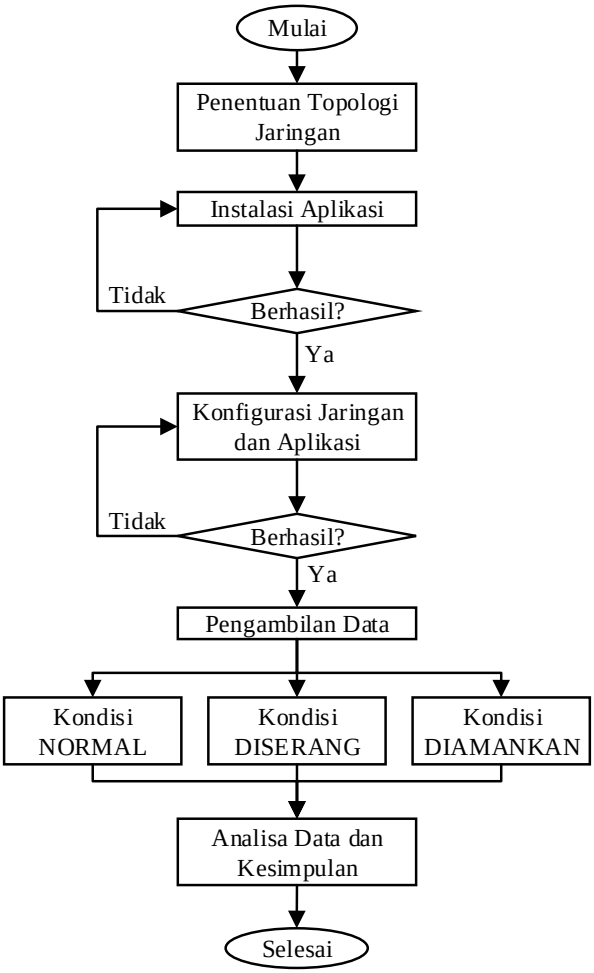
BAB 3
METODE PENELITIAN

3.1 ALUR PENELITIAN

Penelitian ini memiliki tujuan untuk membuat sistem keamanan jaringan yang dapat mengatasi serangan DDOS yang mengandalkan sistem pengaturan lalu lintas dari *firewall* menggunakan *iptables* dan *Proxy Server* menggunakan *Squid*. Alur ini terdiri dari penentuan topologi jaringan yang akan dibangun, pemasangan aplikasi yang dibutuhkan, konfigurasi jaringan dan aplikasi yang digunakan, pengambilan data, serta analisa dari data yang sudah diperoleh.



Gambar 3. 1 Diagram alur penelitian

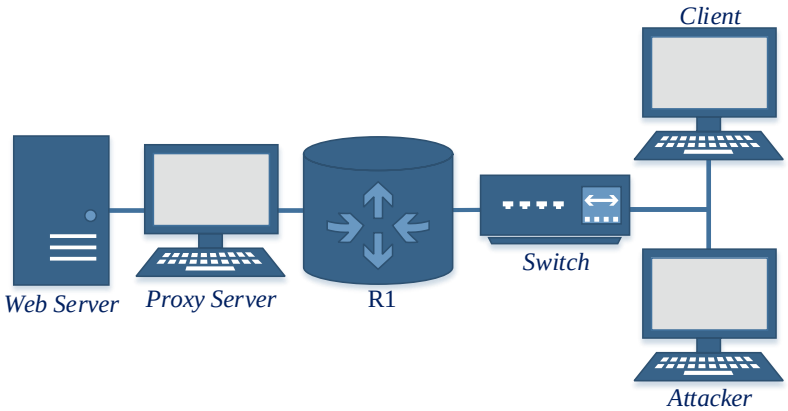
Pada gambar 3.1 menunjukan alur diagram dari perancangan sistem pada penelitian ini. Dimulai dengan tahap menentukan topologi jaringan yang dibangun, lalu pemasangan aplikasi yang dibutuhkan seperti *Apache2*, *Bind9*, *Quagga*, *Squid*

serta LOIC. Tahap selanjutnya dilanjutkan dengan mengatur jaringan dan aplikasi yang digunakan hingga bekerja dengan baik tanpa ada gangguan. Selanjutnya yaitu tahap pengambilan data yang diambil dari 3 kondisi pengujian yaitu normal (akses *web server* sebelum serangan DDOS diluncurkan), kondisi diserang (akses *web server* saat serangan DDOS sedang berlangsung), dan kondisi diamankan (akses *web server* saat serangan DDOS diblokir sistem keamanan).

Setelah hasil data diperoleh pada pengujian akses menuju *web server* target selanjutnya dilakukan analisis terhadap data tersebut. Analisis yang dilakukan bertujuan untuk mengetahui bentuk serangan DDOS yang dilakukan oleh aplikasi LOIC serta menangani serangan yang terjadi pada *web server* target guna menimalisir atau bahkan memutus serangan tersebut. Dampak yang diakibatkan oleh serangan tersebut dapat dilihat pada segi *availability* keamanan jaringan yang meliputi parameter *delay*, *packet loss* dan *troughput* dari akses yang dilakukan menuju *web server* target dan serangan diluncurkan secara bersamaan.

3.2 TOPOLOGI JARINGAN

Topologi jaringan yang dibangun pada penelitian ini dapat dilihat pada gambar 3.2 yang terdiri dari satu unit perangkat *Web Server* sebagai pengendali layanan *website* target, satu unit perangkat *Proxy Server* yang digunakan sebagai pusat pengendali keamanan akses menuju *web server* target, satu unit *router* sebagai perangkat *routing* dari komunikasi yang diposisikan berada di jaringan *Attacker* dan satu unit *Client* yang mengakses layanan dari *web server* serta satu unit *attacker* sebagai perangkat yang melakukan serangan *denial of service* menuju *web server* target.



Gambar 3. 2 Topologi jaringan penelitian

Semua perangkat dijalankan dan dihubungkan secara *inline* melewati virtualisasi dengan menggunakan aplikasi GNS3 melalui *interface Fast-Ethernet*. Virtualisasi *server* dan *attacker* dijalankan menggunakan aplikasi *VirtualBox*. Untuk *server* digunakan sistem operasi *Debian* 8.11 dengan aplikasi *web server* yang digunakan adalah *Apache2* dan aplikasi *proxy server* yang digunakan adalah *Squid3*. Protokol *routing* yang digunakan adalah *Open Shortest Path First* (OSPF) yang dikonfigurasikan pada perangkat *proxy server* dan *router*. Semua konfigurasi IP dilakukan secara manual (*static*) dan alokasi pengalamatan ditunjukan pada tabel 3.1.

Tabel 3. 1 Alokasi pengalamatan IP perangkat

Perangkat	*Interface*	Alamat IP
Web Server	*eth0*	10.10.10.1/24
Proxy Server	*eth0*	10.10.10.2/24
	eth1	20.20.20.1/24
R1	*FastEthernet0/0*	20.20.20.2/24
	FastEthernet0/1	192.168.1.1/24
Client	*FastEthernet*	192.168.1.2/24
Attacker	*FastEthernet*	192.168.1.3/24

Web Server menggunakan alamat 10.10.10.1/24 pada *interface eth0* yang terhubung langsung menuju *interface eth0* dari perangkat *Proxy Server* dengan alamat 10.10.10.2/24. Sedangakan *interface eth1 Proxy Server* dengan alamat 20.20.20.1/24 terhubung langsung menuju *FastEthernet0/0* dari perangkat R1 dengan alamat 20.20.20.2/24. *Interface FastEthernet0/1* dari R1 yang beralamat 192.168.1.1/24 terhubung dalam satu jaringan dengan *Client* di alamat 192.168.1.2/24 dan *Attacker* di alamat 192.168.1.3/24 menggunakan *switch*.

3.3 PEMASANGAN DAN KONFIGURASI APLIKASI

Perangkat *server* membutuhkan beberapa aplikasi untuk dijalankan sebagai penyedia layanan maupun utilitas pembangun sistem keamanan jaringan. Perangkat *Web Server* menggunakan aplikasi *Apache2* dalam melakukan konfigurasi layanan *web*. Perangkat *Proxy Server* menggunakan beberapa aplikasi, yaitu *Squid* sebagai aplikasi layanan *proxy* yang mengatur akses dari *Client* maupun *Attacker*, *iptables* sebagai aplikasi pengatur *firewall* yang bekerja sama dengan *Squid* agar akses *Client* maupun *Attacker* selalu tersaring saat adanya akses menuju alamat tujuan

serta *Bind9* sebagai aplikasi yang menerjemahkan alamat domain dari *web server* target (*Domain Name System Server*). Berikut langkah instalasi dan konfigurasi aplikasi tersebut.

3.3.1 KONFIGURASI *WEB SERVER*

Apache2 dipasang dan dikonfigurasi pada perangkat *web server* sebagai penyedia layanan setiap akses *web* yang dilakukan oleh *Client* maupun *Attacker* dalam bentuk halaman *web*.

```
#apt-get install apache2
#nano /etc/apache2/sites-available/000-default.conf
```

Ubah konfigurasi menjadi:

```
ServerName webskripta.com
ServerAdmin admin@webskripta.com
DocumentRoot /var/ww/html

#a2ensite 000-default.conf
#/etc/init.d/apache2 restart
```

3.3.2 KONFIGURASI *DOMAIN NAME SYSTEM SERVER*

Bind9 dipasang dan dikonfigurasi pada perangkat *Proxy Server* yang digunakan sebagai aplikasi untuk menerjemahkan alamat tautan domain milik *web server* tujuan (DNS *Server*) untuk diakses oleh *Client* maupun *Attacker* melalui *web browser*.

```
#apt-get install bind9
#nano /etc/bind/named.conf.default-zones
```

Tambahkan baris berikut:

```
zone "webskripta.com" {
type master;
file /etc/bind/db.webskripta:};
zone "10.10.10.in-addr.arpa"{
type master;
file /etc/bind/db.10";};

#cp /etc/bind/db.local /etc/bind/db.webskripta
#cp /etc/bind/db.127 /etc/bind/db.10
#nano db.local
```

Ubah dan tambahkan baris berikut:

```
webskripta.com root.webskripta.com.
@ IN NS webskripta.com.
@ IN A 10.10.10.1
#nano db.10
```

Ubah dan tambahkan baris berikut:

```
webskripta.com root.webskripta.com.
@ IN NS webskripta.com.
1 IN PTR webskripta.com.

#nano /etc/resolv.conf
```

Tambahkan baris berikut:

```
nameserver 20.20.20.1

#/etc/init.d/bind9 restart
#dig webskripta.com
#nslookup webskripta.com
```

3.3.3 KONFIGURASI *FIREWALL*

Konfigurasi *firewall* dijalankan dengan tujuan untuk melakukan proses *filtering* (penyaringan) terhadap semua akses yang dilakukan *Client* maupun *Attacker* menuju ke alamat jaringan perangkat *Proxy Server* dan *Web Server*.

```
#nano firewall
```

Tambahkan baris berikut

```
iptables –I OUTPUT –p tcp –m multiport --dport 22,25,111
–s 192.168.1.0/24 –j DROP
iptables –I INPUT –p tcp –tcp-flags ALL SYN --dport 80 –s
192.168.1.0/24 –j DROP
iptables –I INPUT –p icmp –s 192.168.1.0/24 –d
10.10.10.0/24 –j DROP
iptables –I FORWARD –p tcp –tcp-flags ALL SYN --dport 80
–s 192.168.1.0/24 –d 10.10.10.0/24 –j DROP
iptables –I FORWARD –p icmp –j DROP

#bash firewall
```

3.3.4 KONFIGURASI *PROXY SERVER*

Squid dipasang dan dikonfigurasi pada perangkat *Proxy Server* yang digunakan sebagai penyedia layanan *proxy* pengatur akses jaringan menuju *web server* target.

```
#apt-get install squid3
#nano /etc/squid3/squid.conf
```

Cari dan ubah konfigurasi menjadi:

```
cache_mgr webskripta.com
visible_hostname admin
```

Cari *ACL CONNECT* dan tambahkan baris berikut:

```
acl lan src 192.168.1.0/24
acl aksesport port 80
acl key url_regex –i "/etc/squid3/url"
```

```
http_access deny key
http_access allow aksesport
http_access allow lan
http_access deny all

#/etc/init.d/squid3 reload
#/etc/init.d/squid3 restart
#nano /etc/sysctl.conf
```

Ubah baris berikut:

```
net.ipv4.ip_forward=1
```

3.4 SKENARIO PENGUJIAN

Pada penilitian ini akan dibandingkan performa jaringan yang berpengaruh pada beberapa kondisi keamanan jaringan tertentu pada saat sebelum dan juga serangan sedang diluncurkan menuju ke alamat *web server* tujuan.

Tabel 3. 2 Skenario pengujian

Waktu	Layanan	Variabel Kondisi
3 Menit	*Web Server* (HTTP)	Akses Sebelum Serangan dan Tanpa Keamanan
		Akses Saat Peluncuran Serangan Tanpa Keamanan
		Akses Saat Keamanan Berjalan dan Serangan Berjalan

Tabel 3.2 menjelaskan bagaimana skenarion pengujian yang dilakukan berdasarkan waktu, layanan yang digunakan, dan variabel kondisi yang ditetapkan. Pengujian dilakukan terhadap segi keamanan jaringan pada sisi *availability* dengan melihat beberapa parameter seperti delay, *throughput* dan *packet loss* pada protokol TCP dengan menggunakan jumlah serangan DDOS yang dilakukan sebesar 400000 *zombie* berdasarkan variasi penulis. Pengujian dilakukan selama 3 menit untuk melihat pengaruh serangan pada akses menuju *web server* target saat sebelum dan selama *proxy* diaktifkan berdasarkan pada parameter QOS yang digunakan serta bentuk serangan DDOS yang diluncurkan oleh *attacker*. Pengambilan data dilakukan pada jalur *web server* menuju *proxy server*. Hasil akhir yang didapat merupakan rata-rata dari 30 hasil percobaan untuk tiap kondisinya.