Pengembangan Metode Pengumpulan Kata Sandi dengan Memanfaatkan Honeypot Cowrie Menggunakan Pedoman NIST SP 800-63B untuk Mengurangi Kerentanan Sistem = Development of a Password Collection Method by Utilizing Honeypot Cowrie Using NIST SP 800-63B Guidelines to Reduce System Vulnerability

Wahyu Juniardi, author

Abstrak

Keamanan informasi menjadi perhatian utama dalam era digitalisasi saat ini. Salah satu aspek penting dari keamanan informasi adalah perlindungan terhadap kata sandi. Pengumpulan kata sandi yang sering digunakan oleh penyerang dalam upayanya untuk meretas masuk ke dalam sebuah akun atau sistem memiliki peran yang sangat penting dalam memahami kelemahan sebuah sistem. Oleh karena itu, metode pengumpulan kata sandi yang efektif menjadi sangat penting dalam upaya melindungi sistem serta informasi dari sebuah serangan. Pada tesis ini bertujuan untuk mengembangkan metode pengumpulan kata sandi yang menggunakan honeypot cowrie dan mengacu kepada pedoman NIST SP 800-63b. Pedoman NIST SP 800-63b merupakan pedoman yang dikembangkan oleh National Institute of Standards and Technology (NIST) yang memberikan panduan praktis dalam hal kebijakan dan prosedur keamanan kata sandi. Honeypot cowrie merupakan sebuah sistem open source yang dapat dikustomisasi dan diperluas sesuai kebutuhan pengguna. Honeypot cowrie dirancang untuk menarik penyerang dan memantau aktivitas penyerang tersebut, termasuk upaya pembobolan terhadap sebuah kata sandi. Oleh karena itu, honeypot memiliki peranan yang penting untuk mempelajari teknik dan pola serangan yang digunakan oleh penyerang serta dilakukan identifikasi terhadap celah keamanan yang perlu diperbaiki. Pada penelitian kali ini, eksperimen dibagi kedalam dua tahapan, tahap pertama dengan menggunakan konfigurasi bawaan dan tahap kedua dilakukan penyesuaian konfigurasi honeypot cowrie dengan dilakukan variasi terhadap nama pengguna serta kata sandi yang digunakan oleh penyerang menggunakan pedoman NIST SP 800-63b . Hasil dari eksperimen dilakukan perbandingan untuk mengetahui efektivitas dari honeypot cowrie tersebut dalam melakukan pengumpulan kata sandi dengan indikator pengukuran yang berupa jumlah login attempt, username, password, serta password complexity. Dari hasil eksperimen didapati login attempt tahap 1 sebanyak 3364 dan tahap 2 sebanyak 7341, username tahap 1 sebanyak 776 dan tahap 2 sebanyak 904, password tahap 1 sebanyak 1341 dan tahap 2 sebanyak 2101, password complexity tahap 1 sebanyak 546 dan tahap 2 sebanyak 766. Dari data yang didapatkan tersebut, menunjukkan bahwa terjadi peningkatan indikator login attempt sebesar 118,2%, indikator username sebesar 16,49%, indikator password sebesar 56,70%, serta peningkatan indikator password complexity sebesar 40,29%.

.....Information security is a major concern in the current era of digitization. One important aspect of information security is the protection of passwords. The collection of passwords frequently used by attackers in their attempts to breach an account or system plays a crucial role in understanding the weaknesses of a system. Therefore, an effective method of collecting passwords becomes highly important in the effort to protect systems and information from attacks. This thesis aims to develop a password collection method that utilizes the honeypot Cowrie and references the NIST SP 800-63b guidelines. The NIST SP 800-63b guidelines, developed by the National Institute of Standards and Technology (NIST), provide practical

guidance on password security policies and procedures.Cowrie honeypot is an open-source system that can be customized and expanded according to user needs. Cowrie honeypot is designed to attract attackers and monitor their activities, including attempts to crack a password. Thus, honeypots play an important role in studying the techniques and patterns of attacks used by attackers and identifying security vulnerabilities that need to be addressed. In this research, the experiments are divided into two stages: the first stage using the default configuration, and the second stage involving adjustments to the Cowrie honeypot configuration by varying the usernames and passwords used by attackers following the NIST SP 800-63b guidelines. The results of the experiments are compared to determine the effectiveness of the Cowrie honeypot in password collection using measurement indicators such as the number of login attempts, usernames, passwords, and password complexity. The experiment results showed that there were 3364 login attempts in stage 1 and 7341 in stage 2, 776 usernames in stage 1 and 904 in stage 2, 1341 passwords in stage 1 and 2101 in stage 2, and 546 password complexity indicators in stage 1 and 766 in stage 2. These findings indicate an increase of 118.2% in the login attempt indicator, 16.49% in the username indicator, 56.70% in the password indicator, and a 40.29% increase in the password complexity indicator.