BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis *Static and Dynamic Application Security Testing* yang dilakukan pada penelitian ini terhadap ketiga aplikasi yaitu: *Creator*.apk, Undangan Pernikahan.apk, dan Cek Resi J&T.apk dapat disimpulkan:

1) Berdasarkan indikator *risk rating analysis*, ketiga aplikasi masuk ke dalam *malicious application* dengan *severity medium to high*. *Vulnerability* yang ditemukan pada penelitian ini berdasarkan OWASP yaitu: *Insufficient Cyptography* dan *Improper Platform Usage*;
2) Berdasarkan indikator *Threat Actor* dan *Threat Intelligence Platform analysis* dapat diketahui bahwa aplikasi Undangan Pernikahan.apk dan Cek Resi J&T.apk memiliki *malicious link* yang disisipkan ke dalam sebuah aplikasi yaitu: surveyheart[.]com dan ionicio[.]com. Pada Undangan pernikahan.apk juga terdapat API Telegram yang dapat diketahui bahwa Bot Telegram bernama "gacorniannnbot";
3) Berdasarkan indikator TLS/SSL *Security Test*, Aplikasi Undangan Pernikahan.apk dan Cek Resi J&T.apk memungkinkan untuk dilakukan TLS *Pinning/Certificate Transparency Bypass*, sehingga memungkinkan terjadinya serangan *man-in-the-middle*;
4) Dari 4 serangan yang dilakukan pada ketiga VPN (Snap Master, Turbo, dan Thunder) berhasil memblokir serangan C&C dengan persentase tingkat keberhasilan 100%. Namun terjadi penurunan kualitas layanan jaringan yaitu: *download* -24,87 Mbps dan *upload* -14,91 Mbps;
5) Berdasarkan standar TIPHON, kualitas layanan jaringan internet yang dihasilkan ketiga VPN tersebut tergolong *excellent* dan masuk dalam kategori *perfect* dengan indeks 4.

5.2 Saran

Penulis menyadari bahwa penelitian ini masih memiliki keterbatasan pada *tools* yang digunakan untuk melakukan analisis aplikasi. Untuk penelitian selanjutnya, disarankan untuk menggunakan *software enterprise* yang dikorelasikan dengan layanan *cloud platform*.