



**VSGA** Vocational School  
Graduate Academy

# Modul Pelatihan **JUNIOR CYBER SECURITY**

Vocational School Graduate Academy  
Digital Talent Scholarship  
Tahun 2023

## KATA PENGANTAR

Dunia saat ini berada pada era industri 4.0 yang lebih banyak menggunakan teknologi digital dan Indonesia telah mempersiapkan diri untuk masuk ke dalam tahap industri 4.0 tersebut melalui agenda percepatan transformasi digital. Salah satu langkah yang dilakukan dalam percepatan transformasi digital adalah penyiapan talenta digital. Laporan Bank Dunia tahun 2019 menyatakan bahwa Indonesia memiliki kekurangan 9 juta pekerja berketerampilan teknologi informasi dan komunikasi, sehingga perlu dilakukan penyiapan talenta digital untuk memenuhi kebutuhan tersebut dengan alokasi 600.000 orang setiap tahun. Upaya penyiapan talenta digital dilakukan oleh berbagai unsur baik pemerintah, institusi pendidikan, industri, komunitas masyarakat, maupun media publik.

Sejak tahun 2018, Kementerian Komunikasi dan Informatika melalui Badan Penelitian dan Pengembangan Sumber Daya Manusia menginisiasi Program Beasiswa Pelatihan Digital bernama *Digital Talent Scholarship* (DTS) yang telah berhasil dianugerahkan kepada lebih dari 300.000 penerima pelatihan bidang teknologi informasi dan komunikasi. Program *Digital Talent Scholarship* ini ditujukan untuk memberikan pelatihan dan sertifikasi berbagai tema pada bidang informatika, komunikasi, dan telekomunikasi, serta diharapkan melengkapi pemenuhan kebutuhan talenta digital Indonesia.

Program DTS tahun 2023 secara garis besar dibagi menjadi delapan akademi, salah satunya Vocational School Graduate Academy (VSGA). VSGA merupakan program pelatihan berbasis kompetensi kerja nasional bagi lulusan pendidikan vokasi SMK/ sederajat dan diploma bidang *Science, Technology, Engineering, Mathematics* (STEM) yang belum mendapatkan pekerjaan atau sedang tidak bekerja. Tujuan Program VSGA adalah menyiapkan talenta digital dengan standar kompetensi sesuai Standar Kompetensi Kerja Nasional Indonesia (SKKNI). Oleh karena itu, penyusunan modul pelatihan untuk Program VSGA disusun dengan berbasis pada kompetensi (*Competency Based Training*). Kami berpesan agar modul pelatihan berbasis kompetensi yang telah disusun ini dapat menjadi referensi bagi peserta dan pengajar agar pelatihan berjalan efektif dan efisien.

Selamat mengikuti Pelatihan *Digital Talent Scholarship*, mari persiapkan diri kita menjadi talenta digital Indonesia yang kompeten.

Jakarta, April 2023  
Kepala Badan Penelitian dan Pengembangan Sumber Daya Manusia  
Kementerian Komunikasi dan Informatika Republik Indonesia

**Dr. Hary Budiarto, M.Kom**

## Pendahuluan

Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menerapkan prinsip perlindungan informasi untuk pencegahan, deteksi, dan pengelolaan ancaman keamanan siber.

### A. Tujuan Umum

Setelah mempelajari modul ini peserta didik diharapkan mampu dalam menerapkan prinsip perlindungan informasi dengan benar.

### B. Tujuan Khusus

Adapun tujuan mempelajari unit kompetensi melalui buku modul akan mengumpulkan data ini guna memfasilitasi peserta didik sehingga pada akhir pelatihan diharapkan memiliki kemampuan sebagai berikut:

1. Mendefinisikan prosedur keamanan informasi yang tepat untuk tiap klasifikasi.
2. Mengidentifikasi kelemahan dari informasi dalam sistem komunikasi bisnis.
3. Menerapkan akses kontrol lingkungan Komputasi yang sesuai.
4. Mematuhi dan melaksanakan petunjuk yang terdapat pada dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi.
5. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem.

## Latar belakang

Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengumpulkan data untuk data science. Penilaian dilakukan dengan mengacu kepada Kriteria Unjuk Kerja (KUK) dan dilaksanakan di Tempat Uji Kompetensi (TUK), ruang simulasi atau workshop dengan cara:

- 1.1 Lisan
- 1.2 Wawancara
- 1.3 Tes tertulis
- 1.4 Demonstrasi
- 1.5 Metode lain yang relevan

## Deskripsi Pelatihan

Materi Pelatihan ini memfasilitasi pembentukan kompetensi dalam menentukan kebutuhan teknis penerapan prinsip perlindungan informasi.

## Tujuan Pembelajaran

Setelah mengikuti pelatihan ini, peserta mampu menentukan kebutuhan teknis penerapan prinsip perlindungan informasi.

## Kompetensi Dasar

Mampu menentukan kebutuhan teknis penerapan prinsip perlindungan informasi.

## Indikator Hasil Belajar

Ketepatan dalam melakukan proses pengambilan data sesuai dengan *tools* yang telah disiapkan.

## INFORMASI PELATIHAN

INFORMASI PELATIHAN	
Akademi	VSGA untuk Junior Cyber Security
Pelaksana Pelatihan	Kementerian Komunikasi dan Informatika
Tema Pelatihan	<b><i>Junior Cyber Security</i></b>
Sertifikasi	Sertifikasi kompetensi BNSP <i>Junior Cyber Security</i>
Deskripsi Pelatihan	Pelatihan ini menyiapkan peserta agar kompeten dalam melaksanakan pekerjaan <i>junior cyber security</i> yang dapat membantu pekerjaan praktisi <i>cyber security</i> . Kualifikasi pada jabatan ini menuntut seseorang memiliki kompetensi dalam menerapkan prinsip perlindungan informasi, menerapkan prinsip keamanan informasi untuk penggunaan jaringan internet, menerapkan prinsip keamanan informasi pada transaksi elektronik, melaksanakan kebijakan keamanan informasi, mengaplikasikan ketentuan/persyaratan keamanan informasi, mengelola log, dan menerapkan kontrol akses berdasarkan konsep/metodologi yang telah ditetapkan
Output Pelatihan	Setelah mengikuti pelatihan peserta akan mampu menganalisis dan memvisualisasikan data sehingga dapat digunakan dalam pengambilan keputusan
Durasi Pelatihan	24 JP (3 hari)

INFORMASI PELATIHAN	
Jenis Pelatihan	<b>Luring /Offline (40% Pengetahuan - 60% Praktek)</b>
Persyaratan Peserta	<ul style="list-style-type: none"> <li>• Warga Negara Indonesia</li> <li>• Usia Maksimal 29 Tahun pada saat mendaftar</li> <li>• Lulus Pendidikan D3 Bidang TIK/SMK Bidang (TKJ/TI/RPL) yang pernah bekerja minimal 3 tahun</li> <li>• Belum Mendapatkan Pekerjaan Tetap/Pernah Bekerja tapi sedang tidak bekerja</li> <li>• Lolos Seleksi Administrasi dan Tes Substansi</li> </ul>
Persyaratan Sarana Peserta	Laptop/PC dengan spesifikasi: <ul style="list-style-type: none"> <li>• RAM minimal 4 GB</li> <li>• 32/64-bit processor</li> <li>• Operating System Windows 7,8,10, Linux, atau MAC OSX</li> <li>• konektivitas WiFi</li> <li>• Akses Internet Dedicated 256 kbps per peserta per perangkat</li> </ul>
Kriteria Pengajar/ <i>Trainer</i> /Instruktur:	<ol style="list-style-type: none"> <li>1. Minimal Lulusan S2 di bidang TIK; atau Memiliki kompetensi Okupasi Nasional "<i>Junior Cyber Security</i>".</li> <li>2. Pengalaman Kerja diutamakan sebagai tenaga pengajar Pelatihan Bidang TIK minimal selama 2 tahun</li> <li>3. Telah mengikuti pelatihan <i>training of trainner Junior Cyber Security</i></li> </ol>
Tim Penyusun:	<ol style="list-style-type: none"> <li>1. Yan Hadynoer (BSSN)</li> <li>2. Yoyok Darmanto (BSSN)</li> </ol>

## INFORMASI PEMBELAJARAN

RENCANA PELATIHAN		
Pertemuan	Topik	Aktivitas
<b>Hari 1</b>	<ul style="list-style-type: none"> <li>• Pembukaan dan Penjelasan Rencana Pembelajaran</li> <li>• Pre test</li> </ul>	Pemaparan materi, diskusi dan <i>hands-on lab live class 1 JP</i>
	Pengantar <i>Junior Cyber Security</i> (Posisi dan peran <i>junior cyber security</i> )	Pemaparan materi, diskusi dan <i>hands-on</i>

RENCANA PELATIHAN		
Pertemuan	Topik	Aktivitas
		<i>lab live class 1 JP</i>
	Persiapan alat bantu (tools) pelatihan <ul style="list-style-type: none"> <li>- Bit-to-Bit Copy</li> <li>- SET Toolkit</li> <li>- Event Viewer</li> <li>- Virtual Machine</li> </ul>	Pemaparan materi, diskusi dan <i>hands-on lab live class 1 JP</i>
	<b>Menerapkan prinsip perlindungan informasi</b> <ol style="list-style-type: none"> <li>1. Mendefinisikan prosedur keamanan informasi yang tepat untuk tiap klasifikasi</li> <li>2. Mengidentifikasi kelemahan dari informasi dalam sistem komunikasi bisnis</li> <li>3. Menerapkan akses kontrol lingkungan Komputasi yang sesuai</li> <li>4. Mematuhi dan melaksanakan petunjuk yang terdapat pada dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi</li> <li>5. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem.</li> </ol>	Pemaparan materi, diskusi dan <i>hands-on lab live class 2 JP</i>
	<b>Menerapkan prinsip keamanan informasi untuk penggunaan jaringan internet</b> <ol style="list-style-type: none"> <li>1. Mematuhi dan menerapkan kebijakan dan prosedur keamanan informasi yang terkait dengan penggunaan jaringan internet</li> <li>2. Mengidentifikasi tipe kelemahan dan jenis-jenis serangan dalam jaringan internet</li> <li>3. Mengaplikasikan penggunaan jaringan internet secara aman</li> </ol>	Pemaparan materi, diskusi dan <i>hands-on lab live class 3 JP</i>

RENCANA PELATIHAN		
Pertemuan	Topik	Aktivitas
Hari 2	<b>Menerapkan prinsip keamanan informasi pada transaksi elektronik</b> <ol style="list-style-type: none"> <li>1. Mengidentifikasi dan memenuhi kebutuhan terkait kerahasiaan, integritas, bukti dari pengguna dokumen kunci dan kontrak yang diakui</li> <li>2. Menetapkan aspek-aspek transaksi</li> <li>3. Melaksanakan dan memantau perlindungan keamanan untuk sistem infrastruktur dan penggunaan teknologi informasi sesuai dengan rencana implementasi dan prosedur operasi standar</li> </ol>	Pemaparan materi, diskusi dan <i>hands-on lab live class</i> 3 JP
	<b>Melaksanakan kebijakan keamanan informasi</b> <ol style="list-style-type: none"> <li>1. Mengidentifikasi aset penting dalam organisasi</li> <li>2. Memproteksi aset penting dalam organisasi</li> <li>3. Melakukan pemantauan terhadap aktivitas yang rentan ancaman</li> </ol>	Pemaparan materi, diskusi dan <i>hands-on lab live class</i> 2 JP
	<b>Mengaplikasikan ketentuan/persyaratan keamanan informasi</b> <ol style="list-style-type: none"> <li>1. Mengaplikasikan persyaratan untuk program yang spesifik untuk keamanan lingkungan komputasi guna mengidentifikasi kelemahan/kerentanan</li> <li>2. Menyediakan masukan tentang hal yang terkait dengan persyaratan keamanan untuk dimasukkan dalam laporan pekerjaan dan dokumen-dokumen pengadaan terkait</li> <li>3. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem</li> <li>4. Mengidentifikasi persyaratan keamanan dalam prosedur operasi di</li> </ol>	Pemaparan materi, diskusi dan <i>hands-on lab live class</i> 3 JP



RENCANA PELATIHAN		
Pertemuan	Topik	Aktivitas
	lingkungan komputasi 5. Menyusun persyaratan keamanan untuk perangkat keras, piranti lunak, dan penggunaan layanan yang spesifik untuk program keamanan jaringan 6. Mengevaluasi dan/atau menyetujui persyaratan keamanan yang relevan terhadap kemampuan teknologi informasi yang baru	
Hari 3	<b>Mengelola log</b> 1. Menetapkan kebijakan pencatatan <i>log</i> untuk menyertakan peristiwa penting 2. Melakukan kontrol berkas <i>log</i> terhadap kemungkinan diubah atau dihapus 3. Melakukan kontrol tempat menyimpan media file pencatatan terhadap kemungkinan penuh sehingga terjadi kegagalan ketika mencatat kejadian yang terjadi	Pemaparan materi, diskusi dan <i>hands-on lab live class 4 JP</i>
	<b>Menerapkan kontrol akses berdasarkan konsep/metodologi yang telah ditetapkan</b> 1. Menerapkan kontrol akses lingkungan komputasi yang sesuai 2. Melaksanakan kebijakan organisasi dan kebijakan <i>password</i> organisasi 3. Mengelola akun hak jaringan dan hak akses ke sistem jaringan dan infrastrukturnya 4. Mengimplementasikan peringatan secara online untuk menginformasikan para pengguna atas peraturan akses dari seluruh infrastruktur dan penggunaan sistem teknologi informasi 5. Menyusun prosedur untuk memastikan pengguna sistem menyadari tanggung jawab keamanan mereka sebelum memberikan akses ke sistem informasi organisasi 6. Melakukan kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi	Pemaparan materi, diskusi dan <i>hands-on lab live class 4 JP</i>



RENCANA PELATIHAN		
Pertemuan	Topik	Aktivitas
	keamanan agar menerima pelatihan keamanan dasar dan berkelanjutan serta mendapatkan sertifikasi yang sesuai untuk melaksanakan tugas keamanan	

#### Materi Pokok

1. Mendefinisikan prosedur keamanan informasi yang tepat untuk tiap klasifikasi.
2. Mengidentifikasi kelemahan dari informasi dalam sistem komunikasi bisnis.
3. Menerapkan akses kontrol lingkungan Komputasi yang sesuai.
4. Mematuhi dan melaksanakan petunjuk yang terdapat pada dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi.
5. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem.

#### Sub Materi Pokok

- 1.1. Keamanan Informasi
- 1.2. Aspek Keamanan Informasi
- 1.3. Persyaratan Keamanan Informasi
- 1.4. Teknik dalam menjaga Keamanan Informasi
- 2.1. Sistem Komunikasi
- 2.2. Kelemahan pada Sistem Komunikasi
- 2.3. Keamanan dalam Sistem Komunikasi
- 3.1. Sistem Akses Kontrol
- 3.2. Sistem Log
- 4.1. Taksonomi Cybersecurity
- 4.2. Deskripsi Kerangka dan Standar Keamanan Informasi
- 5.1. Mengenali Log
- 5.2. Analisa Log



## 1. MENDEFINISIKAN PROSEDUR KEAMANAN INFORMASI YANG TEPAT UNTUK TIAP KLASIFIKASI

### 1.1 Keamanan Informasi

Informasi merupakan sekumpulan data yang tersusun sistematis sehingga memiliki makna yang dapat diinterpretasikan. Informasi saat ini bukan hanya tersaji dalam bentuk fisik, namun lebih banyak tersaji dalam format elektronik akibat pengaruh global era digitalisasi. Dikarenakan sifat informasi itu sendiri yang memiliki muatan nilai dan makna, maka menjadi berharga di saat sekarang ini pada era digitalisasi. Oleh karena itu, data dan informasi menjadi target potensial yang disasar untuk diambil secara tidak sah oleh orang-orang yang tidak berhak memilikinya.

Di dalam ilmu teknologi informasi, telah banyak dikenal istilah keamanan informasi sebagai sebuah bentuk proteksi dan perlindungan terhadap sumber dan ketersediaan informasi atas akses yang tidak sah, pencurian, kerusakan, ataupun serangan lainnya. Keamanan informasi itu sendiri memiliki beberapa tujuan, diantaranya sebagai berikut:

#### a. Pencegahan

Mencegah terjadinya tindakan berupa akses tidak sah terhadap data dan informasi menjadi prioritas utama dalam keamanan informasi. Ini berkaitan dengan risiko keamanan yang dapat terjadi terhadap data dan informasi akibat adanya ancaman dan celah keamanan.

#### b. Deteksi

Mengawasi adanya anomali dan ancaman yang dapat terjadi pada keamanan data dan informasi, seperti akses tidak sah atau pencurian informasi. Selain itu, juga dilakukan pemindaian terhadap sistem sebagai bentuk investigasi dalam menelusuri anomali dan ancaman keamanan tersebut.

#### c. Pemulihan

Serangan terhadap sistem dapat menyebabkan kerusakan ataupun kehilangan data dan informasi di dalamnya. Selain itu, bencana alam juga dapat mengakibatkan kerusakan dan kehilangan data secara fisik. Untuk itu, pemulihan data dan informasi yang rusak atau hilang sangat dibutuhkan untuk menjaga keberlangsungan sistem.

### 1.2 Aspek Keamanan Informasi

Keamanan informasi tersusun dari sejumlah aspek yang disyaratkan, apabila salah satu aspek tidak dapat terpenuhi maka dapat dikatakan terjadi kegagalan dalam menerapkan keamanan informasi. Aspek-aspek tersebut juga dikenal dengan istilah prinsip keamanan, diantaranya adalah:

#### a. *Confidentiality* (Kerahasiaan)

Jaminan keamanan berupa pen jagaan akan data dan informasi (baik ketika diproduksi, dikirimkan dan disimpan) terhadap akses yang tidak sah. Beberapa contoh data yang diperlukan jaminan kerahasiaan, anatara lain seperti data kerahasiaan militer, riwayat Kesehatan pribadi, transaksi perbankan, dan sebagainya.

#### b. *Integrity* (Keutuhan)

Jaminan keamanan berupa pen jagaan terhadap akurasi data, dimana tidak ada perubahan, modifikasi ataupun kerusakan yang

mengakibatkan terjadinya error pada data. Dalam sudut pandang lain, dapat dikatakan data terjamin keutuhannya tanpa ada perubahan sekecil apapun di dalamnya.

c. *Availability* (Ketersediaan)

Jaminan keamanan berupa penjagaan terhadap ketersediaan data dan informasi, sehingga data selalu tersedia ketika data tersebut dibutuhkan atau diakses melalui sistem.

### 1.3 Persyaratan Keamanan Informasi

Keamanan terhadap data dan informasi dilakukan berdasarkan bagaimana siklus data dan informasi tersebut berjalan, mulai dari data diproses sampai dengan dihapus, maka persyaratan keamanan perlu didefinisikan.

a. Pemrosesan

Lingkungan pemrosesan data dan informasi perlu mendapatkan perlindungan keamanan. Persyaratan keamanan yang dibutuhkan antara lain adalah dengan membentuk lingkungan pemrosesan yang aman. Pemrosesan secara umum terjadi di dalam sistem operasi, sehingga bentuk pengamanan yang dapat diterapkan, contohnya antara lain adalah dengan menerapkan otentikasi akun OS, menjalankan anti-virus, ataupun melakukan backup data di dalam OS.

b. Penyimpanan

Ketika data disimpan maka bentuk persyaratan keamanan yang dibutuhkan adalah hak akses terhadap data dengan penerapan otentikasi dan enkripsi, keutuhan data dengan menerapkan *data checksum*, dan juga melakukan *backup* berkala untuk menjaga ketersediaan data di dalam media penyimpanan.

c. Pengiriman

Transmisi data berkaitan erat dengan penggunaan jaringan komputer, sehingga persyaratan keamanan yang dibutuhkan adalah dengan menerapkan fungsi keamanan pada interkoneksi jaringan, contohnya antara lain adalah dengan menerapkan enkripsi komunikasi jaringan dengan teknologi VPN untuk menjaga kerahasiaan ketika proses pengiriman. Selain itu, jaminan keutuhan data tetap diperlukan untuk memastikan data terkirim dalam bentuk yang akurat tanpa ada modifikasi dan perubahan dengan menerapkan *data checksum*.

d. Penghapusan

Penghapusan data menjadi bagian yang tidak dapat dikesampingkan untuk dijaga keamanannya. Apabila proses penghapusan dilakukan sembarangan, maka data secara digital akan bisa direkonstruksi, walaupun sudah dihapus. Salah satu tindakan yang dapat dilakukan adalah dengan menerapkan teknologi *data shredding/wipping*, dimana data dihapus secara menyeluruh terhadap keseluruhan bit pendukungnya, sehingga akan sulit untuk direkonstruksi ulang menjadi data utuh.

### 1.4 Teknik dalam Menjaga Keamanan Informasi

Untuk menjamin aspek keamanan informasi dapat terjaga, maka dipergunakan beberapa teknik untuk mendukung masing-masing prinsip keamanan yang telah didefinisikan (*confidentiality, integrity, dan availability*).

a. *Confidentiality* (Kerahasiaan)

Prosedur teknis yang dapat diterapkan untuk menjaga keamanan kerahasiaan data dan informasi, dapat dilakukan dalam bentuk:

- Akses Kontrol



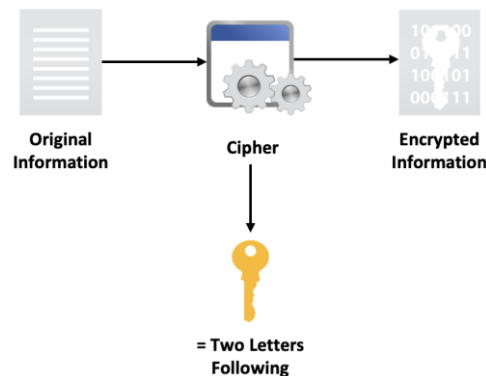
Gambar 1. Tahapan dalam Skema Akses Kontrol

Akses kontrol berkaitan erat dengan proses dalam menentukan dan memberikan hak akses untuk sebuah objek, sumber daya, ataupun data. Komponen di dalam akses kontrol dapat dibagi ke dalam 3 tahap, yaitu identifikasi, otentikasi dan otorisasi.

- Identifikasi berkaitan dengan penentuan asosiasi dan relasi antara identitas dengan sumber daya objek data yang dikelola. Contohnya adalah seperti alamat email, username, password, alamat IP, NIK, dan lain sebagainya.
- Otentikasi merupakan metode untuk validasi sebuah entitas melalui identitasnya dengan parameter keamanan yang sudah direlasikan, seperti (username-password, ID-PIN, name-key, dan lain sebagainya)
- Otorisasi  
Otorisasi menjadi tahapan selanjutnya, setelah identifikasi dan otentikasi berhasil dilakukan, dimana sistem akan mengenali hak akses yang sudah ditetapkan untuk diberikan kewenangan akses tersebut yang sudah terotentikasi kepada objek, data ataupun sistem.

- Enkripsi

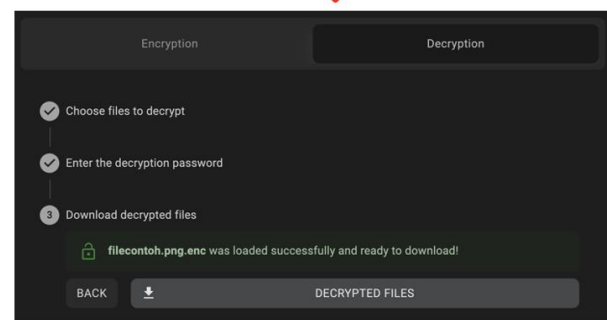
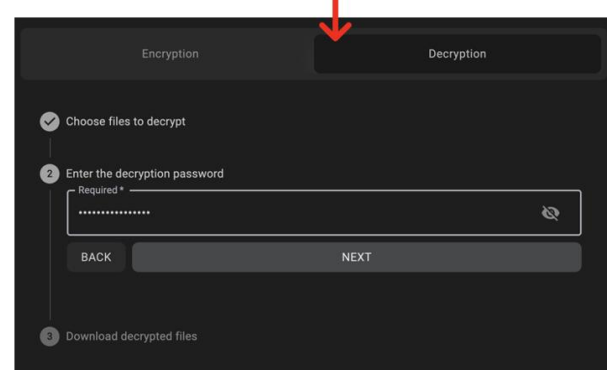
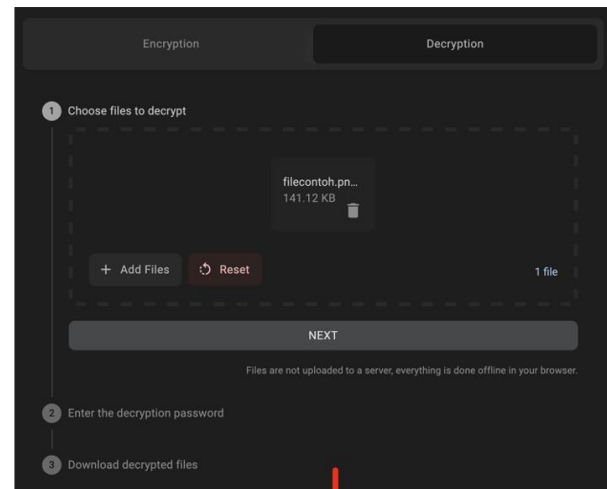
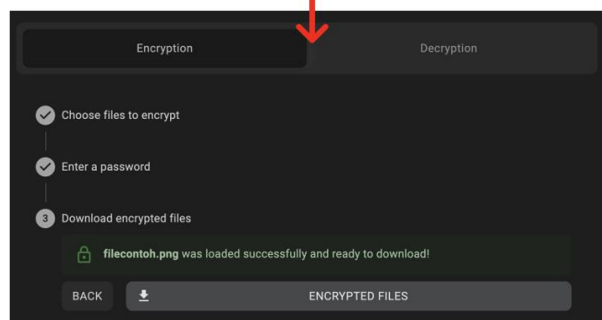
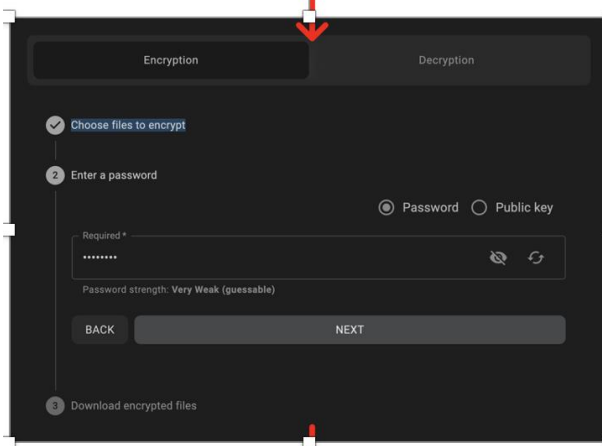
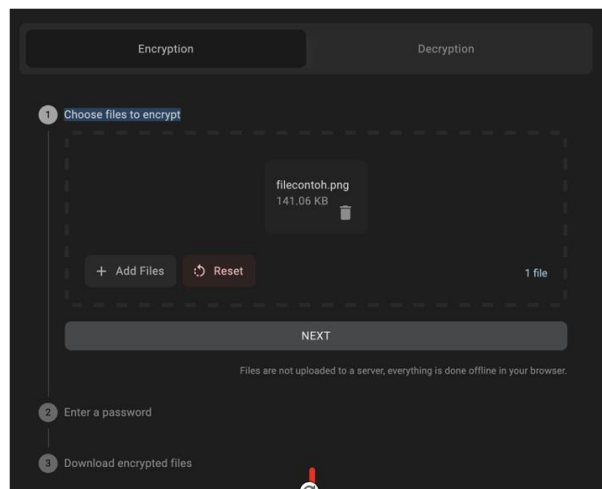
Enkripsi merupakan teknik keamanan yang dapat digunakan untuk menyembunyikan data dari bentuk asli menjadi bentuk lain yang tidak memiliki nilai informasi, sehingga hanya pihak yang sah saja yang dapat mengetahui nilai informasi tersebut.



Gambar 2. Fungsi Enkripsi

Banyak aplikasi yang dapat dimanfaatkan untuk melakukan fungsi enkripsi, salah satunya adalah menggunakan aplikasi enkripsi *file* yang dapat diakses secara *online* melalui alamat situs <https://hat.sh/>. Berikut langkah-langkah penggunaan aplikasi enkripsi tersebut.

- 1) Buka aplikasi *browser*, dan akses ke alamat situs <https://hat.sh/>
- 2) Pilih menu **Encryption** atau **Decryption**
- 3) Pilih file yang akan dienkripsi atau didekripsi
- 4) Masukkan kunci (dalam aplikasi ini digunakan *password*)
- 5) Proses enkripsi atau dekripsi selesai, hasilnya dapat langsung diunduh



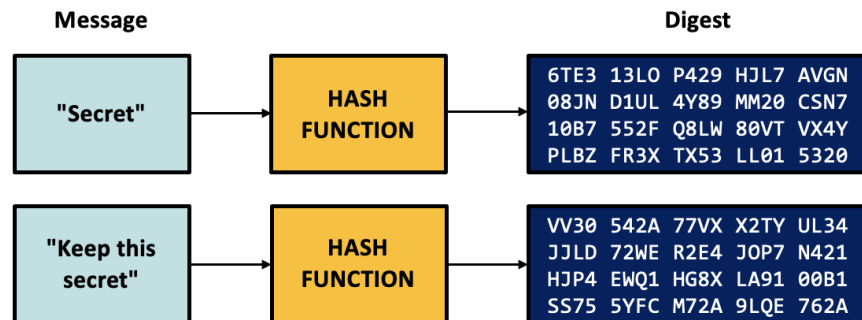
Gambar 3. Penggunaan fungsi enkripsi untuk sebuah *file*

b. *Integrity* (Keutuhan)

Prosedur teknis yang dapat diterapkan untuk menjaga keamanan keutuhan data dan informasi, dapat dilakukan dalam bentuk:

- Fungsi Hash

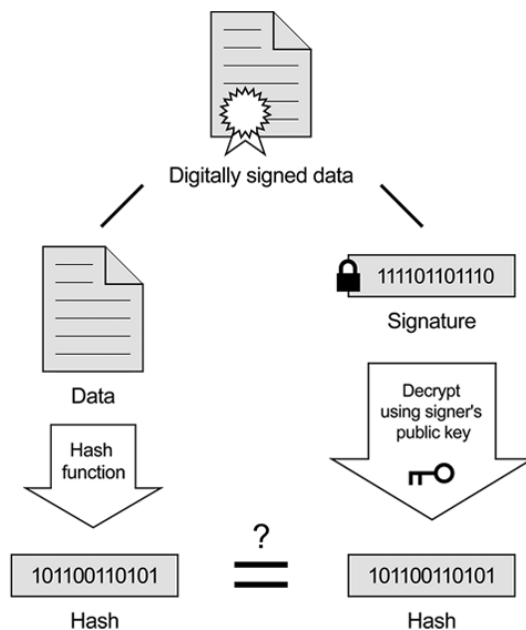
Proses yang menjalankan fungsi dimana fungsi tersebut dapat melakukan perubahan data dari bentuk aslinya menjadi bentuk lain dalam ukuran yang selalu seragam, dan tidak dapat dibalikkan seperti pada teknik enkripsi.



Gambar 4. Fungsi Hash

- *Digital Signature*

*Digital signature* merupakan proses pengimbuhan tanda tangan secara digital dengan menggunakan *certificate* sebagai parameter validasinya. Proses ini memberikan jaminan keamanan untuk sebuah data terhadap ancaman perubahan dan modifikasi data, karena apabila data berubah satu bit saja, maka data tersebut tidak akan tervalidasi sebagai data yang benar dan mengindikasikan telah terjadi perubahan data di dalamnya.

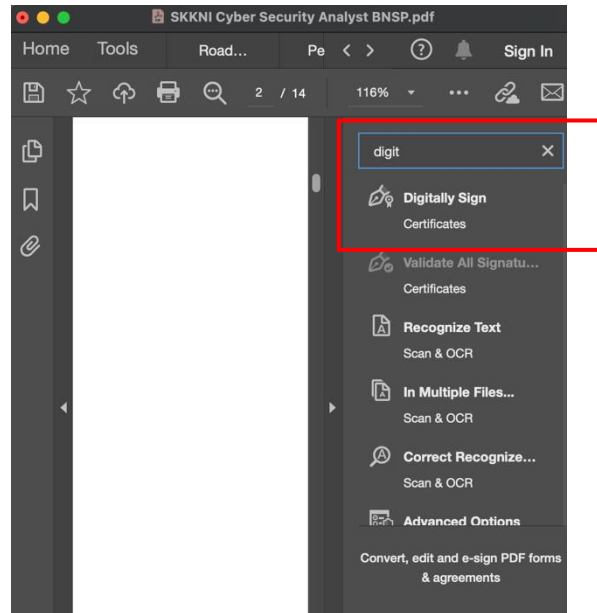


Gambar 5. Proses *Digital Signing*



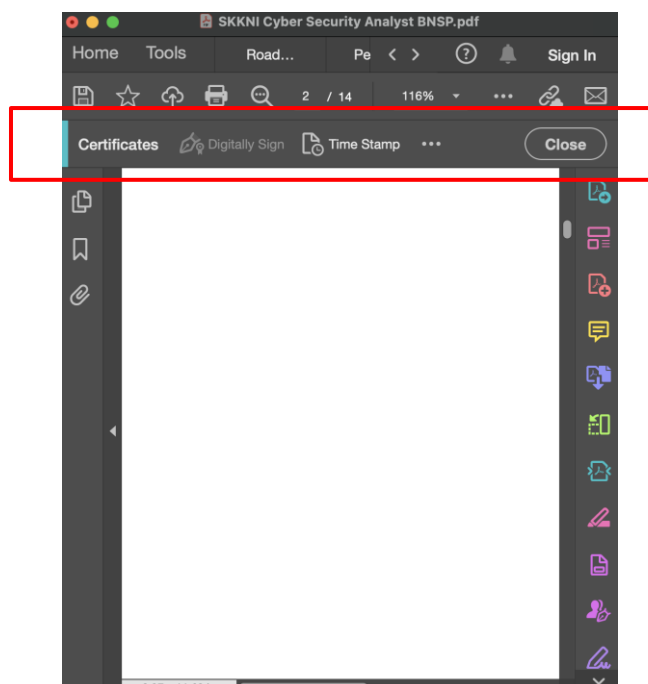
Banyak aplikasi yang dapat dimanfaatkan untuk menerapkan *digital signature*, salah satunya adalah menggunakan aplikasi Adobe Acrobat PDF dengan melakukan langkah-langkah berikut.

- 1) Buka aplikasi Adobe Acrobat PDF, dan buka sebuah file PDF yang hendak diterapkan *digital signature*
- 2) Pada panel *search*, masukan kata pencarian “**Digitally Sign**”



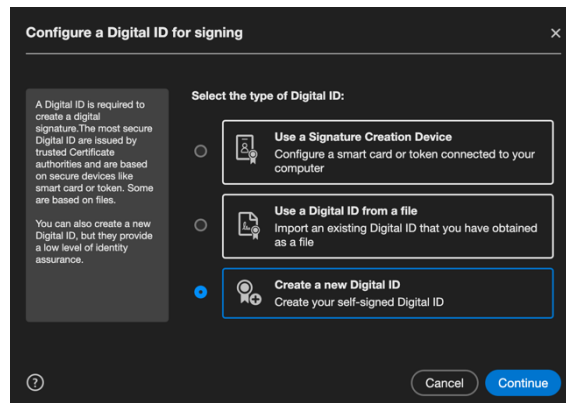
Gambar 6. Panel *search* untuk mencari menu **Digitally Sign**

- 3) Pada halaman *digitally sign*, arahkan kursor ke dalam file PDF kemudian klik di sembarang tempat untuk memunculkan menu *signing*



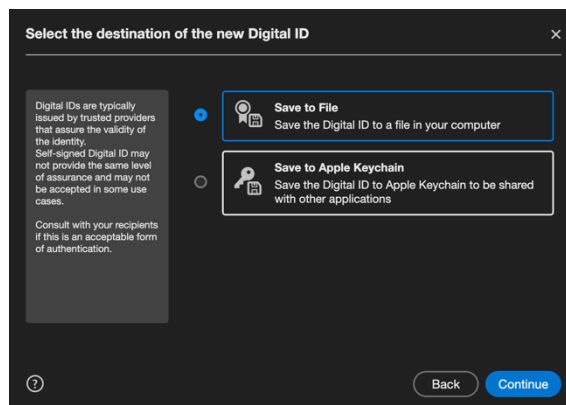
Gambar 7. Tampilan pada halaman **Digitally Sign**

4) Pilih menu **Create a New Digital ID**



Gambar 8. *Dialog box* untuk membuat digital ID (1)

5) Pilih menu **Save to File**

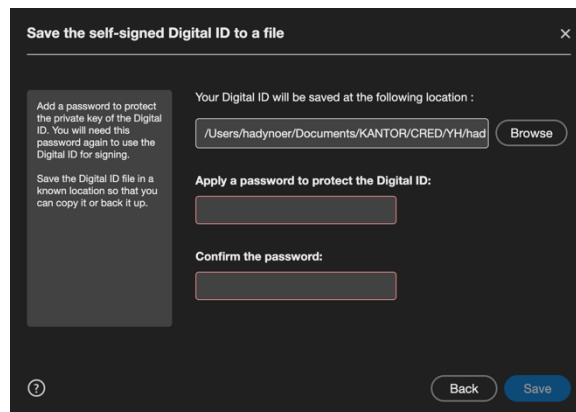


Gambar 9. *Dialog box* untuk membuat digital ID (2)

6) Isikan data diri

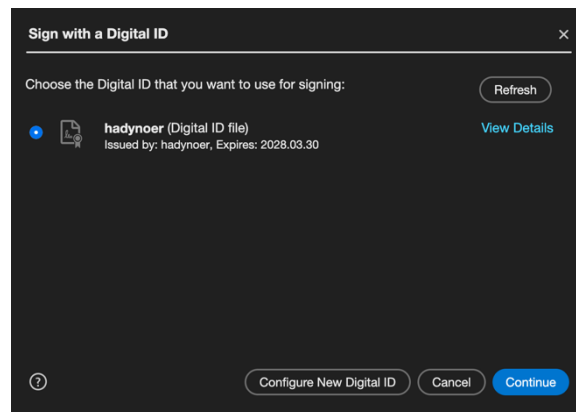
Gambar 10. *Dialog box* untuk membuat digital ID (3)

7) Buat *password* untuk *signature*, kemudian **Save**



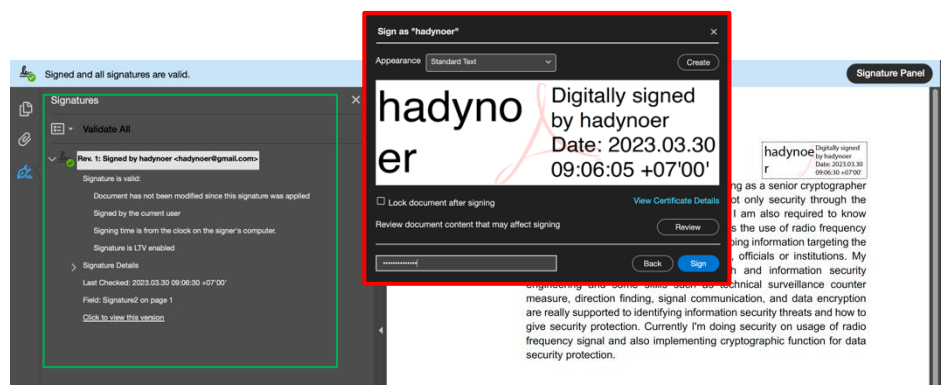
Gambar 11. *Dialog box* untuk membuat digital ID (4)

8) Pilih Digital ID yang tadi telah dibuat



Gambar 12. *Dialog box* untuk pemilihan digital ID untuk **Sign**

9) Masukkan *password* dan lakukan proses **Sign**



Gambar 13. Proses **Sign** (kotak merah) dan hasil validasi (kotak hijau)

c. *Availability* (Ketersediaan)

Prosedur teknis yang dapat diterapkan untuk menjaga keamanan keutuhan data dan informasi, dapat dilakukan dalam bentuk:

- *Redudancy*

Redudansi merupakan penggunaan dua model pelayanan data yang identik satu dengan yang lainnya, hal ini dimaksudkan untuk menjaga apabila salah satu pelayanan data putus/*off*, maka layanan tetap dapat diberikan karena masih ada salah satu yang tetap tersambung/*on*. Redudansi ini dapat dikonfigurasi pada perangkat *hardware* ataupun *software*.

- *Backup*

*Backup* merupakan pencadangan yang diberlakukan pada sebuah objek, data ataupun sistem. Pencadangan tersebut dimaksudkan untuk menjaga ketersediaan objek, data ataupun sistem walaupun terjadi kesalahan atau error pada objek, data atau sistem yang sedang berjalan. Secara umum, *backup* dilakukan secara berkala untuk meminimalisir kehilangan data yang besar akibat ancaman dan serangan keamanan yang tidak dapat diprediksi kejadiannya.

## 2. MENGIDENTIFIKASI KELEMAHAN DARI INFORMASI DALAM SISTEM KOMUNIKASI BISNIS

### 2.1 Sistem Komunikasi

Sistem komunikasi bisnis didefinisikan secara digital dalam berbagai bentuk berdasarkan lapisan protokol untuk komunikasi yang digunakan, diantaranya sebagai berikut:

#### a. email

*email* merupakan layanan di dalam jaringan komputer yang dipergunakan untuk melakukan kirim-terima berita dari satu alamat IP ke alamat IP lainnya melalui pemanfaatan protokol Simple Mail Transfer Protocol (SMTP). Komponen di dalam email tersusun atas beberapa parameter, diantaranya yang menjadi atensi dalam konteks keamanan adalah parameter berikut:

- **Received form**, memberikan informasi tentang siapa pengirim email yang sesungguhnya, karena bisa saja dipalsukan.
- **Deliver to**, memberikan informasi tentang siapa penerima email yang sesungguhnya.
- **Return path**, memberikan informasi mengenai dari domain alamat email mana sesungguhnya email dikirimkan.

```
Delivered-To: hadynoer@gmail.com
Received: by 2002:a5d:4a8e:0:0:0:0 with SMTP id o14csp91922wrq;
Wed, 21 Dec 2022 18:43:10 -0800 (PST)
X-Goog-Smtp-Source: ANRXd3saoC579qVc/Dx3Yj87GT+9jmB3PosqW03290k9aF9Jm90EhtB6DihKv4zPWTuinnYiygW
X-Received: by 2002:a81:4f87:0:100:308:05f4:4343 with SMTP id
d129-2002a814f8700000b003d885f44343mr3721827ywb.4.1671676998358;
Wed, 21 Dec 2022 18:43:10 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1671676998; cv=none;
d=google.com; s=arc-20160816;
b=MeKEoaErl+8WTKSE0cbKf/pevMHQ/PANkVg7UqVdG1cJqW05s3Mvgalnt0vh3g
r4Der7gOP/m32WJNGVbTVLU/u3wqLB6Er8054Y84sP7e645w3BuB4VId0pAKw4d0
Y6Gf/rPicyG5n8bY2N0B8/buPwW/T5DmGfFduhhr/0erLmB3d4Tptsc1Xqx
6BqLGfNwA03Vmxq9pNw0Gm5YKqCvPap7uJX29q6Vts8gLB3D1lgPS+Sobxr4V0Pe7
7PtaAa1NusFwB39ALU9fYUg80TmUdLTvdLTW8N41D08kgGbkVvF+dqzSsJ/1wT/TrE9
BwGm=
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=to:reply-to:subject:message-id:mime-version:from:date
:content-transfer-encoding:dkim-signature:dkim-signature;
bh=MeopC/nZandvK7hQdwaZEn0p8U085Mtk3eJ04e;
b=rFlubNE8j+4nEg5EUHxrk+4303yzh1Ckx14/vs8LDg4Tkkq5gatyg5Tm1hcABHGe
PdVz9Qk+uDIqsvQ5uqVX+3985o8Lq6vYAngV/pRKCag4ChrLZ1LldqAHZRH+tx9
Azw6A2UnNw7u723YCYAp1bJRCNcy+5r1ehw0Mq7hKVB4s2JUgycbdtz2svC5m7
pqj0e05da8GktbavMTQsa3G+natt53LqsBBb10g8Uc0NPfV1PeYAvbb9CfuyZhc4
yz73kjQmgokABK/71K4h0KasBN5n/U41LkIMkThL/CfnbjP6c1PqaET2qb4lv5ZGF
f6Gm=
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@imgsecurity.com header.s=m1 header.b="t/Gbga66";
dkim=pass header.i=@sendgrid.info header.s=smtapi header.b=J0beKdGT;
spf=pass (google.com: domain of bounces+23182037-83a6-hadynoer@gmail.com@sg.imgsecurity.com
designates 167.89.108.176 as permitted sender) smtp.mailfrom="bounces+23182037-83a6-
hadynoer@gmail.com@sg.imgsecurity.com";
dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=imgsecurity.com
Return-Path: bounces+23182037-83a6-hadynoer@gmail.com@sg.imgsecurity.com
Received: from xtrwsqbh.outbound-mail.sendgrid.net (xtrwsqbh.outbound-mail.sendgrid.net. [167.89.108.176])
by mx.google.com with ESMTPS id
d197-2002a814f8e00000b003f67597f117459988ywd.105.2022.12.21.18.43.09
for <hadynoer@gmail.com>
(version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
Wed, 21 Dec 2022 18:43:10 -0800 (PST)
```

Gambar 14. Rincian pada pesan *email*

#### b. file transfer

*file transfer* merupakan layanan di dalam jaringan komputer yang dipergunakan untuk melakukan kirim-terima *file* secara langsung dari satu komputer ke komputer lainnya melalui pemanfaatan protokol File Transfer Protocol (FTP). Layanan pengiriman *file* ini dapat menjadi alternatif pilihan yang banyak digunakan untuk kirim terima *file* di dalam jaringan komputer dengan ukuran besar yang secara umum tidak dapat dikirimkan melalui layanan email.

#### c. Protokol Sistem Komunikasi Lainnya

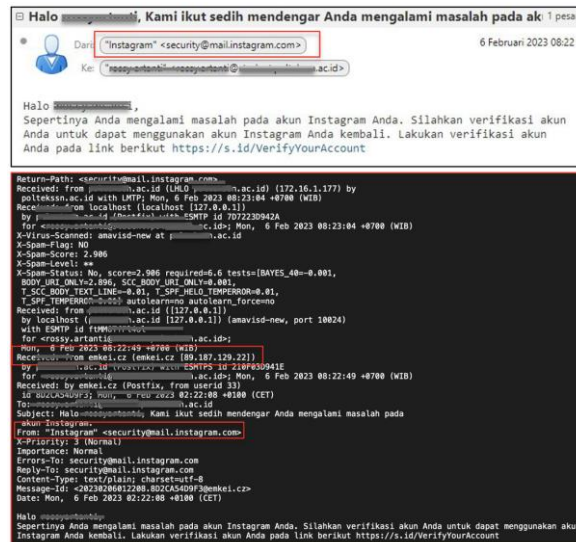
Masih terdapat banyak protokol lainnya yang dapat dipergunakan untuk menjalankan layanan komunikasi data dan informasi, diantaranya seperti telnet dan SSH untuk akses secara *remote*, SNMP untuk komunikasi utilitas, IRC untuk pertukaran pesan, dan lain sebagainya.

### 2.2 Kelemahan pada Sistem Komunikasi

Sebuah sistem tidak terlepas dari adanya kelemahan akan ancaman keamanan, begitu juga dengan sistem komunikasi. Beberapa contoh berikut merupakan ancaman keamanan pada sejumlah sistem komunikasi yang telah didefinisikan.

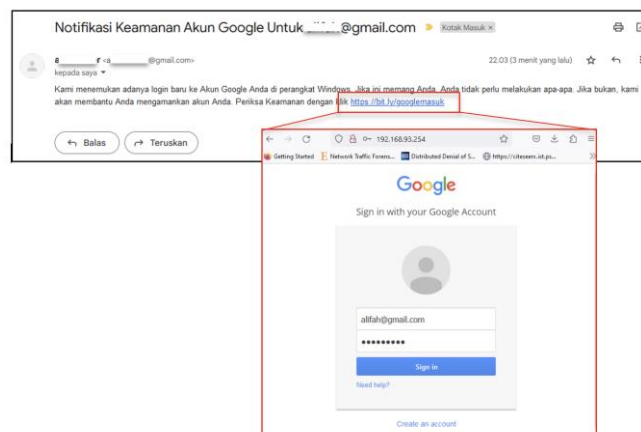
a. *email*

- *Fake Email*, ancaman pada keamanan email dimana id atau alamat pengirim email dapat dikelabui, sehingga penerima seolah-olah menerima pesan yang memang dari pengirim sesungguhnya. Ancaman ini dapat dikenali dengan melihat **Show Original** pada pesan email dan perhatikan pada bagian **Received From**.



Gambar 15. Contoh *Fake Email*

- *Phishing*, ancaman keamanan yang banyak terjadi pada pemanfaatan media komunikasi *email* dengan cara memberikan *link* palsu ke *email* korban yang berisikan halaman *web* untuk *login* masuk ke dalam akun (akun *email*, akun media sosial, akun-akun lainnya). Tujuannya adalah untuk mendapatkan parameter kredensial (*username* dan *password*) milik korban. Ancaman ini dapat dikenali dengan memperhatikan URL yang tampil ketika *link* diakses.



Gambar 16. Contoh *Phishing*

b. *file transfer*

- *Clear Content*, ancaman keamanan pada media komunikasi *file transfer* melalui layanan FTP dimana seluruh data yang dikirim-terimakan masih dalam bentuk asli (belum ada proteksi keamanan), sehingga dapat terjadi kebocoran data dan informasi.

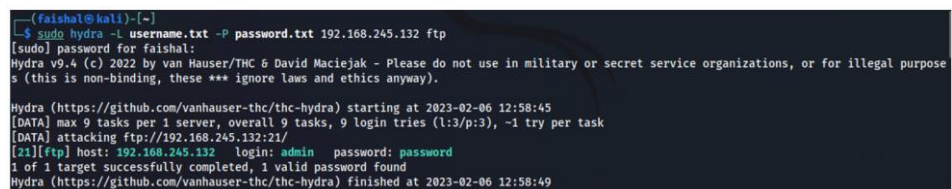


```
220 (vsFTPd 3.0.5)
USER admin
331 Please specify the password.
PASS password
230 Login successful.

SYST
215 UNIX Type: L8
FEAT
211-Features:
  EPRT
  EPSV
  MDTM
  PASV
  REST STREAM
  SIZE
  TVFS
211 End
EPSV
229 Entering Extended Passive Mode (|||16606|)
LIST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
EPSV
229 Entering Extended Passive Mode (|||32078|)
STOR theZoo.git
150 Ok to send data.
226 Transfer complete.
```

Gambar 17. Komunikasi FTP

- *Bruteforce*, ancaman keamanan yang secara umum menasar pada mekanisme otentikasi login dengan cara mencoba-coba seluruh kemungkinan pasangan nilai *username* dan *password* untuk masuk ke dalam sistem menggunakan akun yang sah.



```
(faishal@kali)-[~]
└─$ sudo hydra -L username.txt -P password.txt 192.168.245.132 ftp
[sudo] password for faishal:
hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpose
s (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-06 12:58:45
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (1:3/p:3), -1 try per task
[DATA] attacking ftp://192.168.245.132:21/
[21][ftp] host: 192.168.245.132 login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-06 12:58:49
```

Gambar 18. Contoh serangan *bruteforce*

## 2.3 Keamanan dalam Sistem Komunikasi

Untuk menjaga aspek keamanan informasi pada sistem komunikasi yang telah didefinisikan sebelumnya, dapat diterapkan beberapa teknik keamanan berikut:

a. *email*

- Tidak hanya melihat pada subjek pengirim *email*, tetapi juga melakukan pemeriksaan pada *email header* untuk mengetahui siapa pengirim email yang sesungguhnya. Untuk melihat email header secara utuh, dapat menggunakan fungsi “show original” pada aplikasi browser yang dipergunakan.
- Tidak sembarangan membuka tautan atau melakukan klik pada *link* yang diberikan ataupun terdapat di dalam pesan *email*. Karena bisa saja itu diarahkan kepada halaman lain yang berisikan halaman *phishing*.



b. *file transfer*

- Karakteristik protocol FTP memang tidak memberikan pengamanan dalam data yang dikirim-terimakan, oleh karena itu dapat digunakan protokol serupa yang telah menerapkan pengamanan, seperti Secure FTP (SFTP).
- Inisiasi penggunaan password yang aman, dimana tersusun atas gabungan huruf, angka, karakter, simbol dengan minimal panjang 8 karakter.

	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

Gambar 19. Standar Keamanan *Password*

### 3. MENERAPKAN AKSES KONTROL LINGKUNGAN KOMPUTASI YANG SESUAI

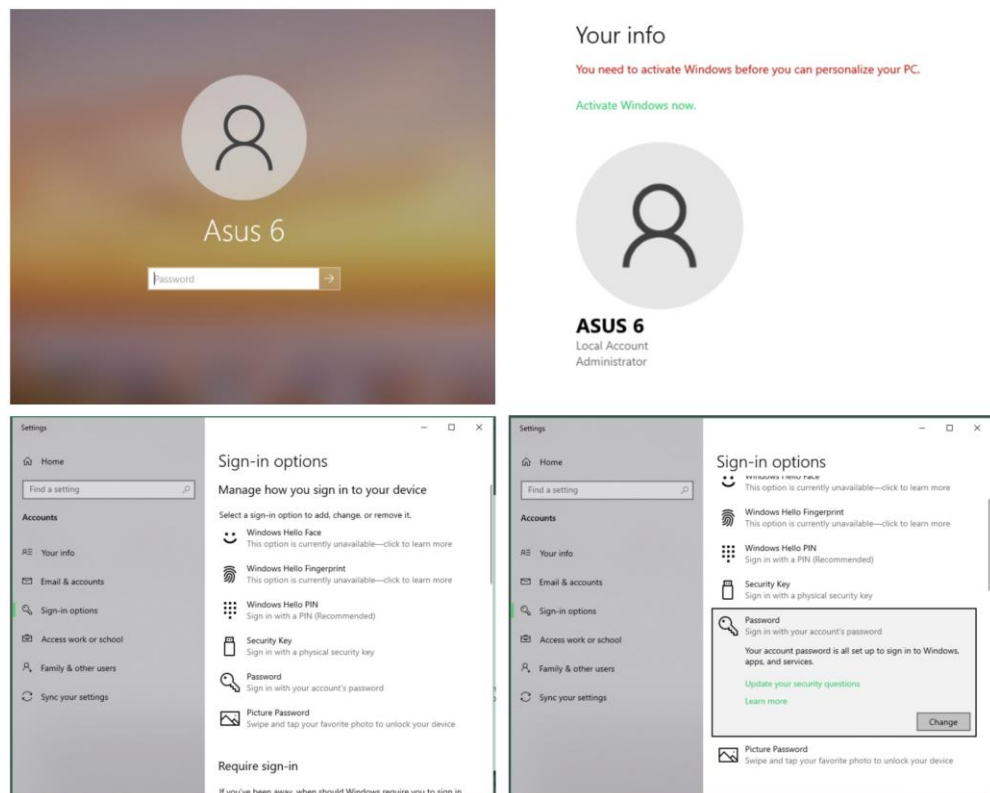
#### 3.1 Sistem Akses Kontrol

Akses kontrol untuk masuk ke dalam sebuah sistem atau aplikasi, dapat dipenuhi dengan menerapkan skema otentikasi. Otentikasi merupakan proses yang dilakukan oleh sistem atau aplikasi dalam mengenali entitas atau pihak yang melakukan akses ke dalam sistem atau aplikasi. Otentikasi dilakukan dengan menetapkan parameter yang valid untuk sebuah sistem atau aplikasi, seperti *username* dan *password* yang umum digunakan. Ketika akses terotentikasi, hal itu menjelaskan bahwa sistem telah mengkonfirmasi bahwa akses yang hendak masuk telah sesuai dengan parameter yang telah ditetapkan sebelumnya. Perlu diingat, bahwa otentikasi tidak melakukan pemeriksaan terhadap hak akses terhadap objek-objek di dalam sistem yang dibatasi secara spesifik. Di dalam sebuah sistem atau aplikasi, hal tersebut dilakukan oleh skema otorisasi.

Otentikasi mensyaratkan sejumlah parameter untuk prosesnya, yang umum adalah *username*/ID dan *password*/PIN/*Security Code*. Dalam sistem operasi dapat didefinisikan model otentikasi yang digunakan, berupa user access. Pada sistem operasi Windows, yang bertindak sebagai administrator secara default adalah akun "admin". Sedangkan untuk sistem operasi UNIX, yang bertindak sebagai administrator secara default adalah akun "root".

##### a. Windows Authentication

Untuk sistem operasi Windows, akses kontrol dapat diterapkan di dalam pengaturan "Control Panel" -> "User Accounts".



Gambar 20. Windows Authentication

#### b. UNIX Authentication

Untuk sistem operasi UNIX akses kontrol untuk pengguna terdapat di dalam pengelolaan *user* dan *group* (*user and group management*). Beberapa fungsi yang dapat dijalankan untuk konfigurasi pengelolaan akses kontrol sistem operasi UNIX, adalah sebagai berikut:

- **adduser** : menambah akun pengguna.
- **passwd** : mengganti password milik akun pengguna.
- **userdel** : menghapus akun pengguna dan file yang berkorelasi dengan akun tersebut.
- **addgroup** : menambah *group*.
- **delgroup** : menghapus *group*.
- **usermod** : mengubah data akun pengguna.
- **chage** : mengubah informasi waktu habis *password*.
- **Sudo** : menjalankan peran sebagai akun pengguna lainnya (yang membutuhkan akses admin).
- **whoami** : melihat akun pengguna yang sedang beroperasi.

### 3.2 Sistem Log

Log merupakan riwayat atau pencatatan setiap aktifitas yang terjadi terhadap sistem. Log menyediakan informasi yang dapat digunakan dalam mendeteksi, merespon, dan juga melakukan investigasi permasalahan keamanan pada yang terjadi di dalam sistem. Log secara umum berisikan informasi mengenai:

- Valid atau tidak validnya, baik itu untuk proses otentikasi ataupun untuk penggunaan sumber daya di dalam sistem,
- Waktu mulai/*start* dan berhenti/*stop* untuk penggunaan proses, aplikasi, dan juga kesalahan/*error* yang terjadi,
- Aktifitas akses jarak jauh (*remote access*),
- Kegagalan dan permasalahan pada hardware,
- Perubahan konfigurasi untuk akun dan kebijakan sistem.

#### a. Windows System Log

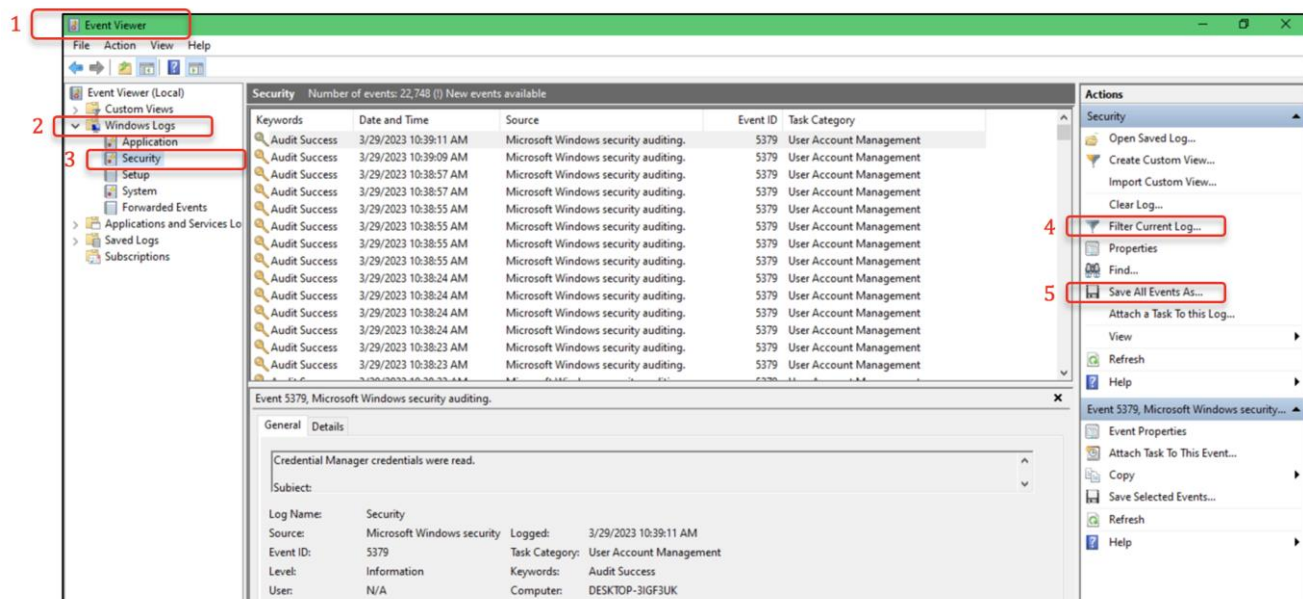
Sistem operasi Windows secara konstan melakukan pencatatan terhadap aktifitas yang terjadi di dalam sistem operasi, mulai dari kesalahan pemrosesan aplikasi (*app crash*) sampai dengan riwayat akses login dari seluruh user yang terdaftar. Log di dalam sistem operasi Windows dapat dimanfaatkan untuk penyelesaian masalah (*troubleshoot*) atau untuk pengumpulan informasi-informasi yang berkaitan dengan keamanan sistem operasi. Pada sistem operasi Windows, aktifitas dicatat berdasarkan kategori berikut yang dapat dilihat secara terperinci pada aplikasi "**Event Viewer**".

- *Application*
- *Security*
- *Setup*
- *System*
- *Forwarded Events*

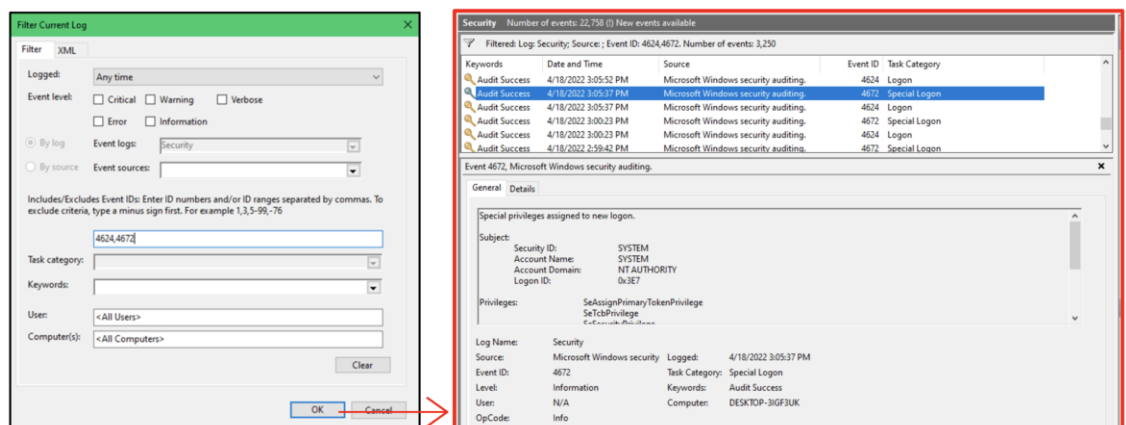
Berdasarkan log yang telah dicatatkan secara *default* oleh sistem operasi Windows, dapat disusun dokumen yang dapat dijadikan bahan pelaporan yang di dalamnya berisikan informasi-informasi log yang

dibutuhkan. Berikut tahapan yang dapat dilakukan untuk membuat dokumen atau laporan mengenai *log* kegiatan akses yang terjadi pada sistem operasi Windows.

- 1) Jalankan aplikasi **Event Viewer**
- 2) Pilih direktori **Windows Log**
- 3) Pilih item **Security**, akan menampilkan seluruh aktifitas di dalam sistem operasi yang berkaitan dengan *security*, termasuk di dalamnya adalah aktifitas akses (*logon* dan *special logon*)
- 4) Pilih *actions* **Filter Current Log**, untuk menampilkan hanya aktifitas yang ingin ditampilkan berdasarkan nomor **event ID**. Misalkan untuk ID yang berkaitan dengan akses adalah ID nomor 4624 (*logon*) atau 4672 (*special logon*)
- 5) Pilih *actions* **Save Filtered Log File As**, untuk menyimpan hasil pemilahan log ke dalam sebuah file (format yang dapat digunakan adalah \*.evtx, \*.xml, \*.csv, ataupun \*.txt)
- 6) File hasil nomor 5) sebelumnya dapat digunakan sebagai dokumen pencatatan log ataupun dokumen pelaporan terhadap aktifitas akses kepada sistem operasi Windows.



Gambar 21. Tahap pemilahan *log* sistem operasi Windows dengan aplikasi **Event Viewer**



Gambar 22. Tahap ke-4 untuk menampilkan hasil pemilahan *log* yang berisikan aktifitas akses

Keywords	Date and Time	Source	Event ID	Task Category	
Audit Success	3/29/2023 10:39:32 AM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/29/2023 10:39:32 AM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/29/2023 10:38:21 AM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/29/2023 10:38:21 AM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/29/2023 10:35:17 AM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/29/2023 10:35:17 AM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/15/2023 10:40:14 PM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/15/2023 10:40:14 PM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/15/2023 5:04:25 PM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/15/2023 5:04:25 PM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/15/2023 4:04:25 PM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/15/2023 4:04:25 PM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/15/2023 3:04:25 PM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/15/2023 3:04:25 PM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/15/2023 2:04:25 PM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/15/2023 2:04:25 PM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/15/2023 1:04:26 PM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/15/2023 1:04:26 PM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/15/2023 9:38:17 AM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/15/2023 9:38:17 AM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/15/2023 9:38:15 AM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/15/2023 9:38:15 AM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/15/2023 9:35:49 AM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/15/2023 9:35:49 AM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/15/2023 9:24:14 AM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/15/2023 9:24:14 AM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/15/2023 9:24:13 AM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/15/2023 9:24:13 AM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.
Audit Success	3/15/2023 9:23:55 AM	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon.
Audit Success	3/15/2023 9:23:55 AM	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.

Gambar 23. Dokumentasi *log* yang berkaitan dengan aktifitas akses di dalam sistem operasi Windows

b. UNIX System Log

Untuk sistem operasi UNIX, aktifitas dicatat berdasarkan kategori berikut yang dapat dilihat secara terperinci pada direktori **/var/log**.

- **/var/log/messages** : General message and system related stuff.
- **/var/log/auth.log** : Authentication logs.
- **/var/log/kern.log** : Kernel logs.
- **/var/log/cron.log** : Crond logs (cron job).
- **/var/log/maillog** : Mail server logs.
- **/var/log/qmail/** : Qmail log directory (more files inside this directory).
- **/var/log/httpd/** : Apache access and error logs directory.
- **/var/log/lighttpd/** : Lighttpd access and error logs directory.
- **/var/log/nginx/** : Nginx access and error logs directory.
- **/var/log/apt/** : Apt/apt-get command history and logs directory.
- **/var/log/boot.log** : System boot log.
- **/var/log/mysqld.log** : MySQL database server log file.
- **/var/log/secure, /var/log/auth.log** : Authentication log.
- **/var/log/utmp, /var/log/wtmp** : Login records file.
- **/var/log/yum.log, /var/log/dnf.log** : Yum/Dnf command log file.

Berdasarkan log yang telah dicatatkan secara *default* oleh sistem operasi UNIX, dapat disusun dokumen yang dapat dijadikan bahan pelaporan yang di dalamnya berisikan informasi-informasi log yang dibutuhkan. Berikut tahapan yang dapat dilakukan untuk membuat dokumen atau laporan mengenai *log* kegiatan akses yang terjadi pada sistem operasi UNIX.

- 1) Buka aplikasi terminal
- 2) Akses ke dalam direktori **/var/log** dengan cara menjalankan perintah:

```
cd /var/log
```

- 3) Lihat isi direktori untuk mencari log yang berisikan aktifitas akses (**auth.log**) dengan cara menjalankan perintah:

```
ls -a
```

```
root@hadynoer:/# cd /var/log/
root@hadynoer:/var/log# ls -a
.                  dist-upgrade      kern.log.2.gz
..                 dmesg             lastlog
alternatives.log   dmesg.0           openvpn
alternatives.log.1 dpkg.log          private
apt               dpkg.log.1       speech-dispatcher
auth.log          faillog           syslog
auth.log.1        fontconfig.log    syslog.1
auth.log.2.gz     gdm3              syslog.2.gz
boot.log          gpu-manager.log   ubuntu-advantage.log
boot.log.1        hp                ubuntu-advantage-timer.log
bootstrap.log     installer         ubuntu-advantage-timer.log.1
btm               journal           unattended-upgrades
btm.1             kern.log          wtmp
cups              kern.log.1
```

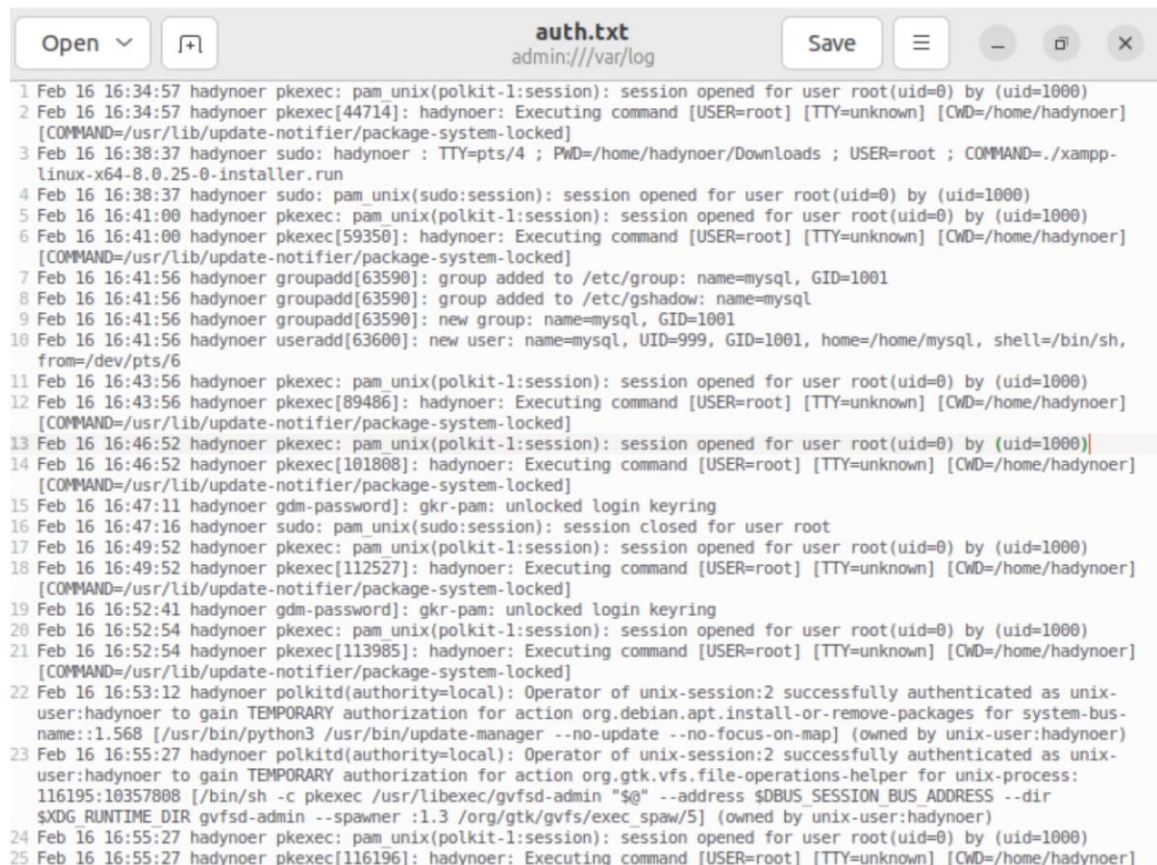


Gambar 24. Isi direktori /var/log

- 4) Simpan isi log ke dalam sebuah file dengan cara menjalankan perintah:

```
cat auth.log >> auth.txt
```

- 5) *File* hasil nomor 4) sebelumnya dapat digunakan sebagai dokumen pencatatan *log* ataupun dokumen pelaporan terhadap aktifitas akses kepada sistem operasi UNIX.



Gambar 25. Dokumentasi *log* yang berkaitan dengan aktifitas akses di dalam sistem operasi UNIX



#### 4. MEMATUHI DAN MELAKSANAKAN PETUNJUK YANG TERDAPAT PADA DOKUMEN YANG DITERBITKAN KHUSUS OLEH PEMERINTAH ATAU BADAN-BADAN RESMI TERKAIT UNTUK MENGELOLA SISTEM OPERASI

##### 4.1 Taksonomi Cybersecurity

Dalam beberapa tahun terakhir, serangan siber berkembang cukup signifikan dan telah banyak mengakibatkan kerugian bisnis dan terancamnya reputasi institusi. Oleh sebab itu, perlu adanya solusi dalam menangani masalah keamanan siber. Dalam menentukan metode yang tepat dalam penentuan solusi penanganan masalah keamanan siber, terlebih dahulu dikenali berbagai macam aspek kebijakan (*policy*) yang mendukung terwujudnya keamanan siber secara utuh, diantaranya adalah:

- *Privacy*
- *Website Security*
- *Cloud Computing Security*
- *Email Security*
- *Information Security*
- *Network Security*
- *Physical Security*
- *Data Protection*
- *Data Retention*
- *Access Control*

##### 4.2 Deskripsi Kerangka dan Standar Keamanan Informasi

- *Privacy*

Pengaturan untuk bagaimana mengelola data pribadi sensitif (data medis, biometrik, keuangan, dan lainnya) secara aman terhadap pengungkapan, penggunaan, akses, pengumpulan, pengiriman dan pertukaran secara tidak sah. Keamanan yang dapat diterapkan adalah dengan memberikan kontrol akses terhadap data dan informasi.
- *Website Security*

Pengaturan untuk bagaimana aplikasi dan layanan online dapat dijalankan secara aman terhadap ancaman keamanan berupa serangan dari luar ataupun kerentanan yang mungkin ada di dalam aplikasi itu sendiri. Keamanan aplikasi dan layanan online dapat dilihat dari hasil pengukuran tingkat keamanan, sehingga data dan informasi di dalam aplikasi terlindungi dari ancaman keamanan terhadap aplikasi, seperti web scripting, trojan, malware dan serangan aplikasi lainnya.
- *Cloud Computing Security*

Pengaturan untuk bagaimana layanan cloud berjalan sesuai dengan standar keamanan, mulai dari aspek keamanan pada kontrol akses, penyimpanan data, enkripsi, keamanan jaringan, sampai dengan bagaimana interaksi dan pertukaran data yang aman.
- *Email Security*

Pengaturan untuk bagaimana penggunaan email yang aman oleh user sesuai dengan rekomendasi keamanan, bagaimana administrator sistem email menerapkan fungsi-fungsi keamanan, dan bagaimana komunikasi yang dibangun telah menerapkan enkripsi dan digital *signing*.
- *Physical Security*

Pengaturan untuk bagaimana aset, sumber daya, peralatan, perangkat keras dan fasilitas organisasi diamankan terhadap ancaman kerusakan dan pencurian. Penerapan keamanan dapat dilakukan dengan akses kontrol, sistem deteksi, pemantauan, dan teknik pengamanan aset lainnya.

- *Network Security*

Pengaturan untuk bagaimana komponen jaringan dijalankan dengan menerapkan kontrol keamanan pada perangkat-perangkat jaringan, seperti *router, switch, server, firewall*, dan lainnya. Kontrol keamanan perlu diterapkan untuk melindungi jaringan terhadap akses tidak sah atau perubahan yang tidak direncanakan. Beberapa teknik keamanan di dalam jaringan yang dapat diterapkan, antara lain adalah dengan segmentasi dan pembatasan jaringan, enkripsi, dan pengamanan jaringan lainnya.

- *Information Security*

Sumber daya informasi juga menjadi aset organisasi yang perlu dilindungi keamanannya. Perlu kebijakan dalam menetapkan pedoman yang wajib dipatuhi oleh pihak untuk melindungi keamanan aset fisik dan digital terhadap akses ilegal, penyalinan, modifikasi, perusakan ataupun pendistribusian secara tidak sah. Aspek kerahasiaan, integritas dan ketersediaan sumber daya informasi perlu dijamin keamanannya dalam pedoman tersebut untuk mengurangi risiko keamanan terhadap sumber daya informasi.

- *Access Control*

Pengaturan untuk bagaimana melindungi sumber daya fisik, sistem informasi, dan sumber daya TI lainnya terhadap akses tidak sah. Teknik pengamanan yang dapat diterapkan adalah dengan melakukan identifikasi, otentikasi, *signing* dan juga melakukan pemantauan kepada siapa saja yang memiliki akses terhadapnya. Kebijakan kontrol akses juga dilakukan untuk mengelola hak akses dari setiap pihak, sehingga data sensitif dapat dilindungi keamanannya dengan tepat.

- *Data Retention*

Pengaturan untuk bagaimana melindungi informasi yang tersaji di dalam sebuah data. Bentuk pengamanannya dapat dilakukan dengan memberikan klasifikasi di dalam penyimpanan data, menyiapkan cadangan data, menerapkan enkripsi data pada jangka waktu tertentu.

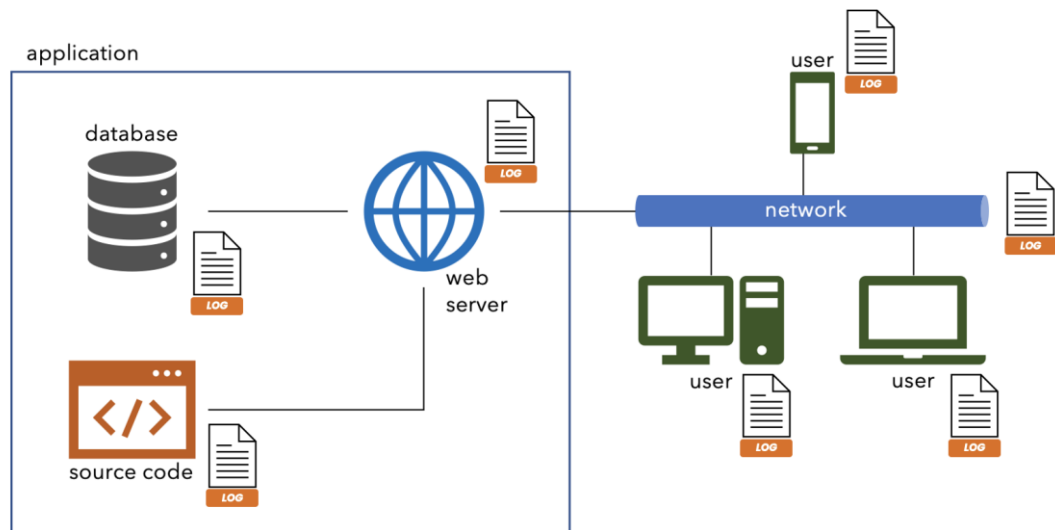
- *Data Protection*

Pengaturan untuk bagaimana melindungi pemrosesan dan pengelolaan data pribadi, sehingga data dapat dikumpulkan, digunakan, dibagikan, disimpan, dipindahkan, ataupun dikirim secara aman. Selain itu, kategorisasi data juga perlu dilakukan untuk memudahkan dalam pemantauan keamanannya.

## 5. MENGUMPULKAN DAN MEMELIHARA DATA YANG DIPERLUKAN UNTUK MEMENUHI PERSYARATAN PELAPORAN KEAMANAN SISTEM

### 5.1 Mengenali Log

Selain pada sistem operasi, komponen-komponen lainnya di dalam sistem informasi juga masing-masing memiliki log, mulai dari OS, web server, database, sampai dengan aplikasi. Untuk memberikan hasil menyeluruh pada hasil analisa log, maka perlu dikumpulkan log-log pada keseluruhan komponen sistem.



Gambar 26. Komponen Penyusun Sistem Informasi

#### a. Sistem Operasi

Pada sistem operasi Windows, aktifitas dicatat berdasarkan kategori berikut yang dapat dilihat secara terperinci pada aplikasi “**Event Viewer**”. Sedangkan untuk sistem operasi UNIX, aktifitas dicatat berdasarkan kategori yang dapat dilihat secara terperinci pada direktori **/var/log**.

#### b. Web Server

Web server merupakan aplikasi yang berfungsi untuk menyediakan layanan web dalam menerima permintaan (*request*) dari *client* berupa halaman web melalui protokol HTTP/HTTPS melalui browser, kemudian *server* mengirimkan kembali (*response*) hasil permintaan tersebut ke dalam bentuk halaman web.

Banyak aplikasi yang dapat dimanfaatkan untuk mengenali log milik *web server*, salah satunya adalah menggunakan aplikasi XAMPP dengan melakukan langkah-langkah berikut.

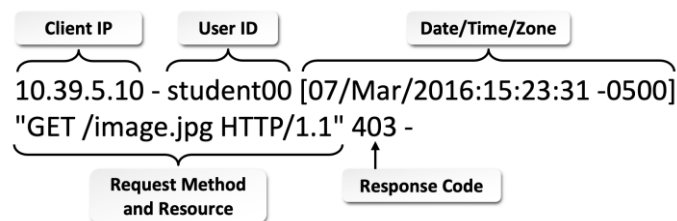
- 1) Jalankan aplikasi **XAMPP**
- 2) Pilih modul **Apache**
- 3) Klik tombol **Logs**, kemudian pilih **access.log**



Gambar 27. Contoh log pada *web server*

Pencatatan aktifitas atau *logging* di dalam web server dituliskan dalam bentuk format yang berisikan informasi-informasi berikut:

- *Client IP address*
- *Client user ID*
- *Date, time, and time zone of reception*
- *Request method and resource requested*
- *HTTP status code of response*
- *Size of resource returned (in bytes)*



Gambar 28. Contoh *Web Server Log*

#### c. *Database*

Database merupakan kumpulan data yang tersusun secara sistematis untuk digunakan dalam kebutuhan operasional sistem atau aplikasi. Dengan aplikasi XAMPP juga dapat dikenali log untuk sebuah *database*.



Gambar 29. Contoh log pada *database*

Pencatatan aktifitas atau *logging* di dalam web server dituliskan dalam bentuk format yang berisikan informasi-informasi berikut:

- Waktu setiap aktifitas (*date, time*)
- Aktifitas normal, seperti *databases starting up*

- Kegagalan sistem, seperti *databases shutting down unexpectedly*
- *Aktifitas admin sign in (success and failure)*
- *Operation, schema, and object of query*
- Indikasi adanya serangan injeksi atau *account hijacking*
- *Increases overhead*

Date ▾	Source	Message
3/8/2016 12:47:22 PM	spid7s	Starting up database 'tempdb'.
3/8/2016 12:47:22 PM	spid7s	Clearing tempdb database.
3/8/2016 2:47:20 PM	spid7s	Starting up database 'model'.
3/8/2016 2:47:20 PM	spid7s	The resource database build version is 11.00.2100. This is an informati
3/8/2016 2:47:20 PM	spid19s	Starting up database 'CharityEventsDB'.
3/8/2016 2:47:20 PM	spid18s	Starting up database 'AdventureWorks2012'.
3/8/2016 2:47:20 PM	spid17s	Starting up database 'ReportServerTempDB'.
3/8/2016 2:47:20 PM	spid16s	Starting up database 'ReportServer'.
3/8/2016 2:47:20 PM	spid15s	Starting up database 'msdb'.
3/8/2016 2:47:20 PM	spid7s	Starting up database 'mssqlsystemresource'.
3/8/2016 2:47:20 PM	spid13s	A new instance of the full-text filter daemon host process has been suc
3/8/2016 2:47:18 PM	Logon	Login failed for user 'NT SERVICE\ReportServer'. Reason: Failed to op
3/8/2016 2:47:18 PM	Logon	Error: 18456, Severity: 14, State: 38.
3/8/2016 2:47:12 PM	Logon	Login failed for user 'NT SERVICE\ReportServer'. Reason: Failed to op
3/8/2016 2:47:12 PM	Logon	Error: 18456, Severity: 14, State: 38.

Gambar 30. Contoh *Database Log*

d. Network

Network atau jaringan merupakan jalur yang berjalan pada *layer* 1-3 (OSI layer) yang dipergunakan oleh setiap user untuk melakukan akses dan berkomunikasi di dalam sistem komputer. Log pada network terdapat di beberapa perangkat jaringan, diantaranya sebagai berikut:

- *Switch/Router*
- Perangkat *wireless*
- *Firewall*
- IDS/IPS
- *Proxy*

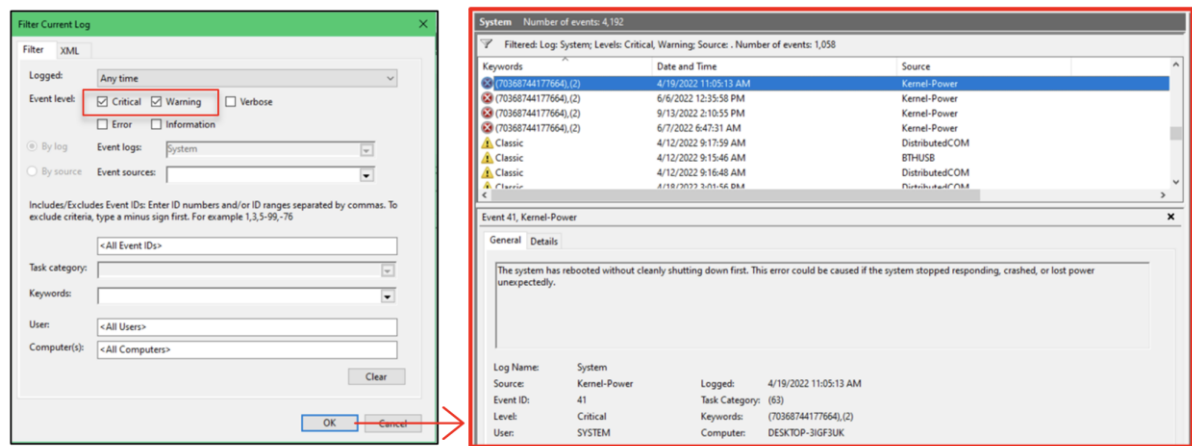
#Version: 1.5											
#Software: Microsoft Windows Firewall											
#Time Format: Local											
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tc											
2016-02-10	08:21:06	ALLOW	UDP	192.168.1.101	224.0.0.252	56022	5355	0	-	-	SEND
2016-02-10	08:21:06	ALLOW	UDP	192.168.1.101	224.0.0.252	56212	5355	0	-	-	SEND
2016-02-10	08:21:29	ALLOW	UDP	192.168.1.101	192.168.1.100	137	137	0	-	-	SEND
2016-02-10	08:21:29	ALLOW	UDP	192.168.1.101	192.168.1.100	5355	55083	0	-	-	SEND
2016-02-10	08:21:29	ALLOW	UDP	192.168.1.101	192.168.1.100	5355	58053	0	-	-	SEND
2016-02-10	08:21:29	ALLOW	ICMP	192.168.1.100	192.168.1.101	-	-	0	-	-	RECEIVE
2016-02-10	08:21:30	ALLOW	ICMP	192.168.1.100	192.168.1.101	-	-	0	-	-	RECEIVE
2016-02-10	08:21:30	ALLOW	TCP	::1	::1	57973	389	0	-	-	SEND
2016-02-10	08:21:30	ALLOW	TCP	::1	::1	57973	389	0	-	-	RECEIVE
2016-02-10	08:21:31	ALLOW	ICMP	192.168.1.100	192.168.1.101	-	-	0	-	-	RECEIVE
2016-02-10	08:21:32	ALLOW	ICMP	192.168.1.100	192.168.1.101	-	-	0	-	-	RECEIVE

Gambar 31. Contoh *Firewall Log*

## 5.2 Analisa Log

Setelah *log* dikumpulkan, maka selanjutnya adalah melakukan analisa terhadap log tersebut. Analisa log bertujuan untuk memberikan gambaran utuh terhadap aktifitas sistem, melihat korelasi antar *log*, menjelaskan kejadian sesungguhnya apabila terdapat insiden keamanan di dalam sistem. Analisa *log* dapat dilakukan dengan menggunakan *tools* untuk membantu dan mempercepat dihasilkannya hasil analisa *log* yang komprehensif. Sebagai contoh, pada sistem operasi Windows dapat dilakukan dan didokumentasikan analisa *log* dengan menggunakan **Event Viewer**. Berikut beberapa tahapan yang dapat dilakukan.

- 1) Jalankan aplikasi **Event Viewer**
- 2) Pilih direktori **Windows Log**
- 3) Pilih item **System**, akan menampilkan seluruh aktifitas di dalam sistem berdasarkan tingkat risiko keamanannya (*Critical*, *Warning*, *Error*, atau *Information*)
- 4) Pilih *actions* **Filter Current Log**, untuk menampilkan hanya aktifitas yang ingin ditampilkan berdasarkan tingkat risiko keamanannya



Gambar 32. Pemilahan *log* berdasarkan tingkat risiko keamanannya

- 5) Pilih *actions* **Save Filtered Log File As**, untuk menyimpan hasil pemilahan log ke dalam sebuah file (format yang dapat digunakan adalah \*.evtx, \*.xml, \*.csv, ataupun \*.txt)
- 6) *File* hasil nomor 5) sebelumnya dapat digunakan sebagai bahan dalam penyusunan dokumen analisa log.

Keywords	Date and Time	Source	Event ID	Task Category	
Critical	9/13/2022 2:10:55 PM	Microsoft-Windows-Kernel-Power	41	-63	The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly.
Critical	6/7/2022 6:47:31 AM	Microsoft-Windows-Kernel-Power	41	-63	The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly.
Critical	6/6/2022 12:35:58 PM	Microsoft-Windows-Kernel-Power	41	-63	The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly.
Critical	4/19/2022 11:05:13 AM	Microsoft-Windows-Kernel-Power	41	-63	The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly.

Gambar 33. Dokumentasi *log* yang berkaitan dengan analisa aktifitas sistem

## Latihan 1

- Penggunaan aplikasi online ataupun *open source* untuk melaksanakan fungsi enkripsi (teks dan file)
- Penggunaan aplikasi online ataupun *open source* untuk melaksanakan fungsi *hash* (teks dan file)

### **Latihan 2**

- Melakukan pemeriksaan terhadap sebuah email yang terindikasi sebagai sebuah *fake email*
- Melakukan pemeriksaan terhadap sebuah email yang terindikasi terdapat tautan (*link*) palsu yang dimanfaatkan untuk *phishing*

### **Latihan 3**

- Melakukan pemeriksaan Windows *log* dengan aplikasi event viewer
- Melakukan pemeriksaan UNIX *log*
- Melakukan pemeriksaan *log* pada *web server* dan *database*
- Melakukan pencatatan *firewall log*
- Mengenali analisa *log* sederhana

## **A. Pengetahuan yang diperlukan untuk menerapkan prinsip perlindungan informasi**

1. Pengetahuan tentang aspek keamanan informasi (CIA triad)
2. Pengetahuan tentang ancaman keamanan siber
3. pengetahuan tentang sistem operasi komputer

## **B. Keterampilan yang diperlukan untuk menerapkan prinsip perlindungan informasi**

1. Kemampuan menjalankan sistem operasi komputer
2. Kemampuan menjalankan program komputer sederhana untuk keamanan informasi
3. Kemampuan mengenali log pada sistem operasi computer

## **C. Sikap Kerja yang diperlukan untuk menerapkan prinsip perlindungan informasi**

1. Harus cermat dalam menjalankan program komputer untuk keamanan informasi
2. Memiliki *security awareness* (kesadaran akan ancaman keamanan informasi)
3. Teliti



Tugas Pelatihan
Kerjakan Latihan 1 sampai dengan latihan 3

Link Referensi Modul
Link aplikasi online untuk fungsi enkripsi ( <a href="https://hat.sh/">https://hat.sh/</a> )

Link Pertanyaan Modul

Bahan Tayang
Bahan ajar modul ini

Link room Pelatihan dan Jadwal live sesi bersama instruktur
Zoom, Meets

Penilaian
Komposisi penilaian Kuis 1 Mengumpulkan data: Nilai 10 (Range 0 -10)

Target Penyelesaian Modul
1hari/sampai 2 JP

# VSGA

Vocational School  
Graduate Academy

**2023**