

Lab - Mengenkripsi dan Mendekripsi Data Menggunakan OpenSSL

# Tujuan

**Bagian 1: Mengenkripsi Pesan dengan OpenSSL Bagian 2: Mendekripsi Pesan dengan OpenSSL**

# Latar Belakang / Skenario

OpenSSL adalah proyek open source yang menyediakan toolkit tangguh, kelas komersial, dan berfitur lengkap untuk protokol Transport Layer Security (TLS) dan Secure Sockets Layer (SSL). Ini juga merupakan perpustakaan kriptografi tujuan

umum. Di lab ini, Anda akan menggunakan OpenSSL untuk mengenkripsi dan mendekripsi pesan teks.

**Catatan:** Meskipun OpenSSL adalah pustaka kriptografi de facto saat ini, penggunaan yang disajikan di lab ini TIDAK direkomendasikan untuk perlindungan yang kuat. Di bawah ini adalah dua masalah keamanan dengan lab ini:

1. Metode yang dijelaskan dalam lab ini menggunakan fungsi derivasi kunci yang lemah. Keamanan HANYA diperkenalkan oleh kata sandi yang sangat kuat.
2. Metode yang dijelaskan di lab ini tidak menjamin integritas file teks.

Laboratorium ini harus digunakan untuk tujuan instruksional saja. Metode yang disajikan di sini TIDAK boleh digunakan untuk mengamankan data yang benar-benar sensitif.

**Sumber Daya yang Dibutuhkan**

* Mesin virtual CyberOps Workstation

# Instruksi

**Bagian 1: Mengenkripsi Pesan dengan OpenSSL**

OpenSSL dapat digunakan sebagai alat mandiri untuk enkripsi. Meskipun banyak algoritme enkripsi dapat digunakan, lab ini berfokus pada AES. Untuk menggunakan AES untuk mengenkripsi file teks langsung dari baris perintah menggunakan OpenSSL, ikuti langkah-langkah di bawah ini:

**Langkah 1: Mengenkripsi File Teks**

1. Masuk ke CyberOPS Workstation VM.
2. Buka jendela terminal.
3. Karena file teks yang akan dienkripsi ada di direktori /home/analyst/lab.support.files/, ubah ke itu direktori:

[analis@secOps ~]$ **cd ./lab.support.files/** [analis@secOps lab.support.files]$

1. Ketik perintah di bawah ini untuk mencantumkan isi file teks **letter\_to\_grandma.txt** terenkripsi pada

layar:

[analyst@secOps lab.support.files]$ **cat letter\_to\_grandma.txt** Hai Nenek, saya menulis surat ini untuk

berterima kasih atas kue cokelat yang Anda kirimkan kepada saya. Saya mendapatkannya pagi ini dan saya sudah makan setengah dari kotak! Mereka benar-benar nikmat!

Saya berharap yang terbaik untukmu. Cinta, Cucu pemakan kue Anda. [analyst@secOps lab.support.files]$

e. Dari jendela terminal yang sama, keluarkan perintah di bawah ini untuk mengenkripsi file teks. Perintah akan menggunakan AES-256 untuk mengenkripsi file teks dan menyimpan versi terenkripsi sebagai **message.enc.** OpenSSL akan meminta kata sandi dan konfirmasi kata sandi. Berikan kata sandi seperti yang diminta dan pastikan untuk mengingat kata sandi.

[analyst@secOps lab.support.files]$ **openssl aes-256-cbc -in letter\_to\_grandma.txt -out message.enc** masukkan kata sandi enkripsi aes-256-cbc:

Memverifikasi - masukkan kata sandi enkripsi aes-256-cbc:

[analyst@secOps lab.support.files]$

Dokumentasikan kata sandi.

1. Saat proses selesai, gunakan kembali perintah **cat** untuk menampilkan isi **message.enc**

mengajukan.

[analyst@secOps lab.support.files]$ **cat message.enc**

Apakah isi file **message.enc** ditampilkan dengan benar? Seperti apa bentuknya? Menjelaskan.

1. Agar file dapat dibaca, jalankan kembali perintah OpenSSL, tetapi kali ini tambahkan opsi **-a .** Opsi **-a** memberi tahu OpenSSL untuk menyandikan pesan terenkripsi menggunakan metode pengkodean Base64 yang berbeda sebelum menyimpan hasilnya dalam file.

**Catatan:** Base64 adalah grup skema pengkodean biner ke teks serupa yang digunakan untuk merepresentasikan data biner dalam format string ASCII.

[analyst@secOps lab.support.files]$ **openssl aes-256-cbc -a -in letter\_to\_grandma.txt -out message.enc** masukkan kata sandi enkripsi aes-256-cbc:

Memverifikasi - masukkan kata sandi enkripsi aes-256-cbc:

1. Sekali lagi, gunakan perintah **cat** untuk menampilkan konten file **message.enc** yang sekarang dibuat ulang :

**Catatan:** Konten **message.enc** akan bervariasi. [analyst@secOps lab.support.files]$ **cat message.enc**

U2FsdGVkX19ApWyrn8RD5zNp0RPCuMGZ98wDc26u/vmj1zyDXobGQhm/dDRZasG7 rfnth5Q8NHValEw8vipKGM66dNFyyr9/hJUzCoqhFpRHgNn+Xs5+TOtz/QCPN1bi 08LGTSzOpfkg76XDCk8uPy1hl/+Ng92sM5rgMzLXfEXtaYe5UgwOD42U/U6q73pj a1ksQrTWsv5mtN7y6mh02Wobo3A1ooHrM7niOwK1a3YKrSp+ZhYzVTrtksWDl6Ci XMufkv+FOGn+SoEEuh7l4fk0LIPEfGsExVFB4TGdTiZQApRw74rTAZaE/dopaJn0 sJmR3+3C+dmgzZIKEHWsJ2pgLvj2Sme79J /XxwQVNpw=

[analyst@secOps lab.support.files]$

Apakah **message.enc** ditampilkan dengan benar sekarang? Menjelaskan.

Dapatkah Anda memikirkan manfaat memiliki **message.enc** Base64-encoded?

**Bagian 2: Mendekripsi Pesan dengan OpenSSL**

Dengan perintah OpenSSL yang serupa, dimungkinkan untuk mendekripsi **message.enc.**

1. Gunakan perintah di bawah ini untuk mendekripsi message.enc:

[analis@secOps lab.support.files]$ **openssl aes-256-cbc –a -d -in message.enc -out decrypted\_letter.txt**

1. OpenSSL akan menanyakan kata sandi yang digunakan untuk mengenkripsi file. Masukkan kata sandi yang sama lagi.
2. Ketika OpenSSL selesai mendekripsi file **message.enc ,** ia menyimpan pesan yang didekripsi dalam file teks bernama

**decrypted\_letter.txt.** Gunakan **cat** untuk menampilkan konten **decrypted\_letter.txt:**

[analyst@secOps lab.support.files]$ **cat decrypted\_letter.txt**

Apakah surat itu didekripsi dengan benar?

Perintah yang digunakan untuk mendekripsi juga berisi opsi -a. Bisakah Anda menjelaskan?