CESS
(Journal of Computing Engineering, System and Science) 8(1) January 2023 209-219

e-ISSN: 2502-714x
p-ISSN: 2502-7131

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: https://jurnal.unimed.ac.id/2012/index.php/cess

Analisis Perbandingan Performa CPU pada Sistem Operasi FreeBSD 64-bit dan RedHat Linux 64-bit terhadap Serangan *Denial of Service* (DoS) Menggunakan Hping3

Comparative Analysis of CPU Performance on FreeBSD 64-bit and RedHat 64-bit Operating System Against Denial of Service (DoS) Using Hping3

Ihsan Fadli Tampati[1*], Faizal Gani Setyawan[2], Wiyar Wilujengning Sejati[3], Aqwam Rosadi Kardian[4]

[1,2,3]Politeknik Siber dan Sandi Negara
Jl. Raya H. Usa, Putat Nutug, Bogor, Indonesia 16120
email: [1]ihsan.fadli@student.poltekssn.ac.id, [2]faizal.gani@student.poltekssn.ac.id
[3]wiyar.wilujengning@student.poltekssn.ac.id, [4]aqwam@staff.jak-stik.ac.id

A B S T R A K

Serangan *Denial of Services* (Dos) merupakan jenis serangan terhadap lalu lintas server. DoS bekerja dengan memberikan beban yang berat terhadap server, sehingga server tidak dapat menampung koneksi dari pengguna-pengguna lain dan dapat menyebabkan kegagalan sistem pada server. Di sisi lain, serangan *Denial of Services* (DoS) dapat digunakan untuk menguji ketahanan server. Server yang akan diuji yaitu menggunakan sistem operasi RedHat Linux dan FreeBSD. Pengujian dilakukan dengan membanjiri sistem dengan serangan DoS menggunakan *tools* hping3, kemudian membandingkan hasil pengujian berupa persentase konsumsi CPU dan konsumsi memori antar sistem operasi untuk mengetahui kerentanan pada masing-masing sistem operasi. Berdasarkan perbandingan hasil pengujian antar sistem operasi, sistem operasi FreeBSD memiliki performa CPU yang lebih baik dari sistem operasi RedHat Linux, namun memiliki kerentanan pada memori internal terhadap serangan DoS. Sedangkan sistem operasi RedHat Linux memiliki performa memori internal yang lebih baik dari sistem operasi FreeBSD, namun memiliki kerentanan pada performa CPU terhadap serangan DoS.

Kata Kunci: *serangan denial of services, tools hping3, analisis performa sistem operasi.*

A B S T R A C T

Denial of Services (Dos) attack is a type of attack against server traffic. DoS works by placing a heavy load on the server, so that the server cannot accommodate connections from other users and can cause system failure on the server. On the other hand, Denial of Services (DoS) attacks can be used to test server resilience. The servers to be tested are using RedHat Linux and FreeBSD operating systems. Testing is carried out by flooding the system with DoS attacks

**Penulis Korespondensi:*
email: ihsan.fadli@student.poltekssn.ac.id

using the hping3 tool, then comparing the test results in the form of percentages of CPU consumption and memory consumption between operating systems to determine vulnerabilities in each operating system. Based on a comparison of test results between operating systems, the FreeBSD operating system has better CPU performance than the RedHat Linux operating system, but has a vulnerability in internal memory to DoS attacks. Meanwhile, the RedHat Linux operating system has better internal memory performance than the FreeBSD operating system, but has a vulnerability in CPU performance against DoS attacks.

Keywords: *denial of services attacks, hping3 tools, operating system performance analysis.*

1. PENDAHULUAN

Seiring dengan berkembangnya zaman, teknologi ikut berkembang dengan pesat, salah satunya komputer. Komputer terdiri dari sistem operasi, perangkat lunak, dan pengguna. Sistem operasi adalah sekumpulan kode program yang dikembangkan secara khusus sehingga dapat berjalan dan beroperasi pada sistem komputer. Sistem operasi memiliki dua fungsi utama, yaitu mengelola penggunaan sumber daya komputer dan menjadi antarmuka antara perangkat keras komputer dengan pengguna [3]. Oleh karena itu, untuk dapat beroperasi, setiap komputer harus memiliki setidaknya satu sistem operasi. Contoh sistem operasi yang banyak digunakan saat ini yaitu Microsoft Windows, Apple MAC OS, Linux, dan BSD. Sistem operasi penting karena berfungsi untuk mengatur proses pada setiap program komputer yang sedang dijalankan, mengatur penggunaan memori, manajemen sistem berkas, serta mengatur proses *input/output* (I/O).

Saat ini, berbagai sistem operasi masih dikembangkan dan dikelola oleh perusahaan dan komunitas penelitian. Misalnya, sistem operasi Linux, perangkat lunak *open source* terbesar di dunia, saat ini digunakan dalam berbagai aplikasi komputasi, mulai dari perangkat tertanam hingga server yang besar. NetFlix menggunakan server berbasis sistem operasi Linux dengan arsitektur *microservice* untuk layanannya, tetapi menggunakan sistem operasi FreeBSD untuk *Content Delivery Network* (CDN) sistem. Oleh karena itu, kami memperkirakan bahwa pengguna akan memilih sistem operasi yang sesuai berdasarkan situasi tertentu di masa depan [15].

Beberapa sistem operasi menawarkan performa CPU yang baik, seperti sistem operasi FreeBSD dan RedHat Linux. FreeBSD adalah sistem operasi mirip Unix yang bersifat *open source* dan turunan dari AT&T Unix melalui BSD Unix. FreeBSD tidak memiliki *copyright*, dapat diunduh secara bebas, dan mudah dikustomisasi untuk menghindari kode program yang berbahaya [8]. Sedangkan, RedHat Linux adalah sistem operasi turunan Linux. Menurut Dr. Earl Joseph, seorang Chief Executive Officer dari Hyperion, Redhat Linux merupakan sistem operasi paling populer yang menawarkan *high performance computing* (HPC), termasuk dari beberapa *supercomputer* dunia.

Namun, setiap sistem operasi pasti memiliki kerentanan. Dari sudut pandang penyerang, kerentanan merupakan peluang untuk melakukan eksploitasi [9]. Pada awalnya, penyerang akan menargetkan sistem kontrol jaringan pada sistem operasi yang memiliki kerentanan untuk mengirimkan paket-paket data. Serangan ini membutuhkan penyerang untuk memiliki pengetahuan tentang protokol komunikasi serta dinamika sistem. Di sisi lain, penyerang yang memiliki informasi terbatas di kontrol sistem dapat menggunakan serangan *Denial of Service* (DoS) [5]. Dengan munculnya paradigma komputasi baru, seperti komputasi awan, serta munculnya teknologi pervasif, seperti *Internet of Things*, serangan *Denial of Services* (DoS)

telah berkembang secara drastis sehingga menjadikannya salah satu ancaman yang paling berbahaya [14]. Salah satu akibat dari serangan DoS yaitu lalu lintas jaringan akan penuh dan mempengaruhi performa sistem operasi.

Keamanan sistem operasi dapat diuji dengan banyak metode. Pengujian yang dilakukan terhadap sistem operasi dan jaringannya berfungsi untuk menemukan kerentanan pada sistem operasi [10]. Adapun salah satu contoh metode pengujian keamanan sistem operasi yaitu dengan meneliti jumlah kerentanan yang ditemukan dalam sistem operasi, kemudian mengaitkannya dengan resiko yang akan dihadapi, sehingga dapat menentukan indeks tingkat keamanan suatu sistem operasi [16]. Venter dan Eloff pada tahun 2004 [17] melakukan analisis kerentanan pada sistem operasi dengan menggunakan *tools vulnerability scanner*; Ruohone, Hyrynsalmi, dan Leppanen pada tahun 2015 [18] melakukan analisis kerentanan pada sistem operasi dengan menganalisis pertubumbuhan kerentanan di setiap sistem operasi menggunakan kesaamaan linier, logistik, dan fungsi gompertz; dan Johnston, Gorton, Lagerstrom, dan Ekstedt pada tahun 2016 [19] melakukan analisis kerentanan pada sistem operasi dengan menggunakan metode *time beetwen vulnerablity disclosures* (TBVD).

Pada penilitan ini, analisis kerentanan sistem operasi dilakukan dengan menguji ketahanan sistem terhadap serangan *Denial of Services* (DoS) menggunakan *tools* hping3, kemudian membandingkan hasil pengujian berupa persentase konsumsi CPU dan konsumsi memori antar sistem operasi. Adapun penelitian ini ditujukan untuk:

a. Mengetahui kerentanan sistem operasi terhadap serangan DoS

b.Mengetahui sistem operasi dengan performa CPU yang lebih baik terhadap serangan *Denial of Service* (DoS).

2. LANDASAN TEORI

2.1 *Common Vulnerabilities Exposure* (CVE)

Kerentanan perangkat lunak adalah kekurangan dan/atau kelemahan yang ada di dalam suatu kode pemrograman. Kerentanan dimanfaatkan oleh penyerang untuk melakukan berbagai jenis serangan, seperti *ransomware*, *phishing*, infeksi *malware*, dan kebocoran data. Setiap kerentanan secara unik diidentifikasi dengan id yang spesifik dalam *Common Vulnerabilities Exposure* (CVE - Paparan Kerentanan Umum) dan memiliki deskripsi, ditulis dalam bahasa alami, serta dalam format teks bentuk bebas. Deskripsi merincikan spesifikasi produk yang terpengaruh dan eksploitasinya dari perspektif pengembang. CVE dapat diperkaya dengan informasi tambahan seperti penilaian *Common Vulnerability Scoring System* (CVSS) dan *Common Weakness Enumeration* (CWEs) [11]. Penelitian ini akan menggunakan *Common Vulnerabilites Exposure* (CVE) untuk mendefinisikan beberapa kerentanan pada sistem operasi RedHat Linux dan sistem operasi FreeBSD.

2.2 Serangan *Denial of Services* (Dos)

Denial of service attack (DoS) adalah semua jenis serangan pada struktur jaringan untuk menonaktifkan server. Serangan yang dilakukan yaitu mengirim jutaan permintaan ke suatu server untuk memperlambat performa server tersebut, kemudian membanjiri server dengan paket besar data yang tidak valid sehingga server akan mengalami kegagalan [12]. Penelitian ini akan menguji performa CPU dan kapasitas memori pada sistem operasi RedHat Linux dan FreeBSD menggunakan *tools* hping3 untuk melancarkan serangan *Denial of Service,* kemudian menganlisis hasil serangan terhadap kedua sistem operasi tersebut.

2.3 *Tools* hping3

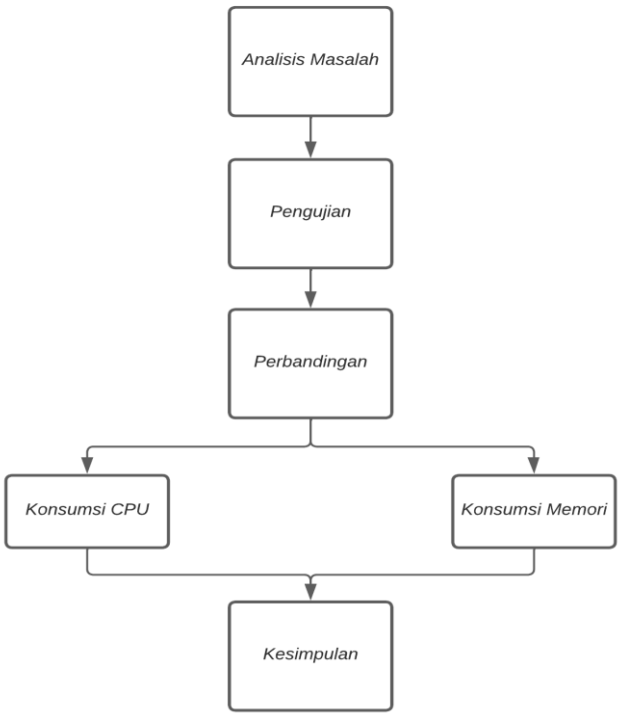
Hping3 adalah alat jaringan yang dapat mengirim paket ICMP/UDP/TCP khusus dan untuk menampilkan balasan target seperti yang dilakukan ping dengan balasan ICMP. Hping3 dapat digunakan untuk menguji protokol firewall, melakukan pemindaian port (palsu), menguji kinerja jaringan menggunakan protokol yang berbeda, melakukan penemuan jalur MTU, melakukan *traceroute* dengan protokol yang berbeda, serta mengaudit protokol TCP/IP. Perintah Hping3 ada di dalam *backtrack* R5 dan memiliki kemampuan untuk mengirim sejumlah besar paket protokol kontrol transmisi berbahaya (TCP) kepada target [13]. Dalam penelitian ini, hping3 akan digunakan untuk melancarkan serangan *Denial of Services* (DoS) berbasis SYN *flooding* pada sistem operasi RedHat Linux dan sistem operasi FreeBSD.

3. METODE

Metode penelitian mencakup semua teknik dan metode yang diambil untuk melakukan penelitian [6]. Metode penelitian yang digunakan bergantung pada jenis penelitian yang dilakukan. Secara umum, metode penelitian dapat dibagi menjadi dua, yaitu metode deskriptif dan metode analisis. Tujuan utama dari metode deskriptif yaitu peneliti tidak memiliki kontrol langsung atas variabel penelitian sehingga hanya bisa melaporkan apa yang sedang terjadi atau apa yang telah terjadi [6]. Hal ini berbeda dengan metode analisis yang mengharuskan peneliti menggunakan fakta atau informasi yang diperoleh atau sudah ada untuk menganalisis dan mengambil kesimpulan [6].

3.1 Tahapan Penelitian

Penelitian ini menggunakan metode perbandingan secara kuantitatif terhadap persentase konsumsi CPU pada dua sistem operasi setelah melakukan simulasi serangan DoS terhadap kedua sistem operasi tersebut. Adapun tahap metode penelitian yang dilakukan yaitu analisis masalah, pengujian, perbandingan, dan penarikan kesimpulan.



Gambar 1. Tahapan Penelitian

3.2. Analisis Masalah

Analisis masalah dilakukan untuk mengetahui permasalahan, kemudian mengolahnya untuk menentukan metode analisis dan menguji berbagai solusi untuk mengatasi masalah tersebut. Permasalahan yang sering terjadi pada CPU suatu komputer yaitu menurunnya performa komputer. Hal ini dipengaruhi oleh banyak faktor, antara lain *instruction set*, *clock speed*, *bandwidth*, kecepatan *Front Side Bus* (FSB), dan memori.

a. Instruction Set
Set instruksi adalah sekumpulan instruksi yang dapat dimengerti oleh sebuah CPU dengan sebuah kamus berisi daftar perintah apa saja yang dapat dilakukan oleh sebuah prosesor [4]. Set instruksi biasa dikenal dengan kumpulan kode dalam bahasa mesin.

b. Clock Speed
Clock speed merupakan suatu ukuran kecepatan saat CPU memproses banyak instruksi dalam satu waktu.

c. Bandwidth
Bandwidth merupakan suatu ukuran terhadap banyaknya data yang diproses oleh CPU dalam satu waktu.

d. Kecepatan *Front Side Bus* (FSB)
Kecepatan FSB mengindikasikan seberapa cepat CPU dapat berkomunikasi dengan memori.

e. Memori
Merupakan suatu tempat dalam komputer untuk menyimpan data secara terbatas, bergantung pada kapasitas yang telah ditentukan.

Penelitian ini berfokus pada permasalahan bandwith jaringan dan memori suatu komputer yang mengalami overload dan mengakibatkan permasalahan pada CPU. Hal ini dapat terjadi karena banyaknya paket TCP/UDP/ICMP yang diterima oleh komputer. Paket-paket yang terlalu banyak dikirim, akan membuat port pada suatu jaringan komputer penuh sehingga bandwith jaringan meningkat, clock speed dan FSB menurun, memori penuh, dan akhirnya menurunkan performa komputer. Dalam kasus ini, konsumsi CPU dan/atau memori dapat mencapai 100% sehingga membuat komputer menjadi hang.

3.3. Pengujian

CPU merupakan otak dari suatu komputer. Hal ini dikarenakan CPU memiliki fungsi utama untuk memproses data. Pada saat *runtime*, CPU beroperasi pada *slab* yang berbeda untuk menghindari permasalahan saat beroperasi [1]. Namun permasalahan pada CPU dapat timbul jika banyaknya konsumsi terhadap CPU yang mengakibatkan komputer menjadi *hang*. Pengujian dilakukan secara kualitatif dengan mengirimkan paket-paket TCP/UDP/ICMP dalam lama waktu dan jumlah tertentu. Pemberian paket-paket tersebut akan dilakukan dengan melakukan simulasi serangan DoS terhadap suatu komputer dengan menggunakan *tools* hping3. Hping3 digunakan untuk mengirimkan paket data yang dibuat secara khusus kepada target [2].

3.4. Perbandingan

Perbandingan akan dilakukan dengan membandingkan data konsumsi penggunaan CPU dan penggunaan penggunaan memori yang didapatkan pada proses pengujian sistem operasi RedHat Linux dan FreeBSD. Perbandingan tersebut bertujuan untuk menentukan sistem operasi yang memiliki performa CPU lebih baik.

3.5. Kesimpulan

Kesimpulan didapatkan setelah menganalisis perbandingan dari grafik performa CPU yang didapatkan pada proses pengujian sistem operasi RedHat Linux dan FreeBSD. Kesimpulan yang diambil berdasarkan data kualitatif yang digambarkan dalam bentuk grafik.

4. HASIL DAN PEMBAHASAN

Pada bab ini berisi hasil pengujian serangan *Denial of Service* (DoS) terhadap performa CPU dan memori pada sistem operasi RedHat Linux dan sistem operasi FreeBSD dengan menggunakan *tools* hping3. Kemudian hasil yang didapatkan akan dibahas secara mendalaman untuk menentukan sistem operasi dengan performa CPU dan memori yang lebih baik.

4.1 Identifikasi Kerentanan

Identifikasi kerentanan pada sistem operasi RedHat Linux dan FreeBSD dilakukan melalui kerentanan yang telah ditemukan melalui *Common Vulnerabilities Exposures* (CVE). CVE merupakan basis data yang menyimpan kerentanan-kerentanan terkini yang ditemukan dan berisi deskripsi teknis dari kerentanan tersebut yang dipublikasikan dalam laman resmi CVE [9].Berikut kerentanan pada sistem operasi FreeBSD yang telah ditemukan pada tabel 1:

Tabel 1. Tiga Kerentanan pada Sistem Operasi FreeBSD berdasarkan CVE 2022

CVE	Kerentanan	Protokol
CVE-2022-32264	*Error Handling*	TCP
CVE-2022-27674	*Insufficient Validation*	I/O
CVE-2022-23831	*Insufficient Validation*	I/O

Adapun penjelasan kerentanan yang disebutkan dalam CVE pada tabel 1 sebagai berikut:

a. CVE-2022-32264
   Kerentanan ini memungkinkan penyerang melakukan serangan DoS karena terjadi *error handling* terhadap TSopt pada koneksi TCP.
b. CVE-2022-27674
   Kerentanan ini disebabkan oleh validasi *input*/*output* yang tidak sesuai pada IOCTL AMD sehingga memungkinkan penyerang untuk mendapatkan akses langsung terhadap kernel dan melakukan serangan DoS.
c. CVE-2022-23831
   Kerentanan ini disebabkan oleh validasi *input*/*output* yang tidak sesuai pada IOCTL AMD sehingga memungkinkan penyerang untuk mengirimkan *arbitrary buffer* dan melakukan serangan DoS.

Tabel 2. Tiga Kerentanan pada Sistem Operasi Redhat Linux berdasarkan CVE 2022

CVE	Kerentanan	Protokol
CVE-2022-30599	*SQL Injection*	SQL
CVE-2022-32546	*Unsigned Long Int Data Type*	I/O
CVE-2022-32545	*Unsigned Char Data Type*	I/O

Adapun penjelasan kerentanan yang disebutkan dalam CVE pada tabel 2 sebagai berikut:

a. CVE-2022-30599
   Kerentanan ini memungkinkan penyerang melakukan *SQL Injection* terhadap basis data berbasis SQL yang ada pada sistem operasi RedHat Linux.
b. CVE-2022-32546
   Kerentanan ini menyebabkan *buffer overflow* terhadap tipe data *unsigned long* pada file coders/pcl.c pada sistem operasi RedHat Linux.
c. CVE-2022-32545
   Kerentanan ini menyebabkan *buffer overflow* terhadap tipe data *unsigned char* pada file coders/pcd.c pada sistem operasi RedHat Linux.

Dari kerentanan-kerentanan yang telah dijelaskan pada tabel 1 dan tabel 2, diperoleh informasi bahwa pada sistem operasi RedHat Linux tidak terdapat kerentanan pada protokol TCP, sedangkan pada sistem FreeBSD terdapat kerentanan pada protokol TCP. Pada penelitian ini, serangan DoS akan dilakukan terhadap kedua sistem tersebut dengan memanfaatkan protokol TCP untuk mengirimkan paket-paket dalam rentang waktu yang telah ditentukan pada tabel 3 dan tabel 4.

4.2 Pengumpulan Data

Pengumpulan data dilakukan pada tahap awal pengujian, yaitu dengan melakukan simulasi serangan DoS terhadap sistem operasi RedHat Linux dengan menggunakan *tools* hping3. Data percobaan yang akan diambil diukur dalam rentang waktu 60 detik hingga 420 detik.

Tabel 3. Data Performa Sistem Operasi RedHat Linux

Sistem Operasi	Waktu (detik)	Jumlah Paket TCP/ UDP/ICMP	Konsumsi CPU	Konsumsi Memori
RedHat Linux	60	5.365.504	14%	60%
	120	11.755.909	30%	66%
	180	16.190.879	48%	64%
	240	21.891.985	45%	62%
	300	26.977.099	52%	69%
	360	32.546.880	56%	72%
	420	38.908.900	61%	74%

Tabel 3 merupakan data hasil simulasi serangan DoS pada sistem operasi RedHat Linux. Serangan awal dilakukan dalam waktu satu menit. Kemudian serangan kedua, ketiga, keempat, dan serangan-serangan selanjutnya terdapat penambahan durasi sebanyak satu menit tiap serangan, sehingga total waktu serangan sebanyak tujuh menit. Sistem operasi dimatikan setiap setelah selesai simulasi pada serangan pertama, kedua, ketiga, dan serangan-serangan selanjutnya. Hal ini ditujukan untuk memperoleh kondisi sistem operasi yang identik tiap serangan, sehingga data hasil serangan yang didapatkan maksimal.

Data pada tabel 3 menunjukkan bahwa terjadi lonjakan yang cukup signifikan terhadap konsumsi CPU ketika serangan kedua dilakukan, yaitu terdapat kenaikan sebanyak 16% atau dua kali lipat lebih banyak konsumsi CPU daripada konsumsi CPU pada serangan pertama. Hal ini disebabkan karena paket data yang dikirimkan saat serangan pertama memiliki jumlah lebih dari dua kali lipat dari paket data yang dikirimkan pada serangan pertama.

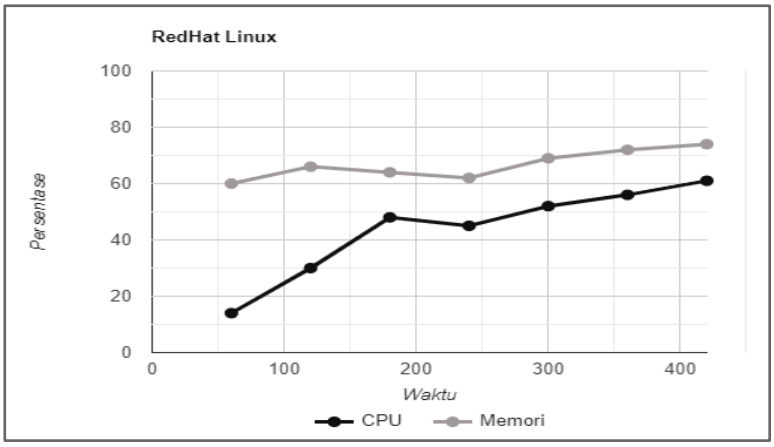
Tabel 4. Data Performa Sistem Operasi FreeBSD

Sistem Operasi	Waktu (detik)	Jumlah Paket TCP/ UDP/ICMP	Konsumsi CPU	Konsumsi Memori
FreeBSD	60	5.568.350	16%	32%
	120	11.214.964	23%	42%
	180	16.527.958	19%	57%
	240	21.944.224	36%	72%
	300	26.539.955	39%	83%
	360	32.943.644	42%	84%
	420	38.957.558	47%	84%

Tabel 4 merupakan data hasil simulasi serangan DoS pada sistem operasi FreeBSD, menunjukkan bahwa terjadi lonjakan yang cukup signifikan terhadap konsumsi memori ketika serangan keempat dilakukan, yaitu terdapat kenaikan sebanyak 15% konsumsi memori internal dari serangan ketiga. Lonjakan konsumsi memori internal yang terjadi juga mengakibatkan lonjakan yang cukup signifikan pada konsumsi CPU, yakni pada serangan keempat meningkat sebanyak 17% dari serangan ketiga.

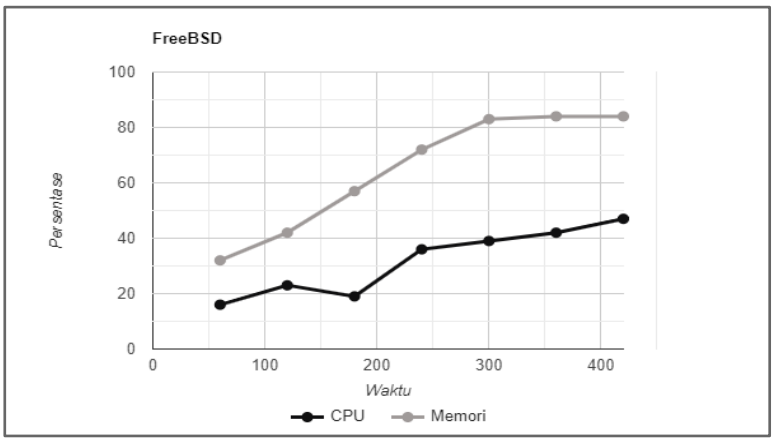
4.3 Analisis Data

Analisis data dilakukan untuk mengetahui hasil dari simulasi serangan DoS pada sistem operasi RedHat Linux dan sistem operasi FreeBSD. Hasil analisis data pengujian terhadap masing-masing sistem operasi yang telah didapatkan akan dibandingkan untuk memperoleh kesimpulan.



Gambar 2. Grafik Konsumsi CPU dan Memori Setelah Serangan Denial of Service (DoS)

Gambar 2 merupakan visualisasi berupa grafik dari data yang telah dikumpulkan pada tabel 3. Grafik pada gambar 2 memberikan gambaran mengenai peningkatan konsumsi memori internal dan konsumsi CPU pada sistem operasi RedHat Linux. Dari grafik tersebut, peningkatan tertinggi konsumsi CPU terjadi pada serangan kedua yang dilakukan dalam waktu dua menit.



Gambar 3. Grafik Konsumsi CPU dan Memori Setelah Serangan Denial of Service (DoS)

Gambar 3 merupakan visualisasi berupa grafik dari data yang telah dikumpulkan pada tabel 4. Grafik pada gambar 3 memberikan gambaran mengenai peningkatan konsumsi memori internal dan konsumsi CPU pada sistem operasi FreeBSD. Dari grafik tersebut, peningkatan tertinggi konsumsi CPU dan konsumsi memori internal terjadi pada serangan keempat yang dilakukan dalam waktu empat menit dan serangan ketiga yang dilakukan dalam waktu tiga menit.

Grafik pada gambar 2 dan gambar 3 menunjukkan adanya perbedaan terhadap konsumsi CPU pada sistem operasi RedHat Linux dan FreeBSD, yaitu adanya penurunan konsumsi CPU dan memori internal ketika serangan keempat dilakukan terhadap sistem operasi RedHat Linux, namun tidak ditemukan kejadian yang serupa pada sistem operasi FreeBSD.

5. KESIMPULAN

Berdasarkan percobaan yang telah dilakukan, terlihat bahwa dalam waktu yang sama dan jumlah paket yang relatif sama, terdapat perbedaan konsumsi penggunaan CPU dan memori internal dari kedua sistem operasi. Terdapat kenaikan penggunaan memori yang cukup signifikan pada sistem operasi FreeBSD setelah simulasi serangan DoS, sedangkan pada sistem operasi RedHat Linux tidak signifikan. Terdapat kenaikan penggunaan CPU yang cukup signifikan pada sistem operasi RedHat Linux setelah simulasi serangan DoS, sedangkan pada sistem operasi FreeBSD tidak signifikan. Sistem operasi FreeBSD mulai mengalami hang saat percobaan dilakukan pada lama waktu 240 detik atau lebih. Sistem operasi RedHat Linux mulai mengalami hang saat percobaan dilakukan pada lama waktu 300 detik atau lebih. Berdasarkan analisis yang telah dilakukan, dapat diambil kesimpulan bahwa sistem operasi FreeBSD memiliki performa CPU yang lebih baik dari sistem operasi RedHat Linux, namun memiliki kerentanan pada memori internal terhadap serangan DoS, sedangkan sistem operasi RedHat Linux memiliki performa memori internal yang lebih baik dari sistem operasi FreeBSD, namun memiliki kerentanan pada performa CPU terhadap serangan DoS. Selain itu, sebaiknya pengembang sistem operasi FreeBSD dan RedHat Linux menutup kerawanan-kerawanan yang telah dipublikasikan oleh CVE untuk meningkatkan performa dan keamanan sistem operasi.

REFERENSI

[1] Zeng, K., Chen, Y., Cho, H., Xing, X., Doupé, A., Shoshitaishvili, Y., & Bao, T., 2022. Understanding and Improving Linux Kernel Exploit Reliability. USENIX, p.2.

[2] Islam, MM., Shahid, S., Awar, KB., Khan, R., & Sohail, M., 2021. Cyber Security: Dos Attack Outcomes are Dangerous. European Journal of Electrical Engineering and Computer Science, p.2.

[3] Malallah, HF., Zeebaree, SRM., Zebari, RR., Sadeeq, MAM., Ageed, ZS., Ibrahim, IM., Yasin, HM., & Merceedi, KJ., 2021. A Comprehensive Study of Kernel (Issues and Concepts) in Different Operating Systems. Asian Journal of Computer Science and Information Technology, p.2.

[4] Widharma, IGS., 2020. Instruction Set dalam Ilmu Komputer.https://www.researchgate.net/publication/346510287, p.10.

[5] Cetinkaya, A., Ishii, Hideaki., & Hayakawa, T., 2019. An Overview on Denial of Service Attacks in Control Systems: Attack Models and Security Analyses. Multidisciplinary Digital Publishing Institute, p.1-2.

[6] Mishra, SB. & Alok, S., 2017. Handbook of Research Methodology. https://www.researchgate.net/publication/319207471, p.1-3.

[7] Stiawan, D., Idris, MY., & Abdullah, AH., 2015. Penetration Testing and Network Auditing: Linux. Journal of Information Processing System, p.1.

[8] Chen, Y & Zhu, A., 2014. The Design and Implementation of Firewall Based on FreeBSD. Institute of Electrical and Electronic Engineering, p.1.

[9] Stiawan, D., Idris, MY., & Abdullah, AH., 2013. Attack and Vulnerability Penetration Testing: FreeBSD. Telkomnika, p.8.

[10] Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. 2008. Technical Guide to Information Security Testing and Assessment. National Institute of Standards and Technology, p.5.

[11] Sow, D., Bulut, MF., Adam, C., Bedell, C., Ocepek, S., Ngweta, L. 2017. Attack Techniques and Threat Identification for Vulnerabilities. Association for Computing Machinery, p.2.
[12] Elleithy, KM., Blagovic, D., Cheng, WK., Sideleau, P. 2005. Denial of Services Attack Techniques: Analysis, Implementation and Comparison. Journal of Systemics, Cybernetics, and Informatics, p.1.
[13] Zeebaree, SRM., Jacksi, K., Zebari, RR. 2020. Impact Analysis of SYN Flood DDoS Attack on HAProxy and NLB Cluster-Based Web Servers. Indonesian Journal of Electrical Engineering and Computer Science, p.3.
[14] Liang, X., Znati., T. 2019. An Empirical Study of Intelligent Approaches to DDoS Detection in Large Scale Networks. International Conference on Computing, Networking, and Communications (ICNC): Network Algorithms and Performance Evaluation, p1.
[15] Matsubara, K., Takagawa, Y. 2020. Adaptive OS Switching for Improving Availability During Web Traffic Surges: A Feasibility Study. IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), p.1.
[16] Kaluarachchilage, PKH., Attanayake, C., Rajasooriya, S., Tsokos, CP. 2020. An Analytical Approach to Assess and Compare the Vulnerability Risk of Operating Systems. Moderns Education and Computer Science (MECS), p.3.
[17] Venter, HS., Eloff, HP. 2004. Vulnerability Forecasting – a Conseptual Model. Computers & Security, 23, p.489-497.
[18] Ruohone, J., Hyrynsalmi, S., Leppanen, V. 2015. The Sigmoidal Growth of Operating System Security Vulnerabilities: an Empirical Revisit. Computers & Security, 55, p.1-20.
[19] Johnson, P., Gorton, D., Lagerström, R., Ekstedt, M. 2016. Time Beetwen Vulnerability Disclosures: a Measure of Software Product Vulnerability. Computers & Security, 62, p.278-295.