Journal of Computer Science and Technology
JCS-TECH Vol.2, No.1, Mei 2022, PP 8-13
e-ISSN 2808-9677, p-ISSN 2809-1140

PENGENALAN AKTIFITAS CYBER THREAT HUNTING : STUDI KASUS HUNTING MALWARE DENGAN METODE MEMORY FORENSIC

Fadillah Nursyahiddin[1], Siti Zulfa Oktaviani[2], Lutvita Dwi Iklima[3], Feby Nurdiyanti[4]
[1,2,3,4] Fakultas Engineering, Computer and Design
Nusa Putra University, Indonesia
fadil.dlz@gmail.com[1], szulfaoktaviani@gmail.com[2], lutvitadwiiklima@gmail.com[3],
febynurdyanti@gmail.com[4]

Abstrak

Cyber Threat Hunting adalah salah satu aktivitas pada lingkup keamanan siber yang sedang berkembang pada saat ini. Threat Hunting menunjukan proses pencarian kerentanan serta aktor kejahatan siber yang kemungkinan sudah berada di dalam system maupun rencana kemungkinan seragan yang akan terjadi di waktu yang akan datang secara proaktif melalui media jarigan untuk mengantisipasi adanya insiden keamanan siber yang akan terjadi pada suatu infrastruktur terkait. tentu dengan adanya threat hunting ini akan melengkapi kegiatan passive monitoring yang hanya mengandalkan alert pada SIEM (Security Information and Event Management), dan studi kasus yang akan saya angkat adalah metode threat hunting pada low level memory sehingga apabila ada aktor kejahatan siber yang lolos pada sistem SIEM dan berkemungkinan sudah berada pada sistem internal dapat terdeteksi dan dapat melakukan kegiatan forensik dan pemulihan sistem terkait.

Kata Kunci: *Forensik Memori, Threat Hunting, Information Security, SIEM, Logs*

Abstract

Cyber Threat Hunting is one of the activities in the cyber security sphere that is currently developing. Threat Hunting shows the process of proactively searching for vulnerabilities and cybercrime actors through network media to anticipate cybersecurity incidents that will occur in a related infrastructure. Of course with this threat hunting, it will complement passive monitoring activities that only rely on alerts on SIEM (Security Information and Event Management), and the case study that I will raise is the threat hunting method at low level memory so that if there are cybercriminal actors who escape the system SIEM and possibly already on internal systems can be detected and can perform forensic and related system recovery activities.

Keywords: *Forensik Memori, Threat Hunting, Information Security, SIEM, Logs*

Article Info | Article history: Received 2022-01-19 | Revised 2022-02-21 | Accepted 2022-04-05 | Publised 2022-05-08
JCS-TECH | Journal of Computer Science and Technology | DOI: 10.54840/jcstech.v2i1.20

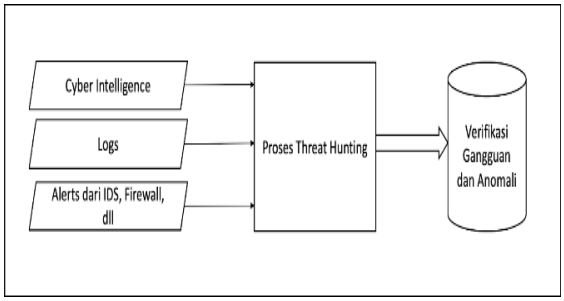
1. Pendahuluan

Cyber Threat Hunting adalah salah satu kegiatan proactive security monitoring dalam bidang kemanan siber yang melengkapi metode passive security monitoring yang mengandalkan tools dan aturan dalam memanage security alert pad asebuah infrastruktur, sehingga belum maksimal karena hanya mengandalkan alert dari sistem yang sidah dirancang. Threat hunting difokuskan untuk menemukan ancaman dan anomali pada jaringan dan sistem sebuah organisasi dengan memantau dan menganalisis logs baik dengan otomatisasi dan human analysis. Pada Gambar 1 menunjukan proses threat hunting dari pengumpulan tiga sumber yaitu Cyber Threat Intelligence, Logs, Alert dari tradisional IDS dan Firewall.

Dalam sebuah paradigma IT Security, terutama dalam hal ini di area Cyber Defence, ada 3 hal yang perlu diingat dan diketahui bersama yaitu Pertama, Anda tidak dapat mencegah semua serangan siber yang ada, Kedua, Network dan infrastruktur bagaimanapun, dan kapanpun, akan selalu terbuka kemungkinanannya untuk terjadi compromise / breach, Ketiga, 100% secure is imposible. Dari ketiga hal tersebut kita dapat memahami bahwa kita tidak dapat mencegah para aktor siber untuk melakukan tindakan kejahatan pada lingkup siber. Satu hal yang yang dapat diupayakan secara maksimal adalah melakukan upaya semaksimal mungkin untuk meminimalisir resiko cyber security attack, meminimalisir dampak dari cyber attack jika attack tersebut telah terjadi, dan bagaimana kita proactive melakukan upaya pencegahan, dan melakukan response jika suatu saat terjadi breach pada infrastruktur kita.

Threat hunting diperlukan karena ada berbagai macam alasan dan tujuan seperti Stealth Activity dari Threat Aktor (Passive security monitoring tidak dapat mendeteksi sebagian besar aktivitas yang tersembunyi yang dulakukan oleh threat aktor.), Spohisticated dan Advance Attack Vector (metode serangan advance baru yang dapat mengabaikan passive monitoring Security), Reducing Incident Response Time (Mengurangi dwell time dalam merespon adanya security incident dan breach)

Pada paper ini akan menjelaskan tentang aktivitas keamanan siber yang populer pada saat ini, menjelaskan tentang kegiatan



threat hunting, praktik dengan studi kasus hunting malware pada low level memory dengan metode memory forensic.

Gambar. 1. Proses Threat hunting dari collect data

2. Skill Threat Hunting

Threat hunting yang berhasil membutuhkan seperangkat ketrampilan teknis dan pola pikir yang tepat. Pertama, kita membutuhkan laporan threat intelligence dari berbagai sumber. Kedua, adalah memahami pola pikir aktor dan memahami sistem F3EAD (Find, Fix, Finish, Exploit, Analyze and Disseminate). Ketiga, Analisis data keamanan yang membutuhkan pemahaman tentang Data Science dan Analytical Models. Beberapa ketrampilan lain juga diperlukan seperti Forensic Analysis, Malicious code analysis, penetration testing, metode komunikasi jaringan, vulnerability analysis, Memahami Attacker Lifecycle pada gambar 2 berikut :

Gambar. 2. Lifecycle Attacker

Threat hunting berbeda dari banyak kegiatan pada metode keamanan siber tradisional. threat hunting adalah tugas yang sangat tidak terstruktur yang menuntut pengetahuan teknis yang mendalam. disini saya akan membandingkan kegiatan threat hunting dengan aktivitas keamanan siber lainnya.

Threat Hunting vs Threat Detection : Kegiatan Threat hunting berdasarkan pada penemuan ancaman yang tidak spesifik dan tidak ada tanda-tanda dan dilakukan secara proaktif. Sedangkan Threat detection secara umum merupakan proses mengindetifikasi ancaman berdasarkan proses yang terstruktur. Alat Threat detection biasanya menganalisis logs jarigan, logs aplikasi, logs data, dan logs aktivitas pengguna untuk menemukan anomali. Threat detection bergantung pada peringatan dari sensor untuk mendeteksi ancaman

Threat Hunting vs Cyber Defence : Cyber defence berfokus pada hardening sistem terhdap serangan siber. Aktifitas ini mencakup konfigurasi keamanan dan penggunaan teknologi pertahanan siber seperti firewall, Intrusion Detection, Intrusion Prevention. Namun penyerang seringa kali dapat menghindari mekanisme tersebut dengan menggunakan teknik-teknik terbaru yang tidak diketahui oleh Cyber defenfer

Threat Hunting vs Penetration Testing : Pentration testing berkaitan dengan menemukan kerentanan, baik dalam konfigurasi software atau sistem. Biasanya, penetration testing dilakukan dengan melakukan analisis kode statis dan dinamis dari software dan sistem terkait. Sebaliknya, Threat hunting bertujuan untuk menemukan penyusup yang ada dalam sistem.

Threat Hunting vs Forensics : Kedua kegiatan tersebut melibatkan analisis data. Namun Forensik dimulai dengan insiden yang sudah diketahui dan flasback untuk memahami bagaimana ancaman itu bisa sampai terjadi, dengan cara mengumpulkan bukti dan dampak yang disebabkan insiden tersebut. Forensik adalah prosedur yang berguna untuk mengambil tindakan hukum saat terjadi insiden serangan siber.

Threat Hunting vs Cyber Intelligence : Cyber intelligence adalah salah satu teknik yang mungkin di gunakanakan untuk mendukung kegiatan threat hunting. Misalnya, jika ada ancaman trojan tertentu yang sudah diketahui, Threat hunting dapat difokuskan untuk menemukan apakah trojan tersebut telah menyusupi tanpa terdeteksi, dengan menggunakan data intelligence siber yang sudah didapatkan.

Threat Hunting vs IDS : Poin yang membedakan antara keduanya yaitu pada metode yang digunakan. IDS menggunakan metode Passive Monitoring yang hanya terpaku pada peringatan atau alert yang muncul ketika ada sebuah kegiatan terdeteksi oleh sistem yang sudah di konfigurasi sedemikian rupa, sendangkan Threat hunting menggunakan metode pro-Active monitoring security yang melibatkan Tools dan keahlian seorang individu untuk kemungkinan mendeteksi ancaman yang tidak terdeteksi oleh sistem IDS.

3. Penelitian dan Studi Kasus

Skenario studi kasus yang akan di praktikan adalah berupa sistem yang stack karena overloaded dengan cara menambahkan kode berbahaya untuk di jalankan dengan aplikasi resmi / terautorisasi pada RAM target sehingga apabila kode berhasil dijalankan maka akan membuka backdoor untuk seorang attacker untuk mengakses sistem secara ilegal, dan sistem host ini juga akan berada pada Virtual Environtment, sistem yang diguanakan adalah Kali Linux untuk melakukan hunting serta membuat dan menkompilasi kode python yang dibutuhkan.

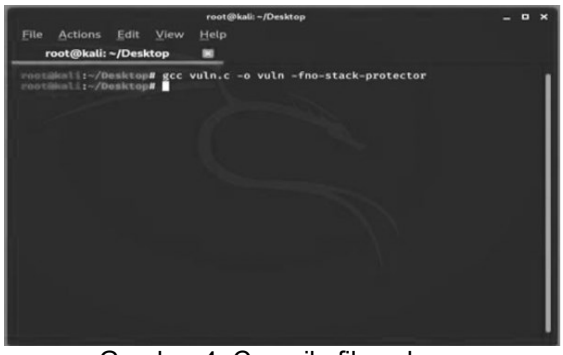
3.1. Langkah 1

Pertama membuat sebuah file dengan nama vuln.c dan menjalankan file tersebut didalam sistem.

Gambar 3. Membuat file vuln.c

3.2. Langkah 2

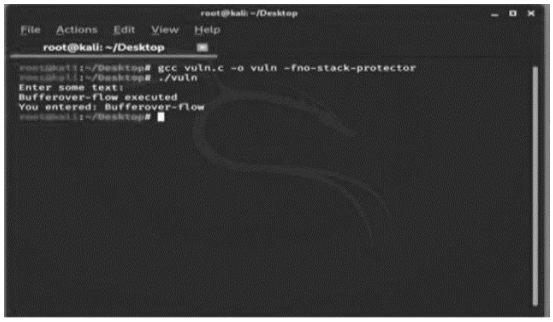
Pada langkan kedua yaitu proses mencompile file vuln.c yang sudah dibuat agar bisa di jalankan pada sistem host.



Gambar 4. Compile file vuln.c

3.3. Langkah 3

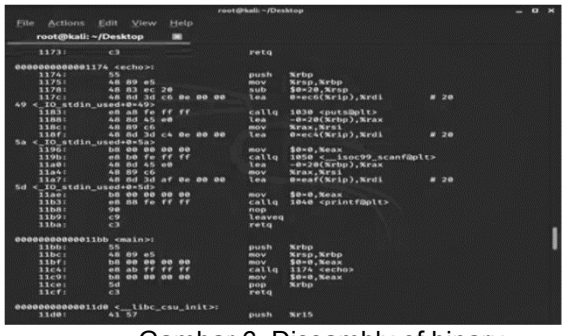
Setelah pembuatan file vuln.c dan proses kompilasi pada tahap ketiga kita akan menjalankan file vuln.c pada system



Gambar 5. Eksekusi program vuln.c

3.4. Langkah 4

Setelah program vuln.c berhasil di jalankan / dieksekusi, sekaran kita akan men-disassembly binariesnya atau membongkar program yang berjalan dalam bentuk binary. Proses pembedahan ini sanga diperlukan dalam proses hunting untuk mengetahui lokasi fungsi tersembunyi dari program tadi. Fungsi ini kami buat untuk memicu bufferoverflow atau smashing the stack terjadi pada sistem.



Gambar.6. Dissambly of binary

Setelah eksekusi sukses di lakukan sampai langkah 4 dan program benar-benar sudah berjalan pada memori, langkah terakhir adalah mendesain payload. Sekarang kita mengetahui bahwa setelah program di eksekusi ada 28 byte telah tersedia untuk terjadinya buffer%rbp akan disimpan dalam 4 byte berikutnya. Oleh karena itu alamat pengirim atau attacker akan disimpan dalam 4 byte berikutnya. Alamat pengirim disini adalah alamat yang %eip harus melompat setelah compilasi fungsi tersembunyi tersebut. Jadi, sederhananya dijelaskan bagaimana payload yang dirancang akan berjalan. yaitu 32 byte, berarti 28 + 4 yang mana 4 byte tersebut adalah fungsi tersembunyi yang mencurigakan.

3.5. Langkah 5

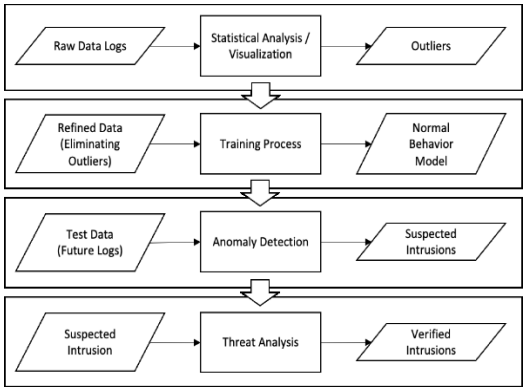
Langkah 5 adalah fase terakhir dari demonstrasi case pada penelitian ini, dan kita akan membuat payload untuk, Sebuah kode yang sukses di eksekusi untuk payload adalah python -c ‘print “P”*32 + “\x9c\x84\x04\x08”’ |. /sts. setelah eksekusi program ini berhasil makan akan ditampilkan pada gambar diatas dengan sangat jelas bahwa program tersebut telah masuk ke sebuah fungsi tertentu, dan alasannya menjalankan kode tersebut adalah untuk menyingkirkan fungsi yang tersisip pada memory overflowed. Setelah dieksekusi kode tersebut maka memory overflowed akan terhindari dan terhapus.

Gambar.7. Piping the payload

4. Solusi Penerapan

Ada banyak teknik yang memungkinkan seseorang dapat mencapai solusi yang hampir sempurna untuk melakukan Hunting. Para peneliti telah menerapkan beberapa teknik mulai dari pencarian manual hinggal model statistik atau probabilitas, visualisasi pada log untuk mendeteksi anomali, bahkan pendekatan yang lebih canggih seperti machine learning (contohnya, decision tree, neural networks, dsb) juga bisa digunakan untuk keperluan hunting dan ancaman terbaru. Pada bagian ini, kami mengusulkan solusi hybrid yang terdiri dari analisis statistik, visualisasi, dan machine learning untuk memverifikasi intrusi. pada gambar 6 menunjukan strategi solusi langkah kami yang dapat digunakan oleh analis security untuk proses threat hunting dari log. pada

langkah pertama kami menerapkan analisis statistik dan teknik visualisasi untuk mengetahui kemungkinan ouliers. Selanjutnya, kami menyaring kumpulan data mentah dengan mengurangi semua kemungkinan outlier dari kumpulan data. Pada langkah kedua, kami akan melatih sistem machine learning untuk membangun model perilaku normal untuk pengujian lebih lanjut. Tahap ketiga adalah tahap mendeteksi anomali.



Gambat. 8. Solusi tahapan proses Threat Hunting

5. Kesimpulan

Kesimpulan dari penelitian serta penjelasan di atas adalah Threat Hunting merupakan kegiatan yang memfokuskan pada aktivitas yang sifatnya berulang kali, dengan melakukan pendekatan untuk mengindentifikasi, dan memahami threat actor yang mungkin sudah masuk dan berada di dalam infrastruktur kita serta melihat indikator, mencari anomaly behavior yang ada pada sistem kita dan mencoba membuat hipotesa mengenai bagaimana seorang threat aktor mampu memasuki environment sisten kita. Dengan demikian, anda dapat memprediksi, atau melihat kemungkinan-kemungkinan celah yang dapat dilakukan oleh threat aktor.

Dengan melakukan contoh studi kasus yang bertema memanfaatkan metode memory forensic untuk kegiatan Threat hunter, Akan mempermudah bagi hunters untuk memutuskan bahwa infrastruktur terkait tersebut tersusupi oleh program yang berpotensi terhadap terjadinya insiden serangan siber yang terhindar dari parameter security monitoring, seperti SIEM (Security Information and Event Management), IDS (Intrusion Detection System), Firewall. yang mana malware atau kode berbahaya tersebut berjalan berjalan pada low level memory.

6. Daftar Pustaka

Priya B Gadgil, Sangeeta Nagpure “Hunting advanced volatile threats using memory forensics”International journal of advance research , ideas and innovations in technology (Volume 4, Issue 4).

Jonathan Graham, Cheryl Hinds, Sandi Samuel” Hunting Malware: An example using Gh0st”International Conference on Computational Science and Computational

The Importance Of Business Information in Cyber Threat Intelligence University of Innsbruck, Department of Computer Science, Innsbruck, Austria.

Mr. Vivek Ravindra Sali, Mrs. H.K.Khanuja “RAM Forensics: The Analysis and Extraction of Malicious processes from memory Image using GUI based Memory Forensic Toolkit “ 2018. Fourth International Conference on Computing Communication Control and Automation(ICCUBEA).

Da-yu kao, Yi-ting chao, Fuching tsai, Chia-yiang huang, “Digital Evidence Analytics Applied in Cybercrime Investigations” 2018 IEEE Conference on Applications, Information and Network Security (AINS).

Mr. Chathuranga Rathnayaka, Dr. Aruna Jamdagni “An Efficient Approach for Advanced Malware Analysis using Memory Forensic Technique” 2017 IEEE Trustcom/BigDataSE/ICESS.

M avroeidis, V., & Bromander, S. (2017). Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. Proceedings of the IEEE.

Closing the Skills Gap with Analytics and Machine Learning by ahmad tantawy October 2017.

SANS Threat Hunting & IR Summit 2018. [16]Salameh, Jamal N. Bani, "A New Technique for Sub-Key Generation in Block Ciphers," World Applied Sciences Journal 19, no. 11.

Priya B Gadgil, Sangeeta Nagpure “Analysis Of Advanced Volatile Threats Using Memory Forensics” Mahatma Education Society‟s Transactions and Journals‟ Conference Proceedings ISBN 978-93-82626- 27-5”.

Dolly Uppal, Vishakha Mehra , Vinod Verma Basic survey on Malware Analysis, Tools and Techniques" nternational Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014.

HaddadPajouh, Hamed, et al. "A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting." Future Generation Computer Systems 85 (2018): 88-96.

Arel, Itamar. "The threat of a reward-driven adversarial artificial general intelligence." Singularity Hypotheses. Springer, Berlin, Heidelberg, 2012. 43-60.