tetap dapat di nikmati oleh para pengguna nantinya tanpa harus menginstal secara manual lagi.

a. Pertama penulis men-*download source driver* Nvidia ini di situs yaitu http://www.nvidia.com/object/linux-display-ia32-295.33-driver.html.

b. Kemudian mamasukkan *repository* nvidia yang sudah di kembangkan oleh para pengguna *linux* dan kemudian *update.*

```
$ sudo apt-add-repository ppa:ubuntu-x-swat/x-updates
$ sudo apt-get update
```

c. Setelah proses *update* selesai, maka *driver* yang sudah di *download* tadi siap untuk di pasang dengan mengetikkan perintah :

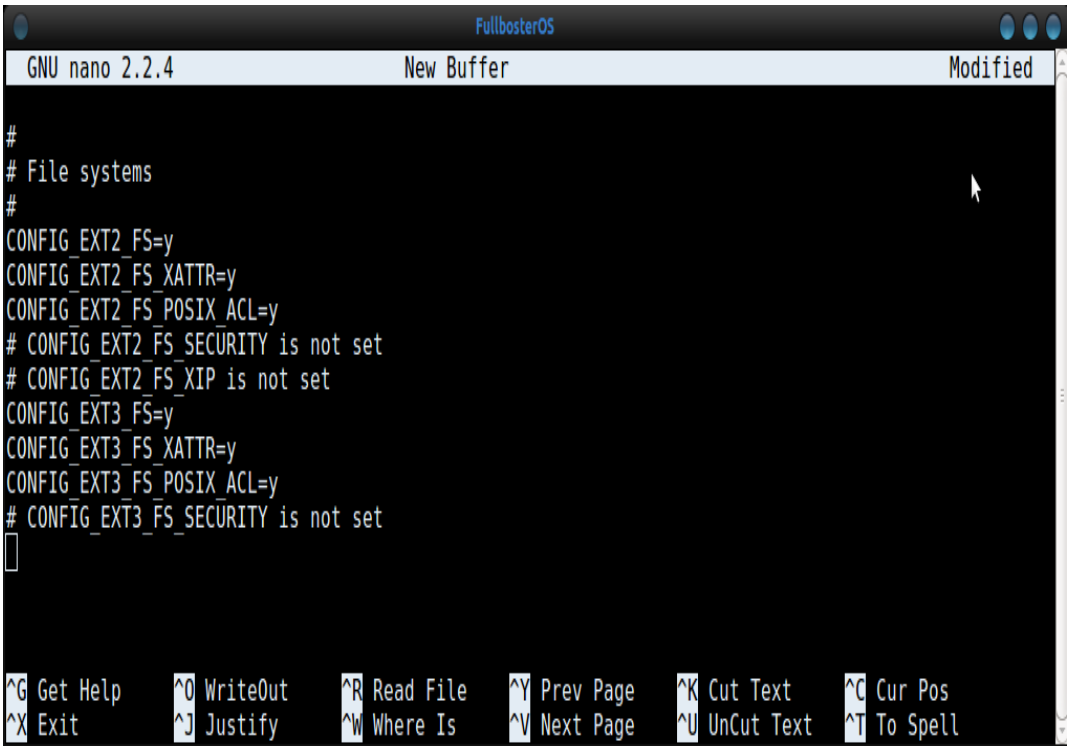
```
$ sudo apt-get install nvidia-current
```

Setelah semua pemasangan berhasil terinstal, maka sistem harus melakukan *reboot* dan *driver* VGA akan secara otomatis berjalan saat penginstalan sistem.

4.3.3 Konfigurasi dan *Upgrade Kernell*

Hal pertama yang akan dijelaskan dalam pembahasan ini adalah konfigurasi *kernel.* Konfigurasi ini menentukan *feature* yang nantinya akan ditanam di dalam *kernel*.

File yang dipakai untuk menyimpan konfigurasi bernama *.config* yang didalamnya berisi konfigurasi *kernel* dan menentukan apakah komponen dari *kernel* akan dikompilasi langsung kedalam *kernel*, dikompilasi sebagai *modul kernel* atau tidak diikut sertakan dalam kompilasi. Karena panjangnya *file* konfigurasi *kernel* ini, maka pembahasan disini hanya membahas hal-hal yang sekiranya bersesuaian dengan penelitian ini. Berikut ini adalah potongan *file .config* pada bagian konfigurasi *filesystem* yang nanti didukung *kernel.*



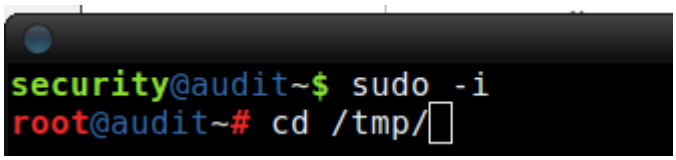
Gambar 4.41 Potongan Konfigurasi kernel

Potongan konfigurasi diatas digunakan untuk menentukan *filesystem* apa yang nantinya dimasukan ke dalam *kernel*. Jika didepan baris terdapat tanda pagar artinya *feature* atau dukungan untuk item tersebut tidak ikut disertakan. Sedangkan jika bertanda Y, artinya *feature* tersebut disertakan kedalam sistem dan jika bertanda M artinya *feature* tersebut akan dikompilasi sebagai *modul kernel*. Alasan sebagian dari *feature* tersebut dijadikan *modul kernel* bertujuan untuk mengurangi besarnya ukuran *kernel* itu sendiri.

Kernel yang di gunakan pada penelitian ini adalah *kernel* 2.6.39-3 Keunggulan *kernel* ini adalah mampu menyeimbangkan perangkat keras dan perangkat lunak khususnya perangkat lunak yang mendukung sistem jaringan. Disini penulis sudah men-*download kernel* versi stabil di situs resmi *Linux Kernel*

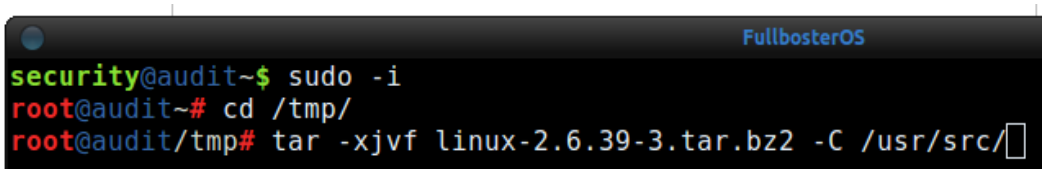
yaitu ***kernel.org*** dan agar lebih mudah penulis meletakkan *kernel* yang sudah di *download* pada *folder /tmp* sistem. Berikut langkah-langkah meng-*upgrade kernel* pada distribusi ini.

1. Buka *terminal* masukkan ke ***folder /tmp*** dengan mengetikkan perintah :



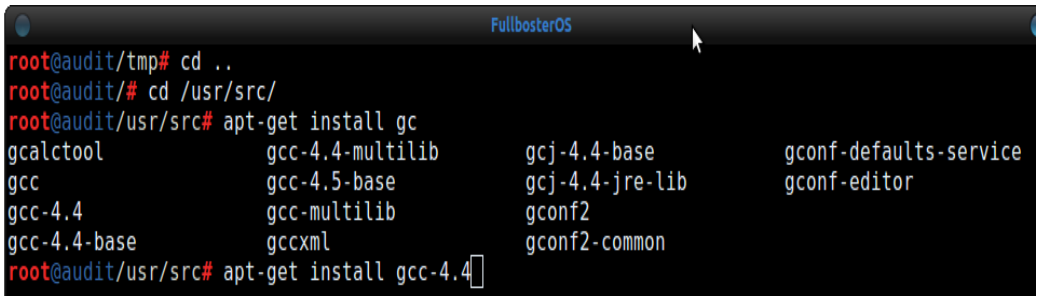
Gambar 4.42 Directory temporary

2. Kemudian *ekstak kernel* yang berada pada *folder /tmp* ke *direktori* ***/usr/src*** dengan mengetikkan perintah :



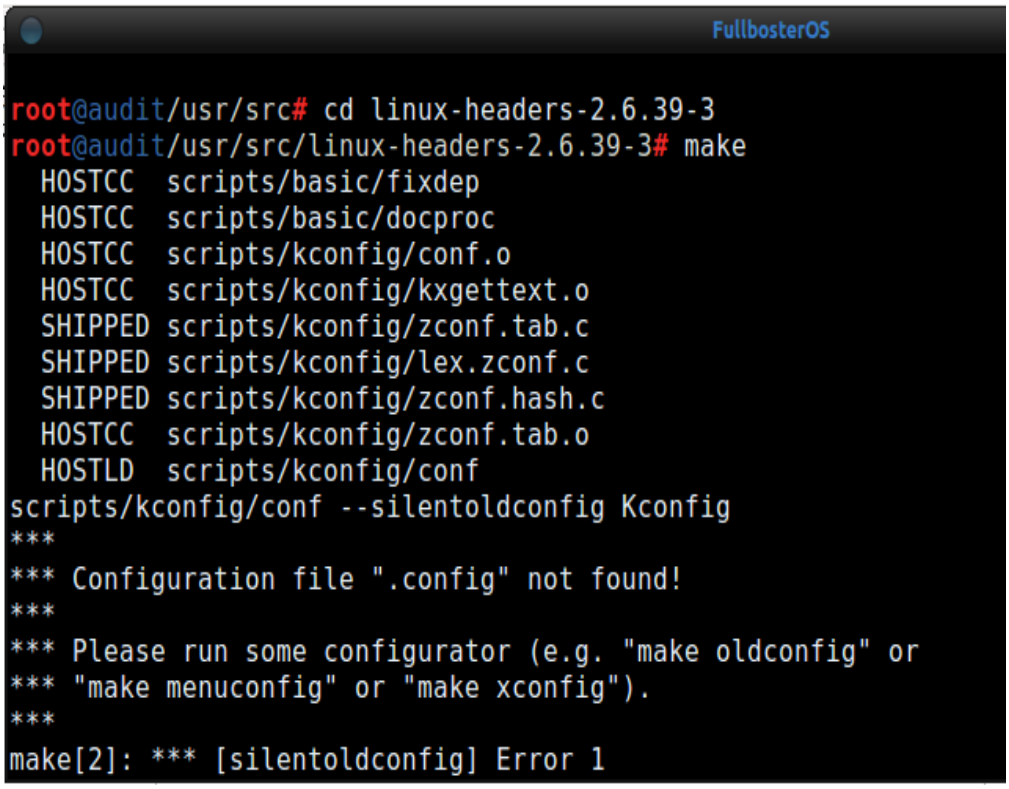
Gambar 4.43 me-ekstrak kernel

3. Setelah berhasil di *ekstak* masuk ke *folder /usr/src.* Kemudian instal paket *gcc* dengan mengetikkan perintah :



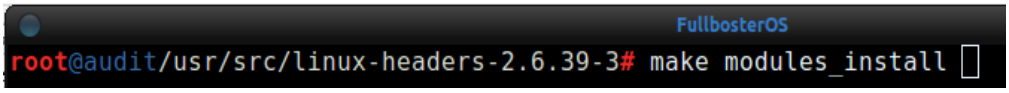
Gambar 4.44 Instalasi paket GCC

4. Masuk ke *directory linux*-2.6.39-3 kemudian *compile kernel*, ketikkan perintah :



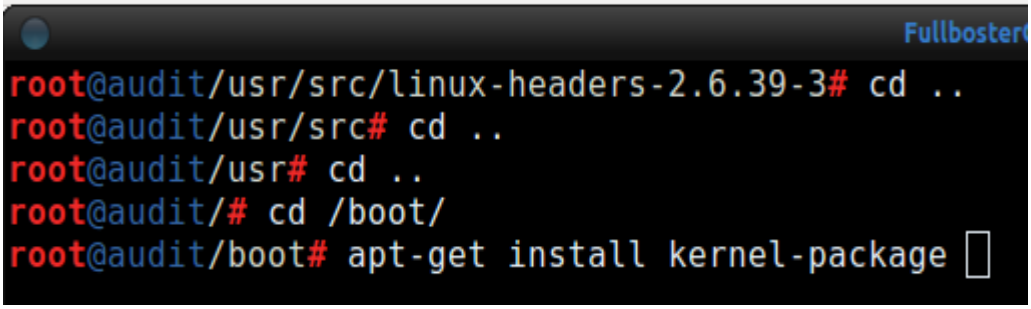
Gambar 4.45 Compile Kernel

5. Setelah berhasil kemudian jalankan perintah ini :



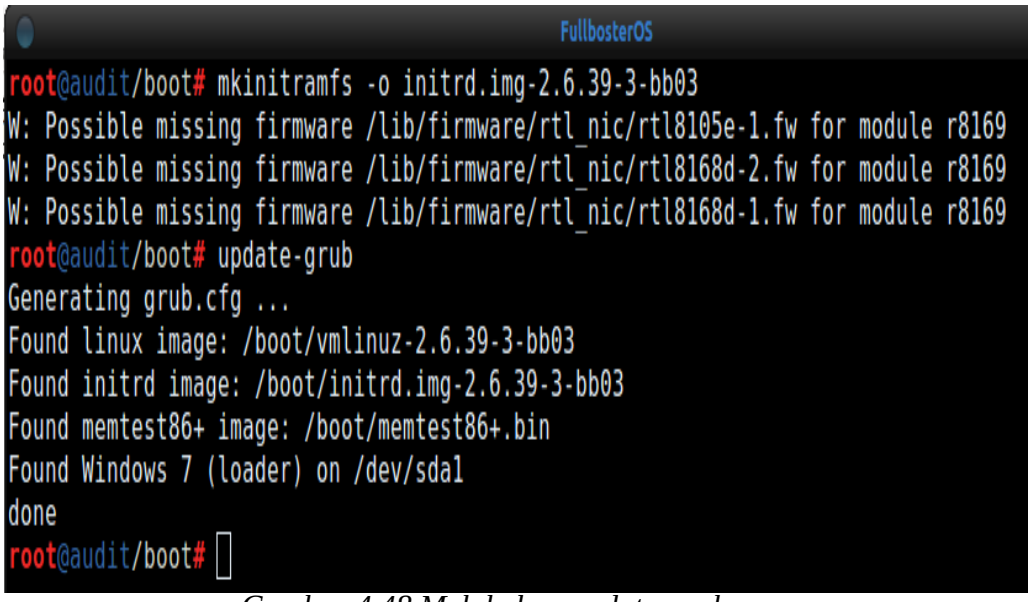
Gambar 4.46 Make module install

6. Jika berhasil maka pada *directory /boot* akan ada 3 *file* baru yaitu : *sistem.map 2.6.39-3, config-2.6.39-3, vmlinuz-2.6.39-3*



Gambar 4.47 Instalasi kernel-package

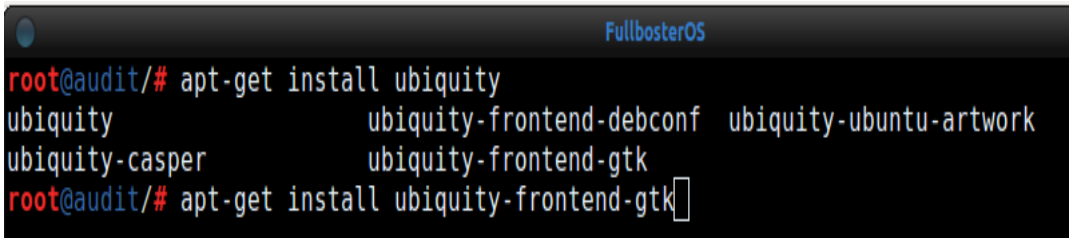
7. Kemudian setelah tahap di atas tinggal meng-*update grub* sistem kemudian *restart* komputer.



Gambar 4.48 Melakukan update-grub

4.3.4 Instalasi *Ubiquity*

Ubiquity adalah teknologi menu *installer* pada *Linux*, dengan memasangkan *ubiquity* ke dalam sistem, nantinya para pengguna tidak hanya menggunakan distribusi ini hanya sebagai *Live*-CD melainkan pengguna juga bisa menginstal langsung *Linux* keamanan jaringan ini ke dalam komputer, untuk dimaksimalkan fungsinya. Berikut perintah pada *terminal* saat memasang *ubiquity* dapat terlihat pada gambar 4.49.



Gambar 4.49 Instalasi Ubiquity

4.4 Persiapan Terakhir

Sebelum memulai proses *remaster*, hal yang paling penting dilakukan adalah memberikan *code name* kepada distribusi yang akan dibuat, disini penulis memberikan nama ***Fullboster-OS***, agar nantinya distro ini memiliki identitas pribadi sebelum betul-betul siap untuk dipakai oleh orang banyak. Untuk memberikan nama tersebut penulis melakukan pengeditan pada *file source* dibawah ini.

```
$ /etc/lsb_release
$ /etc/issue
$ /etc/issue.net

DISTRIB_ID=Fullboster-OS
DISTRIB_RELEASE=v.1
DISTRIB_CODENAME=Network Security Audit
DISTRIB_DESCRIPTION="Fullboster-OS"
```

Setalah melakukan penamaan identitas, pastikan untuk menghapus setiap *file temporary* yang tidak lagi diperlukan, untuk memperkecil ukuran *image* dan agar proses *load image* nantinya cepat. Berikut cara penulis lakukan untuk menghapus *file* sampah yang tidak diperlukan lagi oleh sistem.

```
$ sudo apt-get clean
$ sudo rm -rf /tmp/*
```

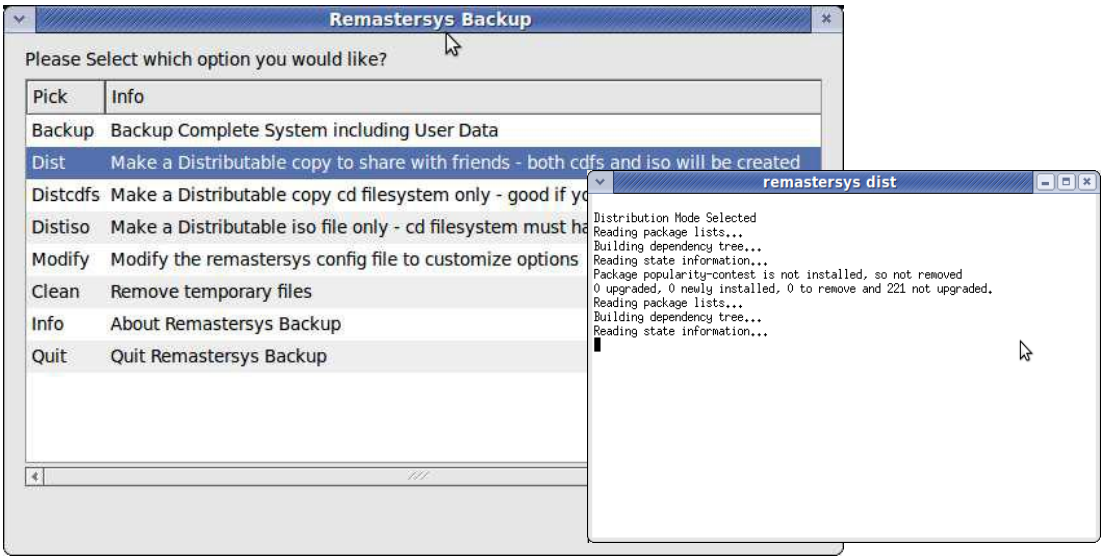
4.5 Menjalankan *Remastersys*

Remastersys dapat dioperasikan dengan dua cara yaitu *mode teks* menggunakan perintah *shell* maupun modus grafis melalui menu administrasi.

Untuk merubah nama *file* ISO yang akan kita buat menggunakan *remastersys* terlebih dahulu *edit file* konfigurasi *remastersys* selanjutnya setelah melakukan konfigurasi baru jalankan proses *remaster* dengan menjalankan perintah seperti dibawah ini melalui *terminal console.*

$ sudo gedit /etc/remastersys.conf
$ sudo remastersys dist

Disini penulis menjalankan aplikasi *remastersys* melalui *mode* GUI karena pada *mode* ini kita bisa memodifikasi nama ISO yang akan digunakan, letak penyimpanan, dan lainnya yang jauh lebih mudah dibandingkan melalui konfigurasi *terminal*. Dan aplikasi ini terletak pada ***System>Administration>Remastersys*** *Backup* pilih *opsi Dist* seperti pada gambar 4.50 dbawah ini.



Gambar 4.50 Proses Remastersys Distribusi Linux

Proses pembuatan *image* ini sendiri memakan waktu cukup lama, dan memakan ruang kosong yang besar. *Image* dari hasil proses ini secara *default* berada pada *folder* ***/home/remastersys***, ukuran *image* yang dihasilkan bervariasi tergantung berapa banyak paket yang kita instal ke sistem. *Format* dari *image* sendiri adalah ISO, yang dapat di *burn* menggunakan program seperti *Nero Burning Room* atau *Brasero* yaitu aplikasi *burner* yang juga di sertakan pada ***Distro Fullboster-OS*** yang mudah dalam pengoperasiannya. Proses ini akan memakan ruang *harddisk* yang sangat besar hingga jika kita selesai dan memburning *image* ke *disc* dapat menghapus *file image* dan *temporary* yang dibuat dengan mengetikan perintah dibawah ini pada *terminal.*

```
$ sudo remastersys clean
```

Jangan menjalankan perintah sebelum memindahkan *image* ISO distribusi *Linux* yang telah dibuat , karena perintah diatas akan menghapus semua hasil kerja dalam sistem yang telah dikerjakan tadi dengan remastersys.

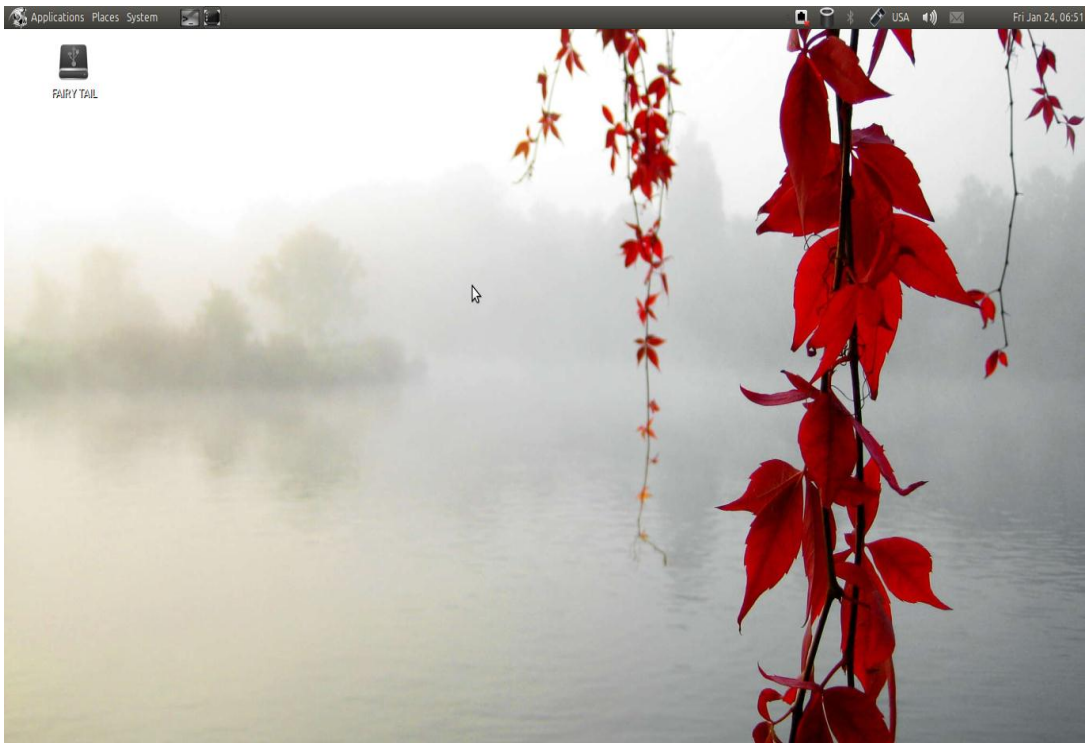
4.6 Pengujian Fullboster-OS

Sistem ini sudah diuji dibeberapa komputer, namun pengujian utama dilakukan di komputer pengembangan. Komputer pengembangan adalah komputer dimana sistem ini dibuat. Untuk menguji sistem ini, langkah-langkah yang dilakukan adalah:

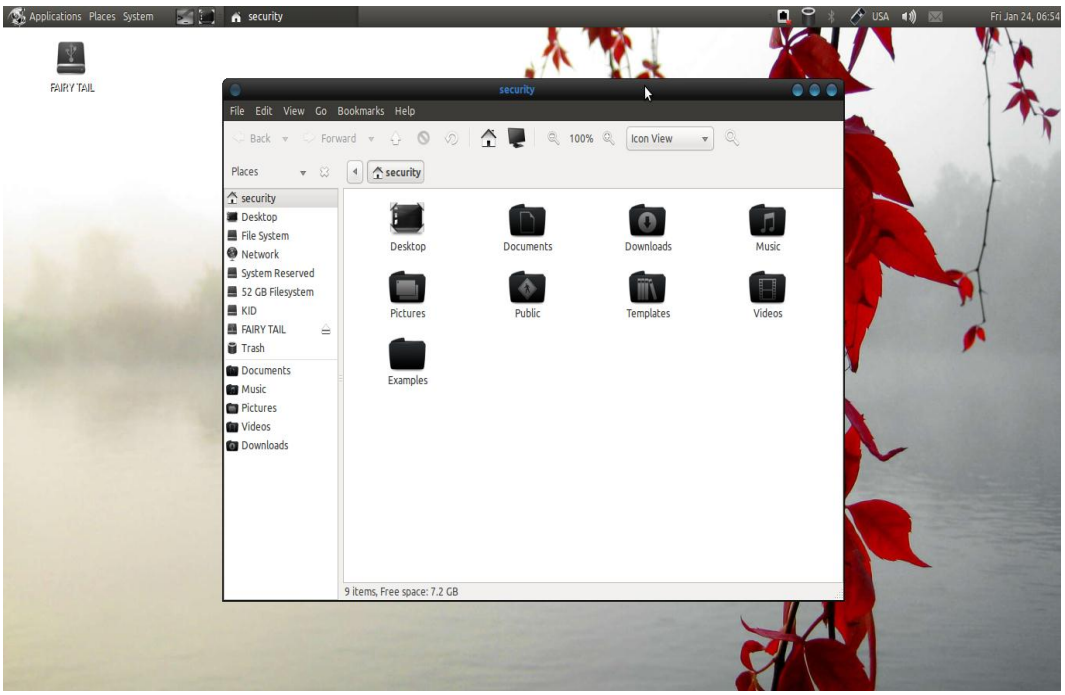
1. Men-*setting* komputer agar *boot* dari media CD-ROM
2. Setelah proses *booting* selesai, pengguna bisa langsung masuk ke dalam *live* CD.

3. Pada *Mode Live* CD ada dua *opsi* yang bisa di manfaatkan oleh pengguna nantinya, yaitu yang pertama pengguna bisa langsung menggunakan *distro* dalam bentuk *Live* CD tanpa harus menginstal nya ke dalam komputer dan yang kedua adalah bentuk *installer* sehingga pengguna bisa memanfaatkan *ubiquity* pada sistem untuk menginstal sistem operasi ***Fullboster-OS*** langsung ke dalam komputer.

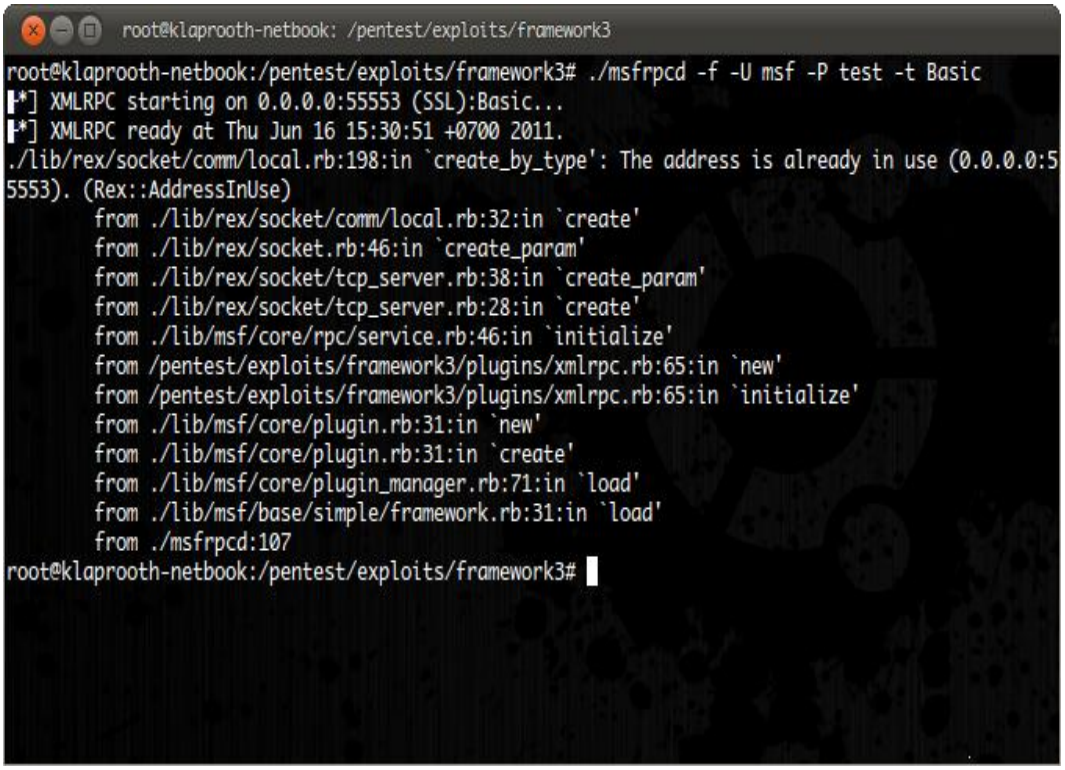
Berikut tampilan ***Linux Fullboster-OS*** yang telah dibuat menjadi sistem operasi *linux* baru :



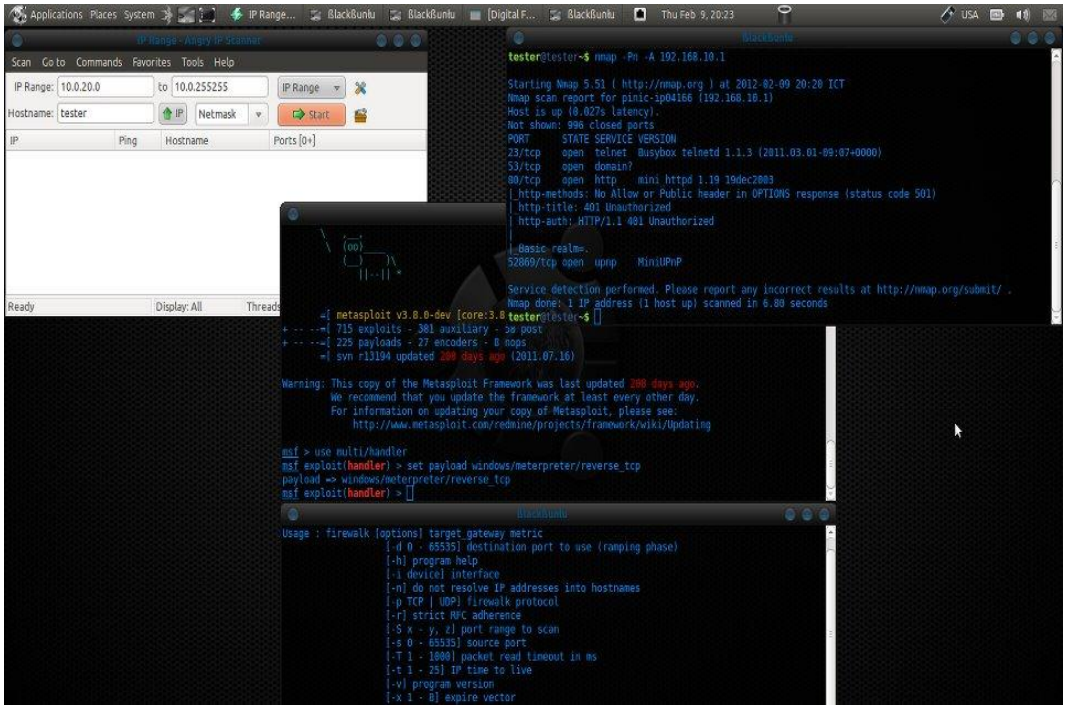
Gambar 4.51 Desktop Fullboster-OS



Gambar 4.52 Nautilus Fullboster-OS



Gambar 4.53 Armitage saat dijalankan pada Fullboster-OS



Gambar 4.54 Melakukan penetrasi dengan metasploit

4.7 Kendala Pada Sistem

Pada penelitian ini, banyak sudah tahapan-tahapan yang dijelaskan untuk merancang sistem *linux*, mulai dari pemilihan distro, instalasi paket pendukung utama, meng-*compile kernel* dan yang terakhir adalah tahap pengujian sistem. Sistem ini penulis kembangkan dengan sebaik mungkin dengan merujuk pada sistem terdahulunya agar nyaman digunakan baik itu aplikasinya maupun kestabilannya yang sudah diuji pada berbagai perangkat keras dan terbukti berhasil. Tetapi ada beberapa kendala yang penulis simpulkan pada tahap penggunaannya, yaitu pada tahap instalasi, mungkin sistem ini tidak terlalu masalah bagi pengguna yang sudah familiar menggunakan *Linux*, namun akan menjadi masalah besar bagi para pengguna awal yang akan melakukan instalasi tanpa membaca dan mempelajari sistem *linux*, resiko yang bisa diambil yaitu ter-

format-nya *harddisk*, hilangnya *grub menu* dan lain-lain. Berikut kendala yang berhasil penulis simpulkan.

1. Ukuran ISO masih terlalu besar yaitu 3.7 *GygaBytes*, untuk melakukan instalasi yang optimal pengguna harus menggunakan DVD-RW dengan kapasitas 4GB, dan penulis merekomendasikan pada pengguna untuk melakukan instalasi melalui USB yang berukuran 8GB atau lebih dengan bantuan aplikasi *Unetbootin* untuk meng-*ekstak* ISO kedalam USB, agar proses instalasi jauh lebih baik dari pada harus memakai media yang berukuran hampir sama dengan ISO *File*.
2. Sistem *Linux* berbeda dengan *Windows, Linux* menggunakan sistem yang ber-*ekstensi* EXT4 sedangkan *windows* menggunakan NTFS. Pada saat melakukan instalasi ***Fullboster-OS*** terdapat pemilihan partisi sistem. Disini ada 3 pilihan , yang pertama menginstal sistem pada partisi secara acak, kedua menginstal sistem pada partisi kedua komputer, dan yang ketiga menginstal sistem dengan melakukan partisi secara *manual*. Penulis merekomendasikan untuk menginstal *Linux* dengan memilih opsi pilihan ketiga, yaitu secara manual, karena dengan memilih opsi ini pengguna bisa dengan bebas menginstal pada partisi yang disukai, tetapi apa bila memilih pilihan satu dan dua akan memiliki resiko yang sangat tinggi apabila tidak membaca perintah instruksi dengan baik, resikonya adalah *grub menu* akan hilang, partisi ter-*format* dan data akan hilang.

3. Pada saat melakukan instalasi harap menginstal sistem dengan mengikuti petunjuk yang sudah diterakan agar sistem dapat berjalan dengan baik dan mengurangi resiko yang akan terjadi.

BAB V

PENUTUP

5.1 Kesimpulan

Fullboster-OS adalah distribusi *Linux* yang bisa dipakai untuk mengenalkan *Linux* dan keamanan jaringan pada lingkungan yang *free*, baik itu untuk melakukan penetrasi terhadap jaringan, ataupun melindungi dengan melakukan *eksploitasi.*

1. Distribusi ini dipakai untuk mengenalkan bagaimana menjadi seorang pentester yang mempunyai *etical hacking* sehingga selain memahami pemograman, seorang *pentester* harus mempelajari dengan baik bagaimana hubungan dunia keamanan komputer terhadap jaringan dan komputer. Contoh aplikasi yang dapat dimanfaatkan nantinya adalah *etherap, ethercape, wireshark, nmap, armitage, metasploi, exploitdb*, dan masih banyak lagi yang lainnya.
2. Distribusi ini menggunakan *desktop* dan aplikasi yang ringan, diharapkan dengan lahirnya sistem ini dapat membantu teman-teman mahasiswa/mahasiswi yang ingin belajar tetapi mempunyai komputer dengan spesifikasi rendah.

5.2 Saran

Distro ini bukanlah sistem yang sempurna, masih banyak kekurangan, yang untuk kedepannya harus terus diperbaiki dan disempurnakan. Berikut ini adalah daftar saran yang akan menjadi arahan untuk pengembangan selanjutnya .

1. Menambahkan paket Java EE dan Java ME, jika lisensinya memungkinkan, sehingga mampu untuk digunakan dalam penetrasi terhadap aplikasi mobile.
2. Membuat tool administrasi sistem yang terintegrasi untuk memudahkan pengaturan sistem secara keseluruhan.
3. Implementasi manajemen paket. saat ini sistem mengadopsi manajemen paket deb. Di harapkan sistem ini nantinya mempunyai manajemen paket sendiri didalamnya.
4. Menambahkan Repository Lokal dengan bekerja sama dengan pihak kampus yang berupa 1 buah server untuk menyimpan aplikasi yang diinginkan sebagai arsip perangkat lunak open source yang akan dikembangkan.
5. Perluasan dukungan hardware. Saat ini belum mendukung media seperti printer, scanner dan beberapa hardware jenis lain secara otomatis, hanya menambahkan paket ke dalam distribusi sehingga diharapkan kedepannya distro ini bisa mendeteksi hardware yang saat ini belum dikenali.

DAFTAR PUSTAKA

Ardiansyah, Dian. 2003. *Teknologi jaringan komputer*. Media Kita. Jakarta

Darmaputra, Yansen. 2005. *Sistem Operasi Modern*. Penerbit Andi. Yogyakarta.

Dipanegara, Arya. 2010. *Social Networking Hacked*. HP Cyber Community. Jakarta

Hariyanto, Bambang 2007. *Sistem Operasi Edisi 3*. Penerbit Informatika. Bandung.

J. Rosenberg. 2002. *Session Initiation Protocol.* Network Working. Bandung

Prihanti, Harry. 2003. *Membangun jaringan komputer*. Rahmad. Bandung

Purbo, Onno W, 1992. *Jaringan Komputer Menggunakan Protokol TCP/IP*. Bina Aksara. Jakarta

Tanembaum, Andrews. 1996. *Computer Network*. Andi. Yoyakarta

Yuhefizar, 2003. *Tutuorial Komputer dan Jaringan*. Bina Aksara. Jakarta

BIODATA PESERTA

A. IDENTITAS PRIBADI

Nama	: Milzam A
NIM	: 09111024
Tempat/Tgl Lahir	: Kuala Simpang, 5 Desenber 1991

B. KETERANGAN STUDI

Program Studi	: Teknik Informatika
Tahun Masuk	: 2009
Asal SLTA dan Tahun Ijazah SLTA	: SMA Negeri 6 Banda Aceh / 2009

C. STATUS MAHASISWA

Jumlah Saudara Kandung	: 1
Bekerja	: Mahasiswa
Kawin	: -
Kalau Sudah Kawin	: -
Biaya Pendidikan	: 1.300.000

D. LAIN – LAIN

Nama Ayah	: Azwanda MS
Nama Ibu	: Herlina
Agama	: Islam
Alamat/Tempat Tanggal Lahir	: Ketapang, 8 Agustus 1969

E. AKHIR STUDI

Tanggal Lulus/Yudisium	: 29 Maret 2013
Judul KTI/Skripsi	: PENGEMBANGAN SISTEM OPERASI LINUX UNTUK KEAMANAN JARINGAN

Banda Aceh, 11 Maret 2014

Mahasiswa Ybs,

(**Milzam A**)