**JURNAL INFORMATIKA DAN TEKONOLOGI KOMPUTER**
Halaman Jurnal: https://journal.amikveteran.ac.id/index.php/jitek
Halaman UTAMA Jurnal : https://journal.amikveteran.ac.id/index.php

# ANALISA EVALUASI KINERJA *SOFTWARE PASSWORD ATTACKER* PADA BERKAS FILE *ZIP*

**Irhan Hisyam Dwi Nugroho[a], Kadek Pebriawan[b], Ketut Gede Tegar Maranom Jati[c], I Gede Cipta Aphila Diptha[d], I Made Edy Listartha[e], Gede Arna Jude Saskara[f]**

[a] Fakultas Teknik dan Kejuruan / Teknik Informatika, irhan@undiksha.ac.id, Universitas Pendidikan Ganesha
[b] Fakultas Teknik dan Kejuruan / Teknik Informatika, Universitas Pendidikan Ganesha
[c] Fakultas Teknik dan Kejuruan / Teknik Informatika, Universitas Pendidikan Ganesha
[d] Fakultas Teknik dan Kejuruan / Teknik Informatika, Universitas Pendidikan Ganesha
[e] Fakultas Teknik dan Kejuruan / Teknik Informatika, Universitas Pendidikan Ganesha
[f] Fakultas Teknik dan Kejuruan / Teknik Informatika, Universitas Pendidikan Ganesha

***ABSTRACT***

*As we know, in this era of rapid technological progress, we cannot avoid threats to cyber security, cyber security itself is an effort to protect computer systems and data from various threats. In Indonesia alone, as of September 13, 2022, there have been recorded as many as 12.74 million accounts that have experienced leaks, and this makes Indonesia the 3rd country with the most number of data leaks in the world. One solution that can be done to protect the data that is owned is to put it in an archive such as ZIP, ZIP functions to combine several rice into one and reduce the size. And to secure the data in a ZIP file, you can set a password. The password is a combination of letters, numbers and symbols, with this combination it will be difficult for hackers to carry out their actions.*

**Keywords**: *password, zip, cyber security*

**ABSTRAK**

Seperti yang kita ketahui pada zaman kemajuan teknologi yang pesat ini kita tidak dapat terhindar dari adanya ancaman terhadap keamanan siber, keamanan siber sendiri merupakan upaya untuk melindungi sistem komputer dan data dari berbagai ancaman. Di Indonesia sendiri hingga tanggal 13 September 2022 sudah tercatat ada sebanyak 12,74 juta akun yang mengalami kebocoran, dan ini menjadikan Indonesia sebagai negara dengan urutan ke-3 dengan jumlah kebocoran data terbanyak di dunia. Salah satu solusi yang dapat dilakukan untuk melindungi data yang dimiliki adalah dengan memasukkannya kedalam sebuah *archive* seperti zip. zip berfungsi untuk menggabungkan beberapa beras menjadi satu dan ukurannya diperkecil. Dan untuk mengamankan data di dalamnya sebuah berkas *ZIP* dapat diatur *password*-nya. *Password* merupakan kombinasi dari huruf, angka, dan simbol, dengan adanya kombinasi ini akan menyulitkan peretas dalam melakukan aksinya.

**Kata Kunci**: Password, zip, Keamanan siber

## 1. PENDAHULUAN

Tidak dipungkiri, laju perkembangan teknologi yang luar biasa di era digital seperti saat ini memang banyak memberikan dampak positif. Namun dibalik segala kelebihannya, sesuatu hal diyakini akan mendatangkan hal-hal negative juga. Disatu sisi, teknologi mampu menghadirkan kecepatan pendistribusian informasi yang luar biasa. Namun, disisi lain, mengintip tindak kejahatan yang berevolusi dalam bentuk kejahatan cyber. Salah satu cyber crime yang paling populer adalah kebocoran data [1] Informasi Kredensial macam kata sandi (password) adalah satu hal yang perlu dijaga keamananya. Salah satu caranya adalah dengan menggunakan password kuat yang sulit ditebak atau dikombinasikan dengan berbagai angka dan simbol. Meski demikian, sekitar 89 persen orang Indonesia ternyata masih mempertahankan kebiasaan buruk untuk menggunakan password lemah [2]

*Received Desember 25, 2022; Revised Januari 16, 2023; Accepted Maret 24, 2023*

Kata sandi adalah bentuk pengguna yang paling umum teknik otentikasi yang digunakan dalam berbagai komputasi aplikasi seperti ATM perbankan, situs web, sistem operasi masuk dan ponsel. Namun, kata sandi pengguna adalah retak dan ditawar di bawah kerentanan yang berbeda [3]. Musuh mengamati bagaimana pengguna memasukkan kata sandi. Akhirnya, penyerang dapat mengamati dan menggunakan semua opsi yang terkait dengan panjang sandi [4]. Pola serangan brute force semua kemungkinan kombinasi kata sandi sampai yang benar diterima untuk memecahkan metode otentikasi [5]. Ini adalah waktu mengkonsumsi sebagai mencari semua kombinasi dan kebanyakan digunakan untuk memecahkan password terenkripsi. Ini efektif untuk kecil kata sandi panjang. Serangan kamus adalah bentuk kasar serangan paksa tetapi lebih cepat serangan brute force dan upayanya untuk mencocokkan kata sandi dengan kata-kata yang paling sering digunakan dalam keseharian kita kehidupan. Dalam teknik ini, penyerang membuat kamus kata-kata yang paling umum digunakan dan mereka dapat menggunakan kata-kata ini untuk mematahkan mekanisme otentikasi [6].

Sebuah password dapat dibongkar dengan menggunakan program yang disebut sebagai password cracker adalah program yang mencoba membuka sebuah password yang telah terenkripsi dengan menggunakan sebuah algoritma tertentu dengan cara mencoba semua kemungkinan. Teknik ini sangat sederhana tetapi efektivitasnya luar biasa, dan tidak ada satu pun sistem yang aman dari serangan ini meski teknik ini memakan waktu yang sangat lama, khususnya untuk password yang sulit [7] . Dalam melakukan peretasan password terdapat 3 jenis metode secara umum, yaitu : Dictionary attack, brute-Force Attack dan Rainbow Table [8]

Keamanan file adalah suatu cara untuk melindungi file dari ancaman, baik dalam bentuk kesengajaan maupun tidak disengaja. Kemajuan teknologi informasi yang sangat pesat membuat permasalahan keamanan sering bermunculan dalam keamanan file [9].Berkas *ZIP* menjadi objek penelitian kami dalam menguji keamanan password dengan menggunakan 3 tools yang berasal dari *Opera system kali linux* yaitu *John The Ripper (JTR), Hashcat,* dan *Zydra*. ZIP merupakan format file arsip yang digunakan secara luas untuk mengompresi atau memampatkan satu atau beberapa file bersama-sama menjadi ke dalam satu lokasi sehingga mengurangi ukurannya secara keseluruhan serta memudahkan pemindahan file tersebut [10].

Penelitian ini akan memberi manfaat kepada pembaca untuk memberikan wawasan mengenai keamanan password. Semakin singkat password maka file tersebut akan mudah dibobol. Teknik yang digunakan 3 tools ini adalah *brute force*. *Brute Force attack* adalah Metode untuk mengakses perangkat yang diblokir dengan mencoba beberapa kombinasi kata sandi numerik/alfanumerik [11].*Feasibility* dari sebuah *brute force attack* tergantung dari panjangnya cipher yang ingin dipecahkan, dan jumlah komputasi yang tersedia untuk diserang [12].Untuk mendapatkan data hacker menggunakan berbagai cara untuk mendapatkan kata sandi. Metode coba-coba dikenal sebagai serangan brute force adalah dengan hacker mencoba menebak setiap kombinasi password yang memungkinkan [13]

Kebaruan penelitian ini adalah untuk menilai 4 aspek yaitu kecepatan, konsistensi, akurasi dan penulisan *syntax* dari *John The Ripper (JTR), Hashcat,* dan *Zydra*. Dalam melakukan brute force password pada file *zip* dan *winrar*. Dalam menguji tools tersebut kami menggunakan operasi sistem kali linux karena sistem operasi ini sebagai sistem operasi *penetration testing* [14].Tujuan dari penelitian ini untuk memberikan informasi kepada pembaca mengenai tools yang dapat digunakan dalam *brute force password* secara cepat, konsisten, sederhana syntax dan memiliki akurasi tinggi.

## 2. TINJAUAN PUSTAKA

### 2.1 Definisi Brute-force

Algoritma brute force adalah algoritma yang memecahkan masalah dengan sangat sederhana, langsung dan dengan cara yang jelas/lempang. Penyelesaian permasalahan kode cracking dengan menggunakan algoritma brute force akan menempatkan dan mencari semua kemungkinan kode dengan masukan karakter dan panjang kode dengan masukan karakter dan panjang kode tertentu tentunya dengan banyak sekali kombinasi kode. Dengan menggunkaan Algoritma ini pengguna hanya tinggal mendefinisikan karakter yang diinginkan dan berapa ukuran password. Tipe kemungkinan akan di generate oleh algoritma ini [15]

Brute force merupakan sebuah algorithma bekerja dengan memecahkan masalah secara jelas, dan melalui banyak opini atau pilihan, maka algoritma brute force merupakan sebuah metode pemecahan masalah logis yang memiliki kemampuan untuk memperoleh pemecahan masalah dengan baik. Hampir semua masalah yang dipecahkan dengan metode algoritma brute force ini berjalan dengan baik.

Akan tetapi, meski memiliki kelebihan berupa pemecahan yang berjalan baik. Algoritma brute force sangat sulit digunakan pada kebutuhan pemecahan masalah yang cepat. Hal ini disebabkan karena algoritma brute force membutuhkan kumpulan banyak opsi terlebih dahulu sebelum bisa dieksekusi. Hal ini bisa membuat pertimbangan dalam memilih opsi akan menjadi lebih lambat [16]

### 2.2 Password Cracking

*Password cracking* berarti mencoba memulihkan kata sandi dari komputer atau dari data yang dikirimkan komputer. Hal ini tidak memerlukan sebuah metode yang modern. Serangan brute-force dapat dimungkinkan kombinasi diperiksa juga dapat melakukan peretasan kata sandi. Meskipin kata sandi adalah alat keamanan akun yang sangat populer , kata sandi belum tentu menjadi pilihan yang paling aman[17] Itu terutama terjadi jika pengguna membuat kata sandi yang lemah, menggunakannya kembali, dan menyimpan salinan teks biasa disuatu tempat secara online.

Peretas kata sandi dalam melakukan proses mengekstraksi kata sandi dari hash kata sandi dapat terdapat ke dalam tiga cara[18] seperti berikut:

#### 2.2.1 Dictionary attack

Kebanyakan orang menggunakan kata sandii yang lemah dan umum. Mengambil daftar kata dan menambahkan beberapa permutasi seperti mengganti $ dengan S. Memungkinkan cracker kata sandi mempelajari banyak kata sandi dengan sangat cepat.

#### 2.2.2 Brute-force guessing attack

Hanya ada begitu banyak kata sandi potensial dengan panjang tertentu. Meskipun lambat, serangan brute force (mencoba semua kombinasi kata sandi) menjamin penyerang pada akhirnya akan memecahkan kata sandi

#### 2.2.3 Hybrid attack

Serangan hibrid menggabungkan kedua teknik ini. Dimulai dengan memeriksa untuk melihat apakah kata sandi dapat diretas menggunakan dictionary attack, kemudian beralih ke serangan brute-force jika tidak berhasil.

### 2.3 Kali linux

Linux berarti Unix Xlone, kernel yang ditulis oleh linus Torvalds dan dikembangkan dengan bantuan programmer dan hackers dari seluruh dunia. Linux memiliki semua fitur unix, termasuk multitasking, virtual memory, shared library. Demand load, shared copy on write executable, manajemen memori yang tepat dan jaringan TCP/IP[19]. Dengan fitur-fitur layaknya "*real operating system*". Tidak membuat linux menjadi mahal. Justru linux didapatkan secara gratis. Linux didistribusikan di bawah lisensi publik umum (GNU), yaitu lisensi dimana pemilik program tetap memegang hak ciptanya tetapi orang lain boleh mendistribusikan, memodifikasi atau bahkan menjual kembali program tersebut tetapi dengan syarat kode sumber asli harus disertakan dalam distribusi tersebut.

Kali linux adalah *open-source*, distribusi Linux berbasis Debian yang ditujukan untuk pengujian penetrasi dan Audit keamanan tingkat lanjut. Kali Linux adalah sulousi Multi platform, dapat diakses dan tersedia secara bebas untuk para profesional dan keaman informasi. Lebih dari 600 alat pengujian penetrasi terdapat pada sistem operasi kali linux [20] Kali Linux secara khusus dirancang untuk kebutuhan penetrasi.

### 2.4 John the Ripper

John the Ripper pertama kali dirilis pada tahun 1996, John the Ripper (JtR) adalah alat pembobol kata sandi yang awalnya diproduksi untuk sistem berbasis UNIX [21]. JtR dirancang untuk menguki kekuatan kata sandi, kata sandi terenkripsi (hash) dengan *brute-force* dan memecahkan kata sandi melalui *word-list.* Alat ini hadir dalam versi berlisensi GNU dan Berpemilik (Pro). Versi Pro, dirancang untuk digunakan oleh

penguji profesional, memiliki fitur tambahan seperti daftar kata multibahasa yang lebih besar, pengoptimalan kinerja, dan dukungan arsitektur 64-bit.

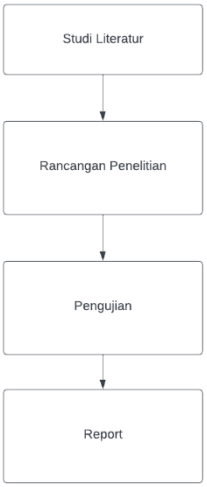
Cara kerja John the Ripper bekerja dengan tiga cara berbeda [21], tujuan umum dari semua ini pada akhirnya adalah untuk menebak kata sandi yang benar, tiga cara tersebut adalah Dictionary attack, Brute-force attack dan Rainbow tables. John adalah alat pembobol kata sandi yang populer dan kuat. Ini sering digunakan oleh penguji penetrasi dan peretas black hat karena keserbagunaan dan kemudahan penggunaanya. Dari penemuan hash otomatis hingga serangan berbasis kamu, John adalah alat yang terbaik yang dimiliki untuk perangkat pentesting[22]

### 2.5 Hashcat
Hashcat adalah cracker kata sandi yang populer dan efektif yang banyak digunakan oleh penguji penetrasi serta penjahat dan mata – mata [23]. Cara terbaik untuk mencegah penyerang menggunakan hascat adalah dengan menguji pertahanan sendiri terlebih dahulu untuk memastikan serangan semacam itu tidak berhail. Pada tingkat dasar, hashcat menebak kata sandi, melakukan hash, lalu membandingkan hash yang dihasilkan dengan hash yang coba diretas. Jika hash cocok, maka tahu kata sandinya. Jika tidak, teruslah menebak.

### 2.6 Zydra
Zydra adalah alat yang memiliki kemampuan untuk melakukan operasi pemulihan kata sandi dan juga memecahkan kata sandi pengguna yang tersedia di file bayangan linux. Alat ini ditulis dengan menggunakan bahasa pemrograman *python* dan mampu menggunakan *brute force* dan pencarian kamus dalam meretas kata sandi pengguna [24]. Dengan fitur multiprosesingnya, zydra memanfaatkan semua prosesor inti yang tersedia, ini membantu mempercepat laju pemecahan kata sandi. Zydra mendukung berbagai format file dan ini membuatnya semakin berguna untuk mendekripsi kata sandi. Alat ini mendukung file ZIP lama, file RAR, file PDF , dan file bayangan Linux. Kemampuannya untuk mendukung file bayangan linux memberikan keuntungan tambahan dalam meretas kata sandi pengguna dalam format bayangan.

Dengan menerapkan *brute-force attack* Zydra akan secara acak menghasilkan semua kata kunci potensial yang dapat digunakan untuk mengakses informasi kata sandi pengguna. Kunci dihasilkan dengan kecepatan tinggi karena tersediannya fitur multiprocessing saat digunakan pada akun pengguna, kata sandi korban akan mudah diakses dengan waktu singkat[24].

## 3. METODOLOGI PENELITIAN
### 3.1 Tahapan Penelitian
Penelitian ini menggunakan kerangka penelitian yang terdiri dari beberapa tahapan antara lain : (1) studi literatur, (2) Rancangan Penelitian, (3) Pengujian, (4) Report.




Gambar 1 : Tahapan Penelitian

Metode artikel ini menggunakan studi pustaka yaitu pengumpulan data dengan cara memahami dan mempelajari teori dari berbagai literatur yang berhubungan dengan penelitian [25]. Menurut Zed (2004) Ada empat tahap studi pustaka dalam penelitian yaitu menyiapkan perlengkapan alat yang diperlukan, menyiapkan bibliografi kerja, mengorganisasikan waktu dan membaca atau mencatat bahan penelitian menurut . Pengumpulan data tersebut menggunakan cara mencari sumber dan mengkonstruksi dari berbagai sumber seperti buku, jurnal dan riset-riset yang sudah pernah dilakukan. Bahan pustaka yang didapat dari berbagai referensi tersebut dianalisis secara kritis dan harus mendalam agar mendukung proposisi dan gagasan.

Rancangan pengujian adalah menguji 3 aspek pada software yaitu kecepatan ,konsistensi, akurasi ,dan penulisan *syntax*. Pengujian dilakukan dengan menguji file *zip* dengan menggunakan password angka sebanyak 5 angka acak ditambah 10 file *zip* dalam pengujian.

Tabel 1. Jenis Password pada file zip

| Password | Jenis Berkas |
|---|---|
| 12345 | Zip |
| 15243 | Zip |
| 12534 | Zip |
| 14235 | Zip |
| 12354 | Zip |
| 32451 | Zip |
| 41523 | Zip |
| 51342 | Zip |
| 14152 | Zip |
| 52415 | Zip |

1) Kecepatan
Indikator kecepatan menguji seberapa cepat tools dalam melakukan *brute force* pada berkas *zip*. Kecepatan berdasarkan waktu yang terdapat pada masing – masing *tools brute force password.*

2) Konsisten
Indikator kosistensi menguji perbandingan selisih seberapa cepat atau lama dalam melakukan *brute force* pada file *zip*.

3) Akurasi
Indikator Akurasi menguji tingkat keberhasilan tools dalam melakukan brute force password pada file *zip*. Nantinya dari 10 berkas *zip* akan ditemukan mana tools yang paling baik dalam melakukan proses brute force attack.

4) Penulisan *Syntax*
Indikator ini menguji seberapa panjang dan pendek perintah yang kita tulis dalam menggunakan tools dalam melakukan *brute force password* pada file *zip*.

Berikut tools yang kami jadikan studi kasus dalam melakukan *brute force password*, antara lain:

Tabel 2. Jenis Tools

| Jenis Tools | Sumber |
|---|---|
| John The Riper (JtR) | kali linux |
| Hashcat | kali linux |
| Zydra | github |

## 4. HASIL DAN PEMBAHASAN

### 4.1 Perbandingan

#### 4.1.1 *John The Ripper(JtR)*

*John the Ripper* (*JtR*) adalah alat pembobol kata sandi yang awalnya diproduksi untuk sistem berbasis *UNIX*

[8]. Itu dirancang untuk menguji kekuatan kata sandi, kata sandi terenkripsi (hash) dengan kekerasan, dan memecahkan kata sandi melalui serangan kamus. File *John the Ripper (JtR)* adalah perangkat lunak bawahan dari sistem operasi Kali linux.

a. Penulisan syntax
   *zip2john [file name.zip] > [file name.txt]*
   *john[file name.txt]*
b. Kecepatan, konsistensi dan efektivitas

Tabel 3. Jenis Tools

| No | Password | Kecepatan | Konsistensi | Efektivitas |
|---|---|---|---|---|
| 1 | 12345 | 00 d | Tingkat konsistensi yang didapat dari pengujian *tools* ini tidak baik karena selisih dari waktu tercepat dan waktu terlama pengujian hanya 11 detik | Pada *Tools John The Ripper* memiliki efektivitas yang rendah karena tidak mampu mendapatkan seluruh *password* yang diujikan |
| 2 | 15243 | 07 d | | |
| 3 | 12534 | 15 d | | |
| 4 | 14235 | 15 d | | |
| 5 | 12354 | 04 d | | |
| 6 | 32451 | - | | |
| 7 | 41523 | - | | |
| 8 | 51342 | - | | |
| 9 | 14152 | 07 d | | |
| 10 | 52415 | - | | |
| Rata-rata | | 8 d | | |

### 4.1.2 *Hashcat*

File *Hashcat* adalah tool yang tidak memerlukan instalasi khusus untuk dijalankan pada sistem. Hal itu adalah salah satu kelebihan dari tool ini. *Free, Open Source, Multi -OS, Multi-Platform, Multi-Devices, Built in Bechmarking System, Integrated Thermal Wacdogs* adalah beberapa fitur yang menjadikan salah satu pasword cracker paling canggih saat ini [26]. Selain itu Hashcat merupakan alat peretas kata sandi dengan *hash MD5,* didukung dengan worldlist yang besar [27]

a. Penulisan *syntax*
   *zip2john [file name.zip] > [file name.txt]*
   *hascat –a 3 –m 13600 [file name.txt] ?d?d?d?d?d*
b. Kecepatan, konsistensi dan efektivitas

Tabel 4. Jenis Tools

| No | Password | Kecepatan | Konsistensi | Efektivitas |
|---|---|---|---|---|
| 1 | 12345 | 04 d | *Tingkat konsistensi* yang didapat dari pengujian *tools* ini sangatlah baik karena selisih dari waktu tercepat | Pada *Tools Hashcat* memiliki efektivitas yang tinggi dan memuaskan karena mampu |
| 2 | 15243 | 08 d | | |
| 3 | 12534 | 06 d | | |
| 4 | 14235 | 06 d | | |
| 5 | 12354 | 08 d | | |
| 6 | 32451 | 03 d | | |
| 7 | 41523 | 05 d | | |
| 8 | 51342 | 05 d | | |

| | | | | |
|---|---|---|---|---|
| 9 | 14152 | 04 d | dan waktu terlama pengujian hanya 5 detik | mendapatkan seluruh *password* yang diujikan |
| 10 | 52415 | 07 d | | |
| Rata-rata | | 5,6 d | | |

### 4.1.3 *Zydra*

*Zydra* adalah alat pemulihan kata sandi yang dapat memulihkan kata sandi dari file dengan menggunakan serangan brute-force atau memecahkan kata sandi *ZIP, RAR* dan *PDF* [28].File dari Zydra diambil dari github (https://github.com/hamedA2/Zydra), selain itu *Zydra* adalah salah satu alat yang mudah dan sederhana untuk pemulihan kata sandi file dan membantu memecahkan kata sandi file bayangan Linux. Ini berisi serangan kamus atau teknik Brute force untuk memulihkan kata sandi [29]

Berikut adalah hasil dari penelitian kami:

a. Penulisan syntax
   *python3 Zydra.py –f [file name.zip] –b digits –m 5 –x 5*
b. Kecepatan, konsistensi dan efektivitas

Tabel 5. Jenis Tools

| No | Password | Kecepatan | Konsistensi | Efektivitas |
|---|---|---|---|---|
| 1 | 12345 | 09,7 d | Tingkat konsistensi yang didapat dari pengujian *tools* ini cukup baik karena selisih dari waktu tercepat dan waktu terlama pengujian didapat waktu selama 14,2 detik | Pada *Tools Hashcat* memiliki efektivitas yang tinggi dan memuaskan karena mampu mendapatkan seluruh *password* yang diujikan |
| 2 | 15243 | 08,8 d | | |
| 3 | 12534 | 10,0 d | | |
| 4 | 14235 | 11,4 d | | |
| 5 | 12354 | 10,2 d | | |
| 6 | 32451 | 16,4 d | | |
| 7 | 41523 | 19,0 d | | |
| 8 | 51342 | 22,5 d | | |
| 9 | 14152 | 11,3 d | | |
| 10 | 52415 | 23,0 d | | |
| Rata-rata | | 14,23 d | | |

## 4.2 Pembahasan

Dapat dilihat hasil analsis diatas, terdapat 4 poin penting dalam bahasan penelitian ini. 4 poin tersebut diantaranya adalah sebagai berikut:

### 4.2.1 Penulisan syntax

Dari ketiga tools yang kami teliti. Penulisan *syntax* yang paling sederhana adalah *zydra* karena kita lansung bisa menulis satu baris untuk menjalankan *tools* agar bisa *brute force* password pada file *zip*. Sedangkan pada tools *Hashcat* dan *John the Riper* memerlukan 2 langkah yaitu perlu merubah file *zip* ke *txt* baru bisa di *brute force.*

### 4.2.2 Kecepatan

Berdasarkan analisis diatas, dapat terlihat dari kecepatan dari masing – masing tools yang kami uji sebagai berikut:

Tabel 6. Rangkuman Kecepatan

| No | Tools | Rata- Rata Kecepatan | Kegagalan |
|---|---|---|---|
| 1 | *John The Riper (JtR)* | *8* detik | 4 |
| 2 | *Hashcat* | 5,6 detik | - |
| 3 | *Zydra* | 14,23 detik | - |

Dapat terlihat pada tabel 6, bahwa tools yang paling tercepat adalah *Hashcat* dengan tingkat kegagalan tidak ada. Dengan rata- rata kecepatan dalam melakukan *brute force password* adalah 5,6 detik.

### 4.2.3 Konsistensi

Berdasarkan analisis diatas, dapat diketahui dari segi konsistensi atau jarak antara waktu tercepat dan terlama. Dari segi konsistensi dari ketiga tools yang kami uji yang paling baik adalah tools *Hashcat* karena mendapatkan selang waktu 5,6 detik.

### 4.2.4 Efektivitas

Berdasarkan penelitian yang telah kami buat. Dalam hal efektivitas tools atau seberapa mampu tools dalam menemukan sebuah password di berkas ZIP dari ketiga tools yang telah kami uji terdapat 2 tools yang lolos dari tahap uji coba kami yaitu: *Hashcat* dan *zydra*.

## 5. KESIMPULAN DAN SARAN

Dari pembahasan kita dapat simpulkan bahwa *password* memiliki hal – hal penting untuk keamanan, sehingga *password* dapat melindungi suatu akun dan file agar selalu aman. Dalam penelitian menguji keamanan password menggunakan 3 tools, dapat disimpulkan bahwa 3 tools yang sudah diuji dengan 4 aspek yaitu yaitu kecepatan ,konsistensi, akurasi , dan penulisan *syntax.* Dalam penelitian menggunakan 3 tools yaitu *John the Ripper (JTR), Hashcat*, dan *Zydra*. Dapat disimpulkan bahwa tool *John The Ripper(JtR)* masih kurang dalam Tingkat konsistensi dan efektivitas yang masih rendah, tool *Hashcat* memiliki Tingkat konsistensi dan efektivitas yang tinggi dan memuaskan, tool *Zydra* memiliki konsistensi yang cukup baik dan memiliki efektivitas yang tinggi dan memuaskan. Tools yang memiliki kecepatan tercepat dari 3 tools adalah Hashcat.

## DAFTAR PUSTAKA

[1] M. Ashari, “Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berharga adalah Data Pribadi.” https://www.djkn.kemenkeu.go.id/kpknl-kisaran/baca-artikel/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html (diakses Des 04, 2022).

[2] C. Bill, “Google: 89 Persen Orang Indonesia Pakai Password Lemah Halaman all - Kompas.com.” https://tekno.kompas.com/read/2021/11/03/15435707/google-89-persen-orang-indonesia-pakai-password-lemah?page=all (diakses Des 05, 2022).

[3] T. M. B. And dan Patil S M, “AUTHENTICATION SCHEME RESISTANT TO SHOULDER SURFING ATTACK USING IMAGE RETRIEVAL International Journal of Knowledge Engineering,” vol. 3, no. 2, hlm. 197–201, 2012, [Daring]. Available: http://www.bioinfopublication.org/jouarchive.php?opt=&jouid=BPJ0000230

[4] D. A. Ankush, B. E. Comp, W. Dhanashree, dan S. S. Husain, “Authentication Scheme for Shoulder surfing using Graphical and Pair Based scheme,” *International Journal of Advance Research in Computer Science and Management Studies*, vol. 2, no. 10, 2014, [Daring]. Available: www.ijarcsms.com

[5] K. Fujita dan Y. Hirakawa, “A study of password authentication method against observing attacks,” dalam *SISY 2008 - 6th International Symposium on Intelligent Systems and Informatics*, 2008. doi: 10.1109/SISY.2008.4664927.

[6] W. Z. Khan, M. Y. Aalsalem, dan Y. Xiang, “A Graphical Password Based System for Small Mobile Devices”, Diakses: Des 05, 2022. [Daring]. Available: www.IJCSI.org

[7] M. Zikrillah, J. Raya, P.-P. Km, K. Ogan Ilir, dan S. Selatan, "Analisa Serangan Password Cracking Pada Windows 10 Menggunakan Tools Pwdump v7.1 dan Cain & Abel."
[8] "John the Ripper explained: An essential password cracker for your hacker toolkit | CSO Online." https://www.csoonline.com/article/3564153/john-the-ripper-explained-an-essential-password-cracker-for-your-hacker-toolkit.html (diakses Des 03, 2022).
[9] R. N. Nasution dan B. Triandi, "IMPLEMENTASI METODE RSA DAN AES UNTUK MENGAMANKAN FILE WINRAR DAN ZIP IMPLEMENTATION OF RSA AND AES METHODS TO SECURE WINRAR AND ZIP FILES," 2020.
[10] "Apa itu File Zip? - Dropbox." https://experience.dropbox.com/id-id/resources/what-is-a-zip-file (diakses Des 04, 2022).
[11] R. A. Abdeen, "An Algorithm for String Searching Based on Brute-Force Algorithm," *IJCSNS International Journal of Computer Science and Network Security*, vol. 11, no. 7, hlm. 24, 2011.
[12] U. Kristen Satya Wacana Salatiga, "Analisa Brute Force Attack menggunakan Scanning Aplikasi pada HTTP Attack Artikel Ilmiah Program Studi Teknik Informatika Fakultas Teknologi Informasi," 2016.
[13] D. Intan Rakhmayanti, "Terungkap! Begini Cara Kerja Hacker Saat Membobol Data Anda." https://www.cnbcindonesia.com/tech/20220913065714-37-371534/terungkap-begini-cara-kerja-hacker-saat-membobol-data-anda (diakses Des 04, 2022).
[14] "Panduan Hacking Website dengan Kali Linux - Mr. Doel - Google Books." https://books.google.co.id/books?hl=en&lr=&id=ZC1IDwAAQBAJ&oi=fnd&pg=PP1&dq=apa+itu+kali+linux&ots=dYOK_4WBV3&sig=C9mxlLaL-pBi_L45sHSmDSjCIks&redir_esc=y#v=onepage&q=kali%20linux%20adalah&f=false (diakses Des 04, 2022).
[15] I. A. Gunawan AMIK Tunas Bangsa Jl Sudirman Blok No dan K. Pematang Siantar, "PENGGUNAAN BRUTE FORCE ATTACK DALAM PENERAPANNYA PADA CRYPT8 DAN CSA-RAINBOW TOOL UNTUK MENCARI BISS," *InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 1, no. 1, hlm. 52–55, Sep 2016, Diakses: Des 25, 2022. [Daring]. Available: https://jurnal.uisu.ac.id/index.php/infotekjar/article/view/48
[16] "Pengertian Algoritma Brute Force dan Greedy." https://dosenit.com/ilmu-komputer/pengertian-algoritma-brute-force-dan-greedy (diakses Des 25, 2022).
[17] "Most common password cracking techniques hackers use | Cybernews." https://cybernews.com/best-password-managers/password-cracking-techniques/ (diakses Des 25, 2022).
[18] "10 most popular password cracking tools [updated 2020] | Infosec Resources." https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/ (diakses Des 25, 2022).
[19] "Kali Linux - Bead Daily." https://beadgrup.com/news/kali-linux/ (diakses Des 25, 2022).
[20] "What is Kali Linux? | Kali Linux Documentation." https://www.kali.org/docs/introduction/what-is-kali-linux/ (diakses Des 25, 2022).
[21] "John the Ripper explained: An essential password cracker for your hacker toolkit | CSO Online." https://www.csoonline.com/article/3564153/john-the-ripper-explained-an-essential-password-cracker-for-your-hacker-toolkit.html#:~:text=John%20the%20Ripper%20definition,crack%20passwords%20via%20dictionary%20attacks. (diakses Des 25, 2022).
[22] "How to Crack Passwords using John The Ripper – Pentesting Tutorial." https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/ (diakses Des 25, 2022).
[23] "Hashcat explained: How this password cracker works | CSO Online." https://www.csoonline.com/article/3542630/hashcat-explained-why-you-might-need-this-password-cracker.html (diakses Des 25, 2022).
[24] "Zydra: Password Recovery | Linux Shadow File Cracker | CYBERPUNK." https://www.cyberpunk.rs/zydra-linux-shadow-file-cracker (diakses Des 25, 2022).
[25] M. Rijal Fadli, "Memahami desain metode penelitian kualitatif," vol. 21, no. 1, hlm. 33–54, 2021, doi: 10.21831/hum.v21i1.

[26] J. D. Santoso, "ANALISIS PASSWORD CRACKCING MNEGGUNAKAN GPU PROCESS," *Jurnal Mantik Penusa*, vol. 3, no. 1.1, 2019, Diakses: Des 05, 2022. [Daring]. Available: https://e-jurnal.pelitanusantara.ac.id/index.php/mantik/article/view/602

[27] A. Kurniadi, "THESIS WPA2-PSK NETWORK SECURITY ANALYSIS USING THE PENETRATION TESTING METHOD (CASE STUDY: TP-LINK ARCHER A6)".

[28] "Zydra -- ZIP Password Cracker." https://www.kalilinux.in/2021/02/crack-password-zip-rar-pdf-using-zydra.html (diakses Des 03, 2022).

[29] "Zydra - Recover Password Protected PDF, ZIP, and RAR - GeeksforGeeks." https://www.geeksforgeeks.org/zydra-recover-password-protected-pdf-zip-and-rar/ (diakses Des 05, 2022).