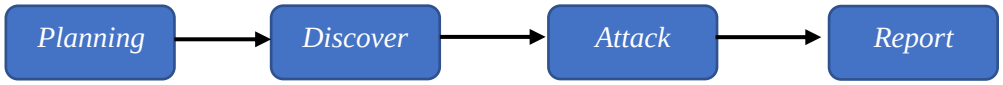
BAB III

METODOLOGI

3.1 Metodologi Penelitian

Alur dari pengerjaan penelitian ini adalah seperti pada gambar 3.1



Gambar 3.1 Tahapan Metodologi

3.2 Tahap *Planning*

Tahapan *planning* menyiapkan *hardware* dan *software* yang akan digunakan dalam melakukan peretasan *MAC address cloning* pada *filtering MAC address*. Menyiapkan topologi jaringan internet yang akan digunakan. Membuat keamanan *filtering MAC address* berbasis *voucher wifi* menggunakan mikhmon yang di koneksikan dengan mikrotik, pengujian keamanan *filtering MAC addres*s mengkoneksikan dengan *smarphone.*

Membuat flowchart alur *log in smartphone* menggunakan voucher *WIFI* dengan kemanan *filtering MAC address*. Meyiapkan meida Peretasan *MAC address cloning* menggunakan *smartphone* sebagai media peretasan dengan menjalankan t*ools* busybox pro, netcut, change my mac dan terminal emulator.

3.3 Tahap *Discovery*

Celah pada keamanan jaringan *filtering MAC address* yang hanya melakukan *filter MAC address* yang diizinkan untuk mengakses suatu jaringan dan sistem keamanan *filtering MAC add*ress tidak bisa membedakan dua *MAC address* yang sama merupakan celah yang dapat diretas dengan metode penyerangan *MAC*

address cloning dan terdapat celah keamanan pada *log in* akses internet menggunakan voucher yang mampu dilewati oleh jenis penyerangan *MAC address cloning*.

3.4 Tahap *Attack*

Tahapan *attack* mengizinkan akses dan menjalankan tools busybox pro, netcut, change my mac, dan terminal emulator pada *superuser smarphone root*. Melakukan pengecekan *tools* sudah terinstall dengan terminal emulator, menjalankan pengujian serangan dengan tahapan mencari *MAC address* target yang terhubung pada jaringan internet menggunakan netcut, kemudian melakukan copy *MAC address* target menggunakan tools change my mac.

Tahapan selanjutnya di bagian *attack* memecahkan rumusan masalah pada penelitian ini, yaitu mengantisipasi serangan *MAC address cloning* dengan melakukan pematauan di *ARP list* pda mikrotik untuk mendetaksi *MAC address* yang sedang melakukan *cloning* dan melakukan pemblokiran *MAC address* pada *firewall* di mikrotik, serta menjelaskan integrasi *ARP list* dan *firewall* sebagai metode untuk melakukan antisipasi penyerangan *MAC address cloning*.

3.5 Tahap *Reporting*

Melaporkan hasil pengujian serangan *MAC address cloning* menggunakan *smartphone* berupa pengujian *tools smarphone* yang digunakan untuk melakuka serangan *MAC address cloning*, melaporkan cara kerja *MAC address cloning* yang mempu melewati keamanan *filtering MAC address*, melaporkan hasil pemantauan *ARP list* sebagai pendeteksi serangan *MAC address cloning* dengan memaparkan hasil pemantauan *packet lost* pada perangkat yang belum di *cloning* dan sudah di *cloning* sebanyak 10 kali pengujian.

Menjelaskan alur data perangkat yang melakukan *cloning MAC address* dilakukan cek tabel *ARP* dengan cara smarphone melakukan *cloning* pada laptop dan menjalankan perintah di cmd untuk mengetahui alur data keluar dari perangkat yang melakukan *MAC address cloning.* Memaparkan hasil penanganan *MAC address cloning* menggunakan *firewall.*