INTISARI

Keamanan menjadi salah satu aspek penting yang harus dimiliki oleh suatu sistem informasi. Berbagai lembaga yang ada di seluruh dunia, mulai dari lembaga pemerintahan, lembaga pendidikan, hingga lembaga bisnis selalu melakukan penelitian tentang keamanan dengan tujuan untuk mengurangi dampak dan ancaman yang dapat terjadi pada suatu sistem informasi. Salah satu penelitian yang paling sering dilakukan adalah penelitian dengan menggunakan kerentanan sebagai objeknya. Kerentanan adalah suatu sisi lemah pada sistem informasi yang dapat dimanfaatkan oleh peretas untuk melakukan serangan. Terdapat berbagai jenis kerentanan yang sudah ditemukan dan diteliti, salah satunya adalah *buffer overflow*. *Buffer overflow* merupakan salah satu kerentanan tertua yang pernah ada. Namun pada beberapa tahun terakhir kerentanan ini sudah mulai terabaikan dan tidak banyak lagi dilakukan penelitian mengenai kerentanan tersebut, padahal beberapa hal mengenai kerentanan tersebut mengalami perkembangan, terutama dalam hal pengamanan dan pencegahannya. Bahkan di Indonesia belum terdapat penelitian, skripsi, atau tesis yang membahas tentang kerentanan tersebut secara menyeluruh. Sehingga dibutuhkan penelitian terhadap kerentanan *buffer overflow* secara lengkap, dari bagaimana seorang peretas memanfaatkan kerentanan tersebut untuk melakukan serangan, hingga bagaimana pengamanan dan pencegahan terbaru yang dapat dilakukan.

Pada penelitian kali ini penulis akan melakukan penelitian tentang bagaimana sebuah kerentanan *buffer overflow* bekerja. Dengan menggunakan *penetration testing* maka akan didapatkan informasi mengenai bagaimana cara *cracker* melakukan serangan melalui kerentanan tersebut. Penelitian ini juga akan membahas tentang pengamanan terbaru yang dapat diimplementasikan untuk mencegah serangan melalui kerentanan *buffer overflow*. Penelitian ini dilakukan dalam bentuk simulasi tes penetrasi terhadap FTP *server* melalui kerentanan *buffer overflow*.

Hasil dari penelitian ini adalah berupa informasi mengenai cara yang digunakan penyerang untuk mengeksploitasi target, dampak dari eksploitasi, dan beberapa metode pengamanan yang dapat digunakan untuk mencegah eksploitasi melalui kerentanan *buffer overflow*, serta bagaimana pengamanan tersebut bekerja.

Kata kunci : *Penetration test*, keamanan, kerentanan, *buffer overflow*, Metasploit Framework

ABSTRACT

Security becomes one of the important aspects that must be owned by an information system. Various institutions around the world, ranging from government agencies, educational institutions, to business institutions always conduct research on security in order to reduce the impact and threats that can occur in an information system. One of the most frequently conducted studies is research using vulnerability as its object. Vulnerability is a weak side of information systems that can be exploited by hackers to carry out attacks. There are various types of vulnerabilities that have been discovered and studied, one of which is buffer overflow. Buffer overflow is one of the oldest vulnerabilities ever. However, in recent years, this vulnerability has begun to be neglected and not much research is carried out on the vulnerability, even though several things about the vulnerability are being developed, especially in terms of security and prevention. Even in Indonesia there are no much research, thesis, or thesis that discusses the vulnerability as a whole. Therefore research on a complete buffer overflow vulnerability is needed, from how a hacker uses the vulnerability to carry out attacks, up to how the latest security and prevention can be done.

In this study the author will conduct research on how a buffer overflow vulnerability works. By using penetration testing, information about how the hacker attacks the vulnerability will be obtained. This research will also discuss the latest coutermeasures that can be implemented to prevent attacks through buffer overflow vulnerabilities. This research was conducted in the form of a penetration test simulation on FTP servers through a buffer overflow vulnerability.

The results of this research are information about the method used by the attacker to exploit the target, the impact of exploitation, and some security methods that can be used to prevent exploitation through buffer overflow vulnerabilities, as well as how the security works.

Keywords : Penetration test, security, vulnerability, buffer overflow, Metasploit Framework.