Journal of Technology and System Information Vol: 1, No 4, 2024, Page: 1-11

Strategi Pencegahan Efektif terhadap Serangan DDoS Slowloris menggunakan Kali Linux dan Linux Mint

Keinanjung Ruswandi*, Muhammad Reza Zulva Pohan, Kevin Viriya Halim, Shelvie Nidya Neyman

Teknologi Rekayasa Komputer, IPB University

Abstrak: Serangan *Distributed Denial of Service* (DDoS) telah menjadi ancaman serius dalam keamanan siber, dengan serangan tipe Slowloris menjadi salah satu yang paling merusak. Penelitian ini mengeksplorasi strategi pencegahan terhadap serangan Slowloris menggunakan pendekatan campuran yang melibatkan Kali Linux sebagai mesin serangan dan Linux Mint sebagai target. Data sekunder dari literatur digunakan untuk memahami serangan DDoS dan teknik pencegahannya, sementara data primer diperoleh melalui eksperimen praktis. Hasilnya menunjukkan bahwa langkah-langkah pencegahan, seperti peningkatan *timeout*, dapat efektif mengurangi dampak serangan Slowloris terhadap kinerja dan ketersediaan layanan pada Linux Mint. Analisis kuantitatif menunjukkan perbedaan yang signifikan dalam respons sistem sebelum dan sesudah implementasi langkah-langkah pencegahan. Penelitian ini memberikan wawasan penting dalam melindungi sistem mereka dari serangan DDoS.

Kata kunci: Keamanan Jaringan, Pencegahan DDoS, Serangan Slowloris.

DOI: https://doi.org/10.47134/jtsi.v1i4.2645
*Correspondence: Keinanjung Ruswandi
Email: keinanjungruswandi@apps.ipb.ac.id

Received: 01-08-2024
Accepted: 15-09-2024
Published: 31-10-2024

Abstract: *Distributed Denial of Service (DDoS) attacks have become a serious threat in cybersecurity, with Slowloris-type attacks being one of the most damaging. This research explores prevention strategies against Slowloris attacks using a blended approach involving Kali Linux as the attack engine and Linux Mint as the target. Secondary data from the literature is used to understand DDoS attacks and prevention techniques, while primary data is obtained through practical experiments. The results show that preventive measures, such as increasing timeouts, can effectively reduce the impact of Slowloris attacks on performance and service availability on Linux Mint. Quantitative analysis showed significant differences in system response before and after the implementation of preventive measures. This research provides important insights in protecting their systems from DDoS attacks.*

Keywords: *DDoS Prevention, Network Security, Slowloris Attack.*

Pendahuluan

Dalam era digital yang terus berkembang, keamanan sistem dan jaringan merupakan hal yang sangat penting bagi organisasi dan individu. Salah satu ancaman utama dalam ranah keamanan *cyber* adalah serangan *Distributed Denial of Service* (DDoS). Serangan DDoS adalah tipe serangan terhadap suatu sistem di jaringan internet yang bertujuan untuk mengeksploitasi sumber daya sistem tersebut. Hasilnya, sistem tersebut tidak dapat berfungsi secara optimal, sehingga menghambat pengguna lain untuk mengakses layanan dari sistem yang diserang (Arief *et al.,* 2024). Serangan DDoS dapat memiliki berbagai bentuk, dan salah satu yang paling dikenal adalah serangan Slowloris. Serangan Slowloris merupakan jenis serangan DDoS yang bertujuan menghabiskan sumber daya server dengan memanfaatkan kelemahan dalam protokol HTTP. Penyerang menggunakan serangkaian koneksi HTTP yang lambat dan mempertahankannya untuk waktu yang lama, sehingga membuat server menjadi tidak responsif terhadap pengguna yang sah (Suharti *et al.,* 2022). Hal ini dapat mengakibatkan gangguan layanan yang signifikan, kerugian finansial, dan reputasi yang rusak bagi organisasi yang menjadi target.

Dalam upaya untuk mengurangi dampak serangan DDoS, berbagai strategi pencegahan telah dikembangkan. Namun, seringkali diperlukan pengujian praktis untuk mengevaluasi efektivitas strategi pencegahan tersebut. Dalam penelitian ini, penggunaan sistem operasi Linux yang umum digunakan, seperti Kali Linux dan Linux Mint, dapat menjadi landasan yang tepat untuk melakukan uji coba pencegahan terhadap serangan DDoS. Kali Linux merupakan sebuah distribusi Linux yang terkenal sebagai alat untuk pengujian penetrasi dan keamanan. Kali Linux menyediakan beragam alat dan skrip yang dirancang khusus untuk mengevaluasi kerentanan sistem dan jaringan (Andria, 2020). Dengan fitur-fitur seperti pemindaian kerentanan, analisis forensik, dan uji coba penetrasi, Kali Linux memberikan lingkungan yang ideal bagi para ahli keamanan untuk menguji dan memperbaiki keamanan sistem sebelum serangan sebenarnya terjadi.

Di sisi lain, Linux Mint merupakan turunan dari Ubuntu, sebuah distribusi Linux yang telah dikenal luas karena popularitasnya, terutama karena desain desktop yang khas. Linux Mint menawarkan dua pilihan desktop utama. Salah satunya adalah *Cinnamon*, yang menyuguhkan lingkungan desktop yang lebih modern (Yuniarti *et al.,* 2023). Meskipun demikian, Linux Mint juga dapat menjadi target yang menarik bagi serangan DDoS dan ancaman keamanan lainnya. Dengan demikian, uji coba pencegahan serangan DDoS yang dilakukan menggunakan Kali Linux dan Linux Mint dapat memberikan wawasan yang berharga dalam melindungi sistem dan jaringan dari serangan siber.

Untuk memahami lebih dalam tentang efektivitas langkah-langkah pencegahan terhadap serangan DDoS, uji coba dilakukan dengan menggunakan Kali Linux sebagai mesin serangan dan Linux Mint sebagai target serangan. Setelah serangan DDoS berhasil dilakukan dari Kali Linux ke Linux Mint, langkah-langkah pencegahan akan diimplementasikan pada Linux Mint untuk mengurangi dampak serangan tersebut. Dengan demikian, hasil dari uji coba ini diharapkan dapat memberikan wawasan baru dalam menghadapi ancaman serangan DDoS dan meningkatkan ketahanan sistem dan jaringan.

Metode

Metode penelitian yang digunakan dalam studi ini adalah metode campuran (*mixed methods*), yang menggabungkan pendekatan kualitatif dan kuantitatif (Hendrayadi *et al.*, 2023). Penelitian ini melibatkan pengumpulan data sekunder melalui studi pustaka yang mencakup berbagai jurnal, buku, artikel ilmiah, dan sumber lain yang relevan dengan topik serangan DDoS tipe Slowloris dan strategi pencegahannya. Selain itu, eksperimen praktis dilakukan untuk mengevaluasi efektivitas pencegahan terhadap serangan Slowloris pada sistem Linux Mint.

Teknik pengumpulan data yang digunakan pada penelitian ini mencakup dua pendekatan utama. Pertama adalah pengumpulan data sekunder, yang dilakukan melalui studi pustaka. Data sekunder ini berasal dari peninjauan literatur dari jurnal ilmiah, buku, artikel, dan sumber akademis lainnya yang membahas serangan DDoS, khususnya Slowloris, serta berbagai metode pencegahan yang telah dikembangkan. Sumber-sumber ini diperoleh dari database akademik, perpustakaan, dan repositori online. Pendekatan kedua adalah pengumpulan data primer melalui eksperimen praktis. Eksperimen ini melibatkan beberapa tahapan, termasuk persiapan lingkungan eksperimen dengan instalasi dan konfigurasi Kali Linux sebagai mesin penyerang dan Linux Mint sebagai target. Selanjutnya, dilakukan pelaksanaan serangan dengan peluncuran serangan Slowloris terhadap server di Linux Mint dan penerapan langkah-langkah pencegahan.

Analisis data yang digunakan dalam penelitian ini terdiri dari dua aspek utama. Pertama adalah analisis kualitatif terhadap data sekunder yang dikumpulkan dari literatur. Analisis ini bertujuan untuk mengidentifikasi konsep-konsep utama, temuan-temuan penting, dan tren dalam penelitian tentang serangan DDoS dan metode pencegahan. Hasil dari analisis kualitatif ini digunakan untuk mendasari dan merancang eksperimen praktis. Sementara itu, pendekatan kedua adalah analisis kuantitatif terhadap data primer yang dikumpulkan dari eksperimen. Analisis ini melibatkan perbandingan kinerja server sebelum dan sesudah penerapan langkah-langkah pencegahan menggunakan uji statistik untuk menentukan signifikansi perbedaan.

Hasil dan Pembahasan

Serangan DDos Tipe Slowloris

Pada bagian ini, peneliti menguraikan detail langkah-langkah yang diambil dalam uji coba serangan DDoS tipe Slowloris terhadap sistem Linux Mint yang menggunakan NGINX sebagai server web. Pendekatan terhadap eksperimen ini terbagi menjadi dua fokus utama, yaitu tindakan yang dilakukan di Linux Mint, yang berperan sebagai sistem target, dan langkah-langkah yang diambil di Kali Linux, yang bertindak sebagai sistem penyerang dalam simulasi serangan. Dengan membagi penjelasan ini menjadi dua bagian, peneliti bertujuan untuk memberikan pemahaman yang jelas tentang bagaimana serangan dilakukan, serta upaya-upaya yang diambil untuk mengevaluasi dampaknya pada sistem yang diserang.

1. Linux Mint

Langkah-langkah ini merupakan bagian dari serangkaian persiapan yang dilakukan dalam pengujian serangan DDoS tipe Slowloris pada sistem Linux Mint yang menggunakan NGINX sebagai server web. Berikut Langkah-langkahnya, yaitu:

Memeriksa Versi NGINX

Memastikan versi NGINX yang terpasang pada Linux Mint untuk mengetahui fitur dan kemampuan yang tersedia.

```
mint@mint:~$ nginx -v
Command 'nginx' not found, but can be installed with:
sudo apt install nginx-core    # version 1.18.0-6ubuntu14.4, or
sudo apt install nginx-extras  # version 1.18.0-6ubuntu14.4
sudo apt install nginx-light   # version 1.18.0-6ubuntu14.4
```

Gambar 1. Memeriksa Versi NGINX

Memperbarui Paket Sistem

Melakukan pembaruan paket untuk memastikan semua perangkat lunak yang digunakan dalam kondisi terbaru dan teraman.

```
mint@mint:~$ sudo apt-get update
Ign:1 cdrom://Linux Mint 21.3 _Virginia_ - Release amd64 20240109 jammy InRelease
Err:2 cdrom://Linux Mint 21.3 _Virginia_ - Release amd64 20240109 jammy Release
  Please use apt-cdrom to make this CD-ROM recognized by APT. apt-get update cannot be used to add new CD-ROMs
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Ign:4 http://packages.linuxmint.com virginia InRelease
Get:5 http://packages.linuxmint.com virginia Release [24.1 kB]
Hit:6 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:7 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
```

Gambar 2. Memperbarui Paket Sistem

Menginstall NGINX Full

Menginstal NGINX versi lengkap yang mencakup semua modul yang diperlukan untuk pengujian.

```
mint@mint:~$ sudo apt-get install nginx-full
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libnginx-mod-http-auth-pam libnginx-mod-http-dav-ext libnginx-mod-http-echo
  libnginx-mod-http-geoip2 libnginx-mod-http-image-filter
  libnginx-mod-http-subs-filter libnginx-mod-http-upstream-fair
  libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream
  libnginx-mod-stream-geoip2 nginx-common nginx-core
Suggested packages:
  fcgiwrap nginx-doc
The following NEW packages will be installed:
  libnginx-mod-http-auth-pam libnginx-mod-http-dav-ext libnginx-mod-http-echo
  libnginx-mod-http-geoip2 libnginx-mod-http-image-filter
  libnginx-mod-http-subs-filter libnginx-mod-http-upstream-fair
  libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream
  libnginx-mod-stream-geoip2 nginx-common nginx-core nginx-full
0 upgraded, 14 newly installed, 0 to remove and 201 not upgraded.
Need to get 775 kB of archives.
After this operation, 2829 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Gambar 3. Menginstall NGINX Full

Memeriksa Status NGINX

Memastikan bahwa NGINX berjalan dengan baik setelah instalasi.

```
mint@mint:~$ systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset:>
     Active: active (running) since Wed 2024-05-22 12:58:56 UTC; 1min 6s ago
       Docs: man:nginx(8)
    Process: 2760 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_proce>
    Process: 2762 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (c>
   Main PID: 2901 (nginx)
      Tasks: 2 (limit: 2202)
     Memory: 4.2M
        CPU: 63ms
     CGroup: /system.slice/nginx.service
             ├─2901 "nginx: master process /usr/sbin/nginx -g daemon on; master>
             └─2904 "nginx: worker process" "" "" "" "" "" "" "" "" "" "" "" "">

May 22 12:58:56 mint systemd[1]: Starting A high performance web server and a r>
May 22 12:58:56 mint systemd[1]: Started A high performance web server and a re>
```

Gambar 4. Memeriksa Status NGINX

Melihat Koneksi Jaringan

Mengecek koneksi jaringan yang aktif untuk memantau bagaimana NGINX menangani koneksi.

```
mint@mint:~$ netstat -plunt
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
udp        0      0 0.0.0.0:631             0.0.0.0:*                           -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:55428           0.0.0.0:*                           -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp6       0      0 fe80::7f7e:d684:f77:546 :::*                                -
udp6       0      0 :::39540                :::*                                -
udp6       0      0 :::5353                 :::*                                -
```

Gambar 5. Melihat Koneksi Jaringan

Memantau Penggunaan Sumber Daya

Menggunakan **top** untuk memantau penggunaan CPU dan memori oleh NGINX selama serangan.

```
mint@mint:~$ top

top - 13:03:19 up 11 min,  1 user,  load average: 0.01, 0.21, 0.25
Tasks: 175 total,   1 running, 170 sleeping,   4 stopped,   0 zombie
%Cpu(s):  4.4 us,  5.5 sy,  0.0 ni, 88.9 id,  0.0 wa,  0.0 hi,  1.1 si,  0.0 st
MiB Mem :   1964.1 total,    156.5 free,    705.9 used,   1101.6 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used.    819.5 avail Mem
```

Gambar 6. Memantau Penggunaan Sumber Daya

Memeriksa Konfigurasi Jaringan

Melihat konfigurasi jaringan untuk memastikan tidak ada masalah dengan jaringan yang dapat mempengaruhi hasil pengujian.

```
mint@mint:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 2001:448a:2020:9874:d404:fc0c:208f:658c  prefixlen 64  scopeid 0x0<global>
        inet6 2001:448a:2020:9874:1233:278a:cbd5:421c  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::7f7e:d684:f772:d8cd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:98:0d:43  txqueuelen 1000  (Ethernet)
        RX packets 11578  bytes 15988757 (15.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4497  bytes 476446 (476.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 145  bytes 13613 (13.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 145  bytes 13613 (13.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Gambar 7. Memeriksa Konfigurasi Jaringan

Memeriksa Akses melalui Web Browser

Mengecek akses ke server NGINX dari web browser Linux Mint untuk memastikan server dapat diakses sebelum serangan dilakukan.

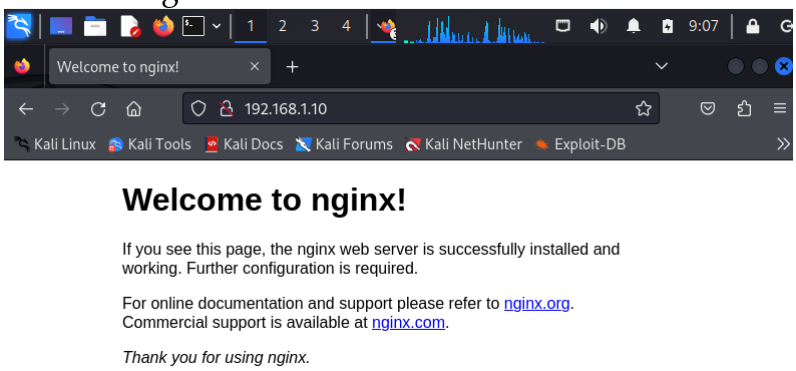
Gambar 8. Memeriksa Akses melalui Web Browser Linux Mint

2. Kali Linux

Pada bagian ini merupakan tahapan dalam persiapan uji coba serangan DDoS tipe Slowloris pada Kali Linux. Dalam penelitian, Kali Linux akan berperan sebagai sistem penyerang yang digunakan untuk melancarkan serangan terhadap sistem Linux Mint yang menjalankan NGINX sebagai server web. Berikut tahapan-tahapan yang dijalankan dalam proses persiapan untuk meluncurkan serangan:

Memeriksa Akses melalui Web Browser

Mengecek akses ke server NGINX dari web browser Kali Linux untuk memastikan server dapat diakses sebelum serangan dilakukan.



Gambar 9. Memeriksa Akses melalui Web Browser Kali Linux

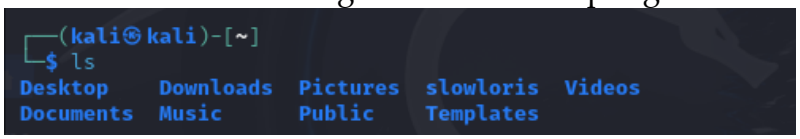
Mengkloning Repositori Slowloris

Mengkloning alat Slowloris dari GitHub untuk digunakan dalam serangan.

Gambar 10. Mengkloning Repositori Slowloris

Navigasi ke Direktori Slowloris

Memastikan alat Slowloris terunduh dengan benar dan siap digunakan.



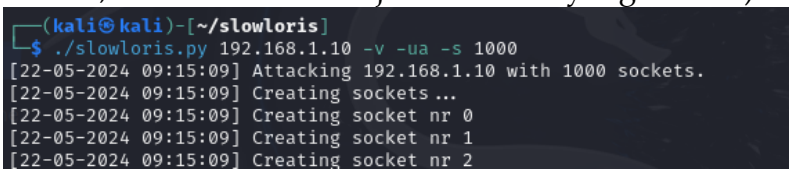
Gambar 11. Navigasi ke Direktori Slowloris (ls) 1

Gambar 12. Navigasi ke Direktori Slowloris (cd slowloris)

Gambar 13. Navigasi ke Direktori Slowloris (ls) 2

Meluncurkan Serangan Slowloris

Meluncurkan serangan Slowloris terhadap alamat IP server NGINX yang menjalankan Linux Mint dengan parameter yang ditentukan (-v untuk verbose, -ua untuk menggunakan user agent yang berbeda, dan -s 1000 untuk jumlah soket yang dibuka).

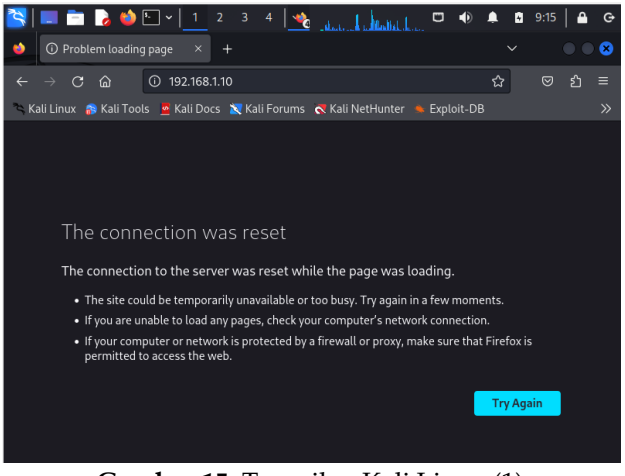


Gambar 14. Meluncurkan Serangan Slowloris

Setelah meluncurkan serangan, dampaknya pada kinerja server NGINX yang menjalankan Linux Mint terasa secara langsung. Waktu respons dari server melambat secara signifikan, bahkan beberapa permintaan mengalami timeout karena server kelebihan beban. Melalui pemantauan menggunakan perintah **top**, peneliti mencatat lonjakan penggunaan CPU dan memori oleh NGINX selama serangan berlangsung. Hal ini menunjukkan bahwa server berusaha keras untuk menangani volume besar permintaan dari serangan Slowloris, menyebabkan penggunaan sumber daya yang intensif.

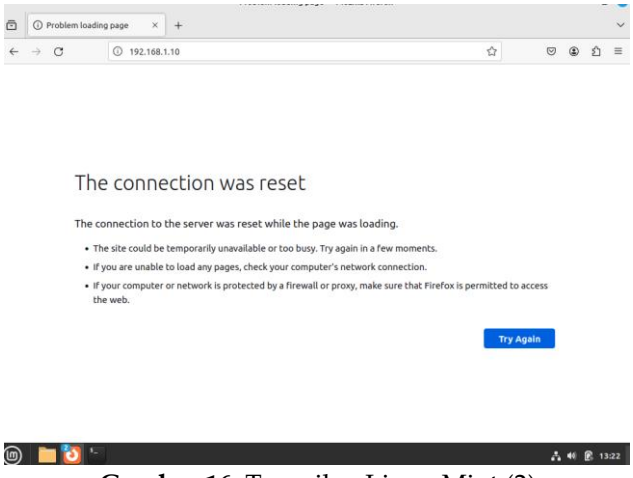
Sementara itu, analisis menggunakan **netstat -plunt** memperlihatkan bahwa ada banyak koneksi terbuka yang tidak selesai, sesuai dengan cara kerja serangan Slowloris yang bertujuan mempertahankan koneksi sebanyak mungkin untuk menghabiskan sumber daya server. Dengan demikian, pengujian ini menggarisbawahi urgensi menerapkan langkah-langkah pencegahan yang efektif untuk melindungi server dari serangan jenis ini, serta pentingnya pemantauan yang cermat terhadap kesehatan sistem untuk mendeteksi dan merespons serangan DDoS dengan cepat demi meminimalkan dampaknya.

Kali Linux:



Gambar 15. Tampilan Kali Linux (1)

Linux Mint:



Gambar 16. Tampilan Linux Mint (2)

Gambar 15 dan **16** merupakan kondisi kritis yang terjadi pada sistem saat menghadapi serangan DDoS tipe Slowloris. Ketika web diserang, infrastruktur menjadi rentan terhadap gangguan yang dapat mengganggu layanan dan bahkan menyebabkan kerugian bagi pengguna. Oleh karena itu, langkah-langkah pencegahan yang tepat dan pemantauan yang

cermat menjadi kunci dalam menjaga kestabilan dan ketersediaan layanan dalam menghadapi ancaman serangan siber.

Pencegahan Serangan Slowloris

Dalam upaya untuk meningkatkan ketahanan sistem terhadap serangan DDoS tipe Slowloris, peneliti menerapkan serangkaian langkah-langkah pencegahan pada Linux Mint yang menggunakan NGINX sebagai server web. Melalui pengaturan khusus pada konfigurasi NGINX, peneliti bertujuan untuk membatasi jumlah koneksi dan permintaan yang dapat diterima oleh server, serta mengoptimalkan pengaturan *timeout* untuk mencegah penumpukan koneksi yang tidak aktif. Langkah-langkah ini diharapkan dapat mengurangi kerentanan server terhadap serangan DDoS dan memastikan ketersediaan layanan yang optimal bagi pengguna.

Konfigurasi NGINX

Langkah pertama, masuk ke direktori konfigurasi NGINX dengan menggunakan perintah **cd /etc/nginx** dan memeriksa isi direktori tersebut dengan perintah **ls -l**. Kemudian, peneliti membuka file konfigurasi nginx.d menggunakan editor teks dengan perintah **sudo nano nginx.d**.

```
mint@mint:~$ cd /etc/nginx
mint@mint:/etc/nginx$ ls -l
total 40
drwxr-xr-x 2 root root   40 May 30  2023 conf.d
-rw-r--r-- 1 root root 1125 May 30  2023 fastcgi.conf
-rw-r--r-- 1 root root 1055 May 30  2023 fastcgi_params
-rw-r--r-- 1 root root 2837 May 30  2023 koi-utf
-rw-r--r-- 1 root root 2223 May 30  2023 koi-win
-rw-r--r-- 1 root root 3957 May 30  2023 mime.types
drwxr-xr-x 2 root root   40 May 30  2023 modules-available
drwxr-xr-x 2 root root  260 May 22 12:58 modules-enabled
-rw-r--r-- 1 root root 1447 May 30  2023 nginx.conf
-rw-r--r-- 1 root root  180 May 30  2023 proxy_params
-rw-r--r-- 1 root root  636 May 30  2023 scgi_params
drwxr-xr-x 2 root root   60 May 22 12:58 sites-available
drwxr-xr-x 2 root root   60 May 22 12:58 sites-enabled
drwxr-xr-x 2 root root   80 May 22 12:58 snippets
-rw-r--r-- 1 root root  664 May 30  2023 uwsgi_params
-rw-r--r-- 1 root root 3071 May 30  2023 win-utf
mint@mint:/etc/nginx$
```

Gambar 17. Konfigurasi NGINX (cd /etc/nginx)

```
mint@mint:/etc/nginx$ sudo nano nginx.d
```

Gambar 18. Konfogurasi NGINX (nano nginx.d)

Penambahan Konfigurasi

Di dalam file konfigurasi nginx.d, peneliti menambahkan konfigurasi berikut.

```
  GNU nano 6.2                                    nginx.d *
limit_conn_zone $library_remote_addr zone=addr:10m;
limit_req_zone $binary_remote_addr zone=one:10m rate=30r/m;

server {
        #...
        location /store/ {
                limit_conn addr 10;
                #...
        }
        #...
        location /login.html {
                limit_req zone=one;
        #...
        }
        client_body_timeout 5s;
        client_header_timeout 5s;
        #...
}

event {
        worker_connection 100000;
}
```

Gambar 19. Penambahan Konfigurasi

Konfigurasi ini menggunakan **limit_conn_zone** dan **limit_req_zone** untuk mengatur zona koneksi dan zona permintaan yang akan digunakan untuk membatasi jumlah koneksi dan permintaan. Di dalam blok **server**, konfigurasi **location** diterapkan untuk menerapkan pembatasan koneksi **limit_conn** pada alamat IP tertentu dan pembatasan permintaan **limit_req** pada zona tertentu. Peneliti juga menambahkan pengaturan *timeout* untuk *body* dan *header* klien dengan nilai 5 detik untuk mencegah koneksi yang tidak aktif terlalu lama. Terakhir, peneliti menentukan jumlah koneksi maksimum yang diizinkan oleh NGINX dengan perintah **worker_connection 100000**.

Restart NGINX

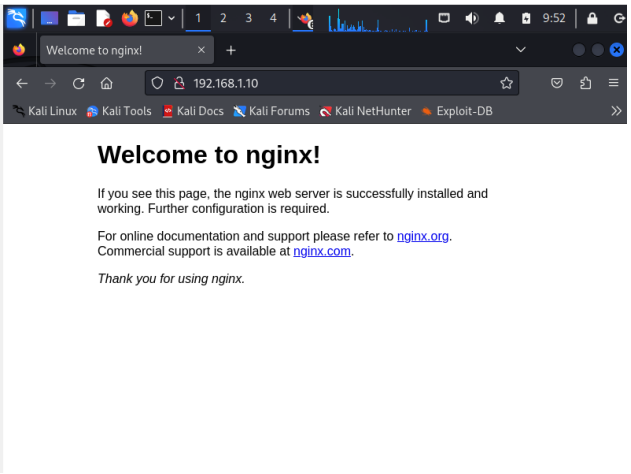
Setelah menambahkan konfigurasi tersebut, peneliti merestart NGINX untuk menerapkan perubahan dengan menggunakan perintah **systemctl restart nginx**.

```
mint@mint:/etc/nginx$ systemctl restart nginx
mint@mint:/etc/nginx$
```

Gambar 20. Restart NGINX

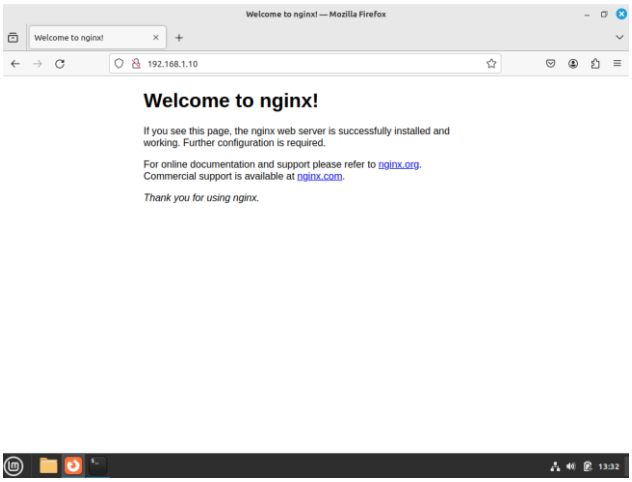
Pada **Gambar 21** dan **22** merupakan hasil pengujian menunjukkan bahwa setelah penerapan konfigurasi tersebut, server NGINX menjadi lebih tahan terhadap serangan Slowloris. Hal ini membuktikan bahwa langkah-langkah pencegahan yang diterapkan efektif dalam mengurangi dampak serangan Slowloris, menjaga ketersediaan layanan, dan memastikan bahwa server tetap dapat melayani permintaan pengguna secara optimal. Dengan demikian, penerapan konfigurasi ini merupakan langkah penting dalam melindungi infrastruktur web dari ancaman serangan DDoS yang terus berkembang.

Kali Linux:



Gambar 21. Tampilan Kali Linux (2)

Linux Mint:



Gambar 22. Tampilan Linux Mint (2)

Simpulan

Penelitian ini berhasil menunjukkan bahwa langkah-langkah pencegahan seperti konfigurasi *firewall*, pembatasan jumlah koneksi, dan pengaturan *timeout* pada server NGINX di Linux Mint dapat secara signifikan mengurangi dampak serangan DDoS tipe Slowloris. Melalui eksperimen yang melibatkan Kali Linux sebagai mesin penyerang dan

Linux Mint sebagai target, ditemukan bahwa penerapan konfigurasi pencegahan tersebut mampu meningkatkan ketahanan server terhadap serangan, mempertahankan ketersediaan layanan, dan mengurangi beban sumber daya yang diakibatkan oleh koneksi HTTP lambat yang terus-menerus. Hasil ini menggarisbawahi pentingnya penerapan langkah-langkah keamanan yang proaktif untuk melindungi sistem dari ancaman DDoS yang terus berkembang.

Daftar Pustaka

Andria. 2020. Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux. Gener. J. 4(2):69–76.

Arief M, Trisnawan PH, Data M. 2024. Implementasi Sistem Deteksi Serangan Slowloris pada Arsitektur Jaringan Software-Defined Network Menggunakan Random Forest. J. Pengemb. Teknol. Inf. dan Ilmu Komput. 8(3):1–10.

Arman M. 2020. Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack. JATISI (Jurnal Tek. Inform. dan Sist. Informasi). 7(1):56–70.doi:10.35957/jatisi.v7i1.284.

Ernawati T, Rachmat FFF. 2021. Keamanan Jaringan dengan Cowrie Honeypot dan Snort Inline-Mode sebagai Intrusion Prevention System. J. RESTI (Rekayasa Sist. dan Teknol. Informasi). 5(1):180–186.doi:10.29207/resti.v5i1.2825.

Faisal I, Handoko D, Putra H. 2024. Penerapan Metode Rule Based Dalam Mendeteksi Serangan Multi Attack Pada Network Attached Storage. J. Komput. Teknol. Inf. dan Sist. Inf. 2(3):545–560.doi:10.62712/juktisi.v2i3.138.

Hendrayadi, Kustati M, Sepriyanti N. 2023. Mixed methode research. J. Rev. Pendidik. dan Pengajaran. 6(4):2402–2410.

Hilmi MA Al, Herdiyanti F, Burjulius R, Lena S. 2024. Pengujian Keamanan Sistem Operasi Linux Studi Kasus : Celah Keamanan FTP pada Metasploitable2. IKRA-ITH Inform. J. Komput. dan Inform. 8(1):110–115.doi:10.37817/ikraith-informatika.v8i1.3205.

Jaya IKNA, Dewi IAU, Mahendra GS. 2022. Implementation of Wireshark Application in Data Security Analysis on LMS Website. J. Comput. Networks, Archit. High Perform. Comput. 4(1):79–86.doi:10.47709/cnahpc.v4i1.1345.

Kestina L, Yuhandri, Nurcahyo GW. 2023. Penanganan Celah Keamanan Website dengan Ethical Hacking dan Issaf Menggunakan Acunetix Vulnerability (Studi Kasus di Bkpsdmd Kabupaten Kerinci). Innov. J. Soc. Sci. Res. 3(4):9192–9203.

Kurniabudi, Harris A, Rosanda E. 2022. Optimalisasi Seleksi Fitur Untuk Deteksi Serangan Pada IoT Menggunakan Classifier Subset Evaluator. JURIKOM (Jurnal Ris. Komputer). 9(4):885.doi:10.30865/jurikom.v9i4.4618.

Mardianto I, Sugiarto D, Ashari KA. 2022. The Elastic Stack Ability Test To Monitor Slowloris Attack on Digital Ocean Server. Ultim. J. Tek. Inform. 13(2):120–126.doi:10.31937/ti.v13i2.2209.

Nam SY, Djuraev S. 2014. Defending HTTP web servers against DDoS attacks through busy period-based attack flow detection. KSII Trans. Internet Inf. Syst. 8(7):2512–2531.doi:10.3837/tiis.2014.07.018.

Nisa F, Ramadona S. 2023. Sistem Pencegahan Serangan Distributed Denial Of Service Pada Jaringan SDN. J. Sistim Inf. dan Teknol. 5(3):1–8.doi:10.60083/jsisfotek.v5i3.269.

Rios VDM, Inácio PRM, Magoni D, Freire.Mário M. Detection of Slowloris Attacks using Machine Learning Algorithms. ACM J. 1(1):1321–1330.doi:10.1145/3605098.3635919.

Sabri S, Ismail N, Hazzim A. 2021. Slowloris DoS Attack Based Simulation. IOP Conf. Ser. Mater. Sci. Eng. 1062(1).doi:10.1088/1757-899X/1062/1/012029.

Sari N, Amnur H, Hidayat R. 2020. Monitoring next cloud sebagai private cloud storage dengan notifikasi telegram. J. Ilm. Teknol. Sist. Inf. 1(4):144–149.

Selvaraj V. 2018. Distributed Denial of Service Attack Detection, Prevention and Mitigation Service on Cloud Environment. J. Comput. Eng. Inf. Technol. 07(03).doi:10.4172/2324-9307.1000205.

Suharti S, Yudhana A, Riadi I. 2022. Forensik Jaringan DDoS menggunakan Metode ADDIE dan HIDS pada Sistem Operasi Proprietary. MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput. 21(3):567–582.doi:10.30812/matrik.v21i3.1732.

Sumar MR, Wahid A, Parenreng JM. 2024. Sistem Keamanan Jaringan Terhadap Serangan DOS (Denial Of Service) Menggunakan Snort Dan Firewall Berbasis Linux OS. Pinisi J. Sciene Techonolgy. 0:1–15.

W Y, Yuliadi, Hamdani F, Fitriana YB, Oper N. 2023. Analisis Keamanan Website Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology (NIST). KLIK Kaji. Ilm. Inform. dan Komput. 3(6):1296–1302.doi:10.30865/klik.v3i6.830.

Wijayanti RA, Firdaus RA, Putra NBN, Kardian AR. 2023. Analisis Perbandingan Penggunaan Kali Linux pada Windows Subsystem for Linux (WSL) dan VirtualBox terhadap OpenSSL Benchmark Testing. J. Educ. 06(01):10146–10154.

Yudhana A, Riadi I, Suharti S. 2021. Distributed Denial of Service (DDoS) Analysis on Virtual Network and Real Network Traffic. J. Informatics Telecommun. Eng. 5(1):112–121.doi:10.31289/jite.v5i1.5344.

Yuniarti DR, Alfarizy HF, Siallagan Z, Rizkyanfi MW. 2023. Analisis Potensi Dan Strategi Pencegahan Cyber Crim Dalam Sistem Logistik Di Era Digital. J. Bisnis, Logistik dan Supply Chain. 3(1):23–32.doi:10.55122/blogchain.v3i1.714.

Yusnanto T, Wahyudiono S, Wicaksono HA. 2022. Analisa Kinerja Sistem Operasi Windows 10 Dengan Linux Mint Menggunakan Aplikasi Zxt Cam, Gnome System Monitor. SENTRI J. Ris. Ilm. 1(2):288–296.doi:10.55681/sentri.v1i2.210.