BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Dari percobaan yang kami lakukan dengan menggunakan Iodine, Dnscat2, dan *malware* DNSExfiltrator, dapat kami simpulkan bahwa *traffic analysis* dengan menghitung *unique hostname* sebagai indikator terjadinya DNS *Tunneling* menggunakan Elasticsearch, Packetbeat, dan Watcher berhasil mendeteksi adanya kegiatan yang mengindikasikan terjadinya DNS *tunneling* dan dapat memberi notifikasi berupa *email* kepada Administrator Jaringan.

Setelah didapatkan nama domain dari hasil pendeteksian, kita dapat menghentikan DNS *tunneling* dengan menggunakan DNS *Sinkhole*. Dari hasil percobaan kami, DNS *Sinkhole* berhasil mencegah DNS *tunneling* karena DNS *tunnel client* tidak bisa menghubungi DNS *tunnel server* karena nama domain tidak bisa di-*resolve* dengan benar.

DNS *tunneling* mempunyai pengaruh signifikan terhadap nilai *jitter* pada komputer yang melakukan DNS *tunneling*, tetapi tidak pada komputer lain. DNS *tunneling* juga mempunyai pengaruh signifikan terhadap nilai *packet loss* UDP pada komputer yang tidak melakukan DNS *tunneling*, tetapi tidak pada komputer yang melakukan DNS *tunneling*.

5.2 Saran

Pengembangan selanjutnya yang kami harapkan untuk penelitian ini antara lain meningkatkan akurasi, sensitivitas, dan mengurangi *false alarm* pada pendeteksian DNS tunneling dengan menggabungkan *traffic analysis* menggunakan *unique hostname* dengan indikator tambahan. Misalnya, mengamati record DNS TXT yang jumlahnya menjadi sangat banyak dibanding record DNS lain seperti A record, MX record, NS record, pada saat proses DNS tunneling.