Analisis Aspek Keamanan Dalam Menghadapi Rootkit Berbasis Mesin Virtual (VMBR)

Xaverius Najoan, ST., MT

Faculty of Engineering, Sam Ratulangi University, Indonesia

xnajoan@unsrat.ac.id

***Abstrak* — Kemajuan teknologi virtualisasi hardware telah membuka halaman baru dalam pertempuran digital. Dengan teknologi mesin virtual, terbuka peluang untuk salah satu pihak menguasai lapisan terbawah suatu sistem, yaitu lapisan hardware. Akibatnya, jika pihak attacker menguasai level ini, maka makin sulit untuk pihak defender mendeteksi aplikasi malware dari attacker.**

Kombinasi antara mesin virtual dan malware tipe rootkit menghasilkan sebuah ancaman baru yang disebut dengan Virtual Machine Based Rootkit (VMBR). Rootkit yang berbasis pada mesin virtual sangat sulit dideteksi dan dilenyapkan karena berada diluar wilayah akses aplikasi dan sistem operasi tersebut

Kata Kunci — Computer Security, Rootkit, Virtual Machine, VMBR

I. PENDAHULUAN

A. *Latar Belakang*

Aplikasi-aplikasi malware sudah mulai bermigrasi ke level yang lebih rendah . Makin kebawah level yang dikuasai, makin sulit dideteksi oleh lawan dan makin berkuasalah dia atas sebuah sistem tertentu. Salah satu tipe malware yang menjadi ancaman berbahaya dan harus dipahami oleh setiap pengguna komputer adalah rootkit. Hal ini disebabkan karena kemampuannya untuk menyembunyikan diri dan mengakali sistem operasi targetnya sehingga sistem operasi tersebut tidak menyadari kehadiran rootkit ini. Malware tipe ini beroperasi pada wilayah kernal dari sistem operasi, sehingga membuat dirinya tidak dapat dijangkau oleh aplikasi antivirus.

B. *Permasalahan*

Kemajuan teknologi virtualisasi hardware telah membuka peluang untuk rootkit bermigrasi dari level kernel sistem operasi ke level yang lebih rendah lagi, yaitu hardware. Kombinasi antara mesin virtual dan rootkit menghasilkan sebuah ancaman baru yang disebut Virtual Machine Based Rootkit (VMBR)[6],. VMBR beroperasi pada level yang lebih rendah lagi dibandingkan dengan rootkit biasa.

C. *Pertanyaan Penelitian*

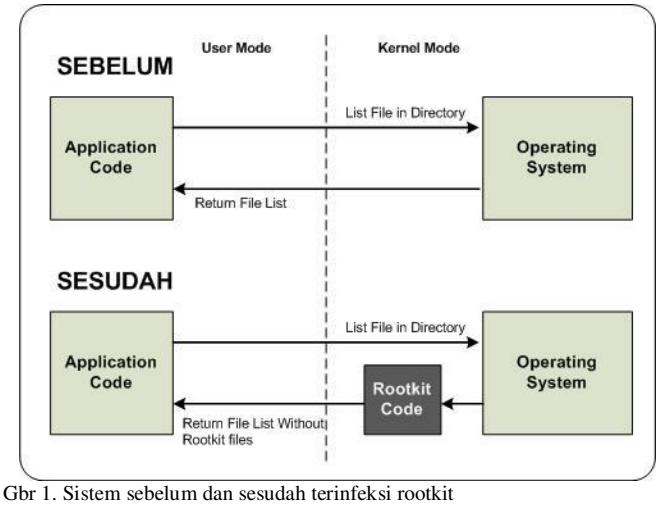
Pertanyaan penelitian adalah bagaimana menghadapi rootkit yang berbasis pada mesin virtual?

II. DASAR TEORI

A. *Rootkit*

Rootkit adalah sekumpulan program yang bertujuan untuk menyembunyikan file, folder, port yang terbuka, registry key, driver dan proses yang sedang berjalan ditempat dia bernaung. Tujuan dari rootkit adalah untuk menyediakan jalan bagi attacker agar aktifitasnya tidak terdeteksi dan tersembunyi. Jika karakteristik virus dan worm didefinisikan oleh satu kata "replication", maka rootkit dapat didefinisikan sebagai "stealth"[1]. Virus mereproduksi diri dan rootkit menyembunyikan diri.

Rootkit akan berusaha menyembunyikan dirinya agar sistem tersebut tidak bisa mendeteksi keberadaannya dan memperkuat aksesnya terhadap sistem target. Rootkit tidak hanya menyembunyikan dirinya, tetapi juga mempunyai kemampuan untuk menyembunyikan prosesnya yang sedang dikerjakannya[4].



Gbr 1. Sistem sebelum dan sesudah terinfeksi rootkit

Rootkit yang beroperasi pada level kernel mode akan mengubah dan memodifikasi beberapa proses dan function pada kernel sistem operasi. Hal ini mengakibatkan aplikasi antivirus yang berada pada user mode tidak dapat mendeteksi keberadaannya. Namun demikian, ada beberapa keterbatasan rootkit level kernel, yaitu :

1) Bisa dideteksi dengan Intrusion Detection System[2], apabila pihak defender berada pada level kernel juga. Sehingga kemenangan akan ditentukan oleh design dan proses dari masing-masing pihak dalam mengantisipasi lawannya.
2) Problematika dengan fungsionalitas dan invisibilitas. Rootkit dengan fungsi yang banyak akan mengurangi derajat invisibilitasnya. Sebaliknya rootkit dengan hanya satu fungsi saja, minimum pada fungsi namun tinggi pada tingkat invisibilitasnya.

B. *Virtual Machine*

Ide dasar dari mesin virtual adalah mengekstraksi perangkat keras seperti CPU, memori, disk drive ke beberapa environment sehingga menciptakan ilusi bahwa masing-masing environment tersebut menjalankan komputernya sendiri. Meskipun secara fisik tidak memiliki hardware, namun mesin virtual menciptakan keadaan virtual "seakan-akan" ada hardware tersebut.

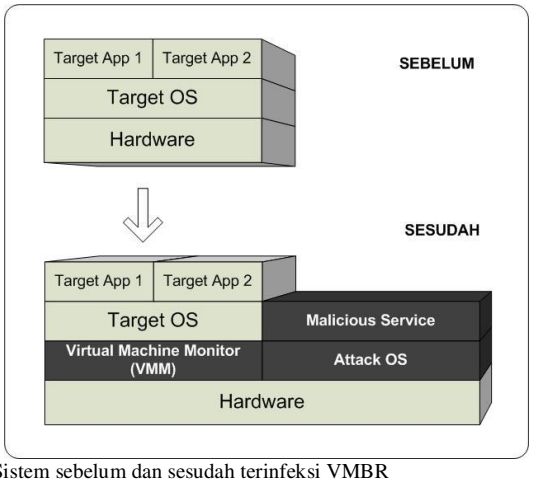
VM muncul karena adanya keinginan untuk menjalankan beberapa sistem operasi pada satu perangkat keras tertentu. Sistem VM memungkinkan pembagian sumber daya perangkat keras yang ada ke tiap-tiap VM yang berbeda. Dengan teknologi virtualisasi, maka sebuah komputer tunggal bisa menjalankan beberapa komputer virtual secara simultan dan bersama-sama.

Lapisan perangkat lunak yang menyediakan virtualisasi disebut VMM atau Virtual Machine Monitor. Diatas VMM dapat diinstall sebuah guest software (sistem operasi dan aplikasi). VMM akan menyediakan abstraksi hardware untuk guest software ini menggunakan emulated hardware. Selanjutnya Guest software akan berinteraksi dengan hardware virtual dengan cara yang sama seperti berinteraksi dengan hardware yang sebenarnya. Contohnya pada instruksi in/out, DMA, dan lain-lain. Semua guest software (termasuk sistem operasi) bekerja pada mode user, sedangkan VMM beroperasi pada level kernel. VMM akan mengisolasi semua sumber daya dari masing-masing mesin virtual dalam berhubungan secara langsung.

Beberapa contoh virtual machine seperti Vmware, mendukung instalasi untuk mesin X86, beberapa variasi sistem operasi linux, NetWare, Solaris dan sistem operasi Windows termasuk sistem operasi 64-bit[5].

C. *Virtual Machine Based Rootkit*

Virtual Machine Monitor (VMM) adalah powerful platform bagi rootkit. Rootkit mempunyai peluang untuk mengeksploitasi level hardware dan menaklukan IDS yang beroperasi pada level kernel. VMBR akan memindahkan sistem operasi target kedalam virtual machine dan menjalankan sistem operasi target (Target OS) diatas lapisan VMM.



Gbr 2. Sistem sebelum dan sesudah terinfeksi VMBR

Rootkit mengisolasi target OS didalam virtual machine, sehingga aplikasi keamanan (contohnya IDS) dari target OS menjadi tidak efektif ketika berhadapan dengan VMBR dan aplikasi malwarenya. Bukan hanya tidak efektif, tapi secara total tidak kelihatan oleh aplikasi kemanan tersebut. Sistem operasi target target akan melihat perubahan yang sedikit bahkan tidak ada perubahan sama sekali pada memory space, disk space, dan executionnya.

Dalam keadaan dimana VMM telah dieksploitasi oleh VMBR, maka VMBR dapat melihat dan memodifikasi semua states dan events yang ada pada target OS seperti keystrokes, paket network, disk state dan memory state, tanpa diketahui oleh target OS. Hal ini disebabkan VMBR mengendalikan secara penuh virtual hardware dari target OS dan aplikasi didalamnya. Selanjutnya VMBR menjadi platform yang aman dalam pengembangan aplikasi malicious tanpa diketahui oleh target OS.

VMBR menggunakan sistem operasi tersendiri (*Attack OS*) sehingga tidak kelihatan oleh aplikasi dari sistem operasi target namun mudah untuk diimplementasikan. Kemampuan untuk tidak tampak memberikan kebebasan kepada malicious services untuk dijalankan pada user mode attack OS tanpa khawatir akan teridentifikasi oleh target OS.

Malicious services VMBR dapat diklasifikasikan dalam 3 kategorI [3].

1) Malicous services yang tidak membutuhkan interaksi dengan target OS. Malicious jenis ini tidak berkomunikasi dengan target OS. Contohnya : spam relays, distributed denial-of-service zombie, dan phising web server.
2) Malicious services yang mengumpulkan informasi dari target OS. Malicious jenis ini akan mengumpulkan data dan events dari target OS. VMBR memungkinkan untuk menjalankan aplikasi keystroke, mencatat (log) paket jaringan, dengan cara memodifikasi VMM dari aplikasi device emulation. Sebagai contoh, VMBR dapat mencatat semua paket jaringan dengan memodifikasi VMM dari emulated kartu jaringan. Modifikasi ini tidak kelihatan oleh target OS karena interface dari kartu jaringan tidak mengalami perubahan.
3) Malicious services yang dengan sengaja mengganggu pelaksanaan eksekusi fungsi dan prosedur dari target OS.
4) Sebagai contoh malicious services dapat mengubah komunikasi jaringan, menghapus pesan email atau mengubah perintah eksekusi dari target aplikasi. VMBR dapat mengkustomisasi VMM dari lapisan device emulator untuk mengubah data pada level hardware.

III. Analisis Aspek Keamanan

A. *Aspek keamanan dibawah layer VMBR*

Cara yang terbaik untuk mendeteksi VMBR (juga untuk aplikasi malicious lainnya) adalah dengan beroperasi pada lapisan yang tidak dikendalikan oleh VMBR. Aplikasi keamanan yang beroperasi pada level dibawah lapisan VMBR dapat melihat VMBR karena cara pandang dari detektor tersebut tidak melalui lapisan virtualisasi dari VMBR. Aplikasi keamanan jenis ini harus dapat membaca memori

fisik (bukan memori virtual) dan melihat beberapa anomali pada sistem yang menunjukan kehadiran VMBR.

Salah satu cara untuk mendapatkan kendali atas lapisan dibawah VMBR adalah dengan menggunakan perangkat keras yang terjamin aman. Beberapa perangkat keras tersebut contohnya: Intel La Grande, AMD platform. Perangkat keras tersebut menyediakan aplikasi untuk bisa mendapatkan posisi kendali lapisan dibawah VMBR.

Cara yang lain adalah dengan melakukan booting komputer melalui CD-ROM, USB atau network boot yang aman. Dengan cara ini, sistem melakukan booting sebelum VMBR diload

Cara yang ketiga untuk mendapatkan kendali atas lapisan dibawah VMBR adalah dengan menggunakan secure VMM, dimana secure VMM ini diload sebelum proses loading dari sistem operasi. Secure VMM juga mencegah proses instalasi dari VMBR. Tujuan utama dari secure boot adalah mencegah malware memiliki akses untuk melakukan perubahan dan modifikasi pada master boot record dan sistem file boot sector. Secure VMM akan memverifikasi otentifikasi jika terjadi perubahan pada master boot record. Dengan demikian, apabila terjadi proses instalasi VMBR, maka secure VMM akan membatalkan proses tersebut

B. *Aspek keamanan diatas layer VMBR*

Sebelumnya telah dijelaskan bahwa semua aplikasi keamanan yang berada diatas lapisan VMBR tidak efektif dalam mendeteksi keberadaan VMBR ini. Hal ini disebabkan VMBR state berada diluar jangkauan aplikasi tersebut yang notabene aplikasi tersebut telah terjerat didalam virtual machine.

Misalkan sistem target bisa melihat aktivitas dari malware diluar virtual machine, tetap saja VMBR mempunyai kemampuan untuk mengubah eksekusi dari aplikasi keamanan sistem target tersebut, sehingga eksekusi tersebut menjadi tidak valid dan sistem memberikan laporan hasil yang salah (report incorrect result).

Dua hal yang telah dijelaskan di atas, menjadi batasan bagi aplikasi keamanan yang beroperasi diatas VMBR. Memang, VMBR secara fisik tidak kelihatan, namun keberadaan VMBR atas sistem dapat dianalisa melalui penurunan kinerja sumber daya dari perangkat keras, seperti CPU time, memori dan disk space dan bandwidth jaringan.

VMBR akan mengemulasi mesin virtual untuk menjalankan proses-proses target OS didalam mesin virtual, sehingga pemakaian sumber daya, dalam hal ini CPU time, menjadi meningkat dan proses pada target OS menjadi lambat. Perbedaan waktu dari CPU time ini dapat menjadi tolak ukur dari pengguna untuk membandingkan CPU time ini dengan waktu sebenarnya (misalnya jam tangan). Perbedaan waktu yang signifikan ini menjadi bahan analisa keberadaan VMBR.

Keberadaan VMBR bisa juga dianalisa dari kinerja pemakaian disk space. Karena VMBR harus mengemulasi proses-proses pada target sistem didalam virtual machine, maka kebutuhan akan sumber daya perangkat keras komputer tersebut menjadi tinggi pula. VMBR akan menggunakan page file pada harddisk ketika aktifitasnya melewati batas maksimum dari kapasitas memori. Aplikasi keamanan dapat diterapkan untuk mendeteksi adanya VMBR dengan cara menjalankan sebuah program tertentu yang membutuhkan memori keseluruhan dari sistem komputer. Penurunan kinerja dari page file pada harddisk akibat eksploitasi VMBR menjadi bahan analisa keberadaan VMBR.

Salah satu gangguan pada sistem target akibat keberadaan dari VMBR adalah pada I/O devices. Seperti yang sudah dijelaskan sebelumnya bahwa VMM akan memvirtualisasikan I/O devices yang digunakan oleh sistem target. Memvirtualisasi I/O devices tanpa mengubah perspektif dari sistem target adalah sebuah hal yang berat. Hal ini disebabkan VMM sebelumnya harus memahami interface dan semantik dari tiap-tiap I/O device. Dengan perkembangan teknologi yang semakin cepat dan begitu banyak variasi perangkat I/O akan sangat sulit untuk memahami interface dan semantik masing-masing variasi . Oleh karena itu aplikasi keamanan dapat menerapkan Intrusion Detector dengan menganalisa perubahan pada I/O device saat VMBR diinstalasi.

IV. KESIMPULAN

Virtual Machine Based Rootkit (VMBR) adalah sebuah aplikasi malware yang lebih sulit untuk dideteksi dibandingkan dengan malware lainnya. Hal ini disebabkan VMBR beroperasi pada lapisan dibawah lapisan sistem target, sehingga semua aplikasi keamanan didalam sistem target tidak bisa mendeteksinya karena VMBR telah menjerat sistem target didalam sebuah virtual machine.

Malware services yang dapat dikembangkan setelah sebuah sistem terinfeksi VMBR contohnya : Phising web server, keylogger dan aplikasi malware untuk mencatat paket data jaringan.

Meskipun VMBR adalah sebuah aplikasi powerful malware, VMBR mempunyai beberapa kekurangan yang dapat menjadi bahan analisa untuk menanggulanginya. Beberapa kekurangan dari VMBR adalah :

1) Sulit pada proses instalasi. Hal ini disebabkan karena VMBR harus mempunyai akses level yang mempunyai kapabilitas untuk mengubah boot sequence.
2) VMBR akan memberikan pengaruh yang signifikan terhadap kinerja sumber daya sistem target. VMBR menurunkan kinerja dari sumber daya CPU, memori dan disk space, karena kebutuhan VMBR untuk menjalankan sistem operasi target didalam virtual machine dan memberikan abstraksi virtual perangkat keras kepada sistem operasi target.

Beberapa cara untuk menanggulangi VMBR adalah dengan menggunakan secure hardware, melakukan booting dari media yang aman, dan menggunakan secure VMM.

VMBR merupakan aplikasi malware yang tidak boleh dipandang sebelah mata dan harus diperhatikan sebagai salah satu aplikasi yang mengganggu keamanan sistem informasi.

REFERENCES

[1] Embleton, S., S. Sparks and C. Zou. 2008. SMM Rootkits: A New Breed of OS Independent Malware. In *Proceeding of the 4th International Conference on*

Security and Privacy in Communication Networks. SecureComm. Istanbul, Turkey.

[2] Garfinkel, T., M. Rosenblum. 2003. A Virtual Machine Introspection Based Architecture for Intrusion Detection. In *Proceeding of the 10th Annual Network and Distributed System Security Symposium*. Internet Society. California, USA.

[3] King, S.T., P.M. Chen, Y. Wang, C. Verbowski, H.J. Wang, and J.R. Lorch. 2006. SubVirt: Implementing Malware with Virtual Machines. In *Proceeding of the 2006 IEEE Symposium on Security and Privacy*. IEEE Computer Society. California, USA.

[4] Ries, C. 2006. *Inside windows rootkits*. VigilantMinds Inc.

[5] VMware Server Virtual Machine Guide. 2006. Technical Report. VMware, Inc.

[6] Windows IT Pro. 2006. *Virtual Machine-based Rootkits*. http://windowsitpro.com/article/articleid/49755/virtual-machine-based-rootkits.html.