BAB III

METODE PENELITIAN

3.1. Objek Penelitian

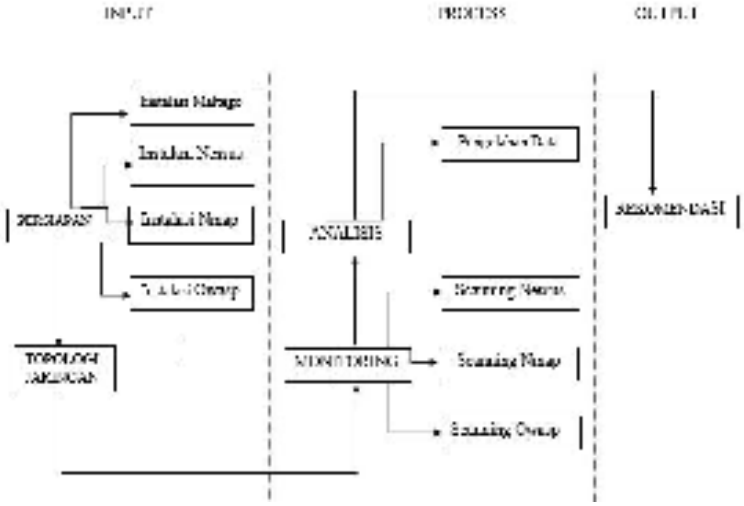
Penelitian ini mengambil objek penelitian di Universitas Buana Perjuangan Karawang (UBP) Karawang dengan memeriksa *web server* SIPT (Sistem Informasi Perguruan Tinggi) yaitu http://sipt2.ubpkarawang.ac.id dengan menggunakan *tools* nessus, nmap, owasp, maltego dan *web browser* serta melakukan wawancara terhadap penanggungjawab web SIPT yaitu Adi Rizky Pratama, M.Kom . Salah satu data yang diperoleh dalam tahap ini adalah mengenai grafik ancaman terhadap SIPT UBP Karawang serta data jumlah ancaman terhadap SIPT UBP Karawang seperti berikut ini:

Gambar 3. 1 Grafik Ancaman Terhadap SIPT UBP Karawang Juli 2021
(Sumber: PUSDATIN SIPT UBP Karawang)

Gambar 3. 2 Data Jumlah Ancaman Terhadap SIPT UBP Karawang
(Sumber: PUSDATIN SIPT UBP Karawang)

3.2. Prosedur Penelitian

Pada tahapan ini menggambarkan bagaimana tahapan penelitian Analisisis *Vulnerability* pada SIPT Universitas Buana Perjuangan Karawang dilakukan. Dalam metode ini menggunakan bagan alur kerjanya. Alur dalam penelitian ini seperti pada Gambar 3.3



Gambar 3. 3 Tahapan dalam penelitian
(Sumber: Penulis)

Penjelasan dari gambar adalah sebagai berikut:

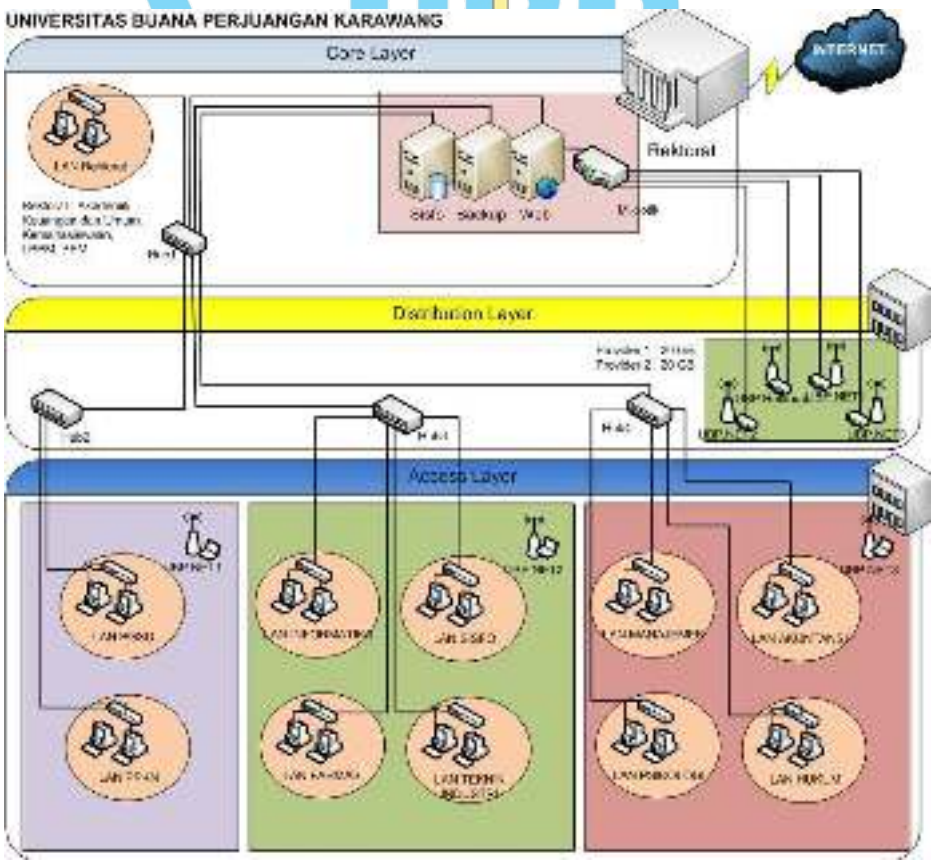
3.2.1. Persiapan

Pada tahap persiapan ini peneliti melakukan instalasi *Software* (perangkat lunak) yang diperlukan. *Tool* yang akan kita instal adalah *tool* Maltego, *tool* Nessus, kemudian *tool* Nmap dan terakhir adalah *tool* Owasp.

3.2.2. Topologi Jaringan

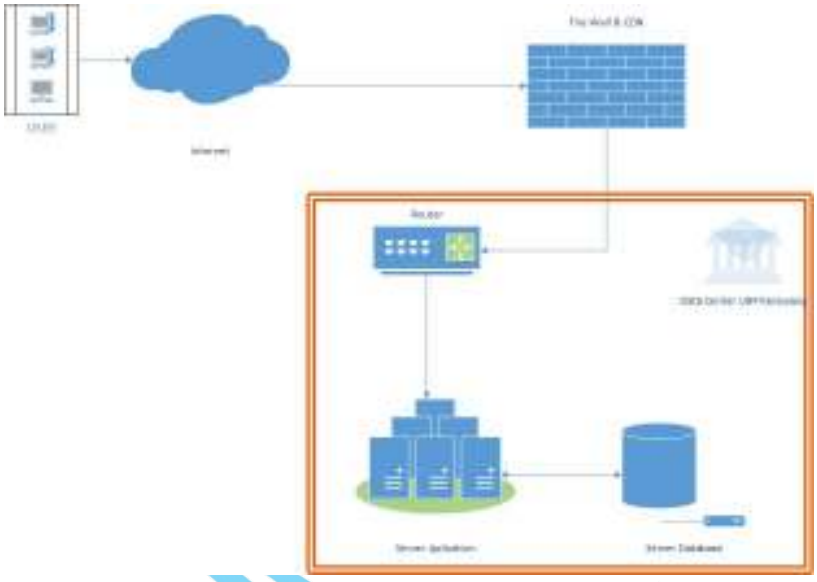
Tahap ini akan mencari tahu *design* topologi jaringan interkoneksi yang dibangun web sipt Universitas Buana Perjuangan Karawang dengan bantuan *tools* maltego. Diharapkan dengan gambar design topologi ini akan memberikan gambaran untuk dianalisa lebih lanjut. Sebelumnya kita telah mendapatkan gambar design topologi jaringan pada *blueprint* pembangunan infrastruktur jaringan Universitas Buana Perjuangan Karawang.

Berikut ini merupakan design infrastruktur jaringan UBP Karawang



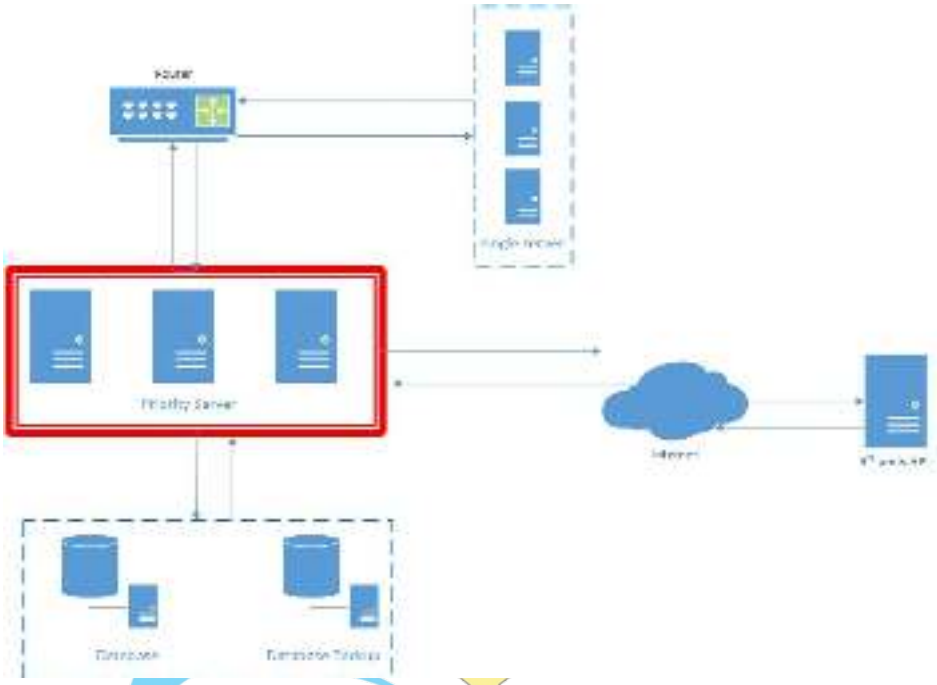
Gambar 3. 4 Design infrastruktur jaringan UBP Karawang
(Sumber: PUSDATIN)

Selain *design* infrastruktur jaringan UBP Karawang terdapat juga *design* arsitektur data *center* . Data *center* merupakan suatu fasilitas yang digunakan untuk penyimpanan data secara digital. Kehadiran data *center* ini merupakan hal yang penting guna menyimpan data-data penting secara terpusat yang dapat diakses 24 jam sehari. Keberadaan data center ini akan sangat besar manfaatnya jika terjadi hal yang tidak terduga yang melanda kampus seperti: banjir, kebakaran dll. Berikut ini merupakan gambar *design* arsitektur data *center*.



Gambar 3. 5 Design Arsitektur Data Center
(Sumber: PUSDATIN)

Design berikutnya merupakan *design* arsitektur jaringan *server*, dimana *design* arsitektur jaringan *server* ini memberikan gambaran mengenai arsitektur jaringan *server* yang dibuat.



Gambar 3. 6 Arsitektur jaringan server
(Sumber: PUSDATIN)

3.2.3. Monitoring

Setelah tahapan topologi jaringan akan dilakukan tahapan monitoring, *monitoring* merupakan tahapan yang penting, agar kita dapat mengetahui *vulnerability* yang ada, di tahapan ini akan dilakukan proses *scanning* dengan memakai *software* nessus, nmap dan owasp. Dimana hasil *scan* melalui nessus akan menampilkan banyaknya kategori *vulnerability* selain itu hasil *scan* melalui nmap akan menampilkan *port-port* IP ada pada *server* SIPT Universitas Buana Perjuangan Karawang sebagai *host* target serta hasil melalui owasp akan menampilkan *URL vulnerability.*

3.2.4. Analisis

Data hasil *monitoring* dan *scanning* yang didapatkan pada tahap sebelumnya dengan *tool* nessus, nmap dan owasp akan diolah di tahap analisis ini. Hasil *scan* dengan *tool* tersebut menampilkan *vulnerability* dan *port-port* yang terbuka pada *server* SIPT Universitas Buana Perjuangan Karawang. Data *vulnerability* yang telah didapatkan selanjutnnya akan diolah menjadi solusi untuk mengurangi *vulnerability* yang ada pada *server* SIPT Universitas Buana Perjuangan Karawang.

3.2.5. Rekomendasi

Tahapan rekomendasi ini akan dijelaskan tentang rekomendasi yang diberkan untuk menutup celah kerentanan *(vulnerability*) yang didapat dari hasil *scan* host target menggunakan *software* nessus dan owasp, dimana data yang sudah diolah berdasarkan tahap analisis sebelumnya akan menampilkan beberapa kategori *vulnerability* yang telah discan menggunakan *software* nessus, setiap celah kerentanan diberikan solusi atau rekomendasi bagaiamana cara mengatasi masalah tersebut.

3.3. Peralatan Penelitian

Pada tiap penelitian dibutuhkan peralatan penelitian guna memudahkan proses penelitian. Dalam hal ini alat bantu teknologi yang digunakan penulis terdiri dari *hardware* dan *software* komputer.

3.3.1. Hardware

Pengertian dari *Hardware* atau dalam bahasa Indonesia disebut juga dengan nama perangkat keras adalah salah satu komponen komputer yang sifatnya dapat dilihat dan disentuh secara langsung atau dalam format nyata untuk membantu mendukung proses komputerisasi (Putri, 2017). Pada penelitian ini peneliti menggunakan *hardware* yang memiliki spesifikasi sebagai berikut:

1. *Computer Name* : DEKSTOP-172CSOL
2. *Processor* : Intel(R) core (TM) i5-7200U CPU @2.50 GHz (4 CPUs) ~ 2.7GHz

3.3.2. Software

Menurut Imam Prayogo Pujiono, perangkat lunak atau software memberikan perintah ke komputer atau perangkat keras atau perangkat lunak lain pada saat dijalankan untuk melakukan tugas, pekerjaan, dan persyaratan tertentu yang diinginkan oleh pengguna. Dalam penelitian ini peneliti menggunakan *software* sebagai berikut:

1. *Operating System*: Windows 10 Pro 64-bit (10.0, Build 18363)

2. *Nmap*

3. *Nessus*

4. *Owasp 2.11.1*

5. *Maltego 4.3.0*

6. *Web Browser*

Tabel 3. 1 Rencana Penelitian

No	Kegiatan	Bulan Ke-1				Bulan Ke-2				Bulan Ke-3				Bulan Ke-4				Bulan Ke-5			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Persiapan																				
2.	Topologi Jaringan																				
3.	Monitoring																				
4.	Analisa																				
5.	Rekomendasi																				