

# IMPLEMENTASI KEAMANAN KOMPUTER PADA ASPEK *CONFIDENTIALITY, INTEGRITY, AVAILABILITY (CIA)* MENGUNAKAN *TOOLS LYNIS AUDIT SYSTEM*

Indro Dwinanto<sup>1</sup>, Hari Setiyani<sup>2</sup>

<sup>1,2</sup>Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Informasi NIIT  
Jl. Asem Dua No. 22, Kel. Cipete Selatan, Kec. Cilandak, Jakarta Selatan  
Email: dwinandie@gmail.com<sup>1</sup>, hari.setiyani@gmail.com<sup>2</sup>

## Abstrak

Kemajuan teknologi dan sistem informasi memberikan banyak keuntungan bagi kehidupan manusia, meskipun aspek negatifnya juga banyak, seperti kejahatan komputer berupa penyadapan data di jaringan komputer oleh pihak yang tidak bertanggung jawab. Keamanan komputer berhubungan dengan pencegahan terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer. Celah keamanan dapat terbuka dikarenakan perangkat komputer di instal program aplikasi yang terhubung jaringan lokal maupun internet membuka port komunikasi. Port komunikasi ada dalam protokol TCP atau *User Datagram Protocol (UDP)* yang merupakan *transportation layer* pada standar OSI. Port komunikasi yang terbuka secara bebas menjadi ancaman keamanan data yang ada dalam sistem jaringan komputer. Tujuan penelitian ini adalah meminimalisir ancaman keamanan komputer dengan *Tools Lynis Audit System*. Metode penelitian yang digunakan adalah studi pustaka, *Network Development Life Cycle (NDLC)*. Hasil yang dicapai penelitian ini adalah mengimplementasikan keamanan komputer dengan *OS Linux Fedora* dan *Tools Lynis Audit System* agar meminimalisir kerugian yang terjadi. Simpulan dari penelitian ini adalah dengan *confidentiality, Integrity dan availability (CIA)* maka ancaman yang terjadi pada komputer menggunakan *OS Linux Fedora* dapat di minimalisir dengan cara mengupdate sistem operasi secara berkala, mengecek data yang dikirim menggunakan *tools hashing*, membuat *password file office* sebelum dikirimkan, dan selalu memisahkan *user biasa* dengan *user privilege (root)*.

**Kata Kunci:** Implementasi, Keamanan Komputer, Tools Lynis Audit Sistem, OS Linux Fedora

## 1. PENDAHULUAN

### 1.1 Latar Belakang

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 mengganggu 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 menunjukkan 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 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* (client), *antivirus*, aplikasi *server* (client) dan lain sebagainya yang mungkin dibutuhkan bahkan juga tidak 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 disalah gunakan 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.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut diatas maka dapat dirumuskan permasalahan sebagai berikut :

1. Bagaimana mengimplementasikan keamanan komputer yang menggunakan OS Linux Fedora agar bisa meminimalisir ancaman / kerugian yang bisa terjadi?
2. Bagaimana menggunakan komputer dalam pekerjaan sehari-hari dalam meminimalisir ancaman keamanan komputer?

## 2. METODE PENELITIAN

Metode penelitian yang digunakan untuk melakukan penelitian adalah:

### 1. Kepustakaan

Penelitian ini menggunakan penelitian kepustakaan atau yang disebut juga dengan *Library Research*. Pengertian studi pustaka adalah kajian teoritis, referensi serta literatur ilmiah lainnya yang berkaitan dengan budaya, nilai dan norma yang berkembang pada situasi sosial yang di teliti (Nanang Suryana, 2021).

### 2. Observasi dan wawancara

Metode Observasi dan wawancara merupakan sistem pengumpulan data dengan cara melakukan pengamatan secara langsung pada objek yang diteliti sehingga dapat data yang akurat. Objek yang diteliti mengenai bagaimana proses yang terjadi di pusat jajanan kuliner.

### 3. Implementasi Keamanan Komputer

Pada tahapan implementasi keamanan komputer dengan menggunakan metode *Network Development Life Cycle* (NDLC) dimulai dengan Analisis, Design, Simulasi Prototype, Implementasi, Monitoring dan Managemen..

## 3. HASIL DAN PEMBAHASAN

Menurut Mulyadi (2015:12), implementasi mengacu pada tindakan untuk mencapai tujuan-tujuan yang telah ditetapkan dalam suatu keputusan. Tindakan ini berusaha untuk mengubah keputusan-keputusan tersebut menjadi pola-pola operasional serta berusaha mencapai perubahan-perubahan besar atau kecil sebagaimana yang telah diputuskan sebelumnya. Implementasi

pada hakikatnya juga merupakan upaya pemahaman apa yang seharusnya terjadi setelah program dilaksanakan. Dalam tataran praktis, implementasi adalah proses pelaksanaan keputusan dasar. Proses tersebut terdiri atas beberapa tahapan yakni:

1. Tahapan pengesahan peraturan perundangan.
2. Pelaksanaan keputusan oleh instansi pelaksana.
3. Kesiadaan kelompok sasaran untuk menjalankan keputusan.
4. Dampak nyata keputusan baik yang dikehendaki maupun tidak.
5. Dampak keputusan sebagaimana yang diharapkan instansi pelaksana.
6. Upaya perbaikan atas kebijakan atau peraturan perundangan.

Proses persiapan implementasi setidaknya menyangkut beberapa hal penting yakni:

1. Penyiapan sumber daya, unit dan metode.
2. Penerjemahan kebijakan menjadi rencana dan arahan yang dapat diterima dan dijalankan.
3. Penyediaan layanan, pembayaran dan hal lain secara rutin.

Menurut Benfano Soewito (2019) dikutip dari situs [mti.binus.ac.id](http://mti.binus.ac.id) dikatakan bahwa arti dari keamanan komputer telah berubah dalam beberapa tahun terakhir. Sebelum masalah keamanan data/informasi menjadi populer, kebanyakan orang berpikir bahwa keamanan *computer* difokuskan pada alat alat *computer* secara fisik. Secara tradisional, fasilitas komputer secara fisik dilindungi karena tiga alasan:

1. Untuk mencegah pencurian atau kerusakan *hardware*.
2. Untuk mencegah pencurian atau kerusakan informasi.
3. Untuk mencegah gangguan layanan.

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. Metode yang digunakan antara lain :

- a. *Encryption*

Membuat data agar data tidak dapat dibaca oleh orang yang tidak berhak.

- b. *Access Controls*

- 1). *Identification*: Pengguna mengklaim identitas dengan nama unik pengguna

- 2). *Authentication*: Pengguna membuktikan dengan otentikasi berupa sandi

- 3). *Authorization*: Memberikan atau membatasi akses ke sumberdaya.

- c. Steganografi dan *Obfuscation*

Steganografi adalah menyembunyikan data dengan data, sedangkan *Obfuscation* adalah suatu metode untuk membuat sesuatu menjadi tidak jelas/sulit di mengerti.

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.

Metode yang digunakan antara lain hasing dengan menggunakan MD5, SHA, HMAC, Tanda tangan digital 2 (dua) kunci konsep Integrity :

- a. Integritas memberikan jaminan bahwa data belum dimodifikasi, dirusak.

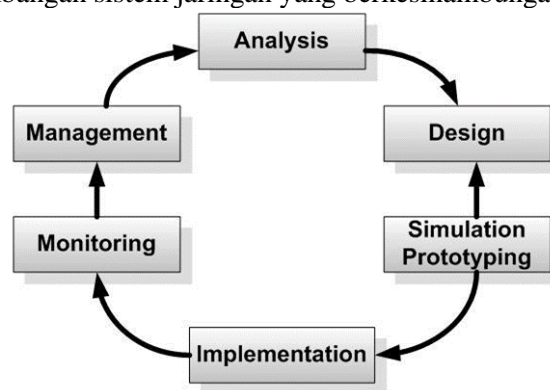
- b. Hasing memverifikasi integritas sebuah data.

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.

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.

Dikutip dari jurnal ilmiah betrik menurut Rudi Kurniawan (2016) dalam Goldman dikatakan bahwa pengertian dari *Network Development Life Cycle* (NDLC) mendefinisikan siklus proses perancangan atau pengembangan suatu sistem jaringan komputer. NDLC mempunyai elemen yang mendefinisikan fase, tahapan, langkah atau mekanisme proses spesifik. Kata cycle merupakan kunci deskriptif dari siklus hidup pengembangan sistem jaringan yang menggambarkan secara keseluruhan proses dan tahapan pengembangan sistem jaringan yang berkesinambungan.



**Gambar 1.** Metode *Network Development Life Cycle* (NDLC)

### 3.1. Analisa Sistem

Analisis sistem adalah merupakan kegiatan penguraian suatu sistem informasi yang utuh dan nyata kedalam bagian-bagian atau komponen-komponen komputer yang bertujuan untuk mengidentifikasi serta mengevaluasi masalah-masalah yang muncul, hambatan-hambatan yang mungkin terjadi dan kebutuhan-kebutuhan yang diharapkan sehingga mengarah kepada suatu solusi untuk perbaikan maupun pengembangan ke arah yang lebih baik dan sesuai dengan kebutuhan serta perkembangan teknologi.

### 3.2. Analisa Kebutuhan Non-Fungsional

Analisis kebutuhan non-fungsional merupakan analisis yang dibutuhkan untuk menentukan spesifikasi kebutuhan sistem. Spesifikasi ini juga meliputi elemen atau komponen-komponen apa saja yang dibutuhkan untuk sistem yang akan dibangun sampai dengan sistem tersebut dapat di implementasikan. Analisis kebutuhan ini juga menentukan spesifikasi masukan yang diperlukan sistem, keluaran yang akan dihasilkan dan proses yang dibutuhkan untuk mengolah masukan sehingga menghasilkan suatu keluaran yang diinginkan.

#### 3.2.1. Analisa Kebutuhan Perangkat Keras (*Hardware*)

Perangkat keras (*Hardware*) adalah semua bagian fisik komputer, dan dibedakan dengan data yang berada didalamnya atau yang beroperasi didalamnya. Dalam pengerjaan proyek ini, digunakan laptop merk *Hewlett Packard* (HP) RAM 4 Gb.

#### 3.2.2. Analisa Kebutuhan Perangkat Lunak (*Software*)

Untuk membangun sistem ini diusulkan spesifikasi perangkat lunak (*Software*) yang akan digunakan yaitu:

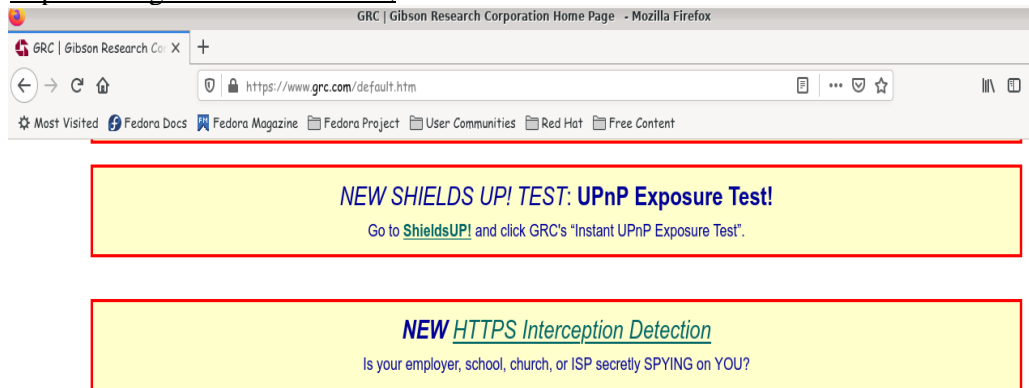
1. Sistem Operasi Linux Fedora.
2. *Virtual Box*.
3. Aplikasi Kali Linux.

Sebelum memasuki aspek keamanan komputer, akan di jelaskan mengenai keamanan komputer pengguna OS Linux Fedora dengan melihat *port-port* yang terbuka, dengan metode *scanning port* melalui webtools (<http://www.grc.com>) dan aplikasi Nmap.

1. Analisis Keamanan Jaringan Menggunakan *Webtools* grc.com

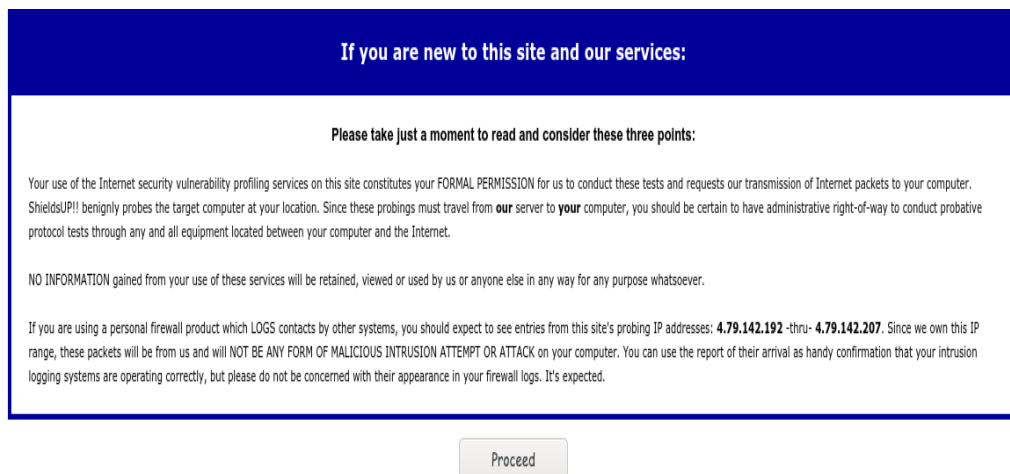
Langkah-langkah teknis proses analisis yang dilakukan pada situs grc.com adalah sebagai berikut:

- a. Pertama masuk kedalam halaman muka dari situs grc.com dengan alamat web <http://www.grc.com/default.htm>:



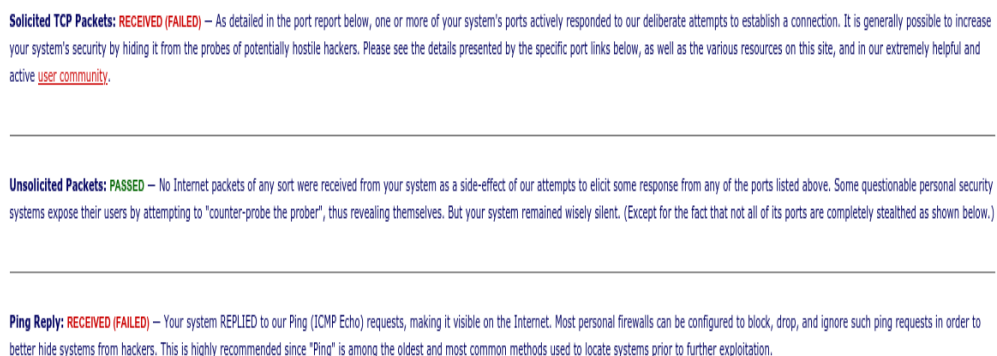
Gambar 2. Halaman Muka Situs grc.com

- b. Kemudian klik Shields Up dan akan memunculkan gambar sebagaimana berikut:



Gambar 3. Situs grc.com Proceed.

- c. Setelah muncul gambar seperti diatas kemudian kita klik tombol *proceed* dan kemudian akan diarahkan ke gambar 4. atau situs pemberitahuan.



Gambar 4. Situs grc.com Pemberitahuan

d. Kemudian akan muncul data port yang terbuka seperti gambar dibawah ini:

Port	Service	Status
0	<nil>	Closed
21	FTP	Stealth
22	SSH	Closed
23	Telnet	Stealth
25	SMTP	Stealth
79	Finger	Closed
80	HTTP	OPEN!
110	POP3	Closed
113	IDENT	Closed
119	NNTP	Closed
135	RPC	Closed
139	Net BIOS	Closed
143	IMAP	Closed
389	LDAP	Closed
443	HTTPS	Stealth
445	MSFT DS	Closed
1002	ms-ils	Closed
1024	DCOM	Closed
1025	Host	Closed
1026	Host	Closed
1027	Host	Closed
1028	Host	Closed
1029	Host	Closed
1030	Host	Closed
1720	H.323	Closed

**Gambar 5.** Situs grc.com Port-Port Yang Terbuka dan Tertutup

Penjelasan :

- 1) Status close: Komputer Anda merespons bahwa port ini ada tetapi saat ini tertutup untuk koneksi;
- 2) Status Stealth : Tidak ada bukti apapun bahwa port (atau bahkan komputer apa pun) ada di alamat IP ini!
- 3) Status Open: Web sangat tidak aman akhir-akhir ini sehingga "eksploitasi" keamanan baru ditemukan hampir setiap hari. Ada banyak masalah yang diketahui dengan Personal Web Server (PWS) *Microsoft* dan *Frontpage Extensions* yang dijalankan banyak orang di mesin pribadi mereka. Jadi memiliki port 80 "terbuka" seperti di sini menyebabkan penyusup bertanya-tanya berapa banyak informasi yang Anda mungkin ingin berikan.

e. *Summary* dari aplikasi adalah seperti gambar dibawah ini



This textual summary may be printed, or marked and copied for subsequent pasting into any other application:

```

-----
GRC Port Authority Report created on UTC: 2020-06-27 at 11:49:20
Results from scan of ports: 0, 21-23, 25, 79, 80, 110, 113,
                           119, 135, 139, 143, 389, 443, 445,
                           1002, 1024-1030, 1720, 5000

  1 Ports Open
 21 Ports Closed
  4 Ports Stealth
-----
 26 Ports Tested

The port found to be OPEN was: 80

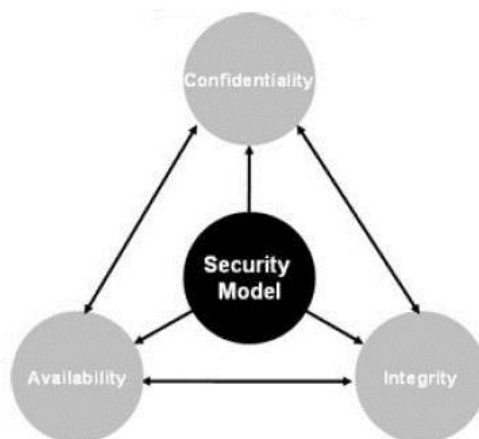
Ports found to be STEALTH were: 21, 23, 25, 443

Other than what is listed above, all ports are CLOSED.

TruStealth: FAILED - NOT all tested ports were STEALTH,
                  - NO unsolicited packets were received,
                  - A PING REPLY (ICMP Echo) WAS RECEIVED.
    
```

**Gambar 6.** Situs grc.com Summary

### 3.3. Design Keamanan Komputer Linux Fedora



**Gambar 7.** Design Keamanan Komputer yang Diharapkan

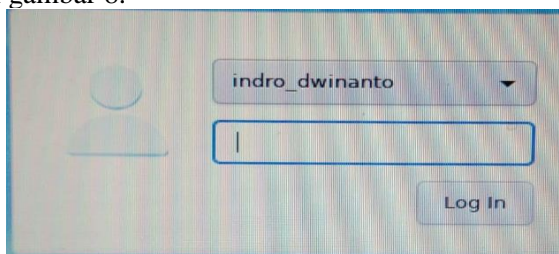
Sumber : <https://handisonj.wordpress.com/2013/09/16/cia-confidentiality-integrity-availability/>

Berdasarkan gambar 7. keamanan komputer Linux Fedora yang sudah ada akan menggunakan design keamanan model *Confidentiality, Availability dan Integrity* (CIA) yang akan dijabarkan berdasarkan analisa keamanan komputer menggunakan bantuan tool Nmap dan tools online dari grc pada bab 3 (tiga) bahwa masih ada port-port yang terbuka yaitu port 53 (DNS), 80 (Web Server) dan 443 (SSL Server) tetapi masih dikategorikan aman untuk digunakan.

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

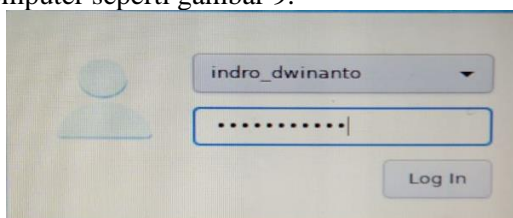
1. Identification : Pengguna mengklaim identitas dengan nama unik pengguna.

Pengguna komputer menyatakan bahwa user adalah miliknya dan bukan milik orang pada saat login ke komputer seperti gambar 8.



**Gambar 8.** User pengguna komputer

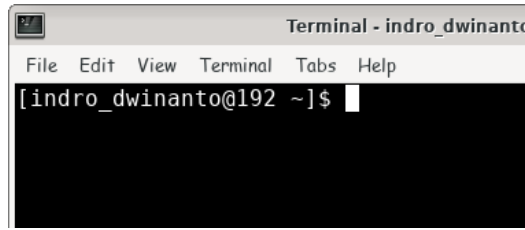
2. Authentication : Pengguna dapat membuktikan dengan otentifikasi menggunakan sandi sesuai dengan sandi yang dimiliki. Setelah pengguna komputer menyatakan bahwa user adalah miliknya kemudian pengguna komputer melakukan otentifikasi menggunakan password yang digunakan oleh nama user pada saat login ke komputer sehingga bisa masuk kedalam operating sistem komputer seperti gambar 9.



**Gambar 9.** User dan password

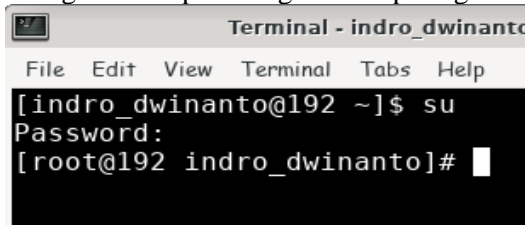
c. Authorization : Memberikan atau membatasi akses ke sumber daya.

Pengguna komputer harus dibuatkan akses dimana pengguna hanya dapat menggunakan operating sistem saja seperti gambar 10.



**Gambar 10.** Akses biasa

ataupun akses untuk merubah baik menambah, menghapus aplikasi pada operating sistem komputer atau lebih dikenal dengan akses previledge/root seperti gambar 4.4



**Gambar 11.** Akses root

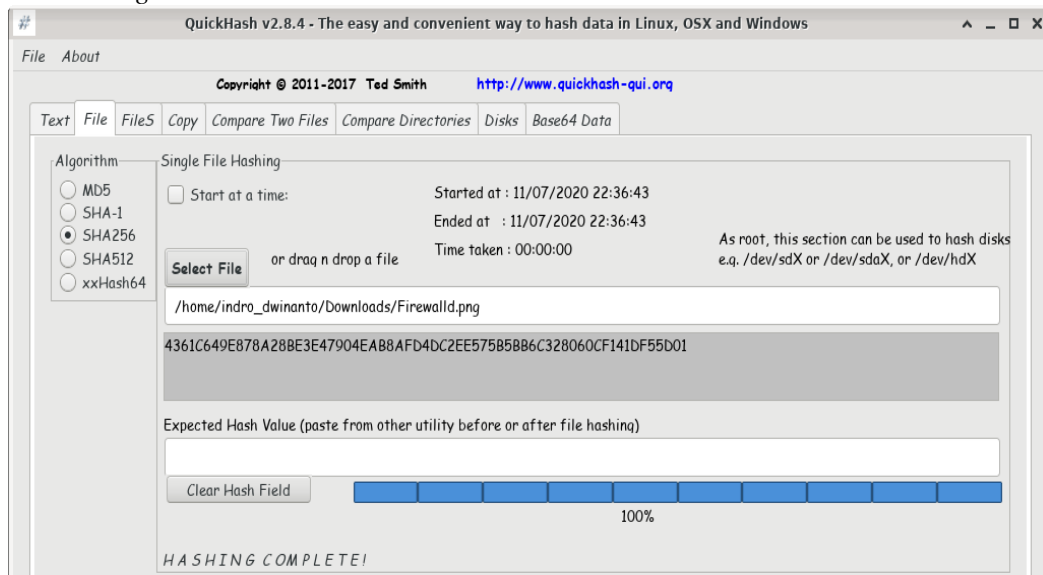
Pembagian akses tersebut digunakan untuk mengurangi dampak kerusakan yang bisa terjadi jika aplikasi dirubah dikarenakan beberapa file pendukung aplikasi tidak support pada operating sistem yang dapat menyebabkan opeating sistem crash.

Implementasi pada aspek *integrity* dibahas mengenai jaminan bahwa data tetap utuh dan lengkap, dan dapat menjaga dari kerusakan atau ancaman lain yang mengakibatkan berubah informasi dari aslinya.

Metode implementasi yang digunakan adalah menggunakan metode :

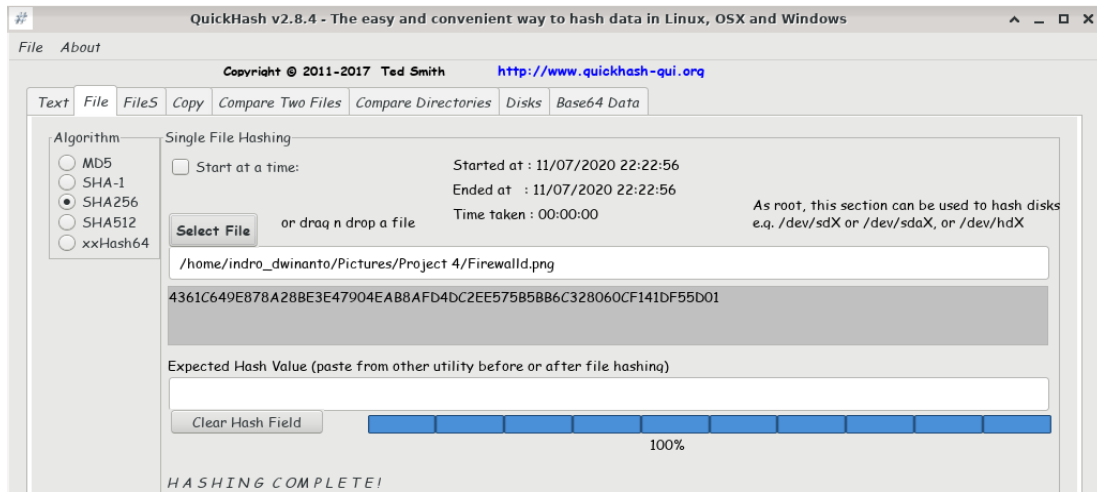
1. *Hasing*

Metode ini menggunakan tool pembantu yaitu *Tools Quick Hash* untuk melakukan *hashing* SHA256 terhadap file yang akan dikirim, baik file tidak dirubah (Gambar 12 dan 13) bisa terlihat bahwa nilai *hashing* dari 2 file tersebut sama.



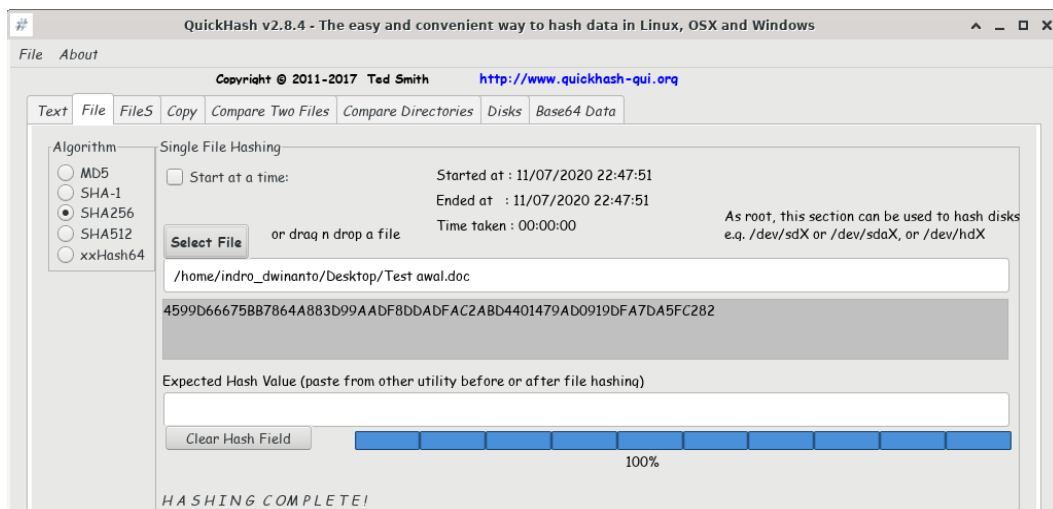
**Gambar 12.** Hashing gambar dengan SHA 256 awal



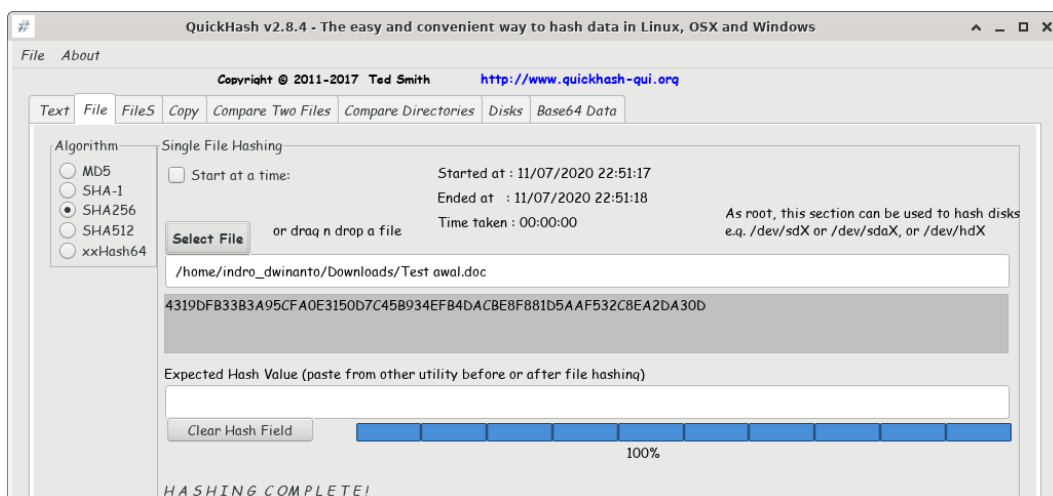


**Gambar 13.** Hashing gambar ke penerima dan file tidak berubah

Sedangkan untuk file yang sudah dirubah sebelum mencapai pengirim akan mengakibatkan nilai hashing berubah ini mengidentifikasi bahwa file sudah mengalami perubahan digambarkan pada gambar 14 dan 15.



**Gambar 14.** Hashing file SHA 256

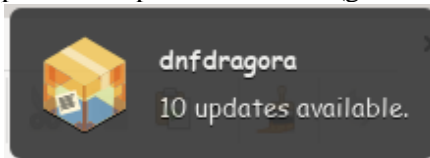


**Gambar 15.** Hashing file ke penerima dan file berubah

Implementasi pada aspek *availability* dimaksudkan untuk 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.

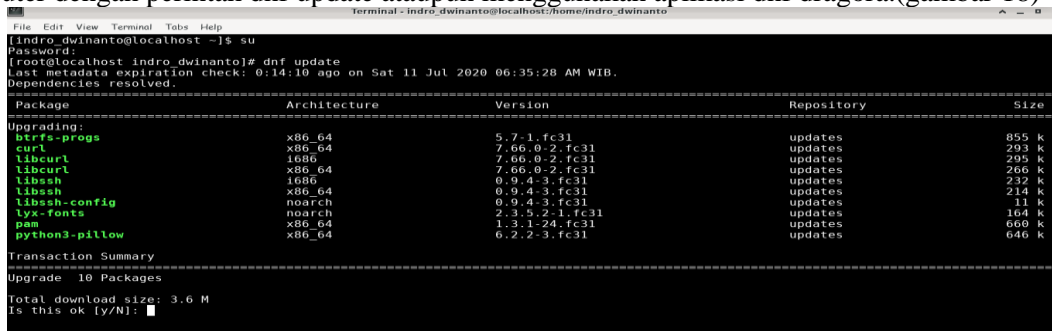
Seperti diketahui bahwa salah satu celah menembus keamanan komputer adalah melalui aplikasi yang ada di komputer, dalam hal pengurangan celah keamanan pada komputer melalui aplikasi mau tidak mau, setiap aplikasi yang ada di komputer harus diupdate untuk mengurangi bug-bug yang ada di suatu aplikasi. Salah satu metode yang digunakan adalah memperbaharui *patch* untuk menambal *bug-bug* yang ada pada OS dengan melakukan *update* sistem operasi.

Untuk pengguna komputer menggunakan OS Linux Fedora sudah disediakan pengingat bahwa komputer harus melakukan update aplikasi ataupun kernel linux (gambar 15)

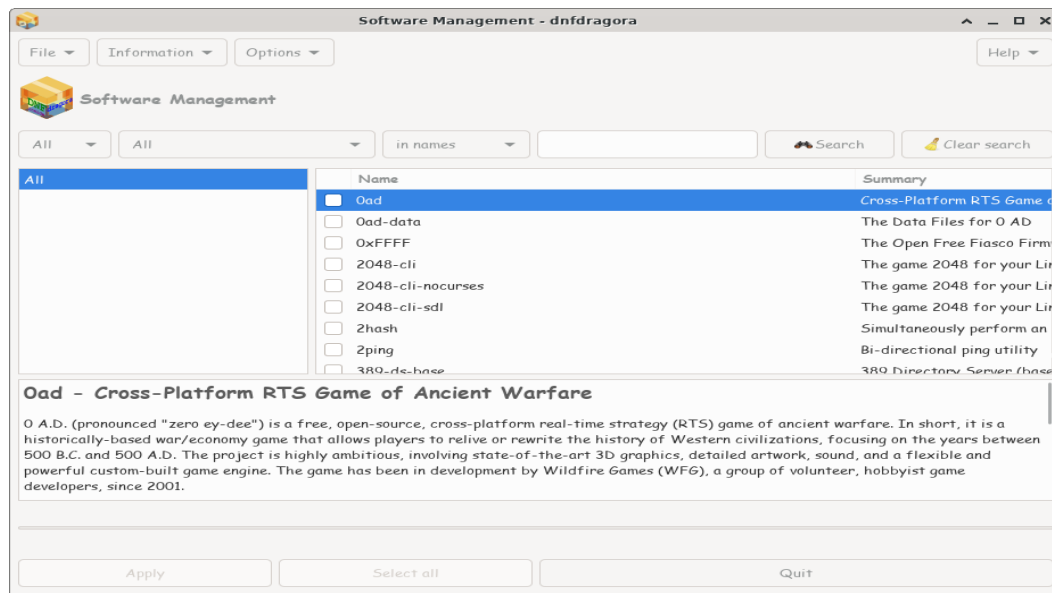


**Gambar 16.** Pengingat Update Aplikasi/kernel

Dalam pengupdatean aplikasi / kernel pada komputer menggunakan OS Fedora Linux dapat menggunakan 2 (dua) cara yaitu menggunakan terminal (gambar 17) dengan memerintahkan komputer dengan perintah `dnf update` ataupun menggunakan aplikasi `dnf dragora` (gambar 18)



**Gambar 17.** Update Aplikasi Menggunakan Terminal Linux



**Gambar 18.** Update Aplikasi Menggunakan Aplikasi dnf dragora

Selanjutnya melakukan audit sistem dengan bantuan tool Lynis Audit Sistem seperti langkah berikut.

```
File Edit View Terminal Tabs Help
[indro_dwinanto@192 ~]$ sudo lynis audit system
[sudo] password for indro_dwinanto:

[ Lynis 3.0.0 ]

#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2020, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
-----
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]
-----

Program version:      3.0.0
Operating system:    Linux
Operating system name: Fedora Linux
```

**Gambar 19.** Perintah awal *Tool Lynis Audit*

Berdasarkan data yang ada dapat ditampilkan summary Lynis Security Scan detail seperti gambar 20, dengan keterangan komponen firewall dan malware scanner ada.

```
File Edit View Terminal Tabs Help

Lynis security scan details:
Hardening index : 70 [#####]
Tests performed : 246
Plugins enabled : 0

Components:
- Firewall [V]
- Malware scanner [V]

Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

Lynis modules:
- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat
```

**Gambar 20.** Lynis security scan details

Dari keseluruhan data yang ditampilkan, disimpulkan bahwa keamanan komputer saat ini sedang dalam kondisi baik yang diterangkan sesuai gambar 21.

```
File Edit View Terminal Tabs Help

-[ Lynis 3.0.0 Results ]-

Great, no warnings

Suggestions (31):
-----
* Consider hardening system services [BOOT-5264]
- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each servic
e
https://cisofy.com/lynis/controls/BOOT-5264/

* If not required, consider explicit disabling of core dump in /etc/security/l
imits.conf file [KRNL-5820]
https://cisofy.com/lynis/controls/KRNL-5820/

* Check PAM configuration, add rounds if applicable and expire passwords to en
crypt with new values [AUTH-9229]
https://cisofy.com/lynis/controls/AUTH-9229/

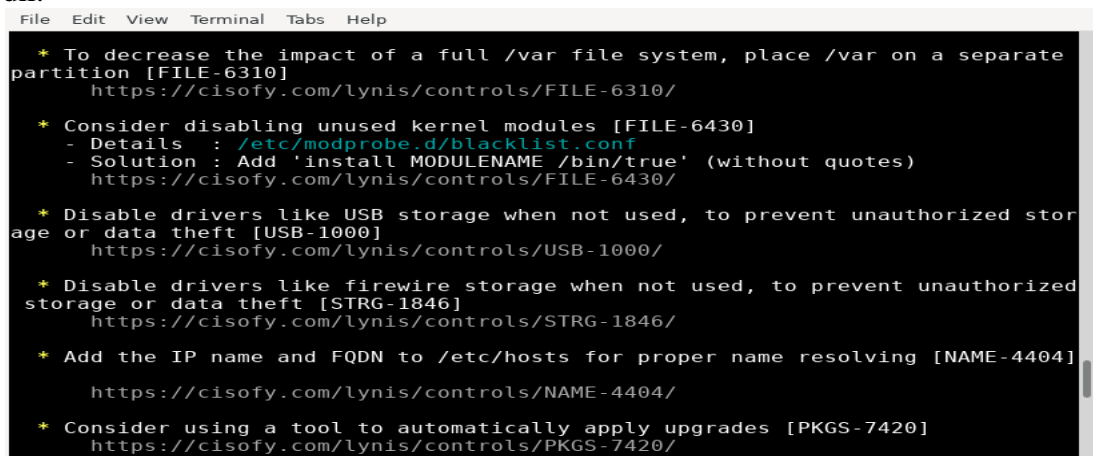
* Configure minimum encryption algorithm rounds in /etc/login.defs [AUTH-9230]
https://cisofy.com/lynis/controls/AUTH-9230/
```

**Gambar 21.** Lynis result

Berdasarkan dari gambar 20. komputer berada dalam kondisi baik dan ada beberapa saran yang Lynis berikan untuk keamanan sistem tambahan diantaranya sesuai gambar 21:

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 dll.



```
File Edit View Terminal Tabs Help
* To decrease the impact of a full /var file system, place /var on a separate
partition [FILE-6310]
  https://cisofy.com/lynis/controls/FILE-6310/
* Consider disabling unused kernel modules [FILE-6430]
  - Details   : /etc/modprobe.d/blacklist.conf
  - Solution  : Add 'install MODULENAME /bin/true' (without quotes)
  https://cisofy.com/lynis/controls/FILE-6430/
* Disable drivers like USB storage when not used, to prevent unauthorized stor
age or data theft [USB-1000]
  https://cisofy.com/lynis/controls/USB-1000/
* Disable drivers like firewire storage when not used, to prevent unauthorized
storage or data theft [STRG-1846]
  https://cisofy.com/lynis/controls/STRG-1846/
* Add the IP name and FQDN to /etc/hosts for proper name resolving [NAME-4404]
  https://cisofy.com/lynis/controls/NAME-4404/
* Consider using a tool to automatically apply upgrades [PKGS-7420]
  https://cisofy.com/lynis/controls/PKGS-7420/
```

Gambar 22. Contoh beberapa saran yang diberikan Lynis

#### 4. 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 memperbaharui 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 privilege* (root).
2. Penggunaan komputer dalam kegiatan sehari-hari haruslah diimbangi oleh *awareness* setiap pengguna akan artinya keamanan komputer. 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.
- Harjono, E. B. (2016). Analisa Dan Implementasi Dalam Membangun Sistem Operasi Linux Menggunakan Metode LSF Dan REMASTER. *Informatika*, I (1), 30–35.
- Kurniawan, Rudi. (2016). Analisis Dan Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode Ndlc (Network Development Life Cycle) Pada Bpu Bagas Raya Lubuklinggau. *Jurnal Ilmiah Betrik*, Vol. 07, No.01, April 2016
- Mulyadi, Deddy. (2015). *Study Kebijakan Publik dan Pelayanan Publik*. Bandung: Alfabeta.
- Revva, I., Jeinever, P., Rasyid, A., Suharto, N., Studi, P., Telekomunikasi, J., Elektro, T., & Negeri, P. (2018). jaringan dituntut bekerja lebih untuk dapat mengamankan jaringan komputer yang dikelolanya. Salah satu bentuk keamanan jaringan yang sering digunakan oleh seorang administrator jaringan dalam pengelolaan. 99–106.
- Suryana, Nanang, Susana Dwi Yulianti. (2021). Aplikasi Penjadwalan Manajemen Artis Daily Schedule (Studi Kasus: PT. Tetap Seratus Selamanya). *Jurnal Maklumatika* Vol. 7, No. 2, Januari 2021.
- Wijaya. (2014). *Internet untuk pemula (Familia (Ed.); Edition 2)*. Jakarta: Gramedia.