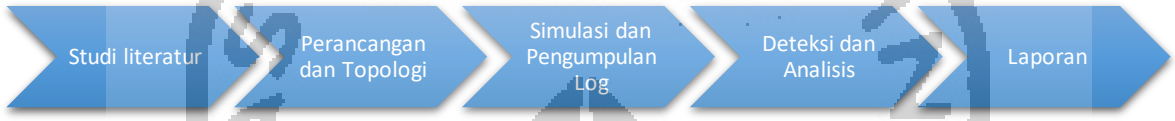
BAB 3
Metodologi Penelitian

Bab ini menjelaskan bagaimana cara penelitian ini dilakukan, sehingga dapat memberikan rincian tentang alur atau langkah-langkah yang dibuat secara sistematis serta dapat digunakan dijadikan pedoman dengan jelas dalam menyelesaikan masalah, membuat analisis terhadap hasil penelitian, serta kesulitan yang dihadapi. Adapun tahapan-tahapan atau langkah-langkah pada penelitian ini dapat dilihat pada gambar 3.1.



Gambar 3.3.1 Alur metodologi penelitian

3.1 Studi Literatur

Studi literatur merupakan kegiatan untuk mempelajari literatur-literatur dan teori yang mendukung dalam melakukan penelitian ini. Studi literatur melalui paper, jurnal, artikel, buku, website yang terkait dengan DNS *tunneling, malware*, dan Elasticsearch.

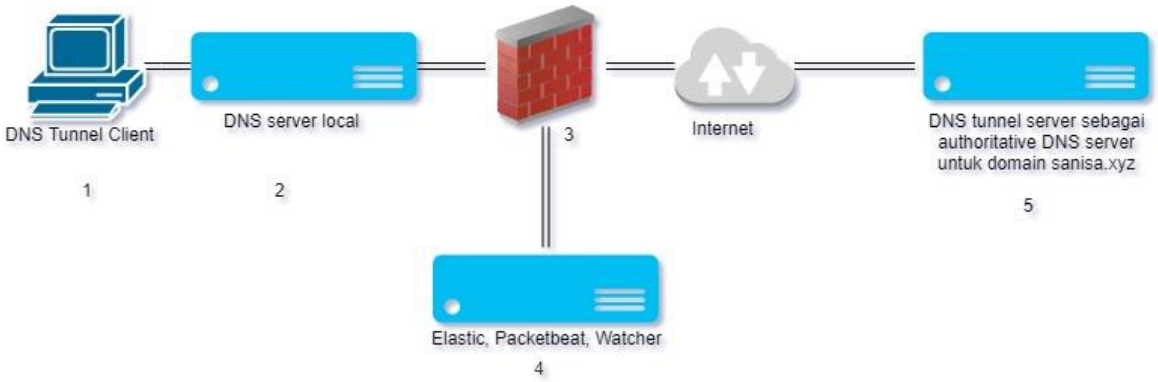
3.2 Perancangan dan Topologi

Merupakan tahapan dimana kami melakukan perancangan *topologi*, identifikasi kebutuhan perangkat lunak maupun perangkat keras untuk melakukan simulasi deteksi DNS *tunneling*.

Untuk menunjang penelitian ini, penulis akan mencoba membangun lab di lingkungan *virtual* agar lebih mudah dan aman dalam melakukan simulasi. Meskipun dibuat di lingkungan virtual, kondisi tersebut sudah sangat mewakili kondisi pada jaringan yang diterapkan pada organisasi.

3.3 Simulasi dan Pengumpulan Log

Simulasi kasus deteksi DNS *tunneling* dengan Elasticsearch bertujuan untuk melakukan pengujian terhadap Elasticsearch dalam mendeteksi adanya DNS *tunneling*. Skenario yang kami gunakan adalah dengan melakukan DNS *tunnel* dengan *tools Iodine, dnscat,* dan menggunakan *malware* bernama DNSExfiltrator. Alur simulasi diilustrasikan dengan gambar dibawah ini.



Gambar 3.3.2 Alur simulasi deteksi DNS tunneling

1) Komputer DNS *tunnel client* akan menjalankan program DNS *tunnel client* yakni Iodine, Dnscat2, dan *malware* DNSExfiltrator.
2) DNS *server local* akan melayani *request* dari komputer *client* pada jaringan lokal.
3) *Firewall* akan me-*routing traffic* ke internet dan melakukan *port mirroring* dari DNS *server local* ke *server* Elasticsearch.
4) *Server* Elasticsearch akan meng-*capture traffic* DNS dan mendeteksi DNS *tunneling*.
5) DNS *tunnel server* yang berfungsi sebagai *authoritative name server domain sanisa.xyz*.

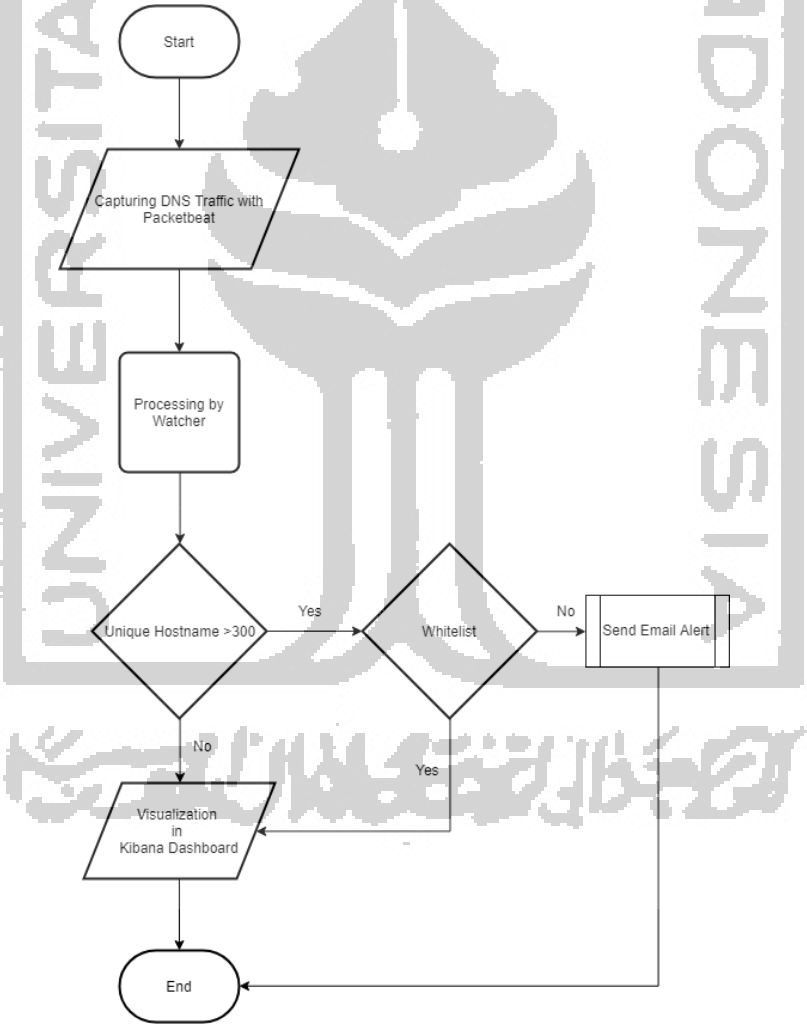
Pengumpulan *log* akan dilakukan oleh Elasticsearch menggunakan *plugin* untuk meng-*capture* paket bernama Packetbeat secara *realtime*. Agar data yang digunakan memadai, maka akan dilakukan generate simulasi trafik menggunakan *tool* bernama DNS Grind dari pentestmonkey(“DNS Grind,” n.d.).

DNS *tunnel* server Iodine dan Dnscat2 akan menjalankan *service*-nya di DNS *tunnel server*. Komputer *client* juga menjalankan DNS *tunnel client* yang akan menghubungi DNS *tunnel server*, percobaan kali ini komputer *client* akan mencoba browsing menggunakan saluran *tunnel* DNS selama beberapa saat untuk mendapatkan *log* DNS *tunnel*.

Elasticsearch akan menjalankan *job* yang akan mendeteksi DNS *tunnel* dari *log* yang terkumpul, visualisasi dari hasil pendeteksian dapat dilihat pada *dashboard kibana*. Elasticsearch akan mendeteksi dan menghitung jumlah *unique hostname*, *domain* yang memiliki jumlah yang besar akan terdeteksi sebagai anomali. Agar mendapatkan hasil yang baik, diperlukan waktu kurang lebih 48 jam.

3.4 Deteksi dan Analisis

Pada tahap ini akan dilakukan analisis untuk mencari tahu apakah *elasticsearch* dapat mendeteksi adanya DNS *tunneling*. Metode yang digunakan adalah *traffic analysis*. Setiap komunikasi DNS *tunneling* akan membuat *hostname* baru, jumlah rata-rata unique hostname normal adalah dibawah 300 (Farnham, 2013), oleh karena itu semakin banyak jumlah *unique hostname* menandakan adanya DNS *tunneling*. Seluruh log yang di-capture melalui *packetbeat* akan diolah dengan *custom script* oleh *watcher*, *watcher* akan menghitung jumlah *unique hostname* berdasarkan *kardinalitas* pada nama domain. Jumlah *unique hostname* pada sebuah nama domain akan divisualisasikan di *Kibana* dengan grafik *bar*, dan jika jumlah *unique hostname* lebih dari 300, dan domain tidak ada dalam *whitelist*, *watcher* akan mengirimkan email notifikasi kepada Administrator jaringan.



Gambar 3.3.3 Alur pendeteksian DNS *tunneling*

3.5 Laporan

Merupakan tahap pembuatan laporan dari hasil simulasi mendeteksi DNS *tunneling* dengan Elasticsearch. Laporan berisi mengenai pendahuluan, literatur review, metodologi penelitian, hasil dan pembahasan, serta penutup yang berisi kesimpulan dan saran.

Laporan yang disusun pada akhirnya diharapkan dapat memberikan gambaran secara menyeluruh mengenai topik penelitian ini, serta dapat memberikan rekomendasi yang bermanfaat untuk penelitian selanjutnya.