BAB 3
METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kuantitatif dengan tujuan untuk mengevaluasi tingkat kesadaran keamanan siber karyawan di PT XYZ. Pendekatan ini dipilih karena mampu menggambarkan kondisi nyata berdasarkan data numerik yang diperoleh dari responden. Populasi dalam penelitian ini adalah seluruh karyawan PT XYZ. Jumlah sampel ditentukan berdasarkan arahan dari pembimbing lapangan atas pertimbangan faktor-faktor seperti ukuran populasi, relevansi data yang dibutuhkan, serta keterbatasan waktu dan sumber daya.

Pengumpulan data dilakukan melalui simulasi serangan *phishing* menggunakan Gophish. Lima indikator utama yang digunakan untuk menilai respon terhadap kampanye ini adalah:

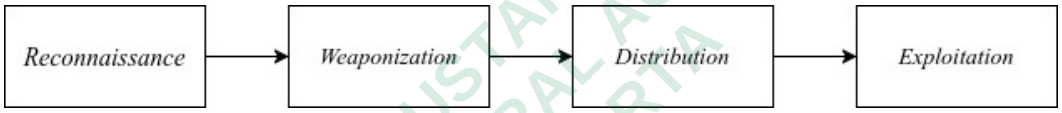
1. *Email Sent*
2. *Email Opened* (*email* dibuka),
3. *Clicked Link* (tautan diklik),
4. *Submitted Data* (data dikirimkan), dan
5. *Email Reported* (*email* dilaporkan sebagai *phishing*).

Kelima indikator tersebut dijadikan sebagai parameter evaluasi dalam analisis tingkat kesadaran keamanan siber. Data yang diperoleh dari simulasi kemudian dianalisis menggunakan metode *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS). Metode TOPSIS digunakan untuk memberikan peringkat terhadap alternatif (dalam hal ini, respon karyawan) berdasarkan kedekatannya dengan solusi ideal, sehingga dapat diketahui nilai preferensi masing-masing individu.

Untuk mempermudah interpretasi hasil, nilai preferensi yang diperoleh dari perhitungan TOPSIS yang ditentukan nilai rata-rata dari hasil preferensi tersebut dan akan diklasifikasikan ke dalam tiga kategori, yaitu rendah, sedang,

dan tinggi. Kategori tersebut dihitung menggunakan pendekatan *equal interval*. Pendekatan ini bersifat deskriptif dan digunakan sebagai tahap lanjutan guna menyajikan hasil dalam bentuk yang lebih informatif dan mudah dipahami.

Simulasi serangan *phishing* dilakukan menggunakan tahapan yang sesuai dengan *framework cyber kill chain. Cyber Kill Chain* (CKC) adalah sebuah model konseptual yang dikembangkan oleh Lockheed Martin untuk mengidentifikasi dan memahami tahapan-tahapan yang umum dilakukan dalam serangan siber. Tahapan CKC terdiri dari 7 tahapan yaitu *reconnaissane, weaponization, delivery, exploitation, installation, command & control (C2),* dan *actions on objectives.* (Martin, 2015).



Gambar 3.1 *Phishing Attack Life Cycle*
Sumber: Peneliti (2025)

Tahapan CKC tersebut kemudian diadopsi berdasarkan kebutuhan simulasi serangan *phishing* yang disesuaikan dan diimplementasikan di lapangan berdasarkan pendekatan *Phishing Attacks Life Cycle* (Do dkk., 2022). Seperti pada gambar 3.1, simulasi serangan *phishing* dalam penelitian ini melalui proses 4 tahapan yaitu *reconnaissance*, *weaponization, distribution,* dan *exploitation*.

3.1 Bahan Penelitian

Bahan yang digunakan dalam penelitian ini terdiri dari dua jenis data, data primer dan data sekunder. Data primer yang digunakan dalam penelitian ini adalah hasil simulasi serangan *phishing* yang dikonveri ke dalam bentuk numerik. Data sekunder yang digunakan dalam penelitian ini adalah data *email* karyawan PT XYZ. Selain itu, sebagai acuan dalam penelitian yang akan datang, penelitian ini juga menggunakan hasil konsultasi dengan Manajer Utama divisi Infrastruktur dan Operasi IT. Dengan menggunakan data dari serangan *phishing* menggunakan

Gophish yang digunakan untuk mengevaluasi kesadaran keamanan siber menggunakan TOPSIS.

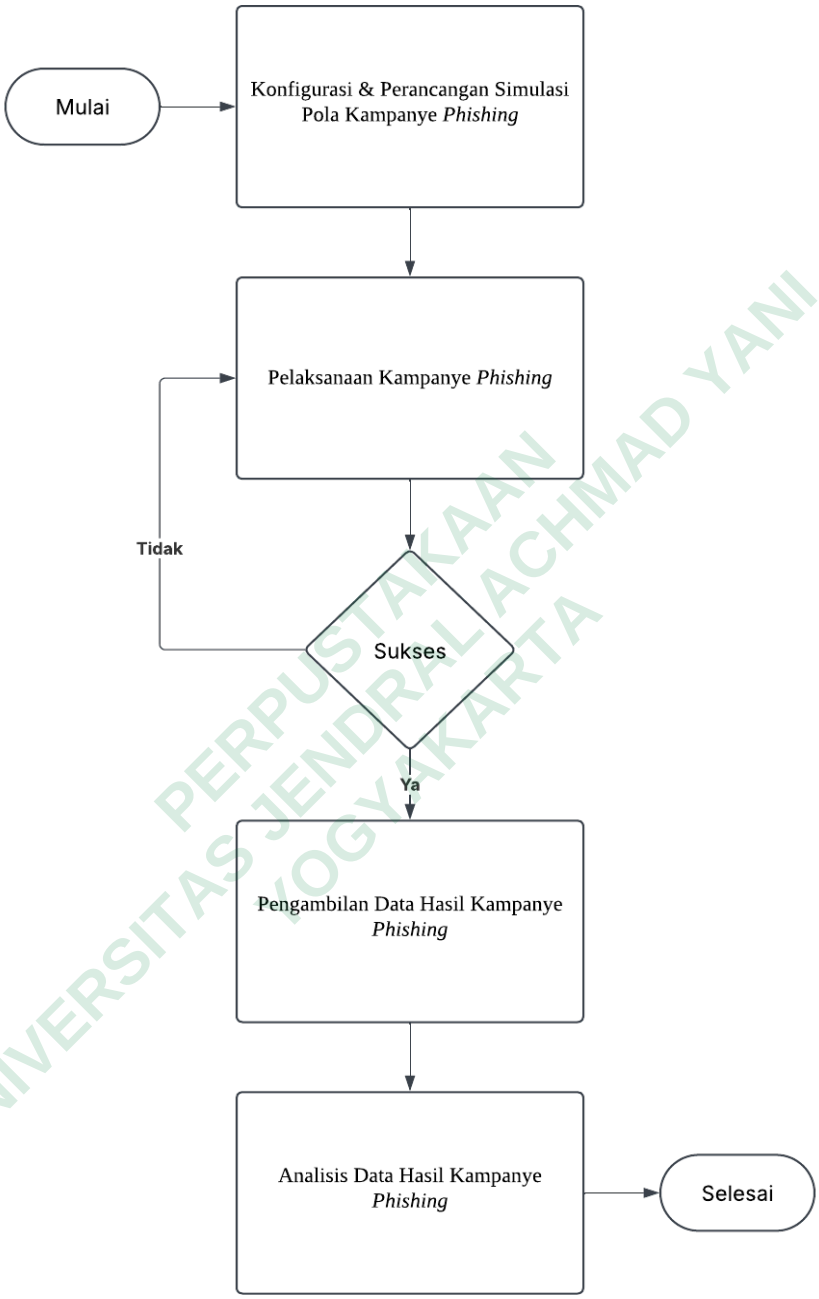
3.2 Alat Penelitian

Penelitian ini menggunakan beberapa alat yang digunakan dalam penelitian. Berikut ini adalah alat yang digunakan :

1. Seperangkat komputer dalam bentuk laptop dengan spesifikasi: *processor* Intel Core i3, RAM 8GB, SSD 512GB, Sistem Operasi Ubuntu 24.04.2 LTS.
2. Seperangkat komputer dalam bentuk *virtual machine* (VM) dengan spesifikasi: *processor* 4Core, RAM 4GB, SSD 50GB.
3. Gophish versi v0.12.1.
4. SSH Terminal.

3.3 Jalan Penelitian

Penelitian ini sesuai dengan jalan penelitian yang telah digambarkan pada gambar 3.2. Jalan penelitian ini merupakan tahapan-tahapan metode yang digunakan dalam penelitian agar dapat berjalan lancar. Tahapan ini meliputi setiap kegiatan dari awal hingga akhir penelitian. Berikut ini tahapan yang dilalui selama proses penelitian berlangsung.



Gambar 3.2 *Flowchart* Jalan Penelitian

Berdasarkan gambar 3.2, berikut ini adalah penjelasan tentang alur jalannya penelitian:

1. Konfigurasi dan Perancangan Simulasi Pola Serangan *Phishing*

   Konfigurasi dan perancangan simulasi pola serangan *phishing* adalah tahap pertama dalam penelitian ini. Tahap ini dimulai dengan melakukan instalasi dan konfigurasi Gophish pada *server* atau *virtual machine* (VM) yang telah disediakan oleh perusahaan.

   Sebelum masuk ke tahap perancangan simulasi pola kampanye, peneliti mengumpulkan data sekunder (r*econnaissance*) yang dilakukan menggunakan metode konsultasi dengan mentor penelitian. Data sekunder yang dimaksud meliputi:

   - **Data sampel** terdiri dari daftar *email* karyawan yang akan digunakan dalam serangan *phishing*.
   - **Studi dokumen** berupa aplikasi perusahaan yang dipelajari melalui konsultasi dengan mentor penelitian.
   - **Durasi serangan *phishing*** ini terdiri dari berapa lama pola serangan *phishing* akan dijalankan. Durasi ini memiliki batasan sesuai dengan waktu penelitian yang telah ditentukan yaitu satu bulan sesuai jadwal penelitian yang sudah dibuat.

   Tujuan pengumpulan data sekunder ini adalah untuk membuat model pola serangan *phishing*. Setelah itu, melakukan konfigurasi lanjutan (*weaponization*) pada:

   a) **File config.json :** konfigurasi file ini ditujukan untuk melakukan pengaturan pada admin dan *phishing server* yang mencakup penentuan URL dan *port* yang bisa diakses dan penentuan sertifikat keamanan (SSL).

   b) ***Systemctl* untuk Gophish :** *Systemctl* adalah sebuah layanan yang beroperasi pada sistem Linux yang berfungsi untuk mengkonfigurasi layanan yang berjalan secara otomatis. Konfigurasi ini diawali dengan pembuatan file *systemctl* Gophish yang berisi pengaturan *Description*,

`After=network.target, ExecStart, Restart=always, User & Group, WantedBy=multi-user.target. File disimpan pada folder sistem linux, tepatnya di "/etc/systemd/system/".`

c) ***Dashboard Admin*** **:** Konfigurasi pada tahap ini berupa SMTP & IMAP Server yang berfungsi sebagai profil peneliti dalam proses serangan *phishing* yang berlangsung melalui *email*, templat *email* & *fake landing page* yang akan digunakan berdasarkan hasil pengumpulan data sekunder atas persetujuan mentor.

Konfigurasi pada tiga poin di atas dilakukan secara bertahap agar tidak terjadinya kesalahan saat Gophish dijalankan. Perancangan pola simulasi serangan *phishing* terletak di poin c, dimana hasil pengumpulan data sekunder disesuaikan dengan alur konfigurasi pada poin c.

2. Pelaksanaan Serangan *Phishing*

Setelah rancangan pada tahap awal selesai, dilakukan eksekusi serangan *phishing* (*distribution*) yang telah disiapkan sebelumnya. Pada tahap ini, peneliti melakukan konfigurasi kampanye pada *dashboard admin* yang menentukan: *sending profile*, pemilihan templat *email* & *fake landing page* yang akan digunakan, hingga penentuan *fake* URL sebagai *end point* serangan *phishing*. Proses ini melibatkan pengiriman *email phishing* atau penyebaran skenario *phishing* kepada target yang telah ditentukan. Eksploitasi (*exploitation*) terjadi ketika target membuka *email phishing*, mengklik tautan berbahaya, atau mengisi data pada halaman palsu. Data interaksi ini kemudian dikumpulkan di *dashboard* Gophish sebagai bagian dari evaluasi kampanye.

3. Evaluasi Keberhasilan Kampanye

Setelah pelaksanaan, dilakukan evaluasi terhadap keberhasilan serangan *phishing* yang dijalankan. Jika kampanye dianggap belum berhasil (T - Tidak), maka dilakukan perbaikan atau penyesuaian pada pola

kampanye, dan proses ini diulangi kembali hingga mencapai tingkat keberhasilan yang diharapkan dan batas waktu yang telah ditetapkan. Jika kampanye berhasil (Y - Ya) atau tidak (T - Tidak) hingga batasan waktu, maka proses dilanjutkan ke tahap berikutnya.

4. Analisis Data Hasil Serangan *Phishing*

Pada tahap ini, dilakukan pengumpulan data terkait hasil serangan *phishing*, seperti jumlah respon pengguna terhadap serangan, rasio *email* terkirim (*email sent*), *email* yang dibuka (*email opened*), klik pada tautan *phishing* (*clicked link*), pengisian data pada halaman palsu (*submitted data*), serta melaporkan bahwa *email* yang didapat itu adalah *phishing* (*email reported*). Data yang telah dikumpulkan kemudian dianalisis menggunakan metode TOPSIS untuk menentukan tingkat kesadaran keamanan siber karyawan sesuai dengan langkah-langkah yang telah dicantumkan pada landasan teori bagian TOPSIS.

Selain itu, tahapan ini dilakukan untuk menilai hasil menyeluruh berdasarkan hasil pengolahan data. Langkah ini bertujuan untuk mencapai tujuan penelitian dan memberikan jawaban atas pertanyaan yang diajukan selama perumusan masalah.

5. Kesimpulan dan Penyelesaian Penelitian

Tahapan terakhir dalam proses penelitian ini adalah menarik kesimpulan atas hasil analisis yang telah dilakukan dengan menuliskan hasil akhir penelitian yang menjawab tujuan penelitian awal dari semua proses yang telah dilakukan. Selain itu kekurangan atas penelitian ini selanjutnya akan dijadikan sebagai rekomendasi untuk penelitian dan studi selanjutnya.