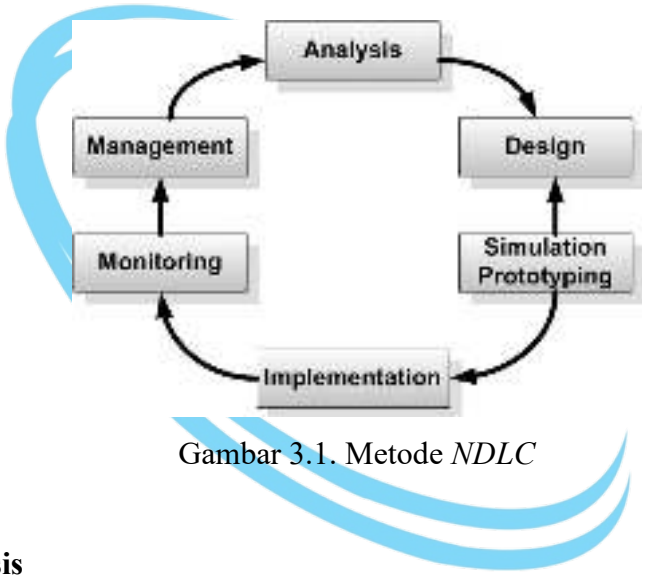
BAB III
METODE PENELITIAN

3.1. Metode

Pada penelitian ini penulis menggunakan metode pengembangan sistem *NDLC* (*Network Development Life Cycle*). *NDLC* merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya dan merupakan teknik analisis terstruktur yang digunakan untuk merencanakan dan mengelola proses pembangunan sistem. *NDLC* memiliki beberapa tahapan diantaranya *analysis*, *design*, *simulation prototyping*, *implementation*, *monitoring*, dan *management*.



Gambar 3.1. Metode *NDLC*

3.1.1. Analysis

Pada tahapan ini penulis melakukan analisis kebutuhan dan permasalahan yang ada pada sistem *server* untuk mendukung proses kelancaran pada penelitian dengan cara melakukan wawancara dan *survey* ke tempat permasalahan atau kelapangan langsung.

1. Wawancara

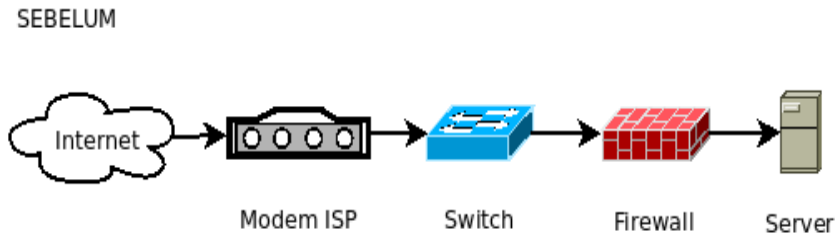
   Pada tahap wawancara, penulis melakukan tanya jawab dengan narasumber atau atasan langsung yang berkaitan dengan sistem *server*. Daftar pertanyaan dan pendukung lainnya dapat dilihat pada daftar lampiran.

2. *Survey*

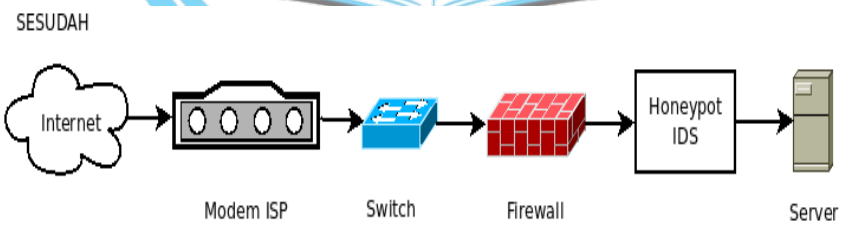
   Pada tahap *survey,* penulis melakukan pengamatan langsung ketempat atau ruang *server* berada untuk mengetahui permasalah yang ada pada sistem *server* dilokasi tersebut.

3.1.2. Design

Pada tahap ini penulis membuat topologi jaringan *server* yang sudah ada sebelumnya pada sistem *server*, yang kemudian akan dibangun sistem keamanan *server* yang baru.



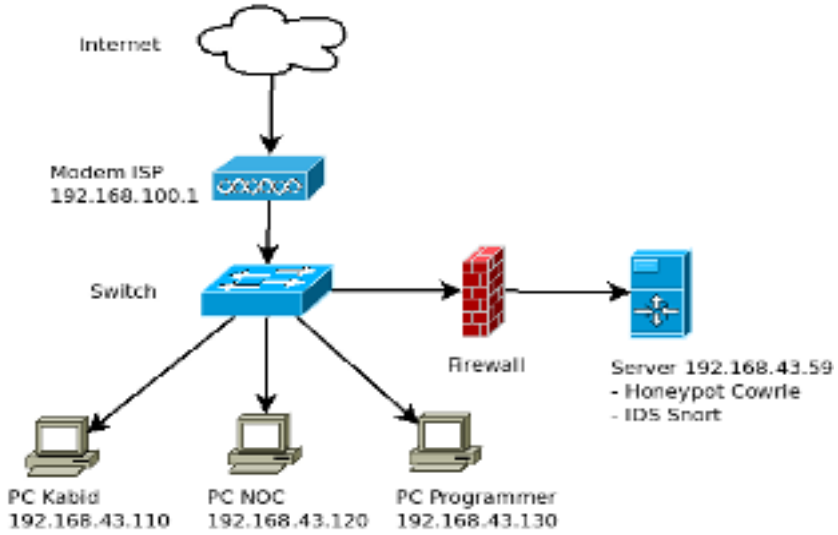
Gambar 3.2. Topologi Jaringan *Server* Sebelumnya



Gambar 3.3. Topologi Jaringan *Server* Baru

3.1.3. Simulation Prototyping

Pada tahap ini yaitu membangun sebuah topologi jaringan *server* yang akan dibangun pada sistem keamanan *server* baru. Tahap ini bertujuan untuk membangun sistem keamanan dan mengimplementasikan sistem tersebut pada *server* yang akan dibangun.



Gambar 3.4. Simulasi Jaringan *Server* Baru

3.1.4. Implementation

Setelah tahap *design* dan *simulation prototype* dilakukan, tahap selanjutnya yaitu implementasi pada sistem keamanan *server*. Tahap ini penulis menerapkan sistem keamanan *server* baru yang telah dibangun. Pada tahap ini akan terlihat bagaimana sistem yang telah dibangun akan memberikan pengaruh dan hasil yang berbeda dari sistem sebelumnnya.

3.1.5. Monitoring

Pada tahap ini yaitu melakukan *monitoring* terhadap sistem keamanan *server* yang telah dibuat, proses *monitoring* dapat dilakukan dengan cara pemantauan langsung terhadap sistem keamanan server dengan menggunakan *web dashboard* pada *kippo graph* yang telah dibangun dan diimplementasikan pada sistem keamanan server baru.

Gambar 3.5. *Web Dashboard Monitoring Kippo Graph*

3.1.6. Management

Tahap *management* merupakan sebuah aturan tahap pemeliharaan dan perawatan yang dibuat untuk keberlangsungan sistem keamanan jaringan *server* yang telah dibangun, supaya sistem keamanan yang dibangun dapat berlangsung lama dan berjalan baik. Daftar aturan pemeliharan sistem keamanan *server* dapat dilihat pada daftar lampiran.

3.2. Peralatan Penelitian

Peralatan yang digunakan dalam penelitian ini berupa perangkat keras dan perangkat lunak .

3.2.1. Perangkat Keras

Untuk mendukung berjalannya perangkat lunak atau *software,* maka dibutuhkan perangkat keras atau *hardware* untuk mendapatkan informasi yang sesuai dengan yang diharapakan. Adapun perangkat keras yang digunakan adalah :

1. Raspberry Pi
2. Laptop
3. Handphone
4. SD Card
5. Power Adapter
6. Keyboard
7. Mouse
8. HDMI
9. Monitor

3.2.2. Perangkat Lunak

Perangkat lunak atau *software* yang digunakan adalah :

1. Nmap
2. Hydra dan Medusa
3. Putty
4. Raspbian OS

3.3. Lokasi dan Waktu Penelitian

Lokasi penelitian ini dilakukan bertempat di :

Tempat : Dinas Komunikasi Informatika Persandian dan Statistik
Alamat : Komplek Perkantoran Pemerintahan Kabupaten Bekasi
Desa : Sukamahi
Kecamatan : Cikarang Pusat
Kabupaten : Bekasi 17530

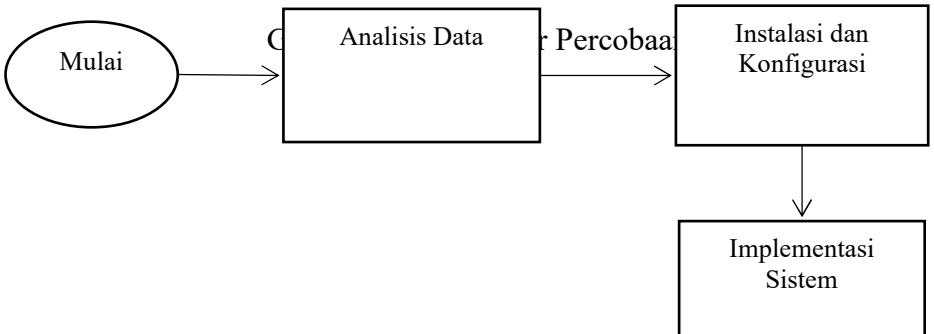
Waktu penelitian dilakukan selama 5 (lima) bulan, dengan rincian dapat dilihat pada tabel 3.1. waktu penelitian dibawah ini :

Tabel 3.1. Waktu Penelitian

No.	Keterangan	Waktu Penelitian				
		Desember	Januari	Februari	Maret	April
1.	Identifikasi Masalah					
2.	Penetapan Tujuan					
3.	Observasi dan Studi Pustaka					
4.	Penyelesaian Masalah					
5.	Penelitian					
6.	Implementasi Sistem					
7.	Pengujian					

3.4. Prosedur Percobaan

Pada prosedur percobaan penelitian, dilakukan beberapa tahapan proses penelitian, dengan rincian dapat dilihat pada gambar 3.1. prosedur percobaan dibawah ini :



Prosedur percobaan penelitian ini yaitu :

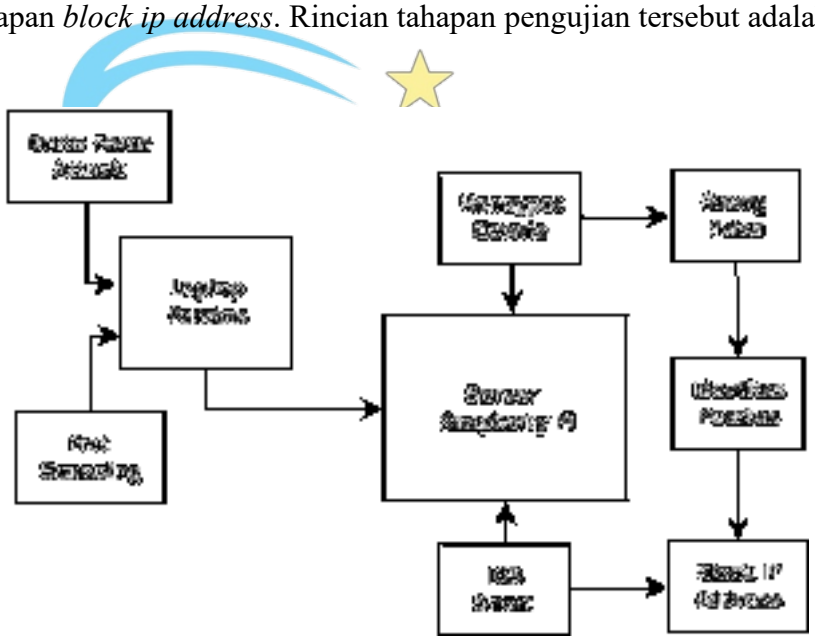
1. Tahap analisis data adalah, proses pengumpulan data mulai dari bahan penelitian hingga peralatan penelitian yang digunakan
2. Tahap instalasi dan konfigurasi adalah proses instalasi dan konfigurasi *tools* yang digunakan pada *server* raspberry pi.
3. Tahap implementasi sistem adalah penerapan sistem yang digunakan pada *server* raspberry pi setelah melalui proses instalasi dan konfigurasi terlebih dahulu.
4. Pada tahap pengujian adalah proses implementasi dan pengujian dari alat hingga sistem pada *server* raspberry pi.
5. Setelah proses pengujian dilakukan, maka penelitian dikatakan berhasil.

3.5. Instalasi dan Konfigurasi

Tahap instalasi dan konfigurasi, penulis melakukan pemasangan sistem keamanan yang digunakan pada *server* raspberry pi, sistem keamanan yang digunakan untuk implementasi sistem keamanan *server* adalah *honeypot cowrie* dan *IDS snort* yang berfungsi untuk menjebak peretas seolah-olah berhasil membobol dan masuk kedalam *server* asli, padahal sebenarnya hanya ruang atau *server* palsu.

3.6. Pengujian

Pengujian pada penelitian sistem ini dilakukan dengan melakukan uji penyerangan ke *server* raspberry pi, dengan melakukan 2 jenis teknik serangan dan 1 tahapan *block ip address*. Rincian tahapan pengujian tersebut adalah :



Gambar 3.7. Implementasi Sistem *Honeypot Cowrie* dan *IDS Snort*

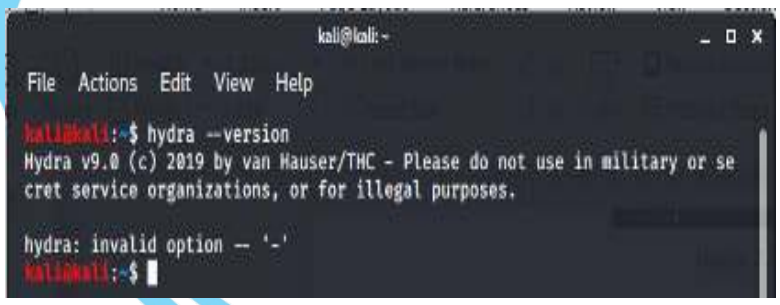
1. Peretas melakukan 2 jenis serangan terhadap *server* raspberry pi menggunakan *tools nmap* untuk *port scanning* dan *tools hydra* dan *medusa* untuk melakukan serangan *brute force attack.*
   a. *Port Scanning*

      Tahap pertama adalah melakukan *port scanning* terhadap *server* target dengan menggunakan *port scanning*.

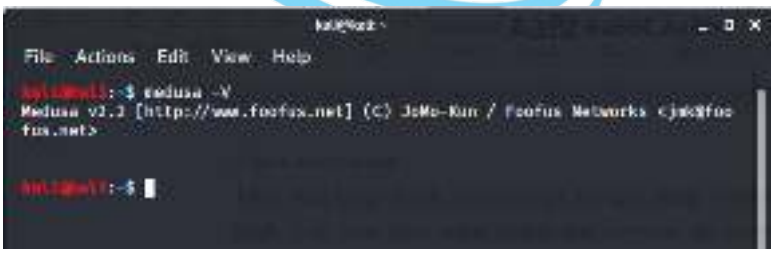
Gambar 3.8. *Tools Nmap*

b. *Brute Force Attack*

Tahap yang kedua adalah melakukan uji serangan dengan melakukan teknik *brute force attack* untuk mendapatkan *username* dan *password server* target dengan percobaan semua kunci yang dibuat secara acak. *Tools* yang digunakan untuk melakukan serangan dengan teknik *brute force attack* ini adalah *hydra* dan *medusa*.



Gambar 3.9. *Tools Hydra* di Kali Linux



Gambar 3.10. *Tools Medusa* di Kali Linux

Pada tahapan penelitian dengan menggunakan teknik *brute force attack* ini dilakukan dengan beberapa tahapan pengujian dengan kombinasi *password*, diantaranya penyerangan dengan menggunakan *password* alfabet, numerik dan karakter campur dengan menggunakan *tools hydra* dan *medusa* terhadap *server* target.

2. *Honeypot cowrie* membuat ruang palsu untuk menjebak peretas kedalam *server* buatan atau bukan *server* yang sebenarnya.
3. Peretas berhasil terjebak oleh *server* yang dibuat oleh *honeypot cowrie.*
4. Identitas peretas berhasil didapatkan atau berhasil di rekam oleh *honeypot cowrie* dan *IDS snort* saat peretas sedang melakukan aktifitas *hacking* tanpa sepengetahuan peretas tersebut.
5. Setelah identitas peretas berhasil didapatkan, selanjutnya adalah melakukan *block ip address* peretas supaya tidak bisa melakukan serangan kembali yang dapat menyebabkan *server down* atau *overload* karena kelebihan paket yang dikirimkan oleh peretas atau *attacker*.