# BAB V
# PENUTUP

## 5.1. Kesimpulan

Berdasarkan penelitian dan pembahasan yang dijelaskan pada bab sebelumnya dapat disimpulkan bahwa:

1. *Malware* Backdoor-apk hanya dapat dijalankan jika aplikasi dan versi Android sesuai dengan *malware* Backdoor-apk.
2. Aplikasi yang telah disisipi *malware* Backdoor-apk tidak dapat di instal pada versi Android 13, tetapi bisa diinstal pada versi Android 5.1.
3. Hasil analisis MobSF dan JADX menyatakan terdapat sejumlah 36 *permission* dengan 19 perbedaan.
4. Hasil analisis MobSF menunjukkan *security score* mengalami penurunan pada aplikasi Turbo VPN setelah disisipi *malware* Backdoor-apk dari 38/100 menjadi 34/100 artinya semakin rendah skor keamanan semakin tinggi kerentanan keamanan yang harus segera diperbaiki.
5. Hasil injeksi *malware* Backdoor-apk adalah dua yaitu Turbo.apk dan Rat.apk dan keduanya harus diinstal pada perangkat Android.
6. Perubahan nama setelah disisipi *malware* pada META-INF dari CERT.RSA menjadi SIGNING.RSA, CERT.SF menjadi SIGNING.SF, dan isi dari MANIFEST.MF.
7. Folder yalzf terindikasi sebagai *malware* yang terdapat pada *package* free/vpn/unblock/proxy/turbovpn.
8. AppContext yang terdapat dalam *package* free/vpn/unblock/proxy/turbovpn/application/ dikategorikan sebagai *hook payload* saat proses injeksi *backdoor* berlangsung.

## 5.2.Saran

1. Pada penelitian selanjutnya, menguji coba penyisipan *malware* pada sistem Android dengan versi Android yang lebih beragam.
2. Menggunakan *malware* yang berbeda selain Backdoor-apk untuk melakukan penyisipan *backdoor* pada penelitian berikutnya.

3. Untuk penelitian mendatang, melakukan pengujian menggunakan aplikasi selain Turbo VPN.