Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849
e-ISSN: 2548-1398
Vol. 9, No. 12, Desember 2024

EVALUASI EFEKTIVITAS HONEYPOT COWRIE DALAM MELAKUKAN PENGUMPULAN PASSWORD DENGAN MENGGUNAKAN PEDOMAN KEAMANAN KATA SANDI NIST SP 800-63B

Wahyu Juniardi[1], Kalamullah Ramli[2]
Universitas Indonesia, Indonesia[1,2]
Email: wahyu.juniardi@ui.ac.id[1], kalamullah.ramli@ui.ac.id[2]

Abstrak

Cowrie adalah sistem honeypot yang umumnya digunakan untuk meniru server SSH yang rentan guna menarik penyerang dan mengumpulkan tindakan yang mereka lakukan. Salah satu penggunaan umum dari Cowrie adalah untuk mengumpulkan kata sandi yang digunakan oleh penyerang dalam mendapatkan akses tidak sah ke sistem menggunakan serangan brute-force. Penelitian ini bertujuan untuk mengevaluasi efektivitas honeypot Cowrie dalam mengumpulkan kata sandi dengan menganalisis data yang dikumpulkan dengan memvariasikan beberapa kombinasi nama pengguna dan kata sandi yang digunakan oleh penyerang dengan menggunakan pedoman kata sandi yang dikeluarkan oleh NIST untuk mengevaluasi kualitas dan keragaman kata sandi yang dikumpulkan. Penelitian ini dibagi ke dalam dua fase, pada fase pertama dilakukan dengan pengaturan bawaan honeypot Cowrie dengan menggunakan nama pengguna dan kata sandi bawaan, dan pada fase kedua menggunakan kombinasi kata sandi 8 karakter, yang merupakan persyaratan minimal kata sandi berdasarkan pedoman kata sandi NIST, yang terdiri dari kombinasi huruf besar, huruf kecil, angka, serta karakter khusus. Hasil penelitian menunjukkan bahwa pemanfaatan honeypot Cowrie dengan menggunakan variasi konfigurasi kata sandi 8 karakter memiliki efektivitas yang lebih tinggi dalam melakukan pengumpulan kata sandi, terlihat dari peningkatan total percobaan login sebesar 118,2%, peningkatan jumlah nama pengguna unik sebesar 16,49%, peningkatan jumlah kata sandi unik sebesar 56,70%, serta peningkatan penggunaan kata sandi dengan kompleksitas lebih dari 8 karakter sebesar 40,29%. Temuan ini menunjukkan bahwa honeypot Cowrie dapat digunakan secara efektif sebagai alat yang berguna untuk mengumpulkan data kata sandi yang akan membantu meningkatkan keamanan sistem, dan dapat memiliki efektivitas yang lebih tinggi dalam melakukan pengumpulan kata sandi ketika dilakukan variasi konfigurasi kata sandi yang digunakan oleh penyerang.

Kata kunci: Honeypot Cowrie, server SSH, brute-force, kata sandi

Abstract

Cowrie is a honeypot system commonly used to emulate vulnerable SSH servers to attract attackers and collect their actions. One common use of Cowrie is to collect passwords used by attackers in gaining unauthorized access to the system using brute-force attacks. This research aims to evaluate the effectiveness of the Cowrie honeypot in collecting passwords by analyzing the data collected by varying several combinations of usernames and passwords used by attackers using password guidelines issued by NIST to evaluate the quality and diversity of the collected passwords. The research was divided into two phases, in the first phase it was conducted with the default settings of the Cowrie honeypot by using the default username and password, and in the second phase using a password combination of 8 characters, which is the minimum password requirement based on the NIST password

How to cite:	Juniardi, W., & Ramli, K. (2024). Evaluasi Efektivitas Honeypot Cowrie dalam Melakukan Pengumpulan Password dengan Menggunakan Pedoman Keamanan Kata Sandi NIST SP 800-63B. *Syntax Literate. (9)12*. http://dx.doi.org/10.36418/syntax-literate.v9i12
E-ISSN:	2548-1398

guidelines, consisting of a combination of uppercase letters, lowercase letters, numbers, as well as special characters. The results showed that the utilization of Cowrie honeypot by using 8-character password configuration variation has a higher effectiveness in collecting passwords, as seen from the increase in total login attempts by 118.2%, the increase in the number of unique usernames by 16.49%, the increase in the number of unique passwords by 56.70%, and the increase in the use of passwords with a complexity of more than 8 characters by 40.29%. These findings suggest that the Cowrie honeypot can be effectively used as a useful tool to collect password data that will help improve system security, and can have a higher effectiveness in performing password collection when variations in the password configuration used by the attacker are made.
***Keywords**: Cowrie honeypot, SSH server, brute-force, password*

Pendahuluan

Serangan di dalam sebuah jaringan dalam beberapa tahun terakhir menjadi lebih sering dan lebih intens (Sadasivam et al., 2018). Meningkatnya jumlah serangan dari tahun ke tahun didominasi oleh *malware* yang merupakan ancaman yang tidak hanya berdampak secara lokal, namun malware juga merupakan ancaman utama yang memiliki dampak secara global (Hapsah & Nasution, 2023; Nastiti et al., 2019; Septiani et al., 2016). Salah satu serangan favorit dari sebuah malware adalah serangan terhadap protokol SSH (Agghey et al., 2021). Seperti yang kita ketahui, SSH merupakan sebuah protocol yang cukup terkenal dan sangat luas telah digunakan oleh administrator jaringan maupun administrator sebuah website dalam melakukan pengelolaan serta remote akses terhadap server ataupun perangkat jaringan mereka di lingkungan kerjanya menggunakan channel yang telah terenkripsi (Wanjau et al., 2021). Peretas seringkali menciptakan *malware* yang secara otomatis melakukan pemindaian terhadap kelemahan sistem yang terdapat di internet. Salah satu serangan yang sering digunakan yaitu dengan menggunakan serangan *brute-force* attack (Wanjau et al., 2021) yang memanfaatkan otentikasi berbasiskan kata sandi yang merupakan salah satu mekanisme keamanan yang banyak digunakan untuk melindungi informasi serta sumber daya yang sensitive (Ezugwu et al., 2023). Serangan *brute-force* merupakan sebuah serangan yang dilakukan secara tidak sah dengan cara mencoba masuk menggunakan *username* serta *password* yang terdiri dari ratusan bahkan ribuan kombinasi *username* serta *password* untuk masuk ke dalam sebuah server (Nursetyo et al., 2019). Karena hal tersebut, maka keamanan kata sandi menjadi perhatian yang penting di dalam dunia keamanan siber pada umumnya dan bagi administrator server pada khususnya dalam mengamankan server yang mereka kelola. Oleh karena itu, salah satu pendekatan yang dapat digunakan untuk dapat mengetahui *username* serta *password* yang sering digunakan dalam melakukan serangan *brute-force* sehingga dapat dimanfaatkan bagi seorang administrator keamanan jaringan dan juga bagi para penggiat keamanan siber adalah dengan menggunakan sebuah *honeypot* (sistem tiruan) untuk dapat mengumpulkan serta melakukan analisis terhadap *username* ataupun *password* yang sering digunakan maupun kombinasi dari *username* dan *password* yang sering digunakan.

Honeypot merupakan sebuah sistem tiruan yang sengaja dibuat untuk menarik perhatian dari penyerang sehingga akan didapatkan berbagai macam informasi serta aktivitas yang dilakukan oleh penyerang tersebut (Cabral et al., 2019). Informasi – informasi seperti alamat IP, *username* serta *password* yang digunakan dalam melakukan percobaan masuk ke dalam sistem, serta *honeypot* juga mampu untuk melakukan perekaman aktivitas yang dilakukan oleh penyerang di dalam server *honeypot* tersebut. Salah satu jenis *honeypot* yang dapat melakukan aktivitas tersebut yaitu dengan

menggunakan *cowrie honeypot* yang bekerja dengan membuat sistem tiruan terhadap protokol SSH sehingga dapat menarik minat dari penyerang untuk dapat mengeksploitasi protokol SSH tersebut (Ernawati & Rachmat, 2021). Dari hasil eksploitasi oleh penyerang tersebut maka akan didapatkan informasi – informasi penting seperti yang telah dijelaskan sebelumnya. Selain itu, dengan kemampuannya, *cowrie honeypot* dapat melakukan pengumpulan data *username* serta *password* yang digunakan oleh penyerang dalam kegiatannya untuk melakukan peretasan terhadap *honeypot* tersebut (Ylonen & Lonvick, 2006).

Beberapa penelitian yang telah dilakukan diantaranya adalah analisis terhadap pengaturan bawaan *cowrie honeypot* serta potensinya dalam menyamarkan identitas dari *cowrie honeypot* jika dilakukan terhadap perubahan beberapa parameter yang ada di dalam *cowrie honeypot* tersebut sehingga dapat meningkatkan nilai penyamaran serta fungsionalitas dari *honeypot* tersebut (Cabral et al., 2019). Pada penelitian Rupiat et al. (2020) dilakukan pengembangan sistem deteksi keamanan server dengan menggunakan *cowrie honeypot* yang menghasilkan kesimpulan bahwa *cowrie honeypot* mampu mendeteksi semua jenis serangan yang menggunakan teknik serangan *brute-force* sehingga dapat mengumpulkan beragam kombinasi *username* serta *password* yang digunakan oleh penyerang dalam melakukan percobaan serangan dengan menggunakan teknik *brute-force* terhadap server *cowrie honeypot* tersebut.

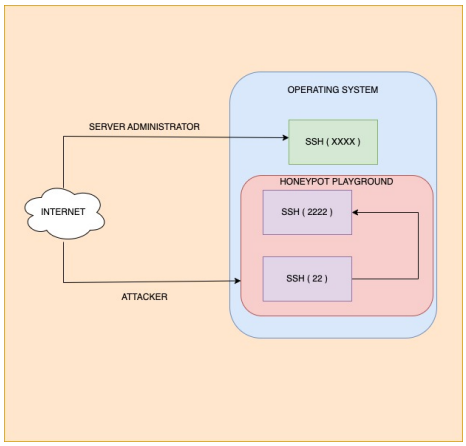
Pada penelitian ini, dilakukan analisis terhadap efektivitas *cowrie honeypot* dalam melakukan pengumpulan kata sandi dengan menggunakan pengaturan kata sandi di dalam server *cowrie honeypot* yang dapat digunakan oleh penyerang untuk masuk ke dalam server *cowrie honeypot* dengan menggunakan pedoman kata sandi yang dikeluarkan oleh NIST sehingga didapatkan lebih banyak keragaman kata sandi yang digunakan oleh penyerang. Hasil penelitian dapat dipergunakan sebagai alat bantu bagi administrator dan juga komunitas keamanan siber untuk dapat memahami potensi dari *cowrie honeypot* dan efektivitas kekuatan dari sebuah kata sandi sehingga dapat digunakan sebagai bahan evaluasi kekuatan dan keamanan kata sandi untuk dapat membantu pengembangan teknologi keamanan informasi dan membantu organisasi dan institusi dalam meningkatkan keamanan sistem dan jaringan mereka.

SSH

Tatu Ylönen, yang merupakan seorang peneliti berkebangsaan Finlandia, pada tahun 1995 merancang SSH-1 yang merupakan versi pertama protokol yang didasari pada peristiwa brute-force terhadap password di lingkungan universitasnya. Tujuan utama dari dari pembuatan SSH yaitu untuk menggantikan rlogin, rsh protokol, telnet yang tidak memberikan enkripsi terhadap data yang di transaksikan. SSH merupakan sebuah protocol untuk mengamankan remote login dan secure network service lainnya di atas sebuah jaringan yang tidak teramankan dimana protocol tersebut memiliki tiga buah komponen utama, yaitu *the transport layer protokol (*SSH-Trans yang) menyediakan server *authentication*, *confidentiality* dan *integrity,* lalu *the user authentication protocol* (SSH-USERAUTH) yang bertanggung jawab terhadap otentikasi user ke server, dan juga *the connection protocol* (SSH-CONNECT) yang melakukan enkripsi tunnel ke dalam beberapa logical channel (Rupiat et al., 2020). SSH biasanya menggunakan port 22. Namun demikian port tersebut dapat dikonfigurasi dengan menggunakan port selain port 22.

Cowrie honeypot

Cowrie honeypot merupakan *honeypot* yang mengemulasikan layanan dengan protokol SSH. *Honeypot* ini di rancang untuk mengetahui pola - pola serangan atau exploitasi terhadap sebuah server serta untuk mempelajari pola serangan pada jenis serangan *brute force* (Rupiat et al., 2020). *Cowrie* dapat beroperasi dalam beberapa mode, yaitu *medium interaction mode* dan *high interaction mode*. Pada *medium interaction mode, cowrie honeypot* mengemulasikan sistem operasi UNIX menggunakan *python* . sedangkan pada *high interaction mode¸ cowrie* memfungsikan sebagai SSH dan telnet untuk mengamati perilaku dai *attacker*. pada *cowrie honeypot*, perintah - perintah linux yang disupport diantaranya seperti *wget, curl, scp* dan beberapa perintah linux lainnya. Secara umum, *cowrie honeypot* memiliki topologi sebagai berikut:



Gambar 1. Alur kerja *cowrie honeypot*

Pada gambar 1 merupakan alur kerja *cowrie honeypot* yang memiliki 2(dua) buah koneksi SSH (Baçer et al., 2021). Koneksi yang pertama merupakan koneksi SSH yang digunakan oleh administrator untuk melakukan pengelolaan terhadap untuk melakukan pengelolaan terhadap untuk melakukan pengelolaan terhadap *cowrie honeypot* yang sedang dikembangkan menggunakan port tidak standard selain port 22. Port SSH yang dipergunakan oleh administrator sudah di amankan sehingga koneksi ke port tersebut hanya dapat dilakukan melalui koneksi yang telah diamankan. Koneksi yang kedua merupakan koneksi SSH yang sengaja dibuka ke publik internet untuk dapat di eksploitasi oleh penyerang. Penyerang yang terkoneksi ke port 22 akan secara otomatis dialihkan ke *virtual environment cowrie honeypot* yang menggunakan port 2222.

NIST SP 800-63B

NIST SP 800-63b adalah sebuah pedoman yang dikeluarkan oleh National Institute of Standards and Technology (NIST) yang berisi tentang keamanan password dan autentikasi. Pedoman ini memberikan rekomendasi tentang bagaimana membuat password yang kuat dan aman untuk digunakan pada berbagai jenis akun dan sistem. Beberapa rekomendasi tersebut antara lain:

1. Panjang password minimal 8 karakter: Semakin panjang password, semakin sulit untuk ditebak oleh attacker. NIST merekomendasikan panjang password minimal 8 karakter.

2. Menggunakan kombinasi karakter: NIST merekomendasikan penggunaan kombinasi karakter seperti huruf besar, huruf kecil, angka, dan karakter khusus (seperti tanda baca). Penggunaan kombinasi karakter dapat meningkatkan kompleksitas password dan membuatnya lebih sulit untuk ditebak.
3. Menghindari penggunaan kata-kata umum atau terkenal: Penggunaan kata-kata umum atau terkenal seperti "password" atau "123456" sangat mudah untuk ditebak oleh attacker. NIST merekomendasikan untuk menghindari penggunaan kata-kata umum atau terkenal sebagai password.
4. Menghindari penggunaan informasi pribadi: Menghindari penggunaan informasi pribadi seperti nama atau tanggal lahir sebagai password. Informasi pribadi tersebut dapat mudah ditebak oleh attacker.
5. Menggunakan password manager: NIST merekomendasikan penggunaan password manager untuk menyimpan dan mengelola password. Dengan menggunakan password manager, pengguna dapat membuat password yang kuat dan kompleks serta menghindari penggunaan password yang sama untuk beberapa akun (Grassi et al., 2020).

Brute-force

Serangan *brute-force* merupakan sebuah teknik yang digunakan untuk mencoba semua kemungkinan kombinasi dari sebuah password atau kunci enkripsi secara berurutan sampai menemukan kombinasi yang benar. Teknik ini umumnya digunakan dalam upaya untuk mendapatkan akses tidak sah ke sistem dan merupakan salah satu ancaman bagi seorang network administrator (Ayankoya & Ohwo, 2019). Hampir sebagian besar keberhasilan serangan *brute-force* disebabkan oleh kombinasi *password* yang pada umumnya lemah yang merupakan *password* buatan manusia (Hossain et al., 2020), oleh karena hal tersebut maka kebanyakan penyerang memanfaatkan daftar password yang telah dikumpulkan sebelumnya.

Metode Penlitian

Simulasi dan Percobaan

Pada penelitian kali ini, dilakukan eksperimen dengan menggunakan *cowrie honeypot* untuk dapat mengetahui efektivitas dari *cowrie honeypot* dalam melakukan pengumpulan kata sandi. Eksperimen akan dibagi ke dalam 2(dua) fase yaitu :

1. Fase 1 : *Auth-random default configuration*
   Pada fase 1, eksperimen dilakukan pada rentang waktu 5 hari. Pada fase ini dijalankan konfigurasi default bawaan dari *cowrie honeypot* yang menggunakan salah satu modul di dalam *cowrie honeypot yaitu* file auth.py di dalam mengemulasi autentikasi dari penyerang. modul auth.py bertanggung jawab untuk memproses permintaan login dari penyerang pada sebuah honeypot. Dengan menggunakan konfigurasi bawaan *honeypot cowrie* ini, attacker akan sengaja diizinkan untuk masuk ke dalam sistem *honeypot* setelah melakukan beberapa kali percobaan login.
2. Fase 2 : *userdb using 8 characters NIST password guidelines*
   Pada fase 2, juga dilakukan eksperimen dalam rentang waktu 5 hari. Pada fase ini, dilakukan perubahan terkait dengan autentikasi penyerang untuk dapat masuk ke dalam di *cowrie honeypot.* Perubahan dilakukan dengan memanfaatkan *username* yang sering muncul pada fase 1, lalu dikombinasikan dengan menggunakan *password* yang mengikuti pedoman SP 800-63b yang dikeluarkan oleh NIST yang mana mensyaratkan panjang *password* 8 karakter dan menggunakan kombinasi yang

berupa huruf besar, huruf kecil, angka, dan karakter khusus. Perubahan tersebut dilakukan pada file *userdb.txt* yang berada pada direktori file *cowrie honeypot* tersebut berada. Kombinasi username serta password yang digunakan pada fase 2 terlihat seperti pada tabel 1 dibawah.

Tabel 1. Konfigurasi Username dan Password Login SSH Honeypot Cowrie

Username	*Password*
postgres	bh7v`l[z
root	f"WC*ObL
admin	Woj4FDg-
oracle	0&Q;"iw%
git	=pHIg2pc
345gs5662d34	YLzLT7y+
test	1@^<:G]F
ftpuser	y7Qe`n3%
ubuntu	^eH'>_g|
user	@6>8z2&7

Parameter yang akan digunakan di dalam pengujian kali ini yaitu :

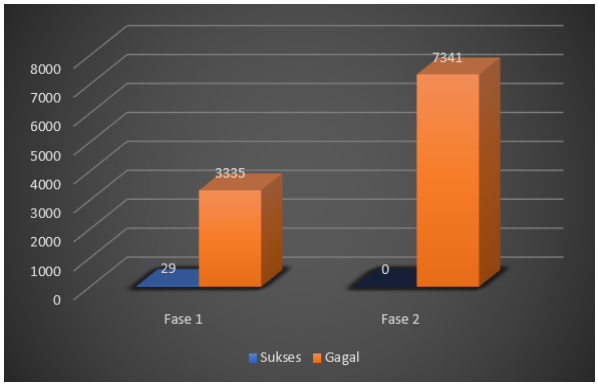
1. *Login attempt* : upaya untuk masuk dari penyerang ke dalam sistem *honeypot* dengan menggunakan kombinasi username dan password tertentu.
2. *Username* : identifikasi yang digunakan oleh penyerang yang berupa string karakter apa saja untuk memperoleh akses ke dalam server SSH yang di emulasikan.
3. *Password* : kombinasi yang berupa string karakter apa saja yang digunakan untuk mengautentikasi penyerang dalam mengakses ke server SSH
4. *Password complexity* : tingkat kesulitan sebuah kata sandi yang terdiri dari kombinasi karakter yang berbeda. Semakin kompleks sebuah kata sandi, maka akan semakin sulit bagi penyerang untuk dapat memecahkannya.

Hasil dan Pembahasan

Berdasarkan hasil eksperimen yang dilakukan pada live environment dengan melalui dua skenario pengujian, maka dilakukan perbandingan berdasarkan beberapa parameter pengujian yang telah ditentukan dalam pengujian yaitu *login attempt, username, password,* dan *password complexity*.

1. *Login attempt*

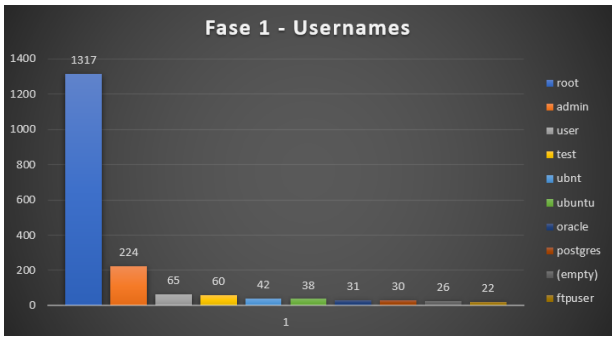
   Login status merupakan variabel keberhasilan dari penyerang dalam melakukan eksploitasi terhadap dimana terdapat dua buah kondisi, yaitu sukses dan gagal seperti yang ditampilkan pada gambar 2.



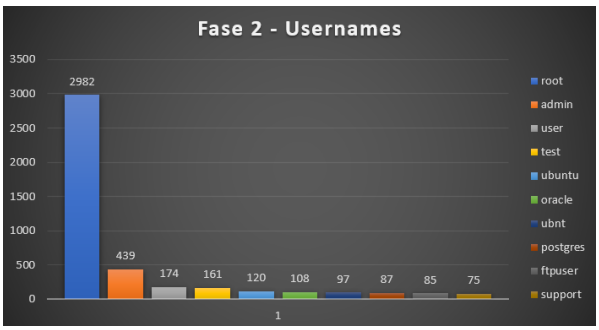
Gambar 2. Jumlah status login Fase 1 dan fase 2

Pada gambar 2 merupakan perbandingan keberhasilan penyerang dalam masuk ke dalam *cowrie honeypot* dimana pada fase 1 terdapat 3335 sukses login dan 29 gagal login dengan menggunakan pengaturan bawaan dari *cowrie honeypot* . Pada fase 2 terdapat perbedaan dimana 100 % penyerang tidak berhasil login ke dalam *cowrie honeypot*. Namun demikian terjadi peningkatan total *login attempt* pada fase 2 sebesar 118,2% (7341) jika dibandingkan pada fase 1 yang terdapat 3364 *login attempt*. Dari hasil ini dapat disimpulkan bahwa dengan melakukan perubahan konfigurasi dengan menggunakan kombinasi password, dapat meningkatkan ketertarikan dari penyerang untuk dapat lebih intens melakukan percobaan SSH *brute-force* kedalam server tersebut.

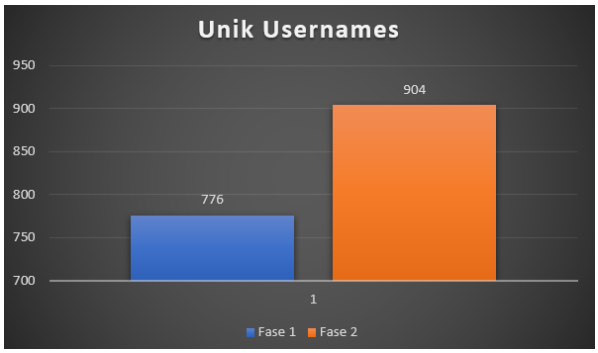
2. *Username*



Gambar 3. Top 10 *username* – fase 1



Gambar 4. Top 10 *username* – fase 2



Gambar 5. Perbandingan jumlah *username* berbeda pada fase 1 dan fase 2

Pada gambar 3 merupakan top 10 *username* yang sering muncul pada fase 1 dimana *username* root masih menjadi favorit bagi penyerang dalam melakukan

serangan *brute-force* untuk mencoba masuk ke dalam sistem secara tidak sah. Pada gambar 4 terjadi peningkatan yang terjadi pada percobaan *login* dengan menggunakan user root dimana pada fase 1 terjadi percobaan 1317 kali dan pada fase 2 terjadi peningkatan percobaan sebanyak 2982 kali. Pada gambar 5, juga terjadi peningkatan jumlah *username* berbeda dimana pada fase 2 terdapat 904 *username* berbeda, sedangkan pada fase 1 terdapat 776 *username* berbeda yang artinya terdapat peningkatan sebesar 16,49 % yang terjadi di fase 2. Dari hasil ini disimpulkan bahwa semakin sulit sebuah sistem untuk di *brute-force*, maka akan semakin banyak variasi kombinasi username yang digunakan oleh penyerang untuk mencoba masuk ke dalam SSH server yang di emulasikan.

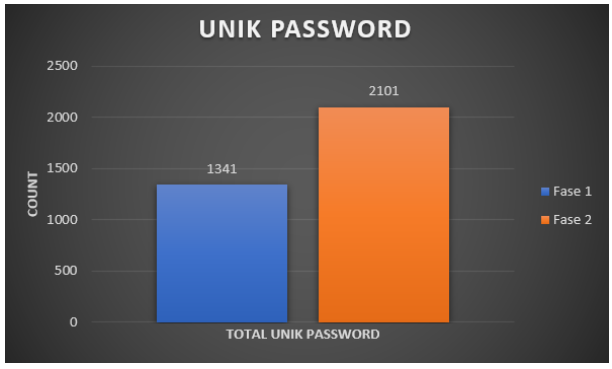
3. *Password*



Gambar 6. Top 10 *password* – fase 1



Gambar 7. Top 10 *password* – fase 2



Gambar 8. Perbandingan jumlah *password* yang berbeda pada fase 1 dan fase 2

Gambar 6 dan gambar 7 merupakan top 10 *password* yang sering muncul selama periode pengujian pada fase 1 dimana penyerang banyak menggunakan kombinasi *password* standard dalam melakukan percobaan serangan *brute-force* ke dalam SSH server yang diemulasikan. Secara umum, pada kedua fase tersebut penyerang melakukan percobaan *brute-force* menggunakan password yang sangat lemah seperti "admin","123456","password" dan beberapa kombinasi umum lainnya dengan harapan masih banyak pengelola server yang lalai dalam mengamankan server mereka. Namun demikian, terdapat peningkatan jumlah *password* unik sebanyak 56,70 % seperti yang terlihat pada gambar 8, dimana pada fase 1 *password* unik yang terdeteksi sebanyak 1341 dan pada fase 2 mengalami peningkatan *password* unik yang terdeteksi sebanyak 2101 *password*. Hal ini menunjukkan bahwa terjadi percobaan yang lebih masif dalam melakukan percobaan *brute-force* kedalam server SSH tersebut yang dikarenakan tidak adanya satupun kombinasi *username* dan *password* yang berhasil masuk ke dalam server tersebut sehingga membuat penyerang untuk melakukan percobaan kombinasi username serta password berbeda yang lebih banyak lagi.

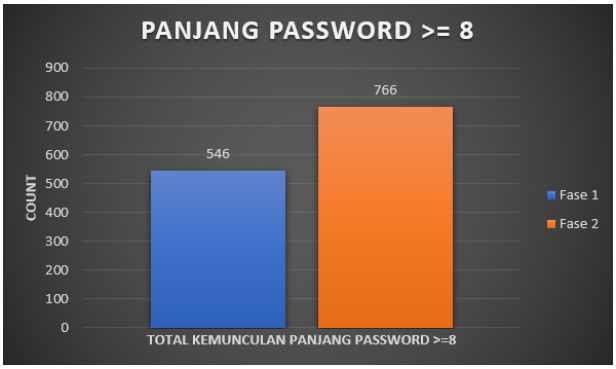
4. *Password complexity*

Tabel 2. Top 10 Unik Password dengan Panjang Karakter Lebih dari 8 Karakter – Fase 1

Password	Length
Drag1823hcacatcuciocolata	25
7hur@y@t3am$#@!(*(	18
J5cmmu=Kyf0-br8CsW	18
PASSWORDPASSWORD1	17
%4+q7d[VJT2^dcgg	16
1q2w3e4r!Q@W#E$R	16
PMGS**56$wx*%*St	16
Support123456789	16
ZAakDHzGeErgyrMs	16
ad1tzscanner123!	16

Tabel 3. Top 10 unik password dengan panjang karakter lebih dari 8 karakter – fase 2

Password	Length
7hur@y@t3am$#@!(*(	18
J5cmmu=Kyf0-br8CsW	18
11111111111111111	17
123456Q2w3E4r!@#$	17
!QAZ@WSX3edc4rfv	16
1qaz!QAZ2wsx@WSX	16
P@ssw0rd!@#$%^&*	16
ZAakDHzGeErgyrMs	16
!QAZXCVGHJKLP\r	15
!Qwerty!23456!.	15
admin_sister123	15



Gambar 9. Perbandingan jumlah total kemunculan panjang *password* lebih dari 8 karakter

Berdasarkan data yang diperoleh pada tabel 2 dan tabel 3, *honeypot cowrie* mampu menarik penyerang untuk dapat lebih masif dalam melakukan percobaan serangan *brute-force* dengan menggunakan kompleksitas kombinasi password yang sangat rumit dan panjang dengan dibuktikan dari informasi yang didapatkan dengan banyaknya *password* yang memiliki kompleksitas panjang lebih dari 8 karakter dimana pada pengujian pada fase 1 terdapat 546 *password* unik dan pengujian pada fase 2 terdapat 766 *password* dengan kompleksitas panjang password lebih deri 8 karakter seperti yang terlihat pada gambar 9. Dari data ini terlihat peningkatan sebesar 40,29 % intensitas kemunculan *password* unik yang terjadi pada fase 2. Hal ini menunjukkan bahwa percobaan dengan menggunakan konfigurasi honeypot dengan pengaturan *password* mengikuti pedoman yang dikeluarkan oleh NIST memiliki daya tarik lebih sehingga dapat meningkatkan efektivitas sebuah *honeypot* dalam melakukan pengumpulan kata sandi yang lebih kompleks dan beragam.

Kesimpulan

Dari hasil penelitian kali ini dapat disimpulkan bahwa *cowrie honeypot* dapat menjadi alat dalam melakukan pengumpulan password secara efektif jika dilakukan dengan perubahan pengaturan pada *cowrie honeypot* dengan melakukan variasi pada mode autentikasi pada *username* serta *password* yang digunakan oleh penyerang untuk dapat masuk ke dalam server *cowrie honeypot* tersebut. Hal ini terlihat dari peningkatan total percobaan login sebesar 118,2%, peningkatan jumlah nama pengguna unik sebesar 16,49%, peningkatan jumlah kata sandi unik sebesar 56,70%, serta peningkatan penggunaan kata sandi dengan kompleksitas lebih dari 8 karakter sebesar 40,29%. Temuan ini menunjukkan bahwa honeypot Cowrie dapat digunakan secara efektif sebagai alat yang berguna untuk mengumpulkan data kata sandi yang akan membantu meningkatkan keamanan sistem.

BIBLIOGRAFI

Agghey, A. Z., Mwinuka, L. J., Pandhare, S. M., Dida, M. A., & Ndibwile, J. D. (2021). Detection of username enumeration attack on ssh protocol: Machine learning approach. *Symmetry*, *13*(11). https://doi.org/10.3390/sym13112192

Ayankoya, F., & Ohwo, B. (2019). Brute-Force Attack Prevention in Cloud Computing Using One-Time Password and Cryptographic Hash Function. *International Journal of Computer Science and Information Security (IJCSIS)*, *17*(2).

Baçer, M., Güven, E. Y., & Aydin, M. A. (2021). SSH and Telnet Protocols Attack Analysis Using Honeypot Technique. *Proceedings - 6th International Conference on Computer Science and Engineering, UBMK 2021*. https://doi.org/10.1109/UBMK52708.2021.9558948

Cabral, W., Valli, C., Sikos, L., & Wakeling, S. (2019). Review and analysis of cowrie artefacts and their potential to be used deceptively. *Proceedings - 6th Annual Conference on Computational Science and Computational Intelligence, CSCI 2019*. https://doi.org/10.1109/CSCI49370.2019.00035

Ernawati, T., & Rachmat, F. F. F. (2021). Keamanan Jaringan dengan Cowrie Honeypot dan Snort Inline-Mode sebagai Intrusion Prevention System. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *5*(1). https://doi.org/10.29207/resti.v5i1.2825

Ezugwu, A., Ukwandu, E., Ugwu, C., Ezema, M., Olebara, C., Ndunagu, J., Ofusori, L., & Ome, U. (2023). Password-based authentication and the experiences of end users. *Scientific African*, *21*. https://doi.org/10.1016/j.sciaf.2023.e01743

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R., Regenscheid, A., Burr, W. E., Richer, J. P., Lefkovitz, N., Danker, J. M., & Choong, Y.-Y. (2020). *Digital identity guidelines: Authentication and lifecycle management [includes updates as of 03-02-2020]*.

Hapsah, Z. F., & Nasution, M. I. P. (2023). Analisis Tingkat Keamanan Data Perusahaan Yang Rentan Terhadap Serangan Cyber Dalam Sistem Informasi Manajemen. *Jurnal Manajemen Dan Akuntansi*, *1*(2).

Hossain, M. D., Ochiai, H., Doudou, F., & Kadobayashi, Y. (2020). SSH and FTP brute-force attacks detection in computer networks: Lstm and machine learning approaches. *2020 5th International Conference on Computer and Communication Systems, ICCCS 2020*. https://doi.org/10.1109/ICCCS49078.2020.9118459

Nastiti, F. E., Hariyadi, D., & Bima, F. (2019). TelegramBot: Crawling Data Serangan Malware dengan Telegram. *Computer Engineering, Science and System Journal*, *4*(1). https://doi.org/10.24114/cess.v4i1.11436

Nursetyo, A., Ignatius Moses Setiadi, D. R., Rachmawanto, E. H., & Sari, C. A. (2019). Website and Network Security Techniques against Brute Force Attacks using Honeypot. *Proceedings of 2019 4th International Conference on Informatics and Computing, ICIC 2019*. https://doi.org/10.1109/ICIC47613.2019.8985686

Rupiat, R., Faisal, S., Al Mudzakir, T., Lestari, S. A. P., & Karawang, P. (2020). Seminar Nasional Hasil Riset Prefix-RTR Deteksi Serangan Peretas Menggunakan Honeypot Cowrie Dan Intrusion Detection System Snort. *No. Ciastech*, 727–736.

Sadasivam, G. K., Hota, C., & Anand, B. (2018). Towards Extensible and Adaptable Methods in Computing. In *Towards Extensible and Adaptable Methods in Computing*. Springer Singapore. https://doi.org/10.1007/978-981-13-2348-5

Septiani, D. R., Widiyasono, N., & Mubarok, H. (2016). Investigasi Serangan Malware Njrat Pada PC. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *2*(2). https://doi.org/10.26418/jp.v2i2.16736

Wanjau, S. K., Wambugu, G. M., & Kamau, G. N. (2021). SSH-Brute Force Attack Detection Model based on Deep Learning. *International Journal of Computer Applications Technology and Research*, *10*(01). https://doi.org/10.7753/ijcatr1001.1008

Ylonen, T., & Lonvick, C. (2006). The Secure Shell (SSH) Protocol Architecture. In *The Secure Shell (SSH) Protocol Architecture*.

Copyright holder:
Wahyu Juniardi, Kalamullah Ramli (2024)

First publication right:
Syntax Literate: Jurnal Ilmiah Indonesia

This article is licensed under:

