Abstrak

Investigasi Forensik RAM untuk Mendeteksi Serangan *Exploit Framework* Metasploit

Metasploit adalah sebuah *framework* yang memberikan fasilitas untuk penyerang melakukan serangan terhadap sistem komputer, dengan memanfaatkan Metasploit penyerang bisa melakukan identifikasi dan menguji kelemahan sistem komputer kemudian mengambil alih sistem komputer tersebut. Fasilitas yang diberikan oleh *Framework* Metasploit memudahkan untuk melakukan serangan yang bersifat legal maupun ilegal terhadap sebuah sistem komputer, dengan demikian banyak profesional *penetration tester* ataupun *ethical hacker* yang memanfaatkan Metasploit untuk melakukan pekerjaannya, namun di sisi lain tentunya adapula pihak-pihak yang tidak bertanggung jawab memanfaatkan Metasploit untuk melancarkan upaya yang bersifat ilegal atau mengarah ke tindak kriminal berupa suatu tindakan peretasan memanfaatkan *exploit* tertentu menggunakan *framework* Metasploit pada komputer. Tindak kriminal yang memanfaatkan *Framework* Metasploit menjadikan tantangan tersendiri bagi investigator digital forensik untuk menemukan bukti digital pada komputer korban.

Serangan *exploit* pada komputer korban perlu dilakukan analisis untuk menemukan barang bukti digitalnya, pada komputer terdapat RAM di mana segala proses yang terjadi pada komputer akan tercatat hal tersebut dimungkinkan barang bukti serangan *exploit* yang dilancarkan menggunakan Metasploit dapat ditemukan di dalam RAM tersebut. RAM komputer bersifat *volatile* yang berarti data yang tersimpan di dalamnya akan hilang jika sistem komputer mati, maka dari itu proses forensik digital harus dilakukan menggunakan metode *live forensics* yang mana prosesnya harus dilakukan dalam keadaan komputer menyala. Oleh karena itu perlu dilakukan penelitian tentang bagaimana melakukan simulasi serangan menggunakan Metasploit, bagaimana melakukan investigasi RAM komputer secara *live forensics* pada sistem operasi Windows 8 dan Windows 10 untuk mengetahui karakteristik artefak barang bukti digital yang ditemukan pada tiap-tiap sistem operasi tersebut setelah dilakukan simulasi serangan menggunakan Metasploit.

Kata kunci

Framework Metasploit, *Exploit,* Digital Forensik, RAM, *Live Forensics*

Abstract

RAM Forensic Investigation to Detect Metasploit Exploit Framework Attacks

Metasploit is a framework that provides facilities for attackers to attack computer systems. By utilizing Metasploit, the attacker can identify and test the weaknesses of the computer system and then take over the computer system. The facilities provided by the Metasploit Framework make it easy to carry out legal and illegal attacks on a computer system. Thus, many penetration tester professionals or ethical hackers use Metasploit to do their work. However, on the other hand, of course, some are not responsible for using Metasploit to launch illegal efforts or lead to criminal acts in the form of an act of hacking using specific exploits. Crimes that utilizes the Metasploit Framework makes it a challenge for digital forensic investigators to find digital evidence on victims' computers.

Exploit attacks on victim's computers need to be analyzed to find digital evidence. On a computer, there is RAM, where all the processes that occur on the computer will be recorded. It is possible that evidence of an exploit attack launched using Metasploit can be found in the RAM. Computer RAM is volatile, which means data stored on it will be lost if the computer system dies. Therefore, the digital forensic process must be carried out using the live forensics method in which the process must be performed in a state of the computer running. Thus, research needs to be conducted on how to simulate attacks using Metasploit, how to investigate computer RAM in live forensics on the Windows 8 and Windows 10 operating systems to determine the characteristics of digital evidence artifacts found on each of these operating systems after a simulation attack using Metasploit.

Keywords

Metasploit *Framework*, *Exploit,* Digital Forensics, RAM, *Live Forensics*