Analisis Hasil DoS SYN Flood Attack Pada Web Server

[1]Fransesko Indrajid 1,[2]Kadek Ferdy Andika, [3]Gusti Kade Surya Aditya Putra, [4]Kadek Karisma Bramanda, [5]Gede Arna Jude Saskara, [6]I Made Edy Listartha

Teknik dan Kejuruan, Universitas Pendidikan Ganesha[1,2,3,4,5,6]

Jl Udayana No. 11, Singaraja, Kec. Buleleng, Kab. Buleleng, Bali[1,2,3,4,5,6]

fransesko@undiksha.ac.id[1], ferdy.andika@undiksha.ac.id[2], kade.surya.aditya@undiksha.ac.id[3], karisma.bramanda@undiksha.ac.id[4], jude.saskara@undiksha.ac.id[5], listartha@undiksha.ac.id[6]

Abstract - The development of technology and information certainly has many good impacts on human life, but behind all this it turns out that this also has a bad impact. The ease of accessing information, besides making us quickly know all things that are good and useful, turns out to be just as fast as making someone aware of things that are not good that can disrupt people's welfare, for example regarding information on how to exploit security holes in using the internet. With the amount of information that has been spread regarding the use of security holes on the internet, now someone can easily learn so that he can launch an attack on the internet that can harm other people. One of the attacks that is currently easy to learn and use is the DoS (Denial of Service) Attack, due to the large amount of information that has been spread about how to use out this attack coupled with computers that are now increasingly sophisticated and the many tools that can be obtained easily and for free, so it is not surprising that we often see many attempts of this attack on the internet. Therefore, for educational purposes, a DoS attack simulation will be carried out in this study to find out how dangerous the impact of this attack is.

Keyword:DoS Attack, DoS SYN Flood, Metasploit, Hping3, Slowloris, Web Server

Abstrak – Perkembangan teknologi dan informasi tentunya membawa banyak dampak yang baik bagi kehidupan manusia tetapi dibelakang itu semua ternyata hal ini juga membawa dampak yang buruk. Kemudahan dalam mengakses informasi, selain membuat kita cepat tahu akan segala seuatu hal yang baik dan berguna ternyata sama cepatnya dengan membuat seseorang mengetahui hal-hal yang tidak baik yang dapat membuat kesejahteraan masyarakat terganggu, contohnya mengenai informasi cara mengekspoitasi celah keamanan dalam menggunakan internet. Dengan banyaknya informasi yang telah tersebar mengenai pemanfaatan celah keamanan di internet, maka sekarang seseorang dapat dengan mudah mepelajari hingga ia dapat melancarkan suatu serangan di internet yang bisa merugikan orang lain. Salah satu serangan yang saat ini dapat dengan mudah dipelajari dan digunakan ialah DoS (Denial of Service) Attack, dikarenakan banyaknya informasi yang telah tersebar mengenai cara melakukan serangan ini ditambah dengan komputer yang kini semakin canggih serta banyaknya tools yang bisa didapatkan dengan mudah dan gratis, maka tidak mengherankan jika kita sering melihat banyaknya percobaan serangan ini di internet. Oleh karena itu demi tujuan edukasi maka akan dilakukan simulasi serangan DoS pada penelitian ini untuk mengetahui seberapa berbahaya dampak dari serangan ini.

Keyword: DoS Attack, DoS SYN Flood, Metasploit, Hping3, Slowloris, Web Server

I. PENDAHULUAN

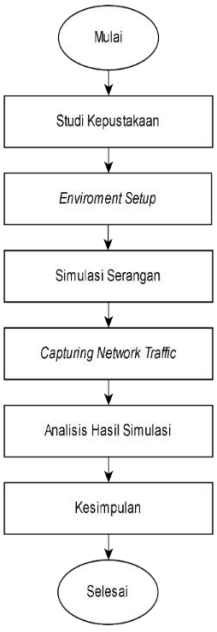
Terus meningkatnya kecepatan internet dari waktu kewaktu selalu diikuti meningkatnya pula serangan cybercriminals dari tahun ketahun[1]. Alasan mengapa hal ini dapat terjadi karena dengan banyaknya informasi yang mudah didapatkan sekarang ini maka sangat memungkinkan untuk mempelajari atau mengetahui tentang segala macam hal tak terkecuali segala sesuatu yang berhubungan dengan keamanan informasi dan jaringan, dengan semakin terbukanya hal ini maka mungkin saja akan semakin banyak orang yang akan mendapatkan pengetahuan mengenai *hacking* atau pun *cracking*[2]. Oleh karena itu, keamanan informasi dan jaringan saat ini sangat penting untuk dilakukan, alasannya tidak lain dan tidak bukan karena pada era ini penyimpanan informasi tidak lagi menggunakan media konvensional seperti kertas, akan tetapi telah menggunakan teknologi komputer yang maju yang dipadukan dengan kecanggihan dari internet[3]. Ada banyak serangan yang dapat dilakukan oleh orang-orang yang tidak bertanggung jawab ini, salah satu contohnya ialah *DoS (Denial of Service) attack*, serangan *DoS* ialah serangan yang umumnya dilakukan dengan cara membanjiri *server* atau *host* sehingga *host* korban kehabisan sumber daya (memori, CPU, lalu lintas) keadaan ini kan tetap dilanjutkan sehingga membuat *host* atau *server* yang diserang tidak dapat melakukan pelayanan kepada pengguna lain[1]. Sederhananya serangan ini adalah serangan yang mampu melumpuhkan server korban karena tingginya lalu lintas jaringan yang membanjiri server korban untuk melayani *host*/penyerang. Dengan tingginya trafik yang dikirimkan maka ukuran bandwidth akan melebihi kapasitas pelayanan server korban lalu menurunkan kinerja dari

layanan server korban, inilah kondisi yang biasa disebut dengan *server down* yang mengakibatkan *server* tidak dapat di akses lagi secara online oleh pengguna yang lain[4]. Dapat dipungkiri jika banyak aksi serangan *DoS* yang terjadi, karena pada dasarnya internet merupakan jaringan yang sifatnya publik yang berarti semua orang dapat menggunakan jaringan ini dengan bebas, mengenai keamanan dan kenyamanan dalam jaringan tidak ada yang dapat menjamin hal tersebut kecuali orang itu sendiri.

Meskipun serangan *DoS* ini merupakan serangan yang cukup sederhana ternyata dampak yang dihasilkan serta penaggulangannya tidak dapat disepelekan. Dalam beberapa bidang serangan yang hanya bertujuan untuk memperlambat suatu *server* mungkin adalah hal yang biasa dan tidak terlalu mempengaruhi organisasi/bisnis tersebut, tetapi berbeda dengan dengan bidang-bidang yang mengedepankan pelayanan dan kepuasan pelanggan dengan menggunakan *server* yang mereka punya, tentu serangan seperti *DoS* ini adalah hal yang sangat fatal bagi sebuah bisnis/organisasi tersebut. Ada banyak varian dari serangan *DoS,* tidak kurang dari 35 macam serangan yang dapat dilakukan yang semuanya bertujuan sama yaitu menimbulkan penolkan layanan karena *server/host* yang diserang telah kehabisan sumberdaya untuk menerima permintaan[1], salah satu jenis serangan *DoS* yang sering digunakan ialah *DoS SYN Flood attack.* Pada dasarnya ketika sebuah komputer yang terhubung ke pada suatu jaringan *server* maka akan terjadi yang disebut dengan koneksi TCP ke *server*, dimana client akan mengirim SYNchronize ke server dan server akan mengenali acknowledge (ACK) request ini dengan mengirim balik SYN-ACK ke client dan client mengirim ACK untuk meresponnya sehingga koneksi akan terbentuk hal ini juga dikenal dengan sebutan *TCP Three Way Handshake*[5]. Serangan *DoS SYN Flood* sendiri mempengaruhi host yang menjalankan proses server TCP/IP yaitu dengan membanjiri server dengan request palsu secara bertubi-tubi akan tetapi paket *ACK* yang harusnya dikirim oleh *client* pada akhir sesi tidak akan dirimkan kembali, sehingga membuat pembentukan koneksi antar *client* dan *server* tetap terbuka sementara *request* baru akan dirimkan secara terus-menerus dengan model yang sama[5]. Akibatnya karena banyaknya pembentukan koneksi masih terbuka ditambah dengan bertambahnya jumlah *request* yang semakin banyak maka *server* kemudian akan sangat sibuk dan tidak akan menerima permintaan lagi atau disebut dengan kondisi *server down*. Dalam penelitian kali ini akan silakukan simulasi dari serangan ini untuk mengetahui bagaimana serangan ini benar-benar bekerja dan seberapa berbahaya serangan ini pada sebuah *web server*.

II. METODE

Metode penetlitian yang digunakan dalam evaluasi serangan *DoS* pada *web server* ini adalah studi kepustakaan *(library study)* dan penelitian eksperimental *(experimental research)*. Adapun tahapan proses penelitian secara sistematis dapat silihat pada **gambar 1** berikut.



Gambar 1 Tahapan Penelitian

Berdasarkan tahapan penelitian yang ada pada **gambar 1**, dapat diuarikan sebagai berikut :

1. Studi kepustakaan, yaitu mengumpulkan berbagai informasi khususnya dari penelitan terdahulu yang berhubungan dengan serangan *Denial of Service* dari artikel-artikel yang bersumber dari berbagai jurnal.
2. *Enviroment Setup,* dalam tahapan ini akan dilakukan persiapan untuk melakukan simulasi. Persiapan yang akan dilakukan yaitu

a. Perangkat simulasi yang digunakan menggunakan sistem operasi *Kali Linux* 64 bit dengan 8 GB RAM, serta 8 core *processor*,
b. Perangkat *web server* target yang diserang dengan sistem operasi *Debian* 32 bit yang menjalankan website dvwa.

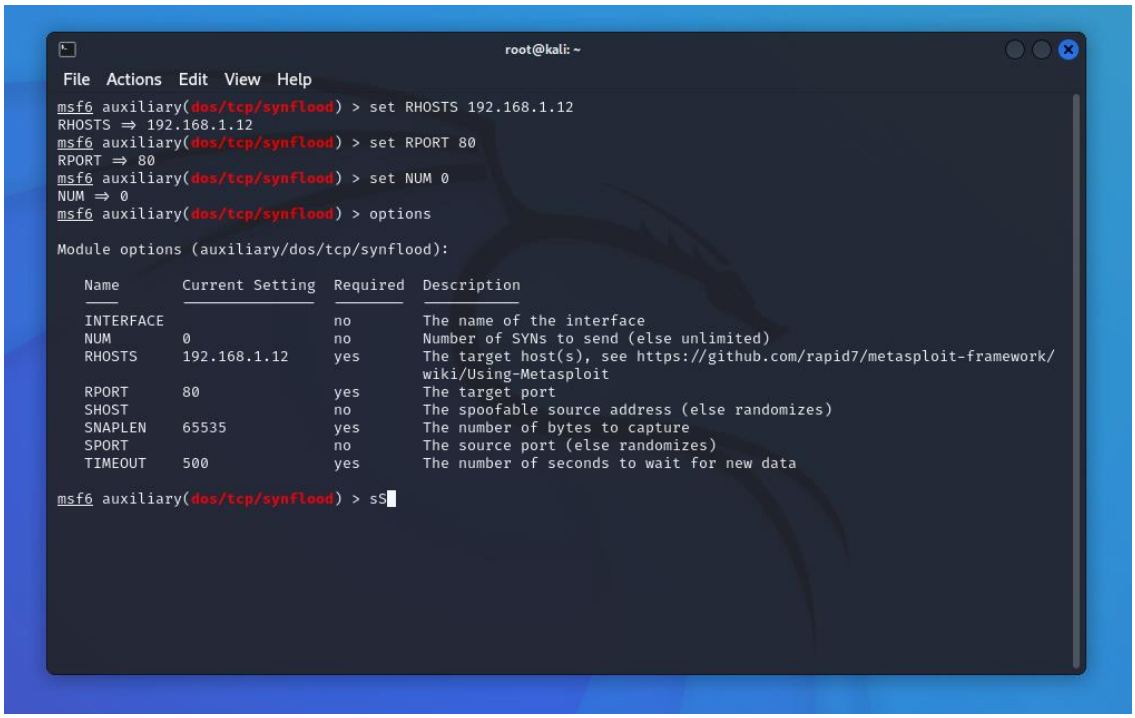
3. Simulasi serangan yaitu melakukan simulasi serangan *DoS* menggunakan *tools* yang telah ditentukan.
4. *Capturing Network Traffic* yaitu melakukan rekaman lalu lintas jaringan yang terjadi pada suatu waktu menggunakan aplikasi *Wireshark*
5. Analisis hasil simulasi, dengan menggunakan data hasil yang didapatkan dari langkah-langkah sebelumnya maka akan dibandingkan hasil dari tiap-tiap *tools* tersebut dengan pembanding yaitu kecepatan dan kuantitas.
6. Kesimpulan, yaitu hasil dari perbadingan *tools* akan disimpulkan sehingga dapat diketahui *tools* yang terbaikdalam melakukan serangan *DoS*.

III. HASIL DAN PEMBAHASAN

Serangan *DoS (Denial of Service)* biasanya dilakukan oleh sekelompok penyerang dengan tujuan untuk melumpuhkan *server* korban[4]. Penyerang akan membanjiri *server* tersebut sehingga sumber daya dari *server* yang diserang akan habis digunakan untuk melayani permintaan penyerang dan tak ada lagi kemampuan untuk melayani pengguna lain atau disebut dengan *server down*. Untuk mengetahui bagaimana serangan *DoS* dapat bekerja maka akan dilakukan simulasi pada sistem operasi *Kali Linux* menggunakan 3 *tools* yaitu *metasploit, Hping3,* dan *slowloris.*

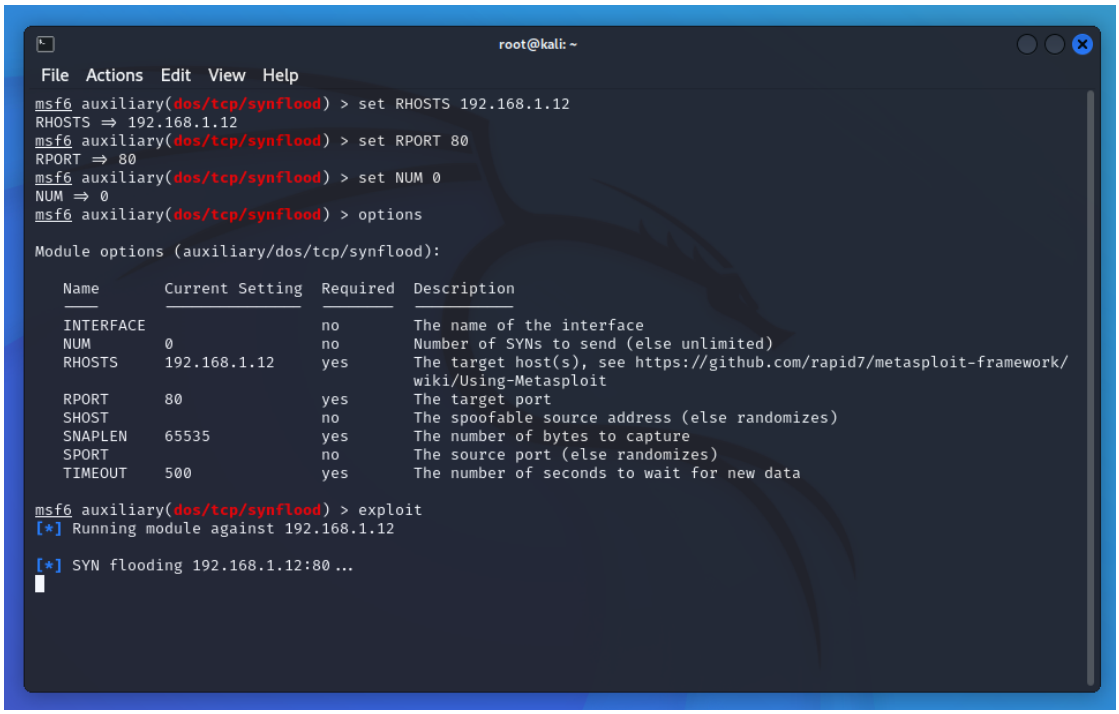
A. Metasploit

Melakukan simulasi serangan *DoS* menggunakan *tool metasploit* pada sebuah web server, **gambar 2** merupakan konfigurasi penggunaan *tools metasploit* dengan mengatur alamat ip yang diserang yaitu 192.168.1.12, port yang diserang yaitu 80, dan menetapkan jumlah paket yang dikirim yaitu sebanyak mungkin dengan memasukkan perintah set NUM 0.



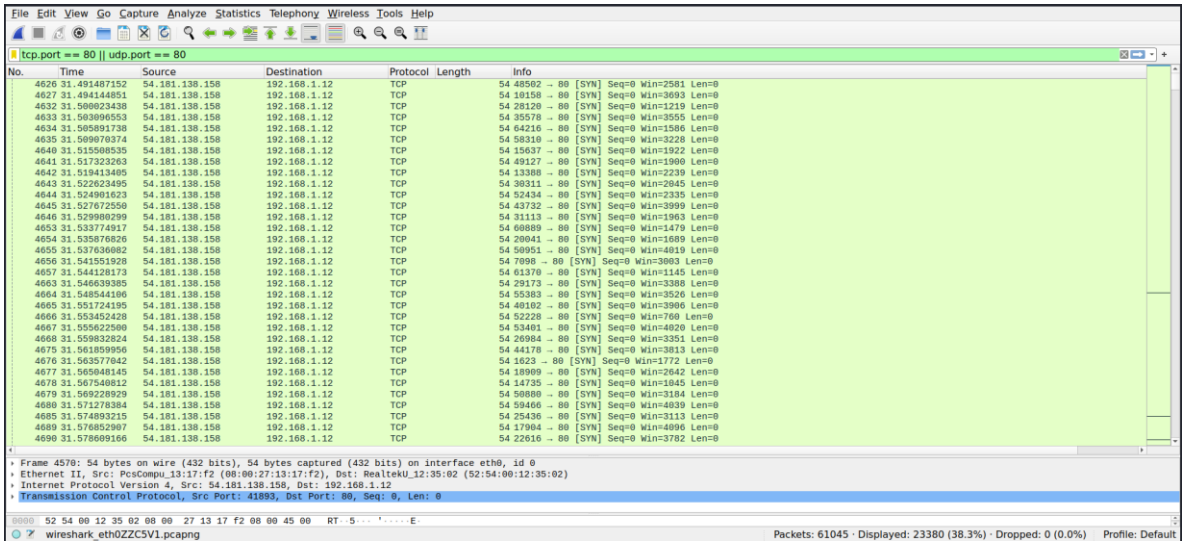
Gambar 2 Konfigurasi Tool *Metasploit*

Setelah melakukan konfigurasi pada *tool metasploit* selanjutnya dapat dimasukkan perintah *exploit* untuk menjalankan serangan, **gambar 3** merupakan tampilan *tool metasploit* saat melakukan serangan *DoS.*



Gambar 3 Tampilan Tool *Metasploit*

Setelah memasukkan perintah untuk melakukan serangan kita dapat melihat paket yang dikirimkan oleh *tool metasploit* dengan menggunakan aplikasi penganalisa jaringan, dalam penelitian kali ini aplikasi yang digunakan ialah *Wireshark.* **gambar 3** memperlihatkan tampilan aplikasi *wireshark* ketika merekam paket yang lewat dalam jaringan ketika *tool metasploit* melakukan serangan.



Gambar 3 Tampilan Wireshark Tool *Metasploit*

Pada **tabel 1** terlihat hasil dari 10 kali percobaan untuk mengetahui berapa jumlah paket yang dikirim oleh *tool metasploit* sesaat setelah *tool* ini dijalankan untuk melakukan simulasi.

Tabel 1 Jumlah Paket Awal Tool *Metasploit*

Percobaan 1	Percobaan 2	Percobaan 3	Percobaan 4	Percobaan 5
1215 paket	1142 paket	783 paket	1069 paket	1107 paket

Percobaan 6	Percobaan 7	Percobaan 8	Percobaan 9	Percobaan 10
1260 paket	766 paket	1239 paket	1014 paket	854 paket

Untuk mendapatkan hasil yang valid mengenai jumlah paket yang dikirimkan dalam rentang waktu tertentu, tim peneliti melakukan 10 kali percobaan simulasi dalamwaktu 1 menit dengan hasil pada **tabel 2** sebagai berikut.

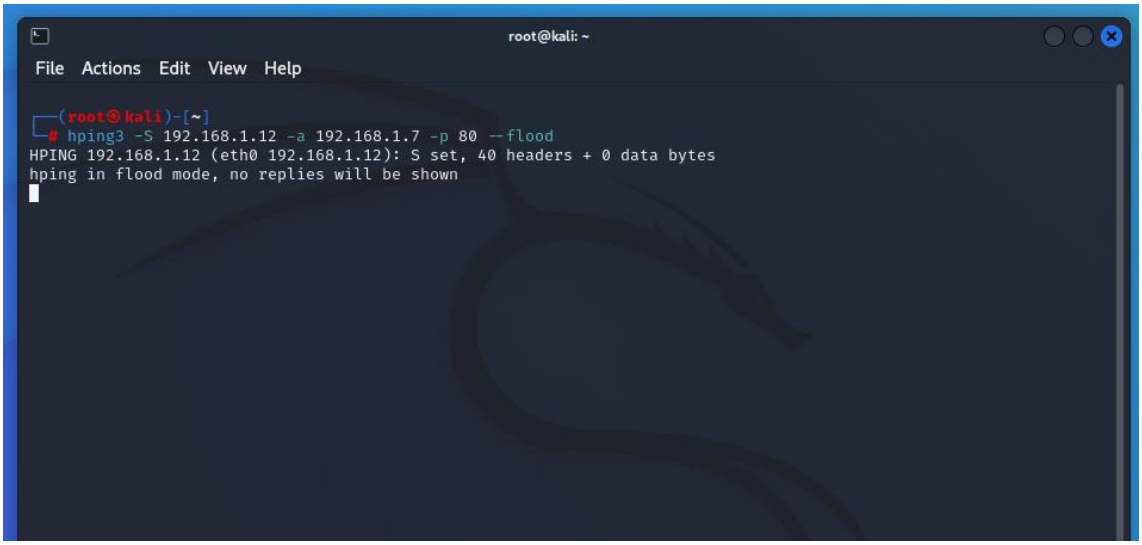
Tabel 2 Hasil Simulasi Tool *Metasploit*

Percobaan 1	Percobaan 2	Percobaan 3	Percobaan 4	Percobaan 5
38771 paket	37569 paket	37372 paket	36115 paket	35368 paket

Percobaan 6	Percobaan 7	Percobaan 8	Percobaan 9	Percobaan 10
34825 paket	34235 paket	36317 paket	35179 paket	37175 paket

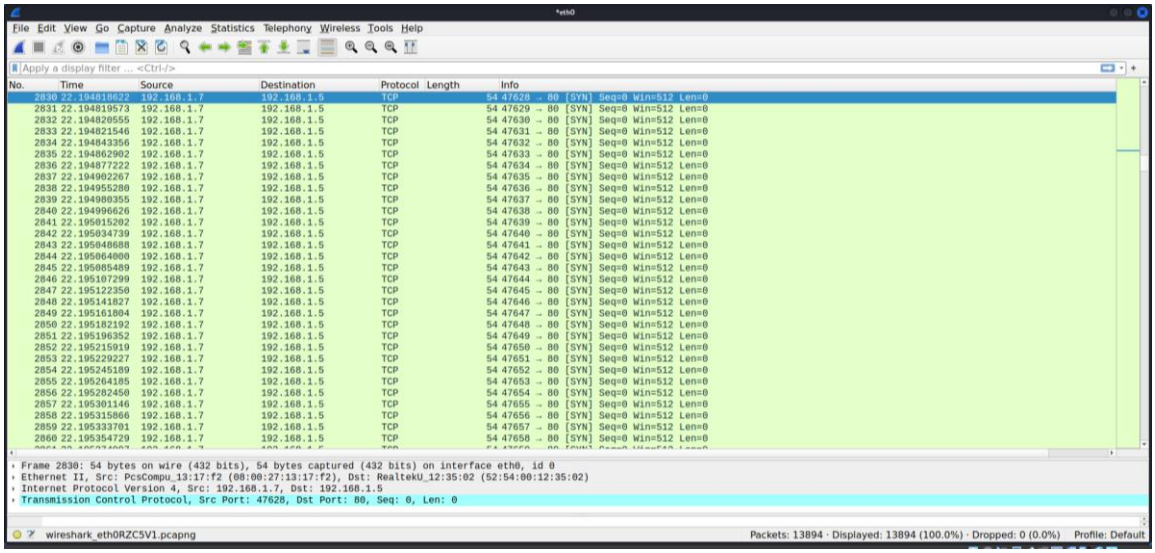
B. *Hping3*

Melakukan simulasi serangan *DoS* menggunakan *tools Hping3* dengan alamat ip target 192.168.1.12, alamat samaran penyerang 192.168.1.7, dan port target 80 dengan jumlah paket sebanyak mungkin, dapat dimasukkan perintah kedalam terminal *Kali Linux* mode *root permision* sebagai berikut *hping3 -S* 192.168.1.12 *-a 192.168.1.7 -p 80 –flood.* **Gambar 5** memperlihatkan tampilan *tool Hping3* ketika dijalankan untuk melakukan serangan *DoS.*



Gambar 5 Tampilan Tool *Hping3*

Pada **gambar 6** terlihat tampilan hasil rekaman yang didaptkan dari aplikasi *Wireshark* untuk melihat paket yang dikirimkan oleh alamat ip samaran penyerang yaitu 192.168.1.7 kepada alamat ip yang diserang yaitu 192.168.1.12.



Gambar 6 Hasil Wireshark Tool *Hping3*

Tabel 3 berikut adalah hasil dari 10 kali percobaan simulasi serangan untuk mengetahui jumlah paket yang dikirim oleh *tool Hping3* seketika menjalankan serangan.

Tabel 3 Jumlah Paket Awal Tool *Hping3*

Percobaan 1	Percobaan 2	Percobaan 3	Percobaan 4	Percobaan 5
11395 paket	17654 paket	12012 paket	7461 paket	23840 paket

Percobaan 6	Percobaan 7	Percobaan 8	Percobaan 9	Percobaan 10
13831 paket	18381 paket	16561 paket	21840 paket	22020 paket

Dalam **tabel 4** dapat dilihat hasil simulasi serangan *DoS* yang dilakukan menggunakan *tool Hping3* sebanyak 10 kali dengan waktu 1 menit.

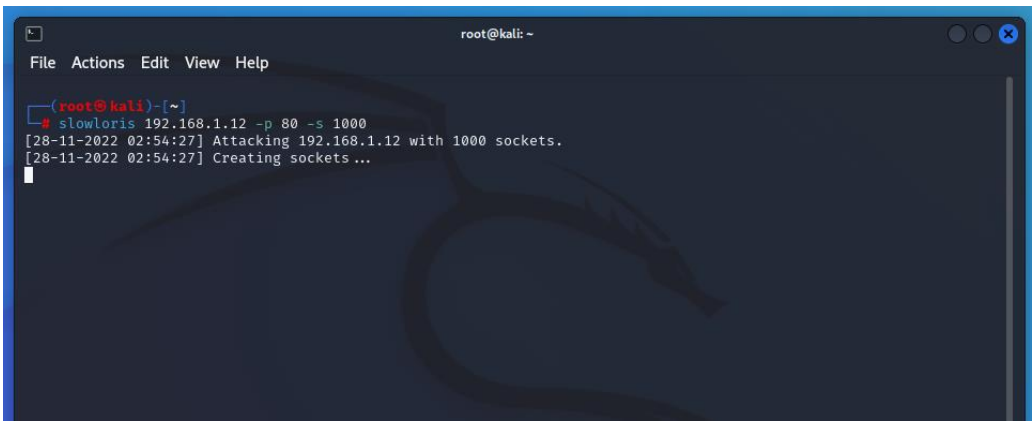
Tabel 4 Hasil Simulasi Tool *Hping3*

Percobaan 1	Percobaan 2	Percobaan 3	Percobaan 4	Percobaan 5
138451 paket	150692 paket	140683 paket	160617 paket	160869 paket

Percobaan 6	Percobaan 7	Percobaan 8	Percobaan 9	Percobaan 10
130397 paket	150327 paket	145194 paket	131035 paket	161406 paket

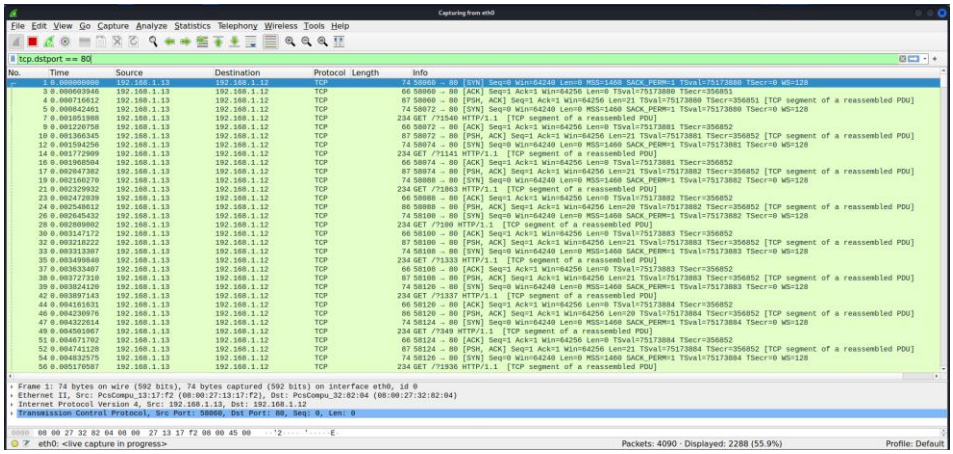
C. *Slowloris*

Untuk melakukan simulasi serangan *DoS* menggunakan *tool slowloris* dapat dilakukan melalui terminal dengan mode *root permission* yang tersedia pada *Kali Linux* dengan memasukkan perintah *slowloris* kemudian diikuti oleh alamat IP target yaitu 192.168.1.12, lalu dilanjutkan dengan perintah *-p* diikuti nomor *port* yang ingin diserang yaitu 80, dan terakhir dilanjutkan dengan *-s* diikuti jumlah *socket* yang ingin dikirimkan pada setiap paket, misalnya 1000. **Gambar 7** akan menujukkan tampilan terminal *Kali Linux* ketika *tool Slowloris* dijalankan.



Gambar 7 Tampilan Tool *Slowloris*

Melalui **Gambar 8** dapat terlihat informasi bahwa *tool slowloris* telah berhasil mengirimkan paket dengan 1000 *socket* ke alamat IP yang diserang yaitu 192.168.1.12, untuk melihat bagaimana lalu lintas pada jaringan ketika serangan berjalan maka dapat dilihat pada aplikasi *Wireshark* sebagai berikut.



Gambar 8 Tampilan Wireshark Tool *Slowloris*

Pada **tabel 5** terlihat hasil dari 10 kali percobaan untuk mengetahui berapa jumlah paket yang dikirim oleh *tool Slowlorist* sesaat setelah *tool* ini dijalankan untuk melakukan simulasi.

Tabel 5 Jumlah Paket Awal Tool *Slowloris*

Percobaan 1	Percobaan 2	Percobaan 3	Percobaan 4	Percobaan 5
442 paket	472 paket	449 paket	609 paket	947 paket

Percobaan 6	Percobaan 7	Percobaan 8	Percobaan 9	Percobaan 10
934 paket	578 paket	1023 paket	1042 paket	935 paket

Berikut adalah hasil dari 10 kali simulasi serangan *DoS* mengenai jumlah paket yang dikirimkan oleh *Tool Slowloris* pada alamat IP target selama 1 menit.

Tabel 6 Hasil Simulasi Tool *Slowloris*

Percobaan 1	Percobaan 2	Percobaan 3	Percobaan 4	Percobaan 5
3433 paket	3394 paket	3314 paket	3348 paket	3460 paket

Percobaan 6	Percobaan 7	Percobaan 8	Percobaan 9	Percobaan 10
3401 paket	3237 paket	3288 paket	3399 paket	3295 paket

D. Perbandingan Hasil Simulasi

Suatu alat/*tools* dikatakan berhasil ketika tujuan yang diinginkan dari pengguna tersebut dapat tercapai dengan bantuan *tools* tersebut, hal tersebut juga berlaku sama dengan *tools* yang digunakan untuk melakukan serangan *DoS.* Melalui simulasi yang telah dilakukan ketiga *tools* dapat dikatakan berhasil karena ketiga *tools* yang digunakan telah berhasil melancarkan serangan *DoS* ke target yang telah ditentukan, akan tetapi dikarenakan adanya perbedaan hasil dalam proses simulasi yang dilakukan, maka perbandingan yang dapat dilakukan terbagi menjadi dua yaitu :

1. Kecepatan
   Kecepatan yang dimaksud dalam perbandingan ini adalah seberapa cepat suatu *tools* membuat suatu *web server* menjadi *down*, untuk membandingkan hal ini maka hasil data simulasi yang akan dibandingkan ialah rerata hasil 10 kali percobaan simulasi jumlah paket yang dikirimkan suatu *tools* seketika digunakan untuk menjalankan serangan *DoS*, dalam **tabel 7** dapat dilihat hasil rerata dari 3 *tools* yang digunakan dalam simulasi.

Tabel 7 Rerata Kecepatan Tools

Metasploit	*Hping3*	*Slowloris*
1044,9 paket	16499,5 paket	743,1 paket

2. Kuantitas
   Perbandingan kuantitas yang dimaksud ialah seberapa banyak paket yang dikirimkan oleh suatu *tools* dalam suatu periode waktu, untuk membandingkan hal ini maka hasil data simulasi yang akan dibandingkan ialah rerata hasil 10 kali percobaan simulasi jumlah paket yang dikirimkan oleh suati *tools* selama 1 menit, dalam **tabel 8** dapat dilihat hasil rerata dari 3 *tools* yang digunakan dalam simulasi.

Tabel 8 Rerata Kuantitas Tools

Metasploit	*Hping3*	*Slowloris*
36292,6 paket	146967,1 paket	3356,9 paket

IV. KESIMPULAN

Berdasarkan hasil dan pembahasan simulasi serangan *DoS* ynag telah dilakukan menggunakan *Metasploit, Hping3,* dan *Slowloris* maka dapat disimpulkan beberapa hal sebagai berikut :

- Ketiga *tools* yang digunakan yaitu *Metasploit, Hping3,* dan *Slowloris* telah berhasil melakukan serangan *DoS* ke IP target yang telah ditentukan dengan bukti melambatnya server target (*down)* dan adanya paket yang dikirimkan dengan junlah yang besar.
- Dalam hal kecepatan untuk melumpuhkan *web server* target dapat disimpulkan bahwa *tools* terbaik yaitu *Hping3,* kemudian *Metasploit*, dan yang terakhir yaitu *Slowloris.*
- Dalam hal kuantitas untuk membuat *web server* target tetap dalam kondisi *down* maka dapat disimpulkan bahwa *tools* terbaik yaitu *Hping3,* kemudian *Metasploit*, dan yang terakhir yaitu *Slowloris.*
- Melalui perbandingan yang telah dilakukan dapat disimpulkan bahwa *tools* terbaik yang digunakan dalam melakukan serangan *DoS* ialah *Hping3* karena lebih baik dari *tools* lainnya dalam hal kecepatan dan kuantitas.
- Serangan *DoS (Denial of Service)* ini merupakan serangan yang berbahaya yang dapat merugikan orang lain untuk itu apapun alasannya serangan *DoS* ini tidak boleh dilakukan untuk merugikan orang lain atau mengganggu kenyamanan orang lain dalam menggunakan internet.

REFERENSI

[1] M. Arman, "Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 7, no. 1, pp. 56–70, Apr. 2020, doi: 10.35957/JATISI.V7I1.284.

[2] - Syaifuddin, - Syaifuddin, D. Risqiwati, and E. A. Irawan, "Realtime Pencegahan Serangan Brute Force dan DDOS Pada Ubuntu Server," *Techno.Com*, vol. 17, no. 4, pp. 347–354, Nov. 2018, doi: 10.33633/tc.v17i4.1766.

[3] S. Dwiyatno, A. P. Sari, A. Irawan, and S. Safig, "PENDETEKSI SERANGAN DDoS (DISTRIBUTED DENIAL OF SERVICE) MENGGUNAKAN HONEYPOT DI PT. TORINI JAYA ABADI," *Jurnal Sistem Informasi dan Informatika (Simika)*, vol. 2, no. 2, pp. 64–80, Aug. 2019, doi: 10.47080/SIMIKA.V2I2.606.

[4] D. Kurnia, "Analisis Pertahanan Website pada Protokol TCP dan UDP dari Serangan DDoS," *Jurnal Ilmiah Core IT : Community Research Information Technology*, vol. 7, no. 1, Apr. 2019, Accessed: Nov. 24, 2022. [Online]. Available: http://ijcoreit.org/index.php/coreit/article/view/101

[5] S. Komputer and S. Tinggi Manajemen Informatika dan Komputer Royal, "IMPLEMENTASI TEKNOLOGI FIREWALL SEBAGAI KEAMANAN SERVER DARI SYN FLOOD ATTACK," *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)*, vol. 7, no. 2, pp. 159–164, Apr. 2021, doi: 10.33330/JURTEKSI.V7I2.933.