BAB 5
KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Dari penelitian ini dapat ditarik kesimpulan bahwa.

1. Hasil perbandingan metadata menunjukkan adanya kerentanan pada aplikasi *game* versi mod yaitu dari aspek penambahan informasi nama aplikasi, nama paket yang berbeda, ukuran yang lebih besar, dan tanggal pembaruan versi mod yang lebih baru.
2. Hasil pengamatan karakteristik ketika *game* versi mod dijalankan, juga menunjukkan kerentanan pada fitur *unlimited money* yang ditawarkan. Secara tidak langsung, fitur tersebut mengindikasikan adanya perubahan kode sumber di dalam *game*.
3. Hasil analisis statis menggunakan *tools* MobSF antara *game* modifikasi dan *game* asli menunjukkan adanya kerentanan diantaranya pada aspek perizinan aplikasi, analisis sertifikat, dan analisis *manifest*. Yang menjadi pembeda adalah, pada versi *game* modifikasi telah terjadi perubahan signifikan pada integritas data dan distribusi *email* ke *library* tertentu.
4. Hasil analisis dinamis menggunakan *packet analysis* dengan *tools* PCAPDroid, menunjukkan adanya perubahan dari aspek data yang dikirim oleh IP tujuan ke IP sumber di versi *game* mod cenderung meningkat jika dibandingkan dengan versi asli.

5.2 SARAN

Adapun saran yang dapat peneliti berikan setelah melakukan penelitian ini adalah sebagai berikut :

1. Aplikasi modifikasi, termasuk *game* mod terbukti memiliki kerentanan yang dapat membahayakan perangkat pengguna karena sumbernya berasal dari pihak ketiga yang tidak jelas asal-usulnya. Jika pengguna setuju untuk menggunakan aplikasi modifikasi, maka secara tidak

langsung juga menyerahkan keamanannya pada pihak tersebut tanpa tahu potensi risiko yang mungkin timbul. Mungkin pengguna merasa aman selama menggunakan aplikasi modifikasi. Namun perlu diingat bahwa :

- Pengembang aplikasi modifikasi tidak menjamin perlindungan privasi dan keamanan pengguna seperti pada versi resmi.
- Penggunaan aplikasi modifikasi dapat mengakibatkan pencurian data pribadi.
- Aplikasi modifikasi patut dicurigai dari adanya kode berbahaya yang dapat menyerang perangkat pengguna.

Maka dari itu, disarankan untuk selalu menggunakan aplikasi dari sumber resmi dan tidak menggunakan aplikasi modifikasi untuk menjaga keamanan pengguna dan terhindar dari penyalahgunaan privasi.

2. Penelitian selanjutnya dapat memperpanjang durasi perekaman data analisis dinamis *packet analysis* untuk lebih mendalam memindai dan menganalisis penggunaan IP yang terlibat untuk mendapatkan pemahaman yang lebih detail tentang interaksi aplikasi dengan jaringan, termasuk pada pola perilaku yang mencurigakan atau tidak diinginkan.
3. Melakukan perbandingan sebelum dan sesudah aplikasi Android diinstall dan dijalankan terhadap *malvertising* menggunakan AdGuardHome pada ekosistem jaringan khusus.