INNOVATIVE: Journal Of Social Science Research
Volume 3 Nomor 2 Tahun 2023 Page 721-736
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Implementasi Sistem Keamanan Komputer Host Menggunakan Sistem Operasi Fedora Linux

Samsoni[1], Aprilia Handayani[2*], Elsa Apriliani[3], Zaman Padrisi[4], Rama Albin Sugiartha[5], Muhamad Arsyil Adzhim[6], Fariz Muhammad[7], Titis Wicaksono[8], Fajar Anggi Saputro[9], Fernosha Al Faridzi[10]
Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Tangerang, Indonesia
Email:dosen02719@ynpam.ac.id[2*]

Abstrak

Dewasa ini, perkembangan teknologi dan informasi semakin pesat tentunya akan memberikan banyak keuntungan bagi kehidupan manusia. Meski begitu, aspek negatifnya juga banyak, seperti kejahatan komputer atau penyerangan berupa penyadapan data di jaringan komputer oleh pihak yang tidak bertanggung jawab. Keamanan komputer berhubungan dengan pencegahan diri terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer dengan memberikan batasan akses orang lain yang dapat menggangu sistem. Salah satu dalam mengimplementasikan keamanan komputer yaitu dengan menggunakan sistem operasi Fedora Linux. Tujuan penelitian ini adalah untuk meminimalisir ancaman yang dapat merugikan pengguna komputer serta. Metodologi penelitian ini menggunakan metode *Network Development Life Cycle* (NDLC) dimulai dengan Analisis, *Design*, Simulasi *Prototype*, Implementasi, *Monitoring* dan *Management*. Hasil yang dicapai penelitian ini adalah mengimplementasikan keamanan komputer host dengan Fedora Linux serta menghasilkan pemahaman kepada masyarakat awam bahwa keamanan komputer merupakan hal penting dalam penggunaan komputer. Simpulan pada penelitian ini adalah keamanan komputer merupakan hal yang wajib diketahui oleh semua orang yang beraktifitas menggunakan komputer, dengan berpatokan pada aspek keamanan komputer yaitu *confidentiality, Integrity dan availability* (CIA) maka ancaman yang bisa terjadi pada komputer menggunakan OS Linux Fedora dapat di minimalisir.

Kata Kunci: *Implementasi, Keamanan Komputer, Fedora Linux.*

Abstract

*Today, the rapid de*velopment of technology and information will certainly provide many advantages for human life. Even so, there are also many negative aspects, such as computer crime or attacks in the form of tapping data on computer networks by irresponsible parties. Computer security relates to self-prevention against unrecognized intruders in a computer system by providing access restrictions for other people who can interfere with the system. One way to implement computer security is to use the Fedora Linux operating system. The purpose of this research is to minimize threats that can harm computer users as well. The research methodology uses the Network Development Life Cycle (NDLC) method starting with Analysis, Design, Prototype Simulation, Implementation, Monitoring and Management. The results achieved by this research are to implement host computer security with Fedora Linux and produce an understanding to the general public that computer security is an important thing in computer use. The conclusion of this study is that computer security is something that must be known by everyone who uses computers, based on the aspects of computer security, namely confidentiality, integrity and availability (CIA), threats that can occur on computers using the Linux Fedora OS can be minimized.

Keywords: *Implementation, Computer Security, Fedora Linux.*

PENDAHULUAN

Dewasa ini, perkembangan teknologi dan informasi semakin pesat dan tidak dapat terbendung lagi. Kemajuan sistem informasi memberikan banyak keuntungan bagi kehidupan manusia. Meski begitu, aspek negatifnya juga banyak, seperti kejahatan komputer atau penyerangan yang berupa penyadapan data di jaringan komputer oleh pihak-pihak yang tidak bertanggung jawab. Hal ini terjadi karena kurang pengamanan yang tepat maupun ketidaktahuan masyarakat awam. Bahkan korban penyadapan ini pun tidak sadar bahwa ada seseorang yang sedang menyadapnya. Tidak hanya itu, penyadap juga melakukan penyerangan dengan berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya.

Keamanan komputer berhubungan dengan pencegahan diri terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer, di dalam keamanan sistem komputer yang perlu dilakukan adalah memberikan batasan akses orang lain yang dapat menggangu sistem. Salah satu syarat dalam melakukan kegiatan keamanan komputer adalah adanya

internet dalam pengelolaannya. Saat ini, internet merupakan sarana komunikasi modern yang tidak lepas dari kehidupan manusia. Teknologi informasi ini dapat diibaratkan sebagai samudera pengetahuan yang tak bertepi dan siap untuk dijelajahi dan juga berguna sebagai penghubung dengan komputer yang satu dengan komputer lainnya.

Menurut Wijaya (2014) pengertian *internet* adalah sebutan untuk jaringan komputer global yang menghubungkan satu komputer dengan komputer lain yang ada diseluruh dunia.

Dari pengertian diatas dapat diterangkan bahwa internet adalah suatu metode untuk menghubungkan berbagai komputer kedalam satu jaringan komputer global, melalui protocol yang disebut *Transmission Control Protocol* (TCP/IP). Protokol adalah suatu petunjuk yang menunjukan pekerjaan yang akan pengguna (user) lakukan dengan internet, apakah akan mengakses situs web, melakukan transfer file, mengirim email dan sebagainya. Protokol bisa dibayangkan seperti suatu *Implementasi Sistem Keamanan Komputer* bahasa yang digunakan untuk berkomunikasi dengan berbagai jenis komputer maupun sistem operasi yang terhubung di *internet*.

Celah-celah keamanan dapat terbuka dikarenakan perangkat komputer di instal dengan program aplikasi seperti aplikasi pengolah dokumen, aplikasi *e-mail*, antivirus, aplikasi *server* dan *client* yang mungkin dibutuhkan. Aplikasi yang sudah di instal tersebut, terutama yang terhubung dengan jaringan baik jaringan lokal maupun jaringan *internet* akan membuka *port* komunikasi, *Port* komunikasi tersebut merupakan *port* yang ada dalam *protokol* TCP atau *User Datagram Protocol* (UDP) yang merupakan anggota dari *transportation layer* pada standar OSI. Melalui *port* komunikasi tersebut, jaringan *internet* atau jaringan diluar jaringan komputer dapat menjangkau perangkat komputer. Begitu pula sebaliknya, perangkat komputer lain yang membuka port komunikasi tertentu dapat dijangkau. Komunikasi dapat berjalan dengan lancar, pertukaran informasi menjadi mudah dan kenyamanan dalam berkomputer bertambah dengan terbukanya *port* komunikasi tersebut. Namun, kadang kala kenyamanan ini sering disalahgunakan oleh sebagian orang. *Port* komunikasi yang terbuka tersebut sering menjadi celah untuk dimasuki secara ilegal yang digunakan sebagai jalan kedalam jaringan internal atau *server-server* didalamnya kemudian mengacaukannya. *Port* komunikasi yang terbuka secara bebas juga bisa menjadi ancaman bagi keamanan data yang ada dalam sistem jaringan komputer. Sangat mungkin penyusup dapat masuk kedalam komputer dan bahkan ke seluruh komputer didalam jaringan komputer jika *port* dibiarkan terbuka secara bebas.

METODE PENELITIAN

Metode pengumpulan data yang digunakan dalam membuat website ini antara lain:

1. Studi Pustaka

   Studi pustaka yaitu merupakan metode pengumpulan data yang dilakukan dengan mencari, membaca dan mengumpulkan dokumen-dokumen sebagai referensi seperti buku dan artikel yang berkaitan dengan objek penelitian.
2. Metode sistem keamanan komputer yang digunakan adalah dengan metode *Network Development Life Cycle* (NDLC) dimulai dengan Analisis, Design, Simulasi Prototype, Implementasi, Monitoring dan Management.

HASIL DAN PEMBAHASAN

Menurut (Sugiyono, 2016) Jaringan Komputer adalah sekelompok komputer terpisah yang dihubungkan satu dengan yang lainnya dengan menggunakan protokol komunikasi melalui media transmisi atau media komunikasi. sehingga dapat saling berbagi informasi, program-program, dan penggunaan bersama.

Sistem Keamanan Jaringan adalah proses untuk mencegah dan mengidentifikasi pengguna yang tidak sah (penyusup) dari jaringan komputer (Revva et al., 2018). Tujuannya adalah untuk mengantisipasi resiko jaringan komputer yang dapat berupa ancaman fisik maupun logik. Yang dimaksud ancaman fisik itu adalah yang merusak bagian fisik komputer atau hardware komputer sedangkan ancaman logik yaitu berupa pencurian data atau penyusup yang membobol akun seseorang. Menurut (Asriyanik, 2016) konsep keamanan harus memenuhi minimalnya 3 (tiga) aspek yaitu :

1. Kerahasiaan (Confidentiality). Dapat menjamin bahwa data bersifat rahasia, maksudnya hanya dapat diakses oleh pihak yang berhak.
2. Keutuhan (Integrity). Dapat menjamin bahwa data tetap utuh dan lengkap, dan dapat menjaga dari kerusakan atau ancaman lain yang mengakibatkan berubah informasi dari aslinya.
3. Ketersediaan (Availability). Dapat menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan, salah satu metode adalah patching, backup data.

Sedangkan aspek – aspek ancaman keamanan adalah (Handoko, 2015):

1. *Interruption*. Merupakan suatu ancaman terhadap *availability*. Informasi dan data yang ada dalam sistem komputer dirusak dan dihapus sehingga jika dibutuhkan, data atau informasi tersebut tidak ada lagi.
2. *Interception*. Merupakan ancaman terhadap kerahasiaan (secrey). Informasi yang ada disadap atau orang yang tidak berhak mendapat akses ke komputer dimana informasi tersebut disimpan.
3. Modifikasi. Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan diubah sesuai keinginan orang tersebut.
4. *Fabrication*. Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru (memalsukan) suatu informasi yang ada sehingga orang yang menirima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi tersebut.

Masalah ancaman keamanan dalam sebuah sistem informasi dibagi menjadi 2 (dua) yaitu :

1. Ancaman aktif dapat di bagi menjadi :
   a. Pencurian data. Jika informasi penting yang terdapat dalam database dapat diakses oleh orang yang tidak berwenang maka hasilnya dapat kehilangan informasi atau uang. Misalnya, mata-mata industri dapat memperoleh informasi persaingan yang berharga, penjahat komputer dapat mencuri uang bank.
   b. Penggunaan sistem secara ilegal. Orang yang tidak berhak mengakses informasi pada suatu sistem yang bukan menjadi hak-nya, dapat mengakses sistem tersebut. Penjahat komputer jenis ini umumnya adalah hacker yaitu orang yang suka menembus sistem keamanan dengan tujuan mendapatkan data atau informasi penting yang diperlukan, memperoleh akses ke sistem telepon, dan membuat sambungan telepon jarak jauh secara tidak sah.
   c. Penghancuran data secara ilegal. Orang yang dapat merusak atau menghancurkan data atau informasi dan membuat berhentinya suatu sistem operasi komputer. Penjahat komputer ini tidak perlu berada ditempat kejadian. Ia dapat masuk melalui jaringan komputer dari suatu terminal dan menyebabkan kerusakan pada semua sistem dan hilangnya data atau informasi penting. Penjahat komputer jenis ini umumnya

disebut sebagai cracker yaitu penjebol sistem komputer yang bertujuan melakukan pencurian data atau merusak sistem.

d. Modifikasi secara ilegal. Perubahan-perubahan pada data atau informasi dan perangkat lunak secara tidak disadari. Jenis modifikasi yang membuat pemilik sistem menjadi bingung karena adanya perubahan pada data dan perangkat lunak disebabkan oleh progam aplikasi yang merusak (malicious software). Program aplikasi yang dapat merusak tersebut terdiri dari program lengkap atau segemen kode yang melaksanakan fungsi yang tidak dikehendaki oleh pemilik sistem. Fungsi ini dapat menghapus file atau menyebabkan sistem terhenti. Jenis aplikasi yang dapat merusak data atau perangkat lunak yang paling populer adalah virus.

2. Ancaman Pasif yang terdiri dari :

a. Kegagalan sistem. Kegagalan sistem atau kegagalan *software* dan *hardware* dapat menyebabkan data tidak konsisten, transaksi tidak berjalan dengan lancar sehingga data menjadi tidak lengkap atau bahkan data menjadi rusak. Selain itu, tegangan listrik yang tidak stabil dapat membuat peralatan-peralatan menjadi rusak dan terbakar.

b. Kesalahan manusia. Kesalahan pengoperasian sistem yang dilakukan oleh manusia dapat mengancam integritas sistem dan data.

c. Bencana Alam. Bencana alam seperti gempa bumi, banjir, kebakaran, hujan badai merupakan faktor yang tidak terduga yang dapat mengancam sistem informasi sehingga mengakibatkan sumber daya pendukung sistem informasi menjadi luluh lantah dalam waktu yang singkat.

Implementasi Sistem Keamanan Komputer

Klasifikasi metode penyerangan adalah :

1. Intrusion. Pada metode ini seorang penyerang dapat menggunakan sistem komputer yang dimiliki orang lain. Sebagian penyerang jenis ini menginginkan akses sebagaimana halnya pengguna yang memiliki hak untuk mengakses sistem.
2. *Denial of Services*. Penyerangan jenis ini mengakibatkan pengguna yang sah tak dapat mengakses sistem karena terjadi kemacetan pada sistem. Contoh dari metode penyerangan ini adalah *Distributed Denial of Services* (DDOS) yang mengakibatkan beberapa situs *Internet* tak bisa diakses. Banyak orang yang melupakan jenis serangan ini dan hanya berkonsentrasi pada intrusion saja.

3. Joyrider. Pada serangan ini disebabkan oleh orang yang merasa iseng dan ingin memperoleh kesenangan dengan cara menyerang suatu sistem. Mereka masuk ke sistem karena beranggapan bahwa mungkin didalam sistem terdapat data yang menarik. Rata-rata mereka hanya terbawa rasa ingin tahu, tapi hal tersebut menyebabkan terjadinya kerusakan atau kehilangan data.
4. Vandal. Jenis serangan ini bertujuan untuk merusak sistem, namun hanya ditujukan untuk situs-situs besar.
5. *Hijacking*. Seseorang menempatkan sistem *monitoring* atau *spying* terhadap pengetikan yang dilakukan pengguna pada PC yang digunakan oleh pengguna. Biasaya teknik penyerangan ini membutuhkan program khusus seperti program *keylog* atau sejenisnya. Saat ini semakin banyak perusahaan yang memanfaatkan jasa dari seseorang yang memiliki kemampuan ini.

Terdapat beberapa jenis mata-mata dalam keamanan jaringan :

1. *The curious* (Si ingin tahu). Tipe penyusup yang pada dasarnya tertarik menemukan jenis sistem dan data yang dimiliki orang lain.
2. The malicious (Si perusak). Tipe penyusup yang berusaha untuk merusak sistem, atau merubah halaman web site.
3. *The high profile intruder* (Si profil tinggi). Penyusup yang berusaha menggunakan sistem untuk memperoleh popularitas dan ketenaran.
4. *The competition* (Si Pesaing). Penyusup yang tertarik pada data yang terdapat dalam sebuah sistem.
5. *Sniffing*. Sesorang yang melakukan monitoring atau penangkapan terhadap paket data yang ditransmisikan dari komputer client ke web server pada jaringan internet (saluran komunikasi).
6. *Spoofing*. Seseorang berusaha membuat pengguna mengunjungi sebuah halaman situs yang salah sehingga membuat pengunjung situs memberikan informasi rahasia kepada pihak yang tidak berhak.
7. Website *Defacing*. Seseorang melakukan serangan pada situs asli kemudian mengganti isi halaman pada server tersebut dengan halaman yang telah dimodifikasi.
8. Virus. Virus adalah kode program yang dapat mengikatkan diri pada aplikasi atau file, di mana program tersebut bisa menyebabkan komputer bekerja di luar kehendak pemakai

sehingga file yang berkestensi terntentu menjadi terinfeksi yangmengakibatkan file menjadi hilang karena disembunyikan (hide), termodifikasi (encrypt) bahkan terhapus (delete).

9. *Trojan Horse.* Salah satu metode penyerangan yang sangat ampuh dan sering digunakan dalam kejahatan-kejahatan di internet. Seseorang memberikan program yang bersifat free atau gratis, yang memiliki fungsi dan mudah digunakan (user friendly), tetapi di dalam program tersebut terdapat program lain yang tidak terlihat oleh user yang berfungsi menghapus data. Misalnya program untuk cracking password, credit-card generator dan lain-lain.
10. *Worm.* Program yang dapat menduplikasikan dirinya sendiri dengan menggunakan media komputer yang mengakibatkan kerusakan pada sistem dan memperlambat kinerja komputer dalam mengaplikasi sebuah program.

Pengertian *internet* adalah " Sebutan untuk jaringan komputer global yang menghubungkan satu komputer dengan *computer* lain yang ada diseluruh dunia". (Wijaya, 2014).

Firewall adalah merupakan alat untuk mengimplementasikan kebijakan *security* (security policy). Sedangkan kebijakan *security*, dibuat berdasarkan perimbangan antara fasilitas yang disediakan dengan implikasi *security*-nya. Semakin ketat kebijakan *security*, semakin kompleks konfigurasi layanan informasi atau semakin sedikit fasilitas yang tersedia di jaringan. (Purwaningru, dkk., 2018). Dalam dunia nyata, firewall adalah dinding yang bisa memisahkan ruangan, sehingga kebakaran pada suatu ruangan tidak menjalar ke ruangan lainnya. Tapi sebenarnya firewall di Internet lebih seperti pertahanan disekeliling benteng, yakni mempertahankan terhadap serangan dari luar. Diantara kegunaannya yaitu :

1. Membatasi gerak orang yang masuk ke dalam jaringan internal.
2. Membatasi gerak orang yang keluar dari jaringan internal.
3. Mencegah penyerang mendekati pertahanan yang berlapis.

Gambar 1. Firewall

(Sumber: http://sumbersolusindo.co.id/product/detail/firewall)

Rule dan *Policy* adalah teknis utama dalam *firewall* yang dimana melalui *rule* dan *policy* seorang *network administrator* dapat mengontrol sistem kerja *firewall* dan dapat melakukan *monitoring* secara dinamis serta memaksimalkan produktivitas kinerja perangkat – perangkat jaringan.

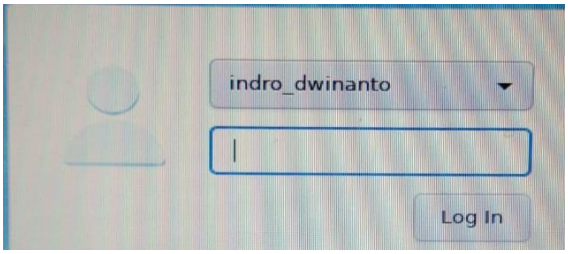
Pengertian Antarmuka (Interface) merupakan mekanisme komunikasi antara pengguna (user) dengan sistem. Antarmuka (Interface) dapat menerima informasi dari pengguna (user) dan memberikan informasi kepada pengguna (user) untuk membantu mengarahkan alur penelusuran masalah sampai ditemukan suatu solusi. *Interface*, berfungsi untuk menginput pengetahuan baru ke dalam basis pengetahuan sistem pakar (Expert System), dengan menampilkan penjelasan sistem dan memberikan panduan pemakaian sistem secara menyeluruh atau *step by step* sehingga pengguna mengerti apa yang akan dilakukan terhadap suatu sistem. Yang terpenting adalah kemudahan dalam memakai atau menjalankan sistem, interaktif, komunikatif, sedangkan kesulitan dalam mengembangkan atau membangun suatu program jangan terlalu diperlihatkan. *Interface* yang ada untuk berbagai sistem, dan menyediakan cara input dan output. Linux adalah sebuah aplikasi atau program yang menggunakan kernel sebagai sistem operasi. Script pertama Linux dirancang dan ditulis oleh seorang mahasiswa dari Finlandia bernama "Linus Torvalds" untuk Intel 80386 arsitektur. Script lain dari Linux yang tersedia di Internet pada tahun 1991. Setelah itu, banyak orang bermain peran penting dalam mengembangkan dan memperluas Linux di berbagai belahan dunia. Sistemnya, peralatan sistem dan pustakanya umumnya berasal dari sistem operasi GNU, yang diumumkan tahun 1983 oleh Richard Stallman. Kontribusi GNU adalah dasar dari munculnya nama alternatif GNU/Linux. Dia menggunakan alat proyek GNU dan dengan demikian sistem

operasi dikembangkan melalui proyek GNU / Linux. (Harjono, 2016). Salah satu distro linux yang digunakan dalam proyek ini adalah distro linux fedora dan distro kali linux.

Selanjutnya berdasarkan analisa keamanan komputer akan dijelaskan implementasi keamanan komputer pada host OS Linux Fedora yang berpedoman pada *Confidentiality, Integrity* dan *Availability* (CIA).

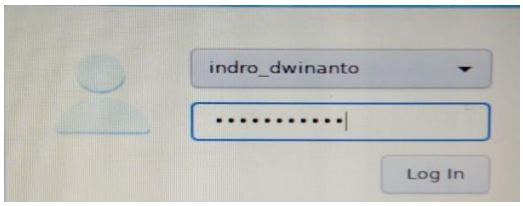
Implementasi pada aspek kerahasiaan (Confidentiality) dapat dilakukan dengan menggunakan metode acces control yang meliputi :

1. Identification: Pengguna mengklaim identitas dengan nama unik pengguna. Pengguna komputer menyatakan bahwa user adalah miliknya dan bukan milik orang pada saat login ke komputer seperti gambar 2.



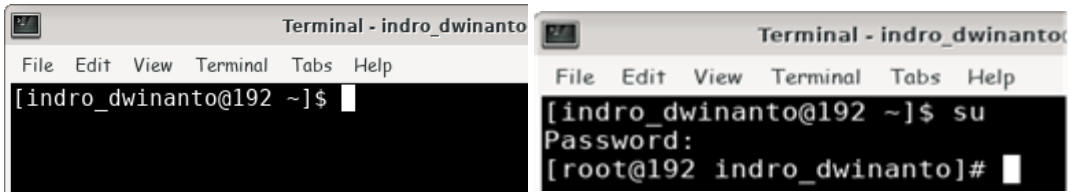
Gambar 2. Login User

2. Authentication: Pengguna membuktikan dengan otentifikasi menggunakan sandi.



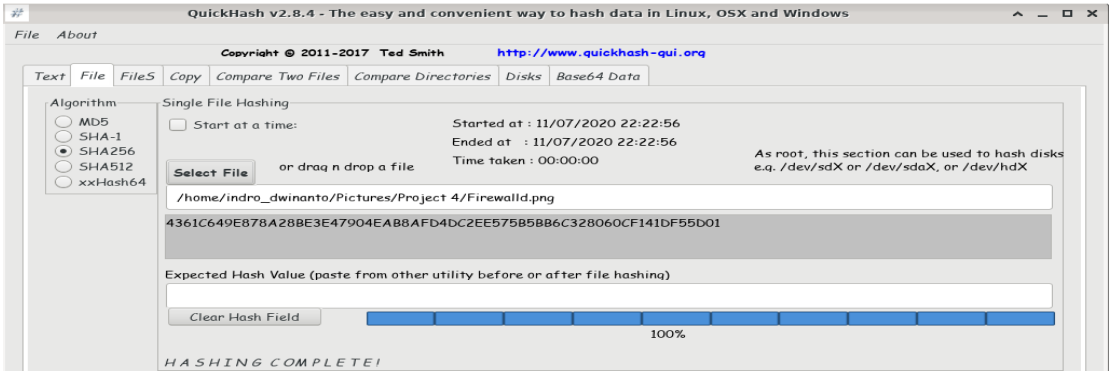
Gambar 3. User dan Password

3. Authorization: Memberikan atau membatasi akses ke sumber daya. Pengguna komputer harus dibuatkan akses dimana pengguna hanya dapat menggunakan operating sistem saja ataupun akses untuk merubah baik menambah, menghapus aplikasi pada operating sistem komputer atau lebih dikenal dengan akses previledge/root seperti gambar 4.

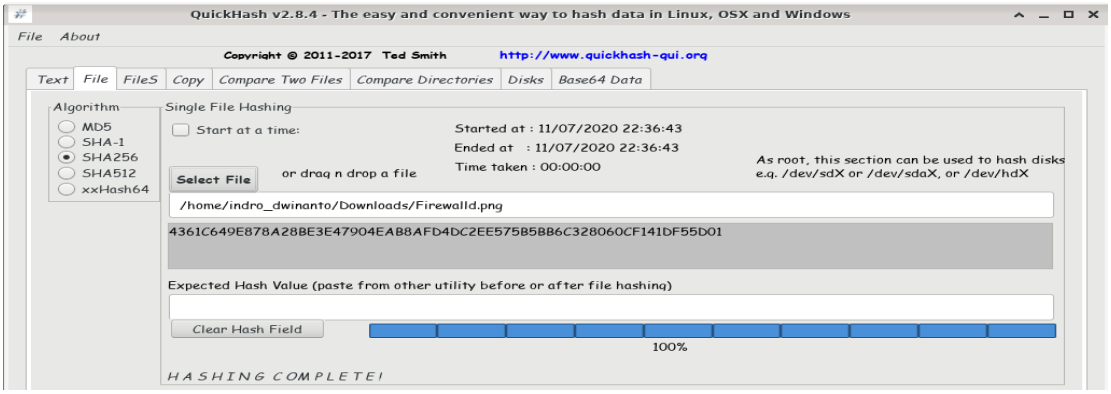


Gambar 4. Akses Biasa dan Akses Root

4. Hasing. Metode ini menggunakan tool pembantu yaitu tools QuickHash untuk melakukan hashing SHA256 terhadap file yang akan dikirim, baik file tidak dirubah (Gambar 5 dan 6) bisa terlihat bahwa nilai hashing dari 2 file tersebut sama.

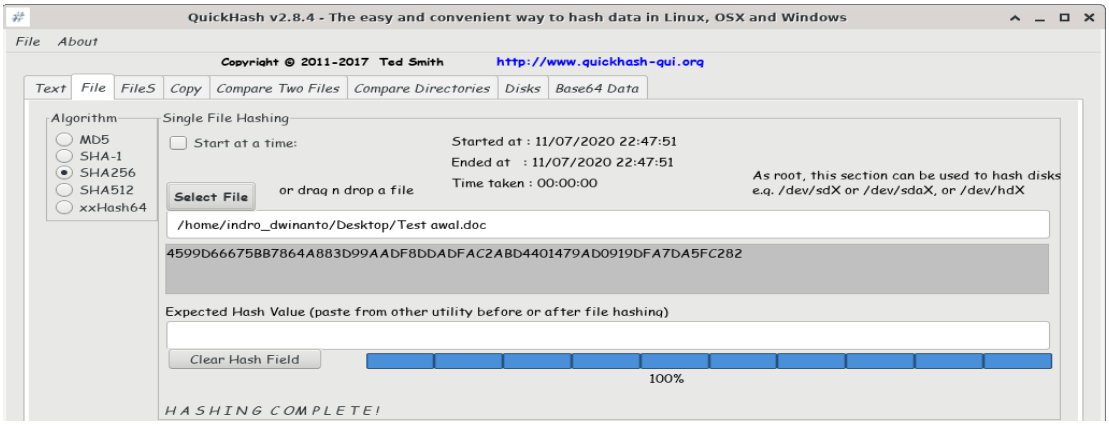


Gambar 5. Hashing gambar dengan SHA 256 awal

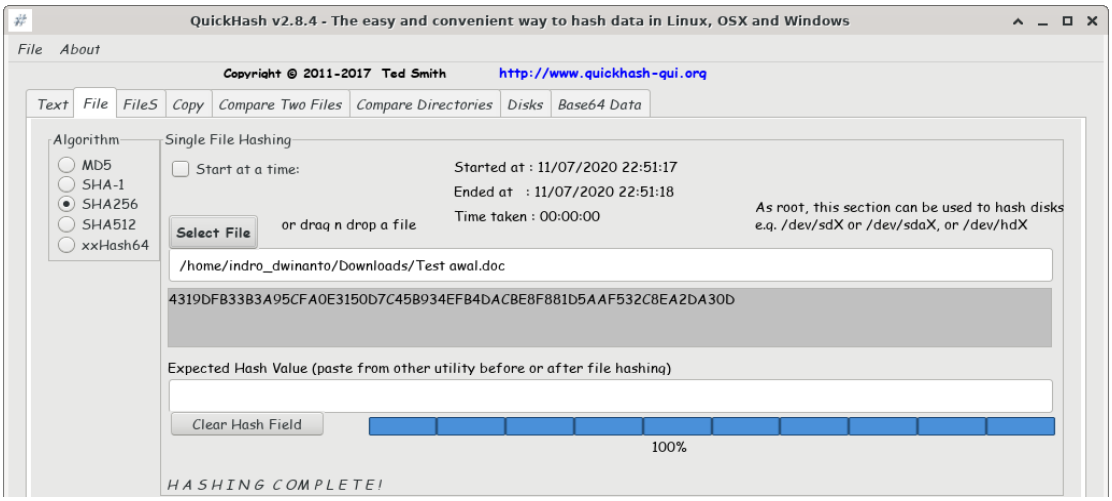


Gambar 6. Hashing gambar ke penerima dan file tidak berubah

Sedangkan untuk file yang sudah dirubah sebelum mencapai pengirim akan mengakibatkan nilai hashing berubah ini mengidentifikasi bahwa file sudah mengalami perubahan.



Gambar 7. Hashing file SHA 256

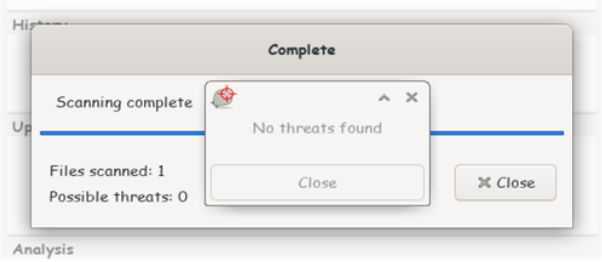


Gambar 8. Hashing file ke penerima dan file berubah

5. Menggunakan metode *user password* pada aplikasi *office* yang akan dikirim kepada orang lain. *Libreeoffice* merupakan aplikasi office default di linux OS fedora dan merupakan aplikasi yang dapat meminimalisir keamanan komputer pada aspek integrity dengan cara menggunakan save file dengan password atau encrypt dengan GPG Key

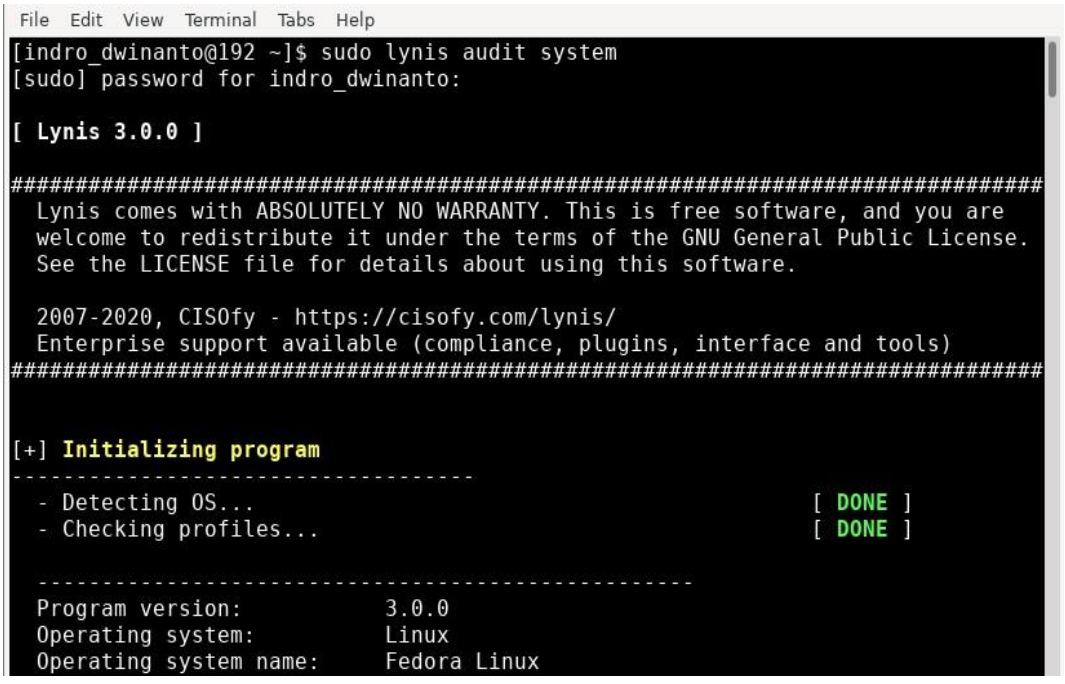
Gambar 9. Tampilan Setting Password dan Membuka Password pada File Aplikasi Office

6. Monitoring keamanan komputer dengan melakukan scanned antivirus setiap saat guna memberikan tambahan keamanan bagi keamanan komputer. Dalam proyek ini saya menggunakan antivirus clamav guna mendteksi virus yang ada, monitoring dengan antivirus ini sangat penting dilakukan guna memastikan keamanan komputer di aspek integrity.



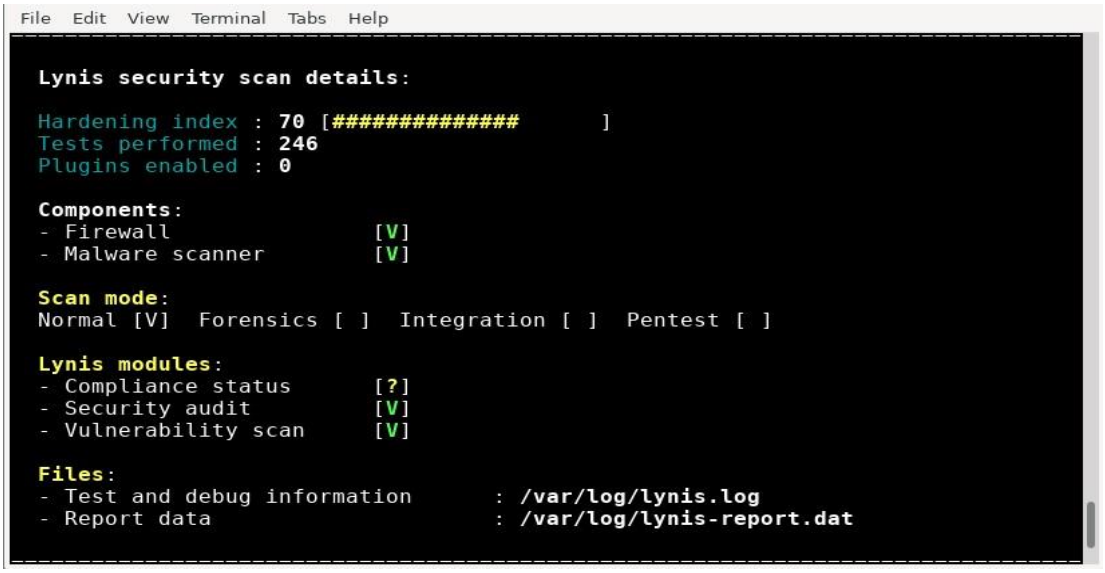
Gambar 10. Scanning Virus Menggunakan Aplikasi Clampav

Selain melakukan scanned antivirus monitoring keamanan komputer dapat dilakukan dengan menggunakan tools *Lynis* Audit Sistem yang tersedia di OS Linux Fedora untuk memastikan bahwa sistem dalam kondisi baik.

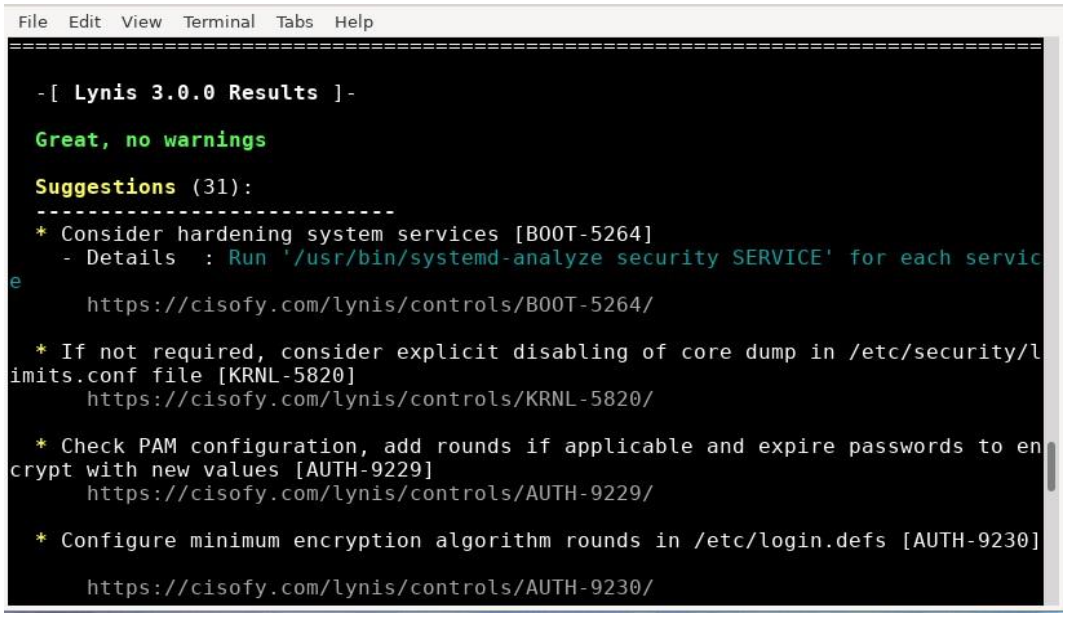


Gambar 11. Melakukan audit sistem dengan bantuan tool Lynis Audit Sistem

Perintah awal Tool *Lynis* Audit Berdasarkan data yang ada dapat ditampilkan summary *Lynis Security Scan* detail seperti gambar 12, dengan keterangan komponen *firewall* dan *malware scanner* ada.



Gambar 12. Lynis security scan details dari keseluruhan data yang ditampilkan

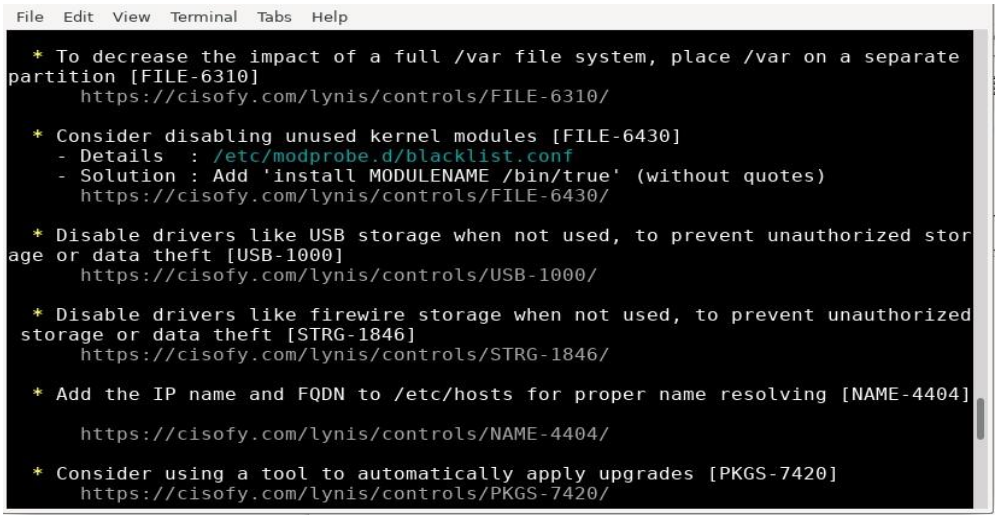


Gambar 13. Hasil Lynis

Berdasarkan dari gambar 13. komputer berada dalam kondisi baik dan ada beberapa saran yang Lynis berikan untuk keamanan sistem tambahan diantaranya sebagai berikut:

1. Menonaktifkan *driver* seperti penyimpanan USB saat tidak digunakan, untuk mencegah penyimpanan tidak sah atau pencurian data.

2. Untuk mengurangi dampak sistem *file full* /var, letakkan /var pada partisi yang terpisah.
3. Pertimbangkan untuk menonaktifkan kernel modul yang tidak digunakan.
4. Bila mungkin, atur kadaluwarsa untuk semua akun yang dilindungi kata sandi.
5. Pertimbangkan untuk menggunakan alat untuk secara otomatis menerapkan pembaharuan dan lain-lain.



Gambar 14. Beberapa saran yang diberikan Lynis

Dengan melakukan proses keamanan komputer setiap saat secara terus menerus sesuai dengan petunjuk implementasi diatas diharapkan dapat mengurangi ancaman-ancaman yang dapat merugikan pengguna komputer dan mengurangi celah-celah ancaman yang dapat terjadi tanpa kita ketahui.

SIMPULAN

Berdasarkan analisa dan implementasi yang telah dilakukan maka dapat disimpulkan bahwa :

1. Keamanan komputer merupakan hal yang wajib diketahui oleh semua orang yang beraktifitas menggunakan *device* komputer, dengan berpatokan pada aspek keamanan komputer yaitu *confidentiality, Integrity* dan *availability* (CIA) maka ancaman yang bisa terjadi pada komputer menggunakan OS *Linux Fedora* dapat di minimalisir dengan cara meng-*update* sistem operasi secara terus menerus, mengecek data yang dikirim dengan menggunakan *tools hashing*, membuat *password file office* sebelum dikirimkan, dan selalu memisahkan user biasa dengan *user previlege* (root).

2. Penggunaan komputer oleh masyarakat awam, harus lebih diperhatikan, karena faktor ketidaktahuannya itu akan menyebabkan kerugian yang besar baik kerugian pribadi maupun perusahaan. Dengan berpedoman pada komponen *confidentiality, Integrity* dan *availability* (CIA) maka ancaman yang bisa terjadi pada komputer bisa di minimalisir.

DAFTAR PUSTAKA

Asriyanik. (2016). Penilaian Keamanan Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi Dengan Menggunakan ISO 27001. Jurnal Ilmiah Sains Dan Teknologi, 6 (2), 501–506.

Handoko, D. (2015). Keamanan Jaringan. Surabaya Jawa Timur: CV. Garuda Mas Sejahtera.

Harjono, E. B. (2016). Analisa Dan Implementasi Dalam Membangun Sistem Operasi Linux Menggunakan Metode LSF Dan Remaster. Informatika, I (1), 30–35.

Purwaningrum, Fajar Adhi, dkk. (2018). Optimalisasi Jaringan Menggunakan Firewall. Ikra-ith Informatika: Jurnal Komputer dan Informatika, Vol: 2, Nomor 3 November 2018.

Revva, I., Jeinever, P., Rasyid, A., Suharto, N. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan Random Port Knocking Berbasis Raspberry PI Yang Dikirim Melewati Telegram. Jurnal Jartel ISSN: 2407-0807 Vol: 7, Nomor 2, Nop.

Sugiyono. (2016). Sistem Keamanan Jaringan Komputer Menggunakan Metode Watchguard Firebox Pada PT. Guna Karya Indonesia. Jurnal CKI, 9(1), 1–8.

Wijaya. (2014). Internet untuk pemula (Familia (Ed.); Edition 2). Jakarta: Gramedia.