

Tugas

bagian ini di copy dan paste di body email message

#####

Tugas 1 Forensik

Hash File + HMAC

Diberikan: 30-9-2025

Dikumpul paling lambat : 5-10-2025

Subject email : HSW3-HY1-NIM masing-masing

Deskripsi tugas ada dibawah

#####

Hash File + HMAC

1. Tujuan

- Menghasilkan hash (fingerprint) dari file.
 - Menghasilkan HMAC dari file menggunakan kunci rahasia.
 - Membandingkan hasil hash/HMAC untuk verifikasi integritas dan autentikasi.
-

2. Alat & Bahan

- Komputer Windows/Linux.
 - Aplikasi hash checker yang mendukung **HMAC**:
 - **Windows**: HashCalc (ada kolom “HMAC” dan “Key”).
 - **Linux**: openssl dgst (mendukung -hmac key).
 - File contoh (misalnya contoh.pdf).
 - Kunci rahasia untuk HMAC (misalnya MySecretKey).
 - salah satu file yg dipakai link file
https://upload.wikimedia.org/wikipedia/commons/4/47/PNG_transparency_demonstration_1.png
-

3. Langkah Kerja

A. Menghasilkan Hash Biasa (MD5/SHA-256)

- **Windows (HashCalc/HashTab)**
 - Instal HashCalc/HashTab.

- Buka aplikasi HashCalc.
- Pilih file yang akan dicek.
- Centang algoritma hash yang diinginkan (MD5, SHA-1, SHA-256).
- Klik “Calculate” → akan muncul nilai hash.

Alternatif PowerShell:

- Buka PowerShell.
- Jalankan `Get-FileHash C:\path\to\file.pdf -Algorithm SHA256`
- Catat nilai hash yang muncul.
- **Linux (terminal):**
 - Jalankan `sha256sum file.pdf` atau `md5sum file.pdf`
 - Catat nilai hash.

B. Menghasilkan HMAC

1. Windows (HashCalc):

- Buka HashCalc.
- Pilih file.
- Centang algoritma hash (misalnya SHA-256).
- Di kolom **Key**, ketik kunci rahasia (misalnya `MySecretKey`).
- Klik “Calculate” → hasil HMAC muncul pada kolom HMAC.

2. Linux (terminal OpenSSL):

- Jalankan:

```
openssl dgst -sha256 -hmac "MySecretKey" contoh.pdf
```

- Catat nilai HMAC yang dihasilkan.

C. Bandingkan Hash dan HMAC

- Ubah sedikit file atau ubah kunci rahasia lalu hitung ulang HMAC.
- Perhatikan bahwa:
 - **Hash biasa** berubah jika file berubah.
 - **HMAC** berubah jika file **atau kunci rahasia** berubah.

D. Eksperimen Keamanan

1. Hitung hash biasa file asli dan file yang sudah diubah → bandingkan.
2. Hitung HMAC file asli dengan kunci A dan kunci B → bandingkan hasil.

4. Laporan

Mahasiswa mencatat:

- Nama file.
- Algoritma hash.
- Hash yang dihasilkan.
- Kunci rahasia untuk HMAC.
- HMAC yang dihasilkan.
- Perbedaan hasil bila file/kunci diubah.
- Kesimpulan