**Jurnal Praktikum**

**Sistem Operasi (CII-2H3)**

**Modul 9: Keamanan**

**Catatan**

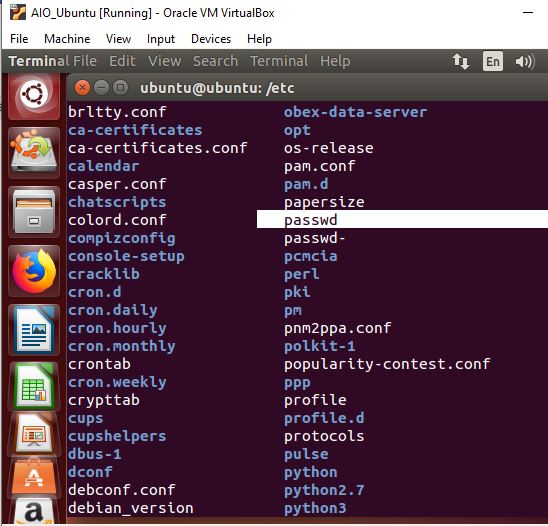
1. Praktikan wajib untuk screenshot setiap langkah yang dikerjakan hingga tampilan output akhir
2. Untuk soal source code, kumpulkan SS-nya saja
3. Praktikan wajib untuk melakukan screenshot lengkap dengan nama root. Contoh : root@username
4. Berikan identitas nama - nim dalam bentuk comment di Source Code
5. Harap kerjakan secara mandiri, jika tidak paham silahkan bertanya kepada Asisten Praktikum masing-masing. Dilarang mengcopy jawaban dan source code dari teman!

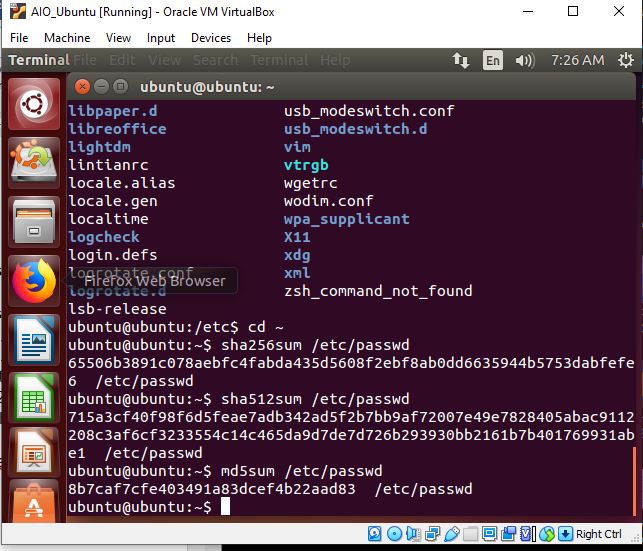
**Tujuan**

1. Mahasiswa mampu mengimplementasikan akses kontrol
2. Mahasiswa mampu mengimplementasikan aspek integritas
3. Mahasiswa mampu mengimplementasikan aspek konfidensialitas

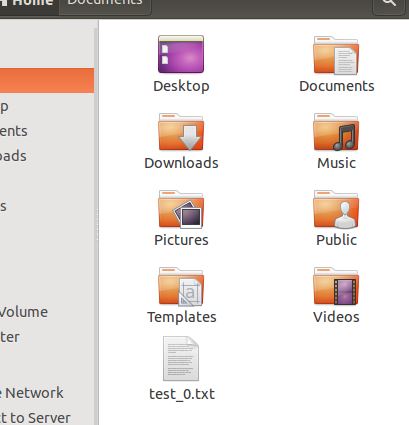
**Jurnal Praktikum**

1. Integritas: dasar hashing
   1. Lakukan hash SHA256, SHA512 dan MD5 untuk file /etc/passwd. Berapa nilai hash dari file /etc/passwd? Screenshot nilai hash dari file tersebut.



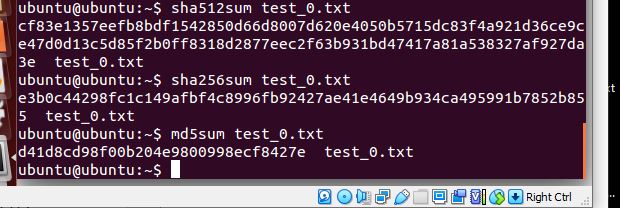


* 1. Buatlah file bernama test\_0.txt pada folder /home/praktikan. Isi file tersebut isi yang ada di file /tmp/passwd (copy paste **isi** file /etc/passwd ke test\_0.txt)

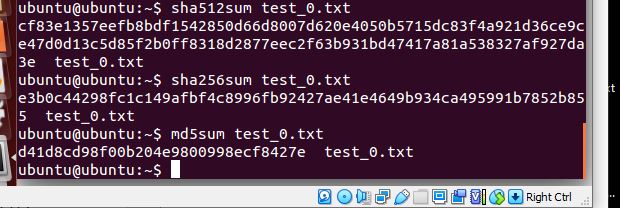


Setelah itu cp /passwd /home/dpay/test\_0.txt

* 1. Lakukan hash SHA256, SHA512 dan MD5 untuk file test\_0.txt. Berapa nilai hash dari file test\_0.txt? Screenshot nilai hash dari file test\_0.txt.



* 1. Rename file test\_0.txt menjadi file\_0.txt. Lakukan hash SHA256, SHA512 dan MD5 untuk file\_0.txt. Berapa nilai hash file\_0.txt? Screenshot nilai hash dari file\_0.txt.

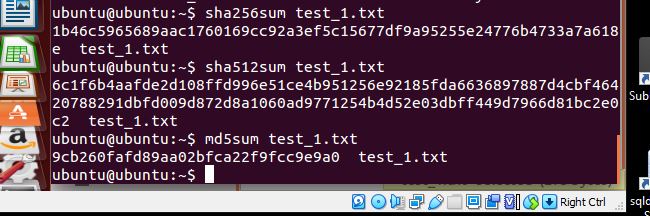


* 1. Apa hasil pengamatan Anda? File apa saja yang mempunyai hash yang sama? Jelaskan!
* Semuanya sama karena isinya sama jadi Hash nya sama.

1. Integritas: avalance
2. Download file bernama test\_1.txt

done

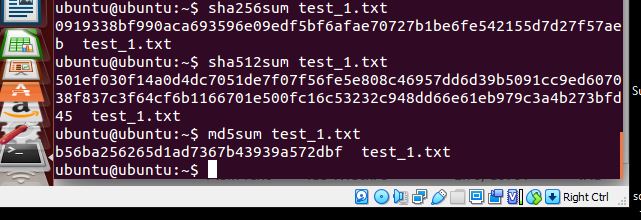
1. Lakukan hash SHA256, SHA512 dan MD5 untuk file test\_1.txt. Berapa nilai hash test\_1.txt? Screenshot nilai hash dari file test\_1.txt.



1. Hapuslah titik diakhir file test\_1.txt tersebut, simpan file tersebut!

Done

1. Lakukan hash dari SHA256, SHA512 dan MD5. Screenshot nilai hash dari file test\_1.txt.



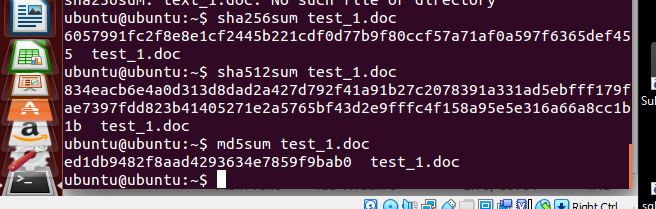
1. Apa analisis (hasil pengamatan) Anda mengenai hal tersebut! Apakah nilai hash sama?

* Hasilnya akan berbeda jika ada sedikit perubahan saja pada file tersebut maka ketika di hash hasilnya akan berbeda secara keseluruhan

1. Integritas: metadata
   1. Download file bernama test\_1.doc

Done

* 1. Lakukan hash SHA256, SHA512 dan MD5 untuk file test\_1.doc. Screenshot nilai hash dari file test\_1.doc.
  2. Buka kembali file test\_1.doc. Lakukan hal ini:
     1. Ketik abcdef. Save test\_1.doc
     2. Hapus abcdef. Save test\_1.doc
  3. Lakukan hash SHA256, SHA512 dan MD5 untuk file test\_1.doc. Screenshot nilai hash dari file test\_1.doc

.

* 1. Hasil pengamatan apa yang diperoleh? Jelaskan alasannya!

Beda hasilnya apapun yang dirubah didalam file tersebut ketika di hash maka hasilnya akan berubah secara keseluruhan, karena terdapat metadata pada file doc jadi waktu edit akan dicatat dan akan merubah hash nya berbeda

1. Konfidensialitas: enfs
   1. Enfs adalah tool untuk melakukan mount dan membuat file system yang terenkripsi. Cara kerjanya adalah sebagai berikut. Ada 2 folder yang akan dibuat, dua folder tersebut saling terkait. Satu folder merupakan folder yang tidak terenkripsi, folder lainnya merupakan hasil enkripsi dari folder pertama.

* Install encfs dengan sudo install encfs
* Selanjutnya membuat folder\_terenkripsi dan folder\_normal

file\_a

file\_b

hasil\_enkripsi \_file\_a

hasil\_enkripsi\_file\_b

folder\_normal

folder\_terenkripsi

* 1. Jalankan perintah berikut:”encfs /home/praktikan/folder\_terenkripsi /home/praktikan/folder\_normal” Pilih y (enter), pilih y (enter), enter, kemudian buatlah password. **Ingatlah password yang dibuat**. Setelah selesai, perhatikan bahwa telah muncul folder bernama folder\_normal dan folder\_terenkripsi.

Mengerti

* 1. Buka file explorer Anda dan copy dua atau tiga buah file (file apa saja) ke folder\_normal. Amati dan tulis hasil observasi Anda pada folder\_terenkripsi!
* Ternyata copy 3 file ke folder\_normal ternyata memang Tidak ada file di folder\_enkripsi nya
  1. Buka file explorer Anda dan hapus salah satu file (sembarang) pada folder\_terenkripsi. Amati dan tulis hasil observasi Anda pada folder\_normal!
* Ternyata ketika dihapus di file enkripsi di file normal juga terhapus
  1. Lakukan umount dengan perintah: “fusermount -u /home/praktikan/folder\_normal”. Amati dan tulis hasil observasi Anda pada folder\_normal dan folder\_terenkripsi
* Ternyata ketika di umount sudah tidak ada folder lagi di folder\_normal tetapi masih ada file di folder\_terenkripsi
  1. Buatlah folder baru bernama folder\_sembarang. Lakukan perintah berikut ini: “enfs /home/praktikan/folder\_terenkripsi /home/praktikan/folder\_sembarang”. Amati dan tulis hasil observasi Anda!
* Ternyata bisa dilakukan umount kemana saja asalkan bukan ke folder\_terenkripsi yang dihapus.

1. Konfidensialitas:gpg
   1. **Membuat kunci publik dan privat**. Jalankan perintah ini: “gpg --gen-key”. Baca dan ikuti perintah yang ada dari program gpg!
   2. Hasil kunci publik dan privat ada di folder ~/.gnupg. Kunci privat tidak boleh keluar dari komputer ini dan hanya Anda saja yang dapat mengaksesnya. Kunci publik akan dibagikan kepada seluruh dunia atau untuk orang yang Anda inginkan saja. Kunci publik adalah pubring.gpg dan kunci private adalah secring.gpg

Lakukan perintah berikut ini untuk mengetahui daftar key yang Anda punya dan fingerprint kunci yang Anda punya!

“gpg --list-keys”

“gpg --fingerprint [nama@email.com](mailto:nama@email.com)”

Screenshot hasil perintah di atas!

* 1. **Export kunci publik Anda**. Jalankan perintah ini: “gpg --armor --export nama@email.anda > mypublic\_key.asc”

mypublic\_key.asc inilah yang akan bagikan kepada teman-teman Anda. Teman Anda akan menggunakan kunci publik Anda jika ingin mengirim pesan rahasia kepada Anda. Hanya Anda yang dapat membaca pesan tersebut karena hanya mempunyai kunci privat yang bersesuaian dengan kunci publik Anda.

Rename mypublic\_key.asc menjadi nim\_anda.asc Contoh: 130118xxxx.asc Taruh file nim\_anda.asc ke folder berikut: <https://drive.google.com/folderview?id=1JpssYX6S07eN9piZeGc6n4NV0NV_86Oq> (akses dengan SSO)

* 1. **Mengimport kunci publik orang lain**. Jalankan perintah ini untuk mengimport (menambahkan kunci publik orang lain ke sistem Anda): “gpg --import nim\_teman\_sebelah\_anda.asc”. Contoh: “gpg --import 130118yyyy.asc” Setelah mengimport kunci publik teman Anda, Anda dapat mengirimkan pesan kepada teman Anda secara terenkripsi. Untuk memastikan bahwa kunci publik telah diimport lakukan perintah “gpg --list-keys” dan nama teman Anda ada pada hasil perintah tersebut.
  2. **Enkripsi pesan**. Buatlah file bernama file\_rahasia\_untuk\_teman\_anda.txt. Isi file tersebut dengan pesan rahasia Anda. Pesan inilah yang akan Anda kirim ke teman Anda. Jalankan perintah ini untuk melakukan enkripsi: “gpg --encrypt --armor -r [alamat\_email\_teman\_anda\_yang\_baru\_diimport@xxx.com](mailto:alamat_email_teman_anda_yang_baru_diimport@xxx.com) file\_rahasia\_untuk\_teman\_anda.txt” Hanya teman anda yang dapat membuka file tersebut. Hasil dari proses tersebut adalah file\_rahasia\_untuk\_teman\_anda.asc (contoh: file\_rahasia\_untuk\_130118yyyy.asc) taruh file\_rahasia\_untuk\_teman\_anda.asc ke folder: <https://drive.google.com/folderview?id=1JZ8oQadKoZPua47cy3L6rnZdYwkdJKm_> (akses dengan SSO)
  3. Buka file yang diperuntukkan bagi Anda dan lakukan dekripsi untuk melihat isi pesan dengan perintah: “gpg file\_rahasia\_nim\_anda.asc”