Lab - Mengenkripsi dan Mendekripsi Data menggunakan Alat Peretas

Tujuan

Bagian 1: Membuat dan Mengenkripsi File

Bagian 2: Pulihkan Kata Sandi File Zip Terenkripsi

Latar Belakang / Skenario

Bagaimana jika Anda bekerja untuk perusahaan besar yang memiliki kebijakan perusahaan terkait media yang dapat dipindahkan? Secara khusus, ini menyatakan bahwa hanya dokumen zip terenkripsi yang dapat disalin ke flash drive USB portabel.

Dalam skenario ini, Chief Financial Officer (CFO) sedang berada di luar kota untuk urusan bisnis dan telah menghubungi Anda dengan panik dengan permintaan bantuan darurat. Saat berada di luar kota untuk urusan bisnis, dia mencoba membuka zip dokumen penting dari file zip terenkripsi di drive USB. Namun, kata sandi yang diberikan untuk membuka file zip tidak valid. CFO menghubungi Anda untuk melihat apakah ada yang bisa Anda lakukan.

Catatan: Skenario yang disediakan sederhana dan hanya berfungsi sebagai contoh.

Mungkin ada beberapa alat yang tersedia untuk memulihkan kata sandi yang hilang. Hal ini terutama berlaku dalam situasi seperti ini di mana analis keamanan siber dapat memperoleh informasi terkait dari CFO. Informasi terkait bisa berupa panjang kata sandi dan gagasan tentang apa itu. Mengetahui informasi terkait secara dramatis membantu saat mencoba memulihkan kata sandi.

Contoh utilitas dan program pemulihan kata sandi termasuk hashcat, John the Ripper, Lophtcrack, dan lainnya. Dalam skenario kami, kami akan menggunakan **fcrackzip** yang merupakan utilitas Linux sederhana untuk memulihkan kata sandi file zip terenkripsi.

Pertimbangkan bahwa alat yang sama ini dapat digunakan oleh penjahat dunia maya untuk menemukan kata sandi yang tidak diketahui. Meskipun mereka tidak akan memiliki akses ke beberapa informasi terkait, seiring berjalannya waktu, kata sandi dapat ditemukan untuk membuka file zip terenkripsi. Jumlah waktu yang diperlukan tergantung pada kekuatan kata sandi dan panjang kata sandi. Kata sandi yang lebih panjang dan rumit (campuran berbagai jenis karakter) lebih aman.

Di lab ini, Anda akan:

- Membuat dan mengenkripsi file teks sampel.
- Mendekripsi file zip terenkripsi.

Catatan: Lab ini harus digunakan hanya untuk tujuan instruksional. 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: Membuat dan Mengenkripsi File

Di bagian ini, Anda akan membuat beberapa file teks yang akan digunakan untuk membuat file zip terenkripsi di langkah selanjutnya.

Langkah 1: Buat file teks.

A. Mulai VM Stasiun Kerja CyberOps.

B. Buka jendela terminal. Verifikasi bahwa Anda berada di direktori home analis. Jika tidak, masukkan **cd ~** di permintaan terminal.

C. Buat folder baru bernama Zip-Files menggunakan perintah **mkdir Zip-Files .**

D. Pindah ke direktori itu menggunakan perintah **cd Zip-Files .**

e. Masukkan berikut ini untuk membuat tiga file teks.

[analyst@secOps Zip-Files]$ **echo Ini adalah contoh file teks > sample-1.txt** [analyst@secOps Zip-Files]$ **echo Ini adalah contoh file teks > sample-2.txt** [analis@secOps Zip- Files]$ **echo Ini adalah contoh file teks > sample-3.txt**

F. Verifikasi bahwa file telah dibuat, menggunakan perintah **ls .**

[analis@secOps Zip-Files]$ **ls -l**

jumlah 12

-rw-r--r-- 1 analis analis 27 13 Mei 10:58 sample-1.txt

-rw-r--r-- 1 analis analis 27 13 Mei 10:58 sample-2.txt

-rw-r--r-- 1 analis analis 27 13 Mei 10:58 sample-3.txt

Langkah 2: Zip dan enkripsi file teks.

Selanjutnya, kita akan membuat beberapa file zip terenkripsi menggunakan panjang kata sandi yang bervariasi. Untuk melakukannya, ketiga file teks tersebut akan dienkripsi menggunakan utilitas **zip .**

A. Buat file zip terenkripsi bernama **file-1.zip** yang berisi tiga file teks menggunakan perintah berikut:

[analyst@secOps Zip-Files]$ **zip –e file-1.zip sampel***

B. Saat diminta kata sandi, masukkan kata sandi satu karakter pilihan Anda. Pada contoh surat **B** dimasukkan. Masukkan huruf yang sama saat diminta untuk memverifikasi.

[analyst@secOps Zip-Files]$ **zip -e file-1.zip sampel-***

Masukkan kata kunci:

Verifikasi kata sandi:

menambahkan: sample-1.txt (disimpan 0%)

menambahkan: sample-2.txt (disimpan 0%)

menambahkan: sample-3.txt (disimpan 0%)

C. Ulangi prosedur untuk membuat 4 file lainnya berikut ini

• **file-2.zip** menggunakan sandi 2 karakter pilihan Anda. Dalam contoh kami, kami menggunakan **R2.** • **file-3.zip** menggunakan sandi 3 karakter pilihan Anda. Dalam contoh kami, kami menggunakan **0B1.** • **file-4.zip** menggunakan kata sandi 4 karakter pilihan Anda. Dalam contoh kami, kami menggunakan **Y0Da.** • **file-5.zip** menggunakan kata sandi 5 karakter pilihan Anda. Dalam contoh kami, kami menggunakan **C-3P0.**

D. Verifikasi bahwa semua file zip telah dibuat menggunakan perintah **ls -lf* .**

[analis@secOps Zip-Files]$ **ls -lf***

-rw-r--r-- 1 analis analis 643 13 Mei 11:01 file-1.zip

-rw-r--r-- 1 analis analis 643 13 Mei 11:02 file-2.zip

-rw-r--r-- 1 analis analis 643 13 Mei 11:03 file-3.zip

-rw-r--r-- 1 analis analis 643 13 Mei 11:03 file-4.zip

-rw-r--r-- 1 analis analis 643 13 Mei 11:03 file-5.zip

e. Coba buka zip menggunakan kata sandi yang salah seperti yang ditunjukkan.

[analyst@secOps Zip-Files]$ **unzip file-1.zip** Arsip: file-1.zip

[file-1.zip] contoh-1.txt kata sandi:

sandi salah--masukkan kembali:
sandi salah--masukkan kembali:
melewatkan: sample-1.txt kata kunci Salah
[file-1.zip] contoh-2.txt kata sandi: kata sandi salah--
masukkan kembali:
sandi salah--masukkan kembali:
melewatkan: sample-2.txt kata kunci Salah
[file-1.zip] kata sandi contoh-3.txt:
kata sandi salah--masukkan kembali: kata
sandi salah--masukkan kembali: melompati:
sample-3.txt kata kunci Salah

Bagian 2: Pulihkan Kata Sandi File Zip Terenkripsi

Pada bagian ini, Anda akan menggunakan utilitas **fcrackzip** untuk memulihkan kata sandi yang hilang dari file zip terenkripsi. Fcrackzip mencari setiap file zip yang diberikan untuk file terenkripsi dan mencoba menebak kata sandinya menggunakan metode brute-force.

Alasan kami membuat file zip dengan panjang kata sandi yang bervariasi adalah untuk melihat apakah panjang kata sandi memengaruhi waktu yang diperlukan untuk menemukan kata sandi.

Langkah 1: Pengantar fcrackzip

Dari jendela terminal, masukkan perintah **fcrackzip –h** untuk melihat opsi perintah terkait.

Dalam contoh kami, kami akan menggunakan opsi perintah **–v, -u,** dan **-l .** Opsi -l akan dicantumkan terakhir karena menentukan kemungkinan panjang kata sandi. Jangan ragu untuk bereksperimen dengan opsi lain.

Langkah 2: Memulihkan Kata Sandi menggunakan fcrackzip

A. Sekarang coba pulihkan kata sandi dari file **file-1.zip .** Ingat, kata sandi satu karakter digunakan untuk mengenkripsi file. Oleh karena itu, gunakan perintah **fcrackzip** berikut :

[analyst@secOps Zip-Files]$ **fcrackzip -vul 1-4 file-1.zip** menemukan file 'sample-1.txt',
(ukuran cp/uc 39/ 27, bendera 9, chk 5754)
ditemukan file 'sample-2.txt', (ukuran cp/uc 39/ 27, bendera 9, chk 5756)
ditemukan file 'sample-3.txt', (ukuran cp/uc 39/ 27, bendera 9, chk 5757)

PASSWORD DITEMUKAN!!!!: pw == B

Catatan: Panjang kata sandi dapat diatur kurang dari 1 – 4 karakter.

Berapa lama untuk menemukan kata sandi?

B. Sekarang coba pulihkan kata sandi dari file **file-2.zip .** Ingat, kata sandi dua karakter digunakan untuk mengenkripsi file. Oleh karena itu, gunakan perintah **fcrackzip** berikut :

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-2.zip** menemukan file 'sample-1.txt',
(ukuran cp/uc menemukan file 'sample-2.txt', (ukuran 39/ 27, bendera 9, chk 5754)
cp/uc ditemukan file 'sample-3.txt', (ukuran cp/uc 39/ 27, bendera 9, chk 5756)
39/ 27, bendera 9, chk 5757)

PASSWORD DITEMUKAN!!!!: pw == R2

Berapa lama untuk menemukan kata sandi?

C. Ulangi prosedur dan pulihkan kata sandi dari file **file-3.zip .** Ingat, bahwa tiga karakter kata sandi digunakan untuk mengenkripsi file. Saatnya untuk melihat berapa lama waktu yang diperlukan untuk menemukan kata sandi 3 huruf. Gunakan perintah **fcrackzip** berikut :

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-3.zip** menemukan file 'sample-1.txt',
(ukuran cp/uc 39/ 27, bendera 9, chk 5754)
ditemukan file 'sample-2.txt', (ukuran cp/uc 39/ 27, bendera 9, chk 5756)
ditemukan file 'sample-3.txt', (ukuran cp/uc 39/ 27, bendera 9, chk 5757)

PASSWORD DITEMUKAN!!!!: pw == 0B1

Berapa lama untuk menemukan kata sandi?

D. Berapa lama untuk memecahkan kata sandi empat karakter? Ulangi prosedur dan pulihkan kata sandi **file-4.zip** file. Saatnya untuk melihat berapa lama waktu yang diperlukan untuk menemukan kata sandi menggunakan perintah **fcrackzip** berikut :

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-4.zip** menemukan file 'sample-1.txt',
(ukuran cp/uc menemukan file 'sample-2.txt', (ukuran 39/ 27, bendera 9, chk 5754)
cp/uc ditemukan file 'sample-3.txt', (ukuran cp/uc 39/ 27, bendera 9, chk 5756)
39/ 27, bendera 9, chk 5757)

memeriksa pw X9M~

PASSWORD DITEMUKAN!!!!: pw == Y0Da

Berapa lama untuk menemukan kata sandi?

e. Berapa lama untuk memecahkan kata sandi lima karakter? Ulangi prosedur dan pulihkan kata sandi **file-5.zip** file. Panjang kata sandi adalah lima karakter, jadi kita perlu menyetel opsi perintah **-l** ke **1-5.** Sekali lagi, waktu untuk melihat berapa lama untuk menemukan kata sandi menggunakan perintah **fcrackzip** berikut :

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-5 file-5.zip** menemukan file 'sample-1.txt',
(ukuran cp/uc menemukan file 'sample-2.txt', (ukuran 39/ 27, bendera 9, chk 5754)
cp/uc ditemukan file 'sample-3.txt', (ukuran cp/uc 39/ 27, bendera 9, chk 5756)
39/ 27, bendera 9, chk 5757)

memeriksa pw CH*~

PASSWORD DITEMUKAN!!!!: pw == C-3P0

Berapa lama untuk menemukan kata sandi?

F. Pulihkan Kata Sandi 6 Karakter menggunakan fcrackzip

Tampaknya kata sandi yang lebih panjang membutuhkan lebih banyak waktu untuk ditemukan dan oleh karena itu, lebih aman. Namun, kata sandi 6 karakter tidak akan menghalangi penjahat dunia maya.

Menurut Anda, berapa lama waktu yang dibutuhkan fcrackzip untuk menemukan kata sandi 6 karakter?

Untuk menjawab pertanyaan itu, buat file bernama **file-6.zip** menggunakan kata sandi 6 karakter pilihan Anda. Dalam contoh kami, kami menggunakan **JarJar.**

[analyst@secOps Zip-Files]$ **zip –e file-6.zip sampel***

G. Ulangi prosedur untuk memulihkan kata sandi file-6.zip **menggunakan fcrackzip** berikut memerintah:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-6 file-6.zip**

Berapa lama fcrackzip untuk menemukan kata sandi?

Kebenaran sederhananya adalah kata sandi yang lebih panjang lebih aman karena membutuhkan waktu lebih lama untuk ditemukan.

Berapa lama Anda akan merekomendasikan kata sandi agar aman?