BAB 1
Pendahuluan

1.1 Pendahuluan

Digitalisasi dalam berbagai sendi kehidupan sudah menjadi hal lumrah di era komputer dan internet saat ini, komputer dan internet menjadi alat yang memudahkan banyak orang dalam menjalani aktivitasnya, tentunya banyak data dan informasi penting yang tersimpan dalam suatu sistem komputer yang digunakan dalam aktivitas keseharian tersebut. Faktor terkait keamanan informasi pada sebuah sisem komputer menjadi bahasan yang menarik dewasa ini mengingat banyaknya serangan siber yang terjadi, *Website Kompas* memberitakan di Indonesia pada bulan Januari hingga Juli 2017 mengalami 177,3 juta serangan siber (nasional.kompas.com).


Home / News / Nasional

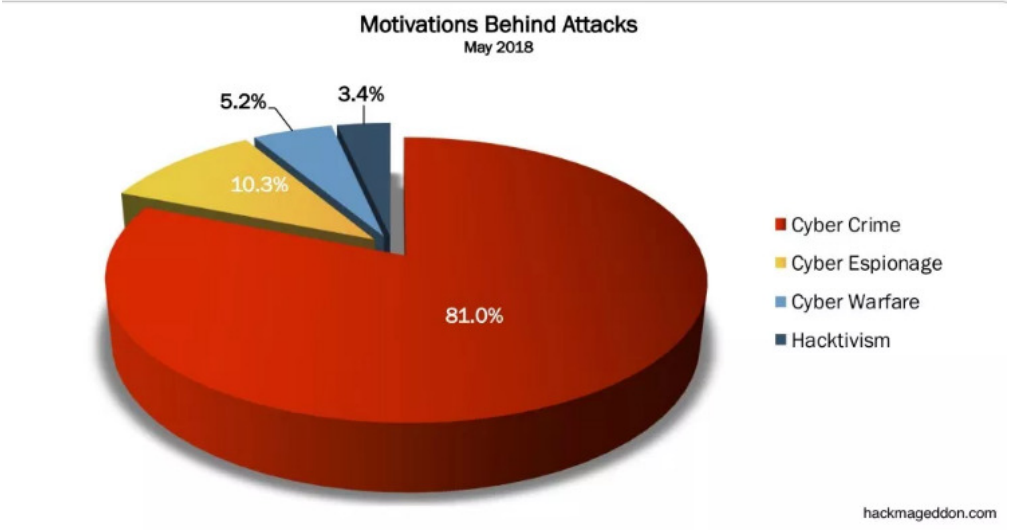
Januari hingga Juli 2017, Indonesia Alami 177,3 Juta Serangan Siber

KRISTIAN ERDIANTO

Kompas.com - 21/11/2017, 21:26 WIB

Gambar 1.1 Berita Serangan Siber di Indonesia (Sumber: nasional.kompas.com)

Serangan siber dilakukan dengan berbagai motivasi, salah satu motivasinya adalah *cybercrime,* menurut data yang diambil dari *website* hackmageddon.com menyebutkan pada bulan Mei 2018 sebesar 81% serangan dilakukan dengan motivasi tersebut (hackmageddon.com). Hal ini menempatkan *cybercrime* pada posisi pertama sebagai motivasi paling banyak dilakukan.



Gambar 1.2 Presentase motivasi dibalik serangan (Sumber: Hackmageddon.com).

Cybercrime dapat didefinisikan sebagai upaya perbuatan yang bertentangan dengan hukum dengan memanfaatkan jaringan komputer sebagai media atau komputer sebagai target dengan berbagai tujuan dan dapat menimbulkan kerugian bagi pihak lain (Arifah, 2011). Berdasarkan dari definisi tersebut maka tindakan pencurian data/informasi baik berupa dokumen penting, informasi pribadi dan lainnya secara ilegal yang memanfaatkan jaringan komputer dan atau perangkat komputer juga termasuk tindak *cybercrime*, salah satu teknik pencurian data/informasi adalah dengan memanfaatkan celah pada komputer korban dengan menggunakan *exploit* tertentu (Timalsina & Gurung, 2017). Dalam mempermudah aksinya seorang peretas biasanya memanfaatkan *tools,* salah satu *tools* yang bisa digunakan untuk melakukan serangan *exploit* adalah Metasploit.

Metasploit adalah *framework* yang dikembangkan untuk kepentingan *penetration testing,* dengan Metasploit bisa dimanfaatkan untuk mengambil alih sebuah sistem komputer dengan menggunakan *exploit* di dalamnya. Secara professional Metasploit biasa digunakan para *penetration tester* atau *ethical hacker* untuk menguji kerentanan pada sebuah sistem. Namun di lain sisi adapula orang-orang tak bertanggung jawab memanfaatkannya untuk tujuan peretasan ilegal terhadap komputer korban (Gupta & Kumar, 2015). Hal ini menjadikan tantangan tersendiri bagi analis forensik digital untuk melakukan investigasi serangan *exploit* menggunakan *framework* Metasploit pada komputer korban.

Untuk itu perlu dilakukan penelitian untuk mencari artefak digital pada komputer korban, sehingga berguna untuk proses investigasi dan deteksi serangan *exploit* menggunakan *framework* Metasploit. Sementara menurut penelitian terdahulu RAM komputer menyimpan berbagai informasi mengenai proses yang sedang berjalanan pada sebuah komputer (Hausknecht, Foit, & Burić, 2015). Oleh sebab itu penelitian akan dilakukan terhadap RAM komputer untuk mengetahui karakteristik bukti digital yang didapatkan ketika terjadi serangan *exploit* menggunakan *framework* Metasploit.

Penelitian mengenai forensik RAM telah banyak dilakukan oleh peneliti terdahulu, penelitian ekstraksi artefak dari RAM pada Windows 7 pernah dilakukan oleh (Thomas, Sherly, & Dija, 2013) pada penelitian tersebut dijelaskan mengenai metodologi untuk melakukan daftar proses yang berjalan, Pemuatan DLL dan ekstraksi proses memori dari proses yang berjalan. Penelitian lain mengenai analisis terhadap RAM komputer pernah dilakukan (Yudhistira, 2018) dalam penelitian tersebut dibuat simulai kasus tentang penyalah gunaan informasi berupa data sensitif password dan username suatu akun-akun tertentu yang masih tersimpan dalam RAM. Lebih lanjut penelitian terdahulu mengenai analisis RAM komputer dilakukan oleh (Rochmadi, 2017) yang mencari bukti digital di dalam RAM dengan kasus anti forensik di mana pengguna menggunakan portable web browser mode private. Namun RAM forensik untuk deteksi *exploit* menggunakan *framework* Metasploit masih jarang dilakukan, selain itu dalam penelitian terdahulu juga masih belum dilakukan studi komparatif mengenai tool akuisisi RAM yang digunakan, hal ini juga perlu dilakukan mengingat faktor *tool* akuisisi RAM yang digunakan juga merupakan hal yang penting dalam proses RAM forensik, untuk itu dalam penelitian ini akan dilakukan penggunaan tiga tool akuisisi RAM yang berbeda yaitu FTK Imager, Dumpit dan Magnet Forensics.

Dari latar belakang yang sudah diuraikan di atas, untuk mengetahui karakteristik bukti digital yang mungkin dapat ditemukan ketika ada serangan *exploit* menggunakan *framework* Metasploit maka perlu dilakukan sebuah penelitian dengan melakukan simulasi serangan menggunakan *framework* Metasploit. Untuk menambah pengetahuan yang lebih banyak dalam penelitian ini akan dilakuan penelitian terhadap RAM komputer yang telah terpasang dengan berbagai sistem operasi diantaranya ialah Windows 8 dan Windows 10. Dalam penelitian ini akan dilakukan menggunakan metode *live* forensik, hal ini dilakukan karena RAM bersifat *volatile* sehingga data pada RAM akan hilang jika sistem mati, dengan *live* forensik diharapakan dapat menjaga barang bukti tidak rusak atau hilang akibat sistem mati (Umar, Yudhana, & Faiz, 2017).

1.2 Rumusan Masalah

Berdasarkan uraian pendahuluan sebelumnya maka dapat diperoleh beberapa rumusan masalah, sebagai berikut:

1. Bagaimana investigasi pada RAM menggunakan metode *live forensics* pada sistem operasi Windows 8 dan Windows 10 untuk mendeteksi serangan *exploit* menggunakan Metasploit *framework*?
2. Bagaimana mengetahui karakteristik artefak bukti digital apa saja yang terdapat pada RAM komputer Windows 8 dan Windows 10 ketika dilakukan simulasi serangan menggunakan *Exploit* melalui Metasploit *Framework*?

1.3 Batasan Masalah

Berikut adalah batasan masalah yang ditentukan pada penelitian ini adalah sebagai berikut:

1. Pada penelitian ini simulasi serangan menggunakan Metasploit dan analisisnya menggunakan komputer yang berjalan pada pada jaringan *Local Area Network*
2. Hanya menggunakan sistem operasi Windows 8 dan Windows 10 sebagai target serangan.
3. Hanya melakukan simulasi serangan menggunakan teknik yang sudah ditentukan pada penelitian ini yaitu teknik penyisipan Trojan ke file exe untuk serangan ke sistem operasi Windows 8
4. Hanya melakukan simulasi serangan menggunakan teknik yang sudsah ditentukan pada penelitian ini yaitu teknik penyisipan Trojan ke file exe untuk serangan ke sistem operasi Windows 8
5. Analisis forensik hanya pada RAM komputer korban

1.4 Tujuan Penelitian

Adapun tujuan dilaksanakannya penelitian ini adalah sebagai berikut:

1. Melakukan serangkaian proses simulasi dan analisis terhadap RAM komputer ketika dilakukan serangan menggunakan teknik *Exploit* menggunakan Metasploit.
2. Mengetahui artefak bukti digital apa saja yang bisa ditemukan pada RAM komputer ketika terjadi serangan *Exploit* menggunakan Metasploit, sehingga bisa dijadikan bukti digital pendukung untuk proses analisis forensik digital.

1.5 Manfaat Penelitian

Berikut adalah manfaat penelitian yang bisa diambil:

1. Memberikan pengetahuan mengenai konsep dasar serangan teknik *Exploit* serta pengetahuan tentang bagaimana melakukan investigasi ketika terjadi serangan *Exploit* menggunakan Metasploit.
2. Mengetahui artefak digital apa saja yang bisa ditemukan pada RAM Komputer dengan sistem operasi windows 8 dan windows 10 ketika terjadi serangan *Exploit* menggunakan Metasploit untuk dijadikan barang bukti digital di pengadilan.

1.6 Metode Penelitian

Pada penelitian kali ini terdapat metode penelitian telah ditentukan oleh penulis, untuk itu berikut adalah tahapan-tahapan metode penelitian yang digunakan dalam penelitian ini:

A. Studi Pustaka

Tahapan pertama dalam penelitian ini adalah melakukan studi pustaka relevan dengan penelitain bertujuan untuk mempermudah penulis untuk memahami konsep topik yang sedang dikerjakan. Studi Pustaka dilakukan dengan cara mencari bahan untuk dijadikan acuan dan landasan dalam penelitian baik berupa referensi atau sumber pustaka yang berasal dari buku, jurnal, makalah, artikel, informasi yang berasal dari internet dan lain-lain.

B. Persiapan dan Identifikasi Kebutuhan

Langkah selanjutnya adalah melakukan analisis tentang kebutuhan seperti apa dan bagaimana untuk membangun atau membuat sebuah *environtment* target pengujian serangan *Exploit* dan analisis RAM komputer. Pada tahapan ini akan dibuat sebuah jaringan komputer yang dapat diakses secara LAN kemudian komputer tersebut akan dijadikan target dan objek penelitian dan akan dianalisis RAM komputernya, selain itu juga akan melakukan analisis untuk membuat skenario kasus yang relevan dengan penelitian.

C. Skenario dan Simulasi Kasus

Tahapan ketiga metode penelitian ini adalah melakukan penyusunan skenario penyerangan terhadap komputer target , serangan yang digunakan dalam penelitain kali ini adalah memanfaatakan *tools* Metasploit Framework untuk melakukan eksploitasi mesin komputer korban.

D. Investigasi RAM Forensik

Tahapan ini adalah melakukan serangkaian RAM komputer dengan metode *Live Forensics*, bertujuan untuk menemukan artefak apa saja yang bisa ditemukan ketika terjadi serangan *Exploit.* Analisis dilakukan dengan cara membandingkan data yang dihasilkan dari *live capture* terhadap RAM Komputer sebelum terjadi serangan *Exploit* dan pada saat *Exploit* terjadi atau pada saat komputer dapat di-*exploit*.

E. Pembuatan Laporan

Setelah serangkaian simulasi dan analisis dilakukan, maka melakukan pembuatan laporan dari seluruh proses penelitian, mulai dari pelaporan tahap awal hingga hasil penelitian.