JURNAL TEKNIK MESIN, ELEKTRO DAN ILMU KOMPUTER

Halaman Jurnal: https://journal.amikveteran.ac.id/index.php/teknik
Halaman UTAMA Jurnal : https://journal.amikveteran.ac.id/index.php

ANALISA PERBANDINGAN TOOLS CEWL,CRUNCH,CUPP DALAM PENGUJIAN PASSWORD CRACKING

Diva Ananda Putra[a], Gede Ananta Cahya Maheswara[b], Ni Luh Listiana Putri Mita Dewi[c], Ilham Ramdhani[d], I Made Edy Listartha[e] dan Gede Arna Jude Saskara[f]

[a] Teknik dan Kejuruan / Teknik Informatika, diva.ananda@undiksha.ac.id , Universitas Pendidikan Ganesha
[b] Teknik dan Kejuruan / Teknik Informatika, ananta.cahya@undiksha.ac.id , Universitas Pendidikan Ganesha
[c] Teknik dan Kejuruan / Teknik Informatika, listiana.putri@undiksha.ac.id , Universitas Pendidikan Ganesha
[d] Teknik dan Kejuruan / Teknik Informatika, ilham.ramdhani@undiksha.ac.id , Universitas Pendidikan Ganesha
[e] Teknik dan Kejuruan / Teknik Informatika, listartha@undiksha.ac.id , Universitas Pendidikan Ganesha
[f] Teknik dan Kejuruan / Teknik Informatika, jude.saskara@undiksha.ac.id , Universitas Pendidikan Ganesha

ABSTRACT

The rapid development of technology has made almost everyone access the internet. A password cracking is a process for dismantling secret passwords from data on a computer system. The amount of information and data contained on the internet is of course accompanied by the high potential for security attacks from this data. Kali Linux is an advanced Linux distribution for conducting Penetration Testing and conducting security audits. The existence of a security hole certainly requires serious attention so that it is not misused by irresponsible parties. To anticipate this, one of them is by analyzing the possibility of security holes in a password. The test was carried out by comparing the tools cewl, crunch, cupp to generate random password.

Keywords: *Password Attack, Kali Linux, Cewl, Crunch, Cupp*.

Abstrak

Perkembangan teknologi yang semakin pesat menjadikan hampir setiap orang melakukan akses internet, *Password cracking* merupakan sebuah proses untuk melakukan pembongkaran *password* rahasia dari sebuah data yang berada pada sebuah sistem komputer. Banyaknya informasi serta data yang terdapat dalam internet juga tentunya dibarengi dengan tingginya potensi serangan keamanan dari data tersebut. *Kali linux* merupakan salah satu distribusi *linux* tingkat lanjut untuk melakukan sebuah *Penetration Testing* serta melakukan audit keamanan. Terdapatnya sebuah celah keamanan tentu memerlukan perhatian serius supaya tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Untuk mengantisipasi hal tersebut, salah satu diantaranya yaitu dengan dengan melakukan analisa terhadap kemungkinan celah keamanan pada suatu *password*. Pengujian yang dilakukan adalah dengan membandingkan *tools cewl, crunch, cupp* untuk melakukan *generate random password*.

Kata Kunci: *Password Attck, Kali Linux, Cewl, Crunch, Cupp*.

1. PENDAHULUAN

Pada era sekarang, perkembangan teknologi yang semakin pesat menjadikan hampir setiap orang pasti melakukan akses *internet*, dari anak-anak hingga dewasa semua melakukanya. Password attack merupakan sebuah proses untuk melakukan pembongkaran password rahasia dari sebuah data yang berada pada sebuah sistem komputer. Secara umum pengertian *password cracking* adalah mencoba menebak secara berulang untuk menemukan celah dari sebuah password[1]. Banyaknya informasi serta data yang terdapat dalam *internet* juga tentunya dibarengi dengan tingginya potensi serangan keamanan dari data tersebut. *Kali linux* merupakan salah satu distribusi *linux* tingkat lanjut untuk melakukan sebuah *Penetration* Testing serta melakukan audit keamanan. *Kali Linux* pada dasarnya

Received February 27, 2023; Revised March 17, 2023; Accepted March 24, 2023

merupakan sebuah pembangunan kembali *BackTrack Linux* secara sempurna yang berdasarkan standar pengembangan Debian[2]. Salah satu masalah keamanan yang terdapat adalah *password cracking*. Terdapatnya sebuah celah keamanan tentu memerlukan perhatian serius supaya tidak disalahgunakan oleh pihak yang tidak bertanggung jawab sehingga dapat menimbulkan kerugian. Berdasar dari hal tersebut, tentunya memerlukan sebuah upaya untuk mencegah ancaman tersebut, salah satu diantaranya yaitu dengan dengan melakukan analisa terhadap kemungkinan celah keamanan pada suatu password. dalam penelitian ini, tool yang digunakan adalah *Cewl, Crunch, Cupp* yang merupakan sebuah tools untuk *generator password* dengan *wordlist*[3]. Penelitian ini bertujuan untuk mengetahui *cracking password* berbasis *wordlist* dengan membandingkan *tools cewl, crunch, cupp.* Hasil dari pengujian yang diperoleh dapat digunakan sebagai acuan untuk mengamankan data dari sistem yang berguna untuk meningkatkan keamanan *password* pengguna dengan cara membuat kombinasi *password* yang Panjang serta unik.

2. TINJAUAN PUSTAKA

2.1. Tools CeWL

CeWL (custom word list generator) merupakan aplikasi yang menjelajahi *URL (Uniform Resource locators)* tertentu sampai kedalaman tertentu, dan mengembalikan daftar kata yang kemudian dapat digunakan untuk *cracker* suatu *password*[4]. Secara opsional, *CeWL* dapat mengikuti tautan eksternal dan juga dapat digunakan sebagai mencari informasi lengkap dalam suatu website. *Tools* lain yang disediakan oleh *tools CeWL adalah FAB (Files Already Bagged). FAB* pada dasarnya melakukan pengekstrakan konten dari pembuat serta dari metadata beberapa file yang bertujuan membuat daftar kemungkinan *username*. *Username* ini dapat digunakan bersama dengan daftar *password* yang dibuat oleh *CeWL. FAB* juga menggunakan sebuah teknik ekstraksi metadata yang sama dengan *CeWL.*

2.2. Tools Crunch

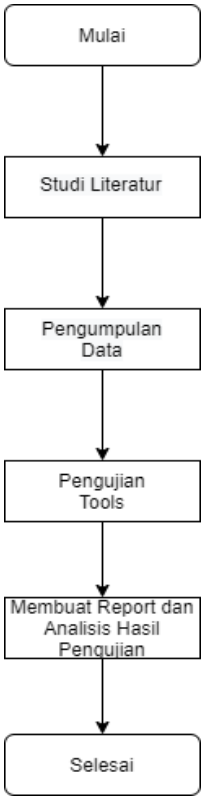
Tools Crunch yang digunakan untuk pengganti *wordlist* adalah suatu hal untuk mencocokan *password* tanpa harus memasukkan kemungkinan-kemungkinan kata dalam bentuk file *txt*. Hasil mencocokan dengan *tool crunch* pasti bisa didapatkan, tetapi memakan waktu yang cukup lama dalam pencocokannya apabila terjadi kombinasi dari sebuah *password access point* begitu Panjang dan unik, karena semua karakter baik huruf, symbol, maupun angka digabungkan dengan berbagai bentuk kombinasi[5].

2.3. Tools Cupp

Cupp (*Common User Password Profiler)* merupakan sebuah aplikasi yang dibuat dalam bahasa pemrograman *python* yang berfungsi untuk membuat *dictionary* atau membuat sebuah daftar kata *password* untuk mendapatkan target yang spesifik[6]. Bentuk autentikasi yang paling umum adalah kombinasi *username* dan *password*. Jika keduanya cocok dengan nilai yang disimpan dalam tabel, pengguna akan diautentikasi untuk terhubung.

3. METODOLOGI PENELITIAN

Metode penelitian ini menggunakan teknik seperti yang ditunjukan pada gambar 1.



Gambar 1. Alur dari metode penelitian

A. Studi Literatur

Pada tahap ini yakni melakukan pencarian dari berbagai sumber untuk mendapatkan informasi dari literasi-literasi terdahulu sebagai landasan teori terhadap permasalahan yang sejenis dengan penelitian ini.

B. Pengumpulan Data

Pada tahap ini dilanjutkan dengan mengumpulkan data menggunakan teknik observasi yang artinya mengamati penelitian secara langsung, kemudian melakukan pencatatan hasil dari penelitian tersebut, dan menganalisa hasil dari penelitian tersebut. Langkah pertama yang dilakukan yaitu mencari tools yang digunakan untuk mengakses password pada worldlist. Adapun tools yang digunakan adalah: cewl, crunch, cupp. Selanjutnya melakukan instalasi cewl, crunch, cupp pada kali linux.

C. Pengujian Tools

Selanjutnya, masuk ke tahap pengujian Tools untuk melakukan generate password dengan menggunakan aplikasi Kali Linux. Dalam pengujian tools cewl, diperlukan url dari website yang dituju untuk melakukan generate random password.

D. Report dan Hasil Pengujian

Setelah pengujian final mencapai 100%, selanjutnya dilakukan generate report untuk memperoleh hasil dari pengujian ketiga tools sebagai bahan dalam proses analisis. Setelah proses analisis selesai, tahap akhir dari penelitian ini adalah penyusunan laporan.

4. HASIL DAN PEMBAHASAN

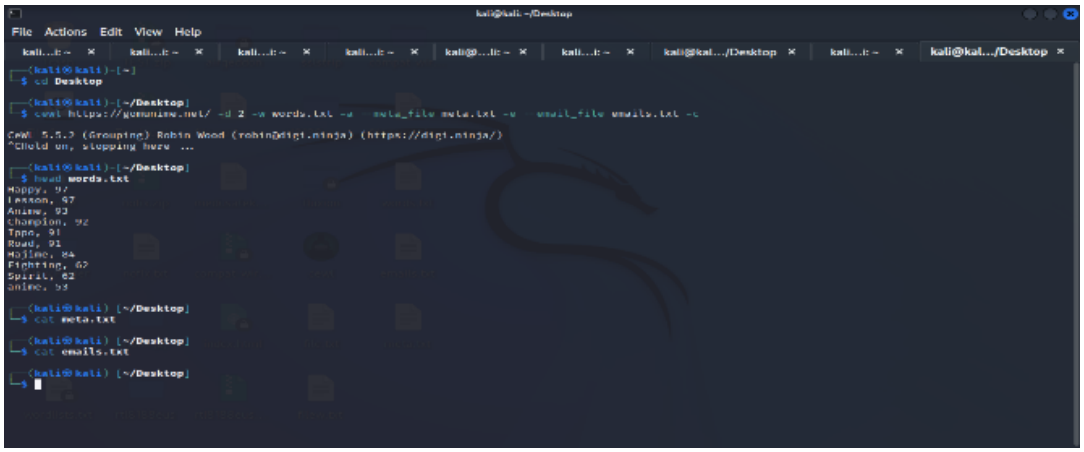
4.1 Tahapan pengujian

Tahap pengujian yang dilakukan menggunakan *tools Cewl, Crunch, Cupp* untuk melakukan *generate random password* dengan menggunakan aplikasi *Kali Linux* terbagi menjadi tiga pengujian sebagai berikut :

4.1.1 Pembuatan Wordlist

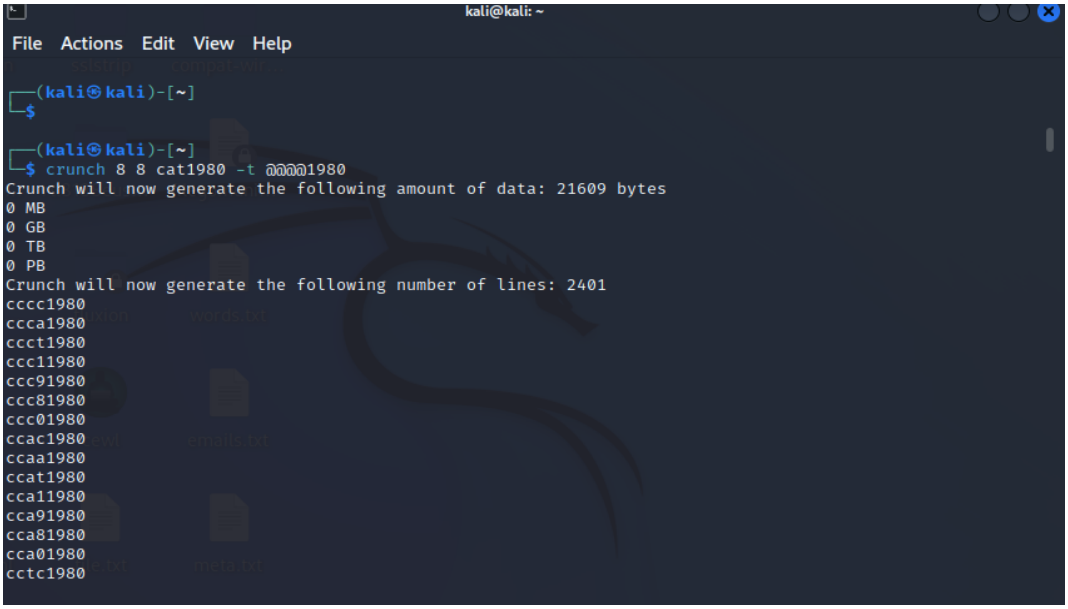
Pembuatan *wordlist* untuk menebak kemungkinan *password default* yaitu dengan melakukan

generate random password menggunakan *tools cewl*, dihasilkan berdasarkan tulisan yang dilakukan di target. Target yang dituju oleh *tools cewl* mengunakan https://gomunime.net/ dengan pengujian ditunjukan pada gambar 2.



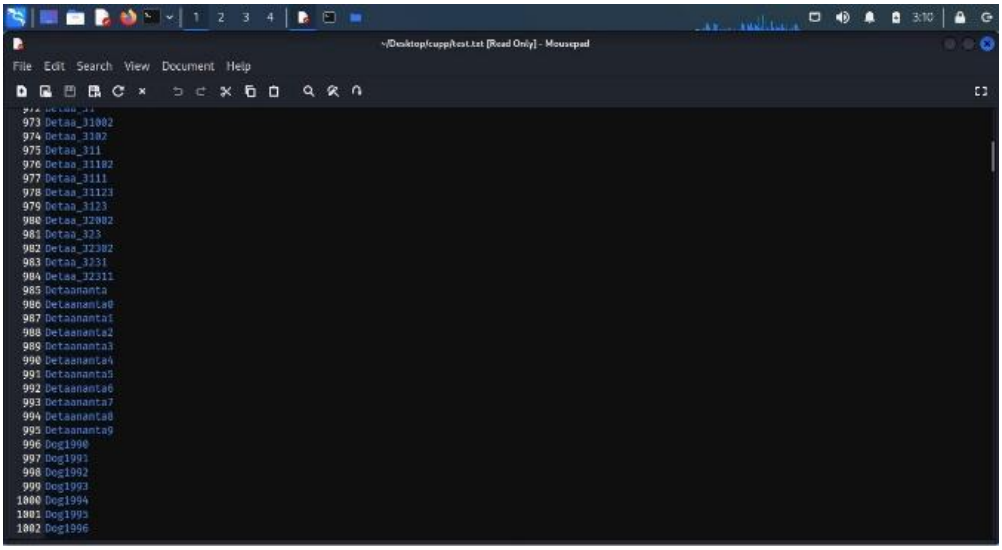
Gambar 2. *Tools cewl*

Pembuatan *wordlist* untuk menebak kemungkinan *password default* dengan melakukan *generate random password* menggunakan *tools crunch*, dihasilkan berdasarkan data yang diinputkan. Pengujian yang dilakukan ditunjukan pada gambar 3.



Gambar 3. *Tools crunch*

Pembuatan *wordlist* untuk menebak kemungkinan *password default* dengan melakukan *generate random password* menggunakan *tools cupp*, dihasilkan berdasarkan data yang diinputkan. Pengujian yang dilakukan ditunjukan pada gambar 4.



Gambar 4. *Tools cupp*

4.1.2 Perhitungan Kecepatan

Pada perhitungan kecepatan *generate random password* dengan menggunakan *tools cewl, crunch, cupp*. Tingkat kecepatan diukur mulai pasa saat *user* menekan *enter* setelah memasukan data yang akan dilakukan *generate* hingga selesai proses *generate random password*.

Tabel 1.
Tahapan Perhitungan Kecepatan

Fokus	Tahapan	Aktivitas	Alat
Perhitungan Kecepatan	*password generation speed calculation*	Pengujian yang dilakukan dengan mengukur tingkat kecepatan *generate random password* terhadap tiga *tools*	*Tools Cewl, Crunch, Cupp*

4.1.3 Perhitugan Kisaran Password

Pada perhitungan kisaran *password* dengan menggunakan *tools cewl, crunch, cupp*. Perhitungan dilakukan dengan mejumlahkan karakter yang *tergenerate* dengan panjang karakter yang ingin *digenerate* dan panjang kunci.

Tabel 2.
Tahapan Perhitungan Kisaran *Password*

Fokus	Tahapan	Aktivitas	Alat
Perhitungan Kisaran *Password*	*Calculation of the Range of Passwords generated*	Pengujian yang dilakukan dengan menghitung kisaran jumlah yang dihasilkan	*Tools Cewl, Crunch, Cupp*

		generate random password terhadap tiga *tools*		

4.2 Hasil Pengujian

Berdasarkan hasil *generate report* dari tahap pengujian yang dilakukan menggunakan *tools Cewl, Crunch, Cupp* untuk melakukan *generate password* dengan menggunakan aplikasi *Kali Linux* terbagi menjadi tiga hasil pengujian, sehingga didapatkan hasil sebagai berikut :

4.1.4 Pembuatan Wordlist

Pembuatan *wordlist* untuk menebak kemungkinan *password default* yaitu dengan melakukan *generate random password* menggunakan *tools cewl, crunch, cup* didapatkan hasil yang disajikan pada tabel 3.

Tabel 3.
Hasil Pengujian Pembuatan *Wordlist*

Fokus	Tahapan	Aktivitas	Alat	Hasil
Pembuatan Wordlist	*generate random password*	Pengujian yang dilakukan dengan pembuatan *wordlist* dengan melakukan *generate random password*	*Tools Cewl*	*Success*
Pembuatan Wordlist	*generate random password*	Pengujian yang dilakukan dengan pembuatan *wordlist* dengan melakukan *generate random password*	*Tools Crunch*	*Success*
Pembuatan Wordlist	*generate random password*	Pengujian yang dilakuk	*Tools Cupp*	*Success*

	an dengan pembuatan *wordlist* dengan melakukan *generate random password*

4.1.5 Perhitungan Kecepatan

Perhitungan kecepatan yang digunakan adalah kecepatan *generate random password* dengan menggunakan *tools cewl, crunch, cup* pada *Kali Linux*. Namun lama waktu hasil *generate random password* ini tidak sepenuhnya akurat dikarenakan testing dilakukan secara *online* sehingga juga terdapat faktor kualitas koneksi juga pada saat mengakses *tools* yang digunakan. Hasil pengujian yang dilakukan ditunjukan pada tabel 4.

Tabel 4.
Hasil Pengujian Perhitungan Kecepatan

Alat	Mulai	Akhir	Lama	Hasil
Tools Cewl	20:25:15	20:29:45	4, 30 min	*Success*
Tools Crunch	20:33:17	20:37:53	4, 36 min	*Success*
Tools Cupp	20:39:18	20:43:42	4, 24 min	*Success*

4.1.6 Perhitungan Kisaran Password

Dalam medapatkan hasil perhitungan kisaran *password* dengan menggunakan *tools cewl, crunch, cupp* yang dihasilkan dapat menggunakan formula seperti berikut, KM = L^(m) + L^(m+1) L^(m+2) + ... + L^(m+n). Dimana KM merupakan jumlah karakter yang *tergenerate*, L merupakan panjang karakter yang ingin *digenerate* serta m merupakan panjang kunci. Hasil pengujian yang dilakukan disajikan pada tabel dibawah.

Tabel 5.
Hasil Pengujian Perhitungan Kisaran *Password* dengan *tools Cewl*

Jenis Password	Panjang Kunci	Jenis Karakter	Jumlah kata yang *tergenerate*
1234567890	8	Angka	800000
abcdefgh	8	Huruf Kecil	2088290821
ABCDEFGH	8	Huruf Kapital	2088290821
?/!@#$%^	8	Karakter Spesial	5472000

Tabel 6.
Hasil Pengujian Perhitungan Kisaran *Password* dengan *tools Crunch*

Jenis Password	Panjang Kunci	Jenis Karakter	Jumlah kata yang *tergenerate*

1234567890	8	Angka	800000
abcdefgh	8	Huruf Kecil	214702671
ABCDEFGH	8	Huruf Kapital	214702671
?/!@#$%^	8	Karakter Spesial	5531000

Tabel 7.
Hasil Pengujian Perhitungan Kisaran *Password* dengan *tools Cupp*

Jenis Password	Panjang Kunci	Jenis Karakter	Jumlah kata yang *tergenerate*
1234567890	8	Angka	1000000
abcdefgh	8	Huruf Kecil	258957235
ABCDEFGH	8	Huruf Kapital	258957235
?/!@#$%^	8	Karakter Spesial	6157000

5. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa tahap pengujian yang dilakukan menggunakan *tools cewl, crunch, cupp* untuk melakukan *generate random password* dengan menggunakan aplikasi *Kali Linux***.** Fokus dari pengujian ini terbagi menjadi tiga yaitu pembuatan *wordlist*, perhitungan kecepatan, perhitungan kisaran *password.* Hasil yang diperoleh berdasarkan ketiga pengujian tersebut yakni dimana *tools cupp* paling efektif untuk melakukan *generate random password* dengan menggunakan aplikasi *Kali Linux*. Dimana dimana pada *tools cupp* jumlah kata yang *tergenerate* lebih banyak jika dibandingkan dengan dua *tools* lainya yakni *cewl* dan *crunch.* Mengenai hal lebih lanjut, penulis menyarankan agar pembaca selalu mengganti *password* secara berkala serta membuat *password* unik dengan kombinasi angka, huruf kecil, huruf besar, dan karakter special untuk mencegah terjadinya penyalahgunaan data pribadi dan timbulnya hal - hal berbahaya.

DAFTAR PUSTAKA

[1] M. Zikrillah, J. Raya, P.-P. Km, K. Ogan Ilir, and S. Selatan, "Analisa Serangan Password Cracking Pada Windows 10 Menggunakan Tools Pwdump v7.1 dan Cain & Abel."

[2] M. I. Rusdi and D. Prasti, "Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux," 2019.

[3] A. Universitas, P. Madiun, ; Jl, S. Budi, and N. 85, "Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux," *Juli 2020 Generation Journal*, vol. 4, no. 2, [Online]. Available: http://www.starrybyte.com

[4] U. Bina, D. Palembang, H. D. Sabdho, and M. Ulfa, "Seminar Hasil Penelitian Vokasi (SEMHAVOK) ANALISIS KEAMANAN JARINGAN WIRELESS MENGGUNAKAN METODE PENETRATION TESTING PADA KANTOR PT. MORA TELEMATIKA INDONESIA REGIONAL PALEMBANG".

[5] I. Taufiqurrohman, N. Widiyasono, H. Mubarok, J. Siliwangi, and N. 24 Tasikmalaya, "Pemanfaatan Raspberry Pi untuk Hacking dan Forensic dengan metode NIST (National Institute of Standards and Technology)," 2017.

[6] T. P. Sukarno, "PERANCANGAN DAN ANALISIS KEAMANAN JARINGAN MENGGUNAKAN HONEYPOT UNTUK MENDETEKSI SERANGAN BRUTE FORCE PADA CLOUD COMPUTING," *repository amikom*, 2017. https://repository.amikom.ac.id/files/2017/Publikasi_13.11.6842.pdf (accessed Nov. 22, 2022).