ANALISIS KELAYAKAN TOOLS DENGAN METODE PENYERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) MENGGUNAKAN FL00D3R, DDOS-RIPPER, DAN RAVEN-STORM

Ida Ayu Mas Putri Mahalini, Ida Bagus Kusuma Dewantara, Ni Putu Diah Ratih Rakasiwi, Ngurah Manik Mahardika, I Made Edy Listartha, Gede Arna Jude Saskara.

Program Studi Sistem Informasi, Universitas Pendidikan Ganesha
Jl. Udayana No.11, Singaraja, Bali
ayu.mas.putri.3@undiksha.ac.id, bagus.kusuma@undiksha.ac.id,
diah.ratih@undiksha.ac.id, manik.mahardika@undiksha.ac.id

Abstract - The website is a tool that is widely used by the public, such as for entertainment, work, dissemination of information and much more. With so many people using the website, web developers are competing to attract a lot of user attention and override the security of the website. There are many attack methods that can be carried out by a hacker, one of which is the DDoS or Distributed Denial of Service method. This method is commonly used by utilizing many devices to attack traffic with a very large number of packets so that the is down. In this test, there are three tools that will be tested in DDoS attacks, namely fl00d3r, DDoS-Ripper, and Raven-Storm. It is hoped that this research can be used by web developers regarding the impact of DDoS-Attack results with these three tools.
Keywords - *DDoS-Attack*, *fl00d3r*, *DDoS-Ripper*, *Raven-Storm*, *Cybersecurity*.

Abstrak - Website merupakan sarana yang banyak digunakan oleh masyarakat, seperti untuk hiburan, pekerjaan, penyebaran informasi dan masih banyak lagi. Dengan banyaknya masyarakat yang menggunakan website membuat para web developer berlomba-lomba menarik banyak perhatian pengguna dan mengesampingkan keamanan dari website tersebut. Banyak sekali metode penyerangan yang bisa dilakukan oleh seorang peretas salah satunya yakni dengan metode DDoS atau Distributed Denial of Service. Metode ini biasa digunakan dengan memanfaatkan banyaknya perangkat untuk menyerang traffic dengan jumlah paket yang sangat banyak sehingga tersebut down. Dalam pengujian ini terdapat tiga tools yang akan diuji coba dalam penyerangan DDoS yaitu fl00d3r, DDoS-Ripper, dan Raven-Storm. Diharapkan dengan penelitian ini dapat digunakan para web developer mengenai dampak hasil dari *DDoS-Attack* dengan ketiga tools tersebut.
Kata Kunci - *DDoS-Attack, fl00d3r, DDoS-Ripper, Raven-Storm*, Keamanan Siber.

I. PENDAHULUAN

Website merupakan sarana yang digunakan oleh semua masyarakat. *Website* biasanya digunakan untuk berbagai macam kegiatan, seperti: 1) Hiburan; 2) Pekerjaan; 3) Penyebaran Informasi; 4) dan lain sebagainya. Sebelum *website* terkenal, kebanyakan orang menggunakan cara konvensional untuk menyebar berbagai informasi. Caranya yaitu dengan memasang spanduk dan mencetak brosur yang jangkauan penyebaran informasinya masih terbatas. Namun dengan dikenalnya *website*, penyampaian informasi dapat dilakukan dengan efektif dan efisien, serta jangkauannya lebih luas dibandingkan dengan cara konvensional.

Seiring perkembangan zaman, tidak sedikit *web developer* yang lebih mengutamakan keindahan *design* tampilan *website* untuk menarik perhatian pengguna, tanpa memikirkan keamanan dari *website* itu sendiri. Pada dasarnya, keamanan dari suatu *website* tidak kalah penting untuk diperhatikan dalam pengembangan sebuah *website*. Hal ini bertujuan untuk menjaga data-data dan informasi yang termuat di dalam *website*. Namun, seiring berkembangnya teknologi, keamanan dari sebuah *website* menjadi hal yang dipertanyakan.

Sebanding dengan tingginya penggunaan *website*, maka tinggi juga tingkat kemunculan kerentanan dari *website* yang sangat beresiko diserang oleh penyerang/*hacker*. *Hacker* ialah seseorang peretas yang mengambil keuntungan dari keterampilan teknisnya untuk mengeksploitasi pertahanan keamanan *cyber*. Banyak penyerang/*hacker* memanfaatkan keterampilan yang mereka miliki untuk hal yang tidak baik serta merugikan banyak pengguna. Namun, tak sedikit juga yang memanfaatkan kemampuan yang mereka miliki untuk hal-hal yang lebih baik dari meretas.

Ada beberapa bentuk penyerangan yang biasa digunakan oleh seorang peretas, salah satunya yaitu DDoS. DDoS atau *Distributed Denial of Service* merupakan serangan yang dilakukan terhadap suatu *website* yang menyebabkan *website* tersebut lambat hingga *down*. DDoS ini memerlukan lebih banyak perangkat dibandingkan DoS yang hanya memerlukan satu perangkat untuk menyerang. Cara kerja dari DDoS ini sendiri yaitu dengan membanjiri *traffic* server dengan jumlah paket yang sangat banyak hingga

melebihi kapasitasnya. Dalam penyerangan DDoS, bisa juga digunakan botnet.

Penyerangan sebuah *website* menggunakan metode DDoS ini diuji dengan 3 tool yaitu *Fl00d3r*, DDoS-*Ripper*, dan *Raven-Storm*. Dari pengujian ini, .peneliti mengambil judul "Analisis Kelayakan Tools Dengan Metode Penyerangan *Distributed Denial Of Service* (DDOS) Menggunakan *Fl00d3r*, DDoS-*Ripper*, dan *Raven-Storm*".

A. *Pengertian Denial of Service (DoS) dan Distributed Denial of Service (DDoS)*

Denial of Service (DoS) dan *Distributed DoS* (DDoS)-*Attack* merupakan bentuk serangan yang dilakukan dengan mengirimkan paket secara terus menerus untuk melumpuhkan target berupa komputer utama ataupun web server. Serangan ini akan mengakibatkan sumber daya mesin ataupun jaringan tidak bisa diakses atau digunakan oleh pengguna. DDoS-*Attack* biasanya berasal dari beberapa mesin yang dioperasikan oleh pengguna ataupun bot, sedangkan DoS-*Attack* dilakukan oleh satu orang atau satu sistem. Pembahasan kali ini lebih berfokus pada DDoS-*Attack*. DDoS-*Attack* merupakan serangan yang mudah untuk dilakukan, namun sulit untuk ditanggulangi. DDoS-*Attack* biasanya ditujukan untuk organisasi atau perusahaan yang terhubung ke internet. DDoS-*Attack* dilakukan terhadap target dalam bentuk dua serangan, yaitu penyerangan dengan menghabiskan semua *bandwidth* dan *resource* dari sistem yang dimiliki target, serta penyerangan dengan menemukan *bug* atau kelemahan pada implementasi *software* yang dapat mengganggu layanan. Pada percobaan DDoS-*Attack* kali ini menggunakan 3 *tools*, yaitu :

1. Fl00d3r

   Fl00d3r adalah sebuah *tools* yang dibuat oleh pengguna *Github* dengan *username* 47hxl-53r. *Tools* yang dibuat ini ditujukan untuk edukasi kepada penggunanya, *fl00d3r* sendiri memiliki fungsi layaknya *tools* DOS lain, dengan kata lain *fl00d3r* memiliki kemampuan untuk mengirim banyak paket data dan membanjiri lalu lintas jaringan target. *Fl00d3r* memiliki 4 fitur protokol, yaitu Target IP (untuk menuliskan alamat IP target), *Port* (untuk menuliskan *port* dari target), *Packet/s* (untuk menuliskan jumlah paket yang akan dikirimkan ke target), dan *Threads*.

2. DDoS-Ripper

   DDoS-*Ripper* adalah serangan *Distributed Denial-of-Service* (DDOS) pada server dengan memotong target atau infrastruktur di sekitarnya dalam banjir lalu lintas internet. DDoS-*Ripper* memiliki beberapa fitur protokol yaitu h (*help*), s (server ip), p (*port default* 80), q (*quiet*), dan t (*turbo default* 135 *or* 443). DDoS-*Attack* mencapai efektivitas menggunakan beberapa sistem komputer yang disusupi sebagai sumber lalu lintas serangan. Mesin pencari dapat mencakup komputer dan sumber daya jaringan lainnya seperti perangkat IoT. Untuk tingkat yang lebih tinggi, serangan DDoS diibaratkan seperti kemacetan lalu lintas tak terduga yang terjebak di jalan raya, mencegah lalu lintas biasa untuk mencapai tujuannya.

3. Raven-Storm

   Raven-Storm adalah *tools* DDoS yang kuat untuk uji penetrasi, termasuk serangan untuk beberapa protokol yang ditulis dalam *Python*. *Raven-Storm* dapat menangani server yang kuat dan dapat dioptimalkan untuk target yang tidak biasa. *Raven-Storm* menyertakan alat untuk membuat pintasan dan bekerja lebih efisien. *Raven-Storm* efektif dan kuat dalam mematikan *host* dan server. Tujuan dari *Raven-Storm* adalah untuk pengujian dan pemahaman. Fitur protokol pada *Raven-Storm* yaitu UDP/TCP, ICMP, HTTP, L2CAP, ARP, dan IEE.

B. *Wireshark*

Wireshark atau *network packet analyzer* adalah *tools* yang digunakan untuk menganalisis paket data jaringan. *Wireshark* berfungsi untuk menangkap paket-paket jaringan dan berusaha menampilkan semua informasi pada paket tersebut dengan sedetail mungkin. Dengan adanya *Wireshark*, monitoring dan analisa paket yang lewat di jaringan dapat berlangsung lebih mudah. Beberapa fitur yang terdapat pada *Wireshark*, yaitu :

a. Berjalan pada sistem operasi *Linux* dan *Windows*.
b. Menangkap paket (*Capturing Packet*) langsung dari *network interface*.

c. Mampu menampilkan hasil tangkapan dengan detail.
d. Dapat melakukan pemfilteran paket.
e. Hasil tangkapan dapat di-*save*, di-*import*, dan di-*export*.[1]

C. *DVWA*

Damn Vulnerable Web Application (DVWA) adalah aplikasi yang digunakan untuk uji celah keamanan, yang berjalan menggunakan *service apache web* server pada protokol HTTP. Tujuan utama menggunakan DVWA yaitu membantu para pemula dan profesional keamanan untuk menguji *skill* yang dimiliki dalam lingkungan hukum serta membantu *web developer* agar lebih memahami proses keamanan aplikasi web.

D. *VirtualBox*

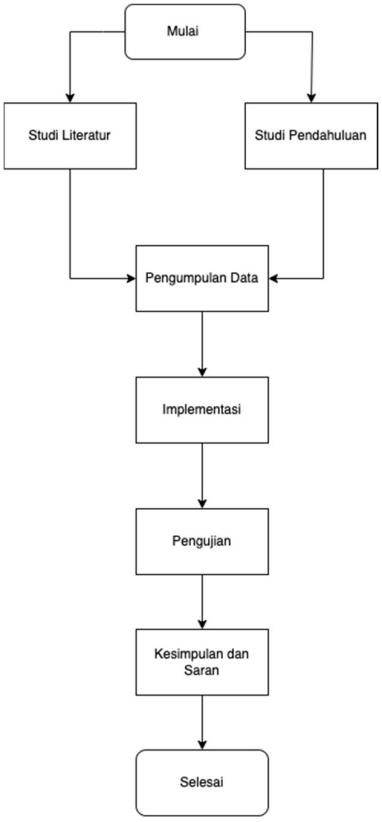
Oracle VM VirtualBox atau sering disebut dengan *VirtualBox* merupakan salah satu prod[2]uk perangkat yang saat ini dikembangkan oleh *Oracle*. *VirtualBox* berfungsi untuk melakukan virtualisasi sistem operasi. Penggunaan *VirtualBox* ditargetkan untuk server, *desktop*, dan penggunaan *embedded*. *Oracle VM VirtualBox* dapat digunakan untuk mengeksekusi sistem operasi tambahan di dalam sistem operasi utama.

E. *Kali Linux*

Kali linux adalah sistem operasi berbasis *Debian linux* yang dikembangkan oleh *Offensive Security*. *Kali linux* dikenal sebagai sistem operasi pengganti *BackTrack* yang merupakan *distro linux* yang khusus dibuat untuk tujuan *penetration testing* keamanan sebuah sistem. *Kali linux* hampir sama seperti sistem operasi berbasis *linux* lainnya, namun *kali linux* memiliki *tools* bawaan untuk pengujian keamanan digital.[3]

II. METODE PENELITIAN

Penelitian ini disusun sebagai penelitian induktif yakni mencari dan mengumpulkan data yang ada di lapangan dan penelitian-penelitian yang telah dilaksanakan dengan tujuan untuk mengetahui data-data yang mendukung dalam menentukan kelayakan tools - tools Distributed Denial of Service (DDOS).



Gambar 1. Diagram Alur Penelitian

1. Mengumpulkan Data
   Langkah awal dalam penelitian ini dimulai dari pengumpulan data, yang dilakukan dengan penelitian lapangan (*field research*). berikut data yang didapatkan dalam menunjang penelitian.
2. Lingkungan Pengujian
   Pengujian ketiga *tools* dilakukan pada tanggal 21 November 2022. Pengujian dilakukan dengan menggunakan 1 buah laptop sebagai target dan 2 buah laptop sebagai penyerang dan 1 buah ponsel sebagai pengukuran waktu yang dibutuhkan dalam melakukan pengujian, serta setting DVWA *Security Impossible*, berikut spesifikasi alat pengujian :

Penguji	Spesifikasi Kali Linux	Spesifikasi VirtualBox	Spesifikasi Perangkat	Jaringan
Target	*Linux 5.18.0-kali-amd64 - Video Memory 128*	*VirtualBox Graphical User Interface Version 6.1.32 r149290 (Qt5.6.2)*	*Asus Vivobook Ryzen 7 5700U Cores 8 - VGA AMD Radeon - Windows 10 - RAM 8GB - Wifi 6*	*Hotspot Ventech - WP/WP3 Personal*

Penguji	Spesifikasi Kali Linux	Spesifikasi VirtualBox	Spesifikasi Perangkat	Jaringan
	MB - Base memory 4096 MB - 6 CPU		*AX200 160MHz*	
Penyerang 1	*Linux 5.18.0-kali-amd64 - video memory 128 MB - base memory 2048 MB - 2 CPU*	*VirtualBox Graphical User Interface Version 6.1.32 r149290 (Qt5.6.2)*	*Acer Aspire 5 - intel i3 12th Gen - intel HD Graphics - RAM 8 - V6 Mediatek Wi-Fi 6 MT7921 - Windows 11*	*Hotspot Ventech - WP/WP3 Personal*
Penyerang 2	*Linux 5.18.0-kali-amd64 video memory 128 MB - Base memory 2304 MB - 2 CPU*	*VirtualBox Graphical User Interface Version 6.1.32 r149290 (Qt5.6.2)*	*HP Laptop 14s-dk1xxx AMD Ryzen 3 Windows 11 RAM 8GB*	*Hotspot Ventech - WP/WP3 Personal*

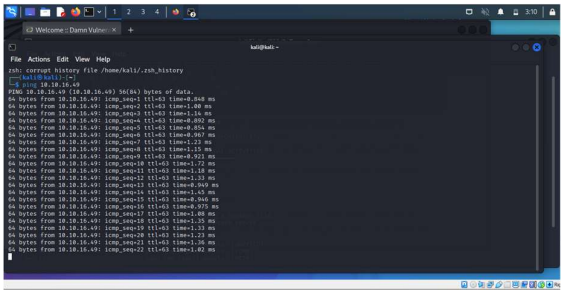
Tabel 1. Lingkungan Pengujian

3. Langkah Pengujian

Pada tahapan pengujian, terdapat langkah - langkah yang harus dilalui yaitu dengan memulai tes ping pada server *localhos*t target yang akan diuji. Sebelum melakukan pengujian target server yang akan dituju, perlu diketahui layanan *port* yang tersedia dalam alamat IP dengan menggunakan Nmap Server. Langkah pengujian dilakukan setelah menentukan layanan *port* yang tersedia, pengujian dilakukan dengan menggunakan 3 *tools* yang akan diuji dan menggunakan *stopwatch* pada ponsel untuk mengukur waktu pengujian.

Gambar 2. Diagram Alur Pengujian

4. Penyiapan *Tools*



Gambar 3. Ping Server

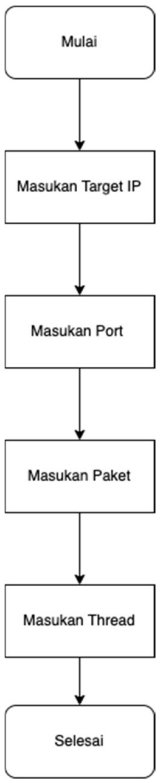
Sebelum melakukan pengujian, tahap pertama yang perlu dilakukan yaitu melakukan uji tes respon server dengan melakukan ping terhadap server *localhost* DVWA. Tujuan dari ping server tersebut untuk mengetahui jika server merespon,

maka pengujian dapat dilakukan. Perangkat yang digunakan untuk pengujian menggunakan 3 *device* laptop. 2 diantaranya digunakan sebagai penyerang, sedangkan 1 laptop lainnya membuka DVWA yang sudah di-*set up* sebagai *localhost* server.

5. Menentukan Port
   Pada langkah selanjutnya yaitu tahap mengecek layanan *port* yang terbuka menggunakan Nmap server. Sehingga didapatkan yaitu *port* 22 ssh, 80 http, 11 rpcbind. Dalam pengujian 3 *tools*, akan digunakan *port* 80 http untuk penyerangan server *localhost*. Berikut analisis dalam pengujian *tools* DDOS :

Gambar 4. Nmap Server

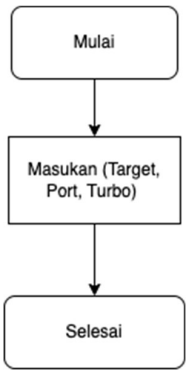
6. Langkah Pengujian *Tools Fl00d3r*
   Fl00d3r memiliki 4 fitur yang diberikan oleh *creator tools* yakni: 1) Target, pengguna menentukan tujuan untuk siapa paket data akan dikirimkan, 2) *Port*, 3) *Packet/s*, 4) *Threads*. Pada langkah awal, menentukan target atau IP target



Gambar 5. Langkah Pengujian *Tools fl00d3r*

untuk dibanjiri *packets*. Pada pengujian DDoS-*Attack* ini, target yang digunakan adalah *localhost virtual machine* DVWA. Setelah memasukan IP target, langkah selanjutnya memasukan *Port* yang digunakan, yang mana sesuai dengan pengecekan Nmap Server tadi adalah *port* 80. Nmap untuk melihat *port* yang akan digunakan adalah HTTP. Setelah menentukan port yang akan diserang, langkah selanjutnya yaitu mengatur *packets* yang akan dikirim. *Packet/s* adalah paket yang akan dikirim per detik, dalam pengujian kali ini digunakan 1000 *packets*. *Threads* yang digunakan pada pengujian ini adalah 1000. Setelah memasukan seluruh data yang dibutuhkan, penyerangan dimulai. Dari keseluruhan tahap menuju penyerangan total terdapat 4 tahap yang dilewati seorang penyerang untuk menyerang sebuah *websit*e.

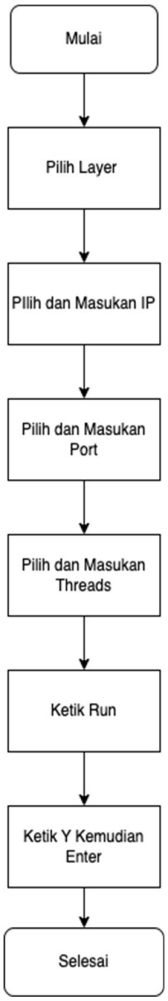
7. Langkah Pengujian *Tools* DDoS-*Ripper*
   DDoS-*Ripper* memiliki sejumlah *tools* yang memberikan kemampuan untuk digunakan oleh penggunanya. Pada pengujian menggunakan tools ini, tahapan penyerangan terbentuk singkat yaitu hanya sekali penginputan dengan 1 baris *command*. Sama seperti sebelumnya, *port* yang digunakan pada pengujian ini yaitu *port* 80. Pada penyerangan menggunakan *tools* DDoS-*Ripper* ini, *tools* memiliki fitur tambahan yakni fitur turbo dengan *max*-nya 443.



Gambar 6. Langkah Pengujian *Tools* DDoS-*Ripper*

8. Langkah Pengujian *Tools Raven-Storm*
   Pengujian menggunakan *tools* ini berbeda dengan *tools* sebelumnya dikarenakan adanya pilihan fitur yang lengkap. *Tools Raven-Storm* memerlukan 6 langkah untuk memulai pengujian penyerangan terhadap target yang ingin diserang. Pada pengujian ini, tahapan awal adalah menentukan *layer*. Pada pengujian *tools Raven-Storm*, digunakan *modules* L4. L4 adalah *modules* untuk menggunakan protokol UDP atau TCP.

Kemudian, langkah selanjutnya adalah menargetkan IP domain yang akan diuji. Seperti dijelaskan sebelumnya, *port* yang digunakan adalah *port* 80 http, kemudian memberikan *threads* berjumlah 1000. Setelah itu, pengujian dimulai dengan perintah *run*.



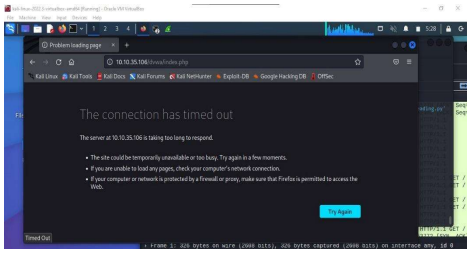
Gambar 7. Langkah Pengujian *Tools Raven-Storm*

III. HASIL DAN PEMBAHASAN

A. Hasil Pengujian *Tools* pada *Website*

1. *Fl00d3r*

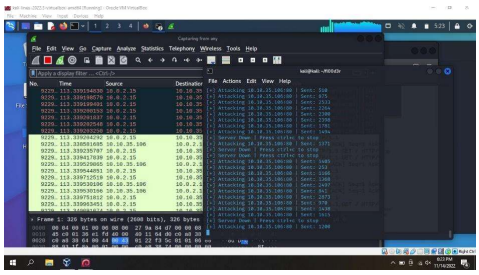
Hasil yang didapatkan pada pengujian dengan *tools Fl00d3r* memerlukan 4 kali tahapan untuk memulai penyerangan, protokol yang digunakan dalam pengujian penyerangan adalah TCP. Dalam penyerangan di setiap pengukuran waktu, terlihat pesan *"The connection has timed out"*saat berlangsungnya penyerangan . Hal ini terjadi



Gambar 8. *Fl00d3r Attack Result*

karena server *localhos*t terlalu lama untuk merespon.

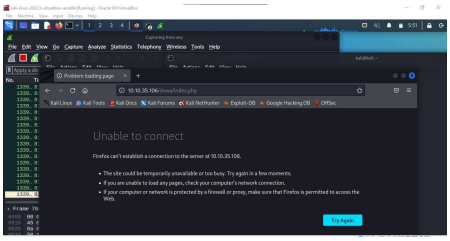
Paket – paket yang masuk dapat dilihat pada wireshark yang digunakan, pengiriman paket – paket yang menumpuk dan membanjiri traffic server akan menyebabkan target lambat. Fl00d3r memberikan tampilan informasi secara langsung untuk memperlihatkan apakah paket – paket sudah dikirimkan oleh tools.



Gambar 9. Paket dan Penyerangan Server

2. *DdoS-Ripper*

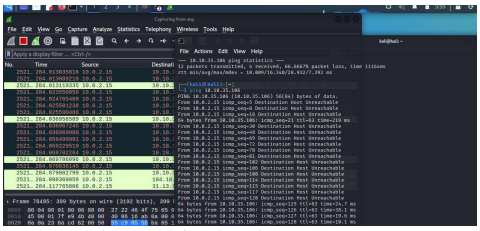
Hasil yang didapatkan oleh *tools DdoS-Ripper* dengan memerlukan 1 kali tahapan adalah server tidak dapat *connect,* protokol penyerangan yang digunakan adalah TCP. Hal ini terjadi karena *traffic* server terlalu sibuk sehingga tidak dapat *re-connect* atau tidak dapat diakses kembali.



Gambar 10. *DdoS-Ripper Attack Result*

DdoS-Ripper mengirimkan paket – paket dengan bantuan *bot zombie* yang dimana sebuah bot komputer akan membantu

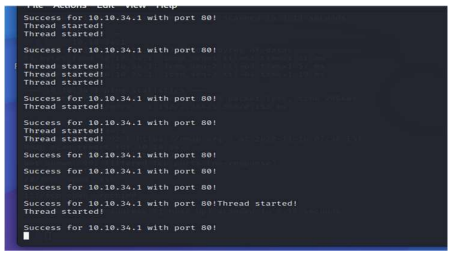
pengiriman paket secara *simultaneous* dengan tujuan membanjiri server dan komputer *client* hingga *down.* Terlihat pada percobaan tes *ping* alamat *IP*, memunculkan pesan "*host unreachable*" dalam kasus ini server target tidak dapat diakses selama penyerangan berlangsung dalam artian server sedang *down.*



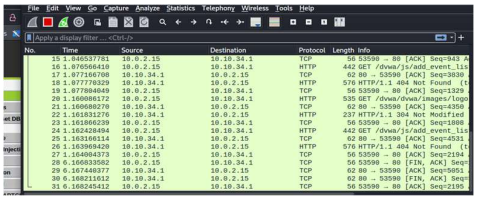
Gambar 11. Paket dan Ping Server

3. *Raven-Storm*

Hasil pada *tools Raven-Storm* dengan 6 kali tahapan yakni tidak terjadi perubahan saat penyerangan berlangsung, protokol yang digunakan saat penyerangan adalah TCP dan UDP. Ketika *thread* dimulai, terdapat pesan



Gambar 12. *Raven-Storm Attack*



Gambar 13. Paket pada *Raven-Storm*

berhasil untuk IP target serta *port* yang di input, namun tidak terdapat perubahan yang menandakan server *down*. Terlihat pada gambar 10, *packets* yang tertuju pada IP target dengan protokol TCP terlihat, namun tidak mempengaruhi server *localhost* DVWA.

B. Tabel *Tools* & Hasil Pengujian

Tools	*F00d3r*	*DdoS-Ripper*	*Raven-Storm*
GUI	Tampilan pengujian terdapat kode ASCII untuk *header* dan 4 *section tools*.	Tampilan pengujian hanya terdapat 1 *section* untuk melakukan penyerangan Terdapat kode ASCII untuk *header*.	Terdapat kode ASCII pada header, terdapat 2 section yakni help dan *modules*. Yang masing – masing memiliki *sub-section*
Fitur	*Target IP, Port, Packet, Threads*	*Help, Server IP, Port, Quite, Turbo*	*Help, Modules*
Protokol	TCP	TCP	UDP & TCP
Hasil	Server *down* serta lambat dalam merespon *"The connection has timeout"*	Server *down "unable to connect"*	Mesin linux lambat, namun server masih dapat merespon
Rata-Rata Waktu	05:28	01:50	09:34
Tahapan Penyerangan	4 Tahapan	1 Tahapan	6 Tahapan

Tabel 2. Hasil Pengujian

IV. KESIMPULAN

Hasil dari pengujian DDoS-*Attack* yang telah dilakukan, jika ditinjau dari segi kecepatan *tools*, DDoS-Ripper merupakan *tools* yang paling efektif diantara ketiga *tools* yang digunakan. Hal ini dibuktikan dengan rata-rata waktu yang diperoleh, yakni penyerangan hingga server *down* hanya memerlukan rata-rata waktu 1 menit 50 detik. *Tools* Fl00d3r menduduki peringkat kedua, hal ini dibuktikan dengan rata-rata waktu penyerangan 5 menit 28 detik. Meskipun memerlukan waktu lebih lama dari *tools* pertama, *tools* Fl00d3r berhasil melumpuhkan server hingga memunculkan pesan *"The connection has timed out"*. Sementara itu, *tools* Raven-Storm tidak berdampak signifikan. Saat dilakukan pengujian menggunakan *tools* tersebut, CPU pada Linux hampir 100% digunakan, namun tidak berpengaruh banyak

pada target yang diserang. Meskipun *tools* Raven-Storm memiliki fitur yang lengkap, pada kasus ini Raven-Storm tidak efektif untuk digunakan dalam pengujian DDoS-*Attack*.

Jika ditinjau dari segi GUI dan fitur, *tools* DDoS-Ripper dan Raven-Storm sedikit lebih unggul dari Fl00d3r, dimana DDoS-Ripper memiliki fitur turbo yang berfungsi untuk mempercepat pengiriman paket, sedangkan Raven-Strom memiliki fitur *modules* yang berfungsi untuk mengatur protokol yang diinginkan

Dari segi efisiensi pengguna, *tools* DDoS-Ripper merupakan *tools* yang efektif dari ketiga tools yang digunakan, dimana dalam penggunaan *tools* DDoS-Ripper hanya melalui 1 tahapan menuju penyerangan sedangkan *Tools* Fl00d3r menempati posisi kedua dengan 4 tahapan dan disusul *tools* Raven-Storm dengan 6 tahapan menuju penyerangan.

Berdasarkan dari pemaparan hasil pengujian yang dilakukan, dapat disimpulkan bahwa tool DDoS-Ripper menjadi tools yang memiliki banyak keunggulan dari tools lainnya, mulai dari waktu rata-rata penyerangan yaitu 1 menit 28 detik, keunggulan fitur turbo yang dimiliki tools tersebut, tahapan eksekusi penyerangan yang hanya membutuhkan 1 kali tombol enter. Sehingga dapat dikatakan tools DDoS-Ripper ini, *tools* yang paling efisien digunakan untuk penyerangan DDOS pada pengujian kali ini.

DAFTAR PUSTAKA

[1] M. F. Adriant and I. M. Mardianto, "Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan," Seminar Nasional Cendekiawan 2015, 2015, Accessed: Nov. 22, 2022. [Online]. Available: https://www.neliti.com/publications/172890/

[2] A. Putra Armadhani, D. Nofriansyah, K. Ibnutama, S. Informasi, and S. Triguna Dharma, "Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab esting Menggunakan Penetration Testing Standart OWASP," Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer), vol. 21, no. 2, pp. 80–88, Aug. 2022, doi: 10.53513/JIS.V21I2.6119.

[3] F. Indyawan, "Apa itu Kali linux : Pengertian, Sejarah dan Fungsinya | Portal Belajar Gratis," kitaadmin.com, Apr. 10, 2022. https://www.kitaadmin.com/2018/08/kali-linux-adalah.html (accessed Nov. 22, 2022).