BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil implementasi dan uji coba *password stealing program*, simpulan dari penelitian ini adalah sebagai berikut.

1. *Password stealing program attack* terhadap *saved password* pada Mozilla Firefox telah berhasil diimplementasikan menggunakan dua jenis *malware*, yaitu *malware* yang berbentuk *executable file* dan *malware* yang menggunakan Digispark. Pengecekan *password* dilakukan dengan memanfaatkan web yang dibangun menggunakan javascript. Proses pengecekan *password* terdiri dari pengukuran tingkat kekuatan *password* menggunakan zxcvbn *password strength estimation library*, pengecekan kebocoran *password* pada *leaked database* menggunakan haveibeenpwned API, dan pengecekan karakteristik *password*.
2. Berdasarkan uji coba yang telah dilakukan terhadap 50 responden, tingkat keberhasilan *password stealing program attack* terhadap *saved password* pada Mozilla Firefox mencapai 78%. *Malware* yang berbentuk *executable file* diujikan pada 43 responden dengan tingkat keberhasilan sebesar 76,74%, sedangkan *malware* yang menggunakan Digispark diujikan pada 7 responden dengan tingkat keberhasilan sebesar 85,71%.
3. Berdasarkan hasil pengecekan 182 *password* yang berbeda dari 32 responden menggunakan zxcvbn *password strength estimation*, diperoleh tingkat kekuatan *password* sebagai berikut. Sebanyak 52,7% *password*

termasuk dalam kategori *guessable* dan 47,3% *password* termasuk dalam kategori *unguessable*. *Password* yang tergolong *guessable* terdiri dari 6,6% *too guessable*, 26,3% *very guessable*, dan 19,8% *somewhat guessable*, sedangkan *password* yang tergolong *unguessable* terbagi menjadi 23,1% *safely unguessable* dan 24,2% *very unguessable*.

4. Berdasarkan hasil pengecekan 182 password yang berbeda dari 32 responden pada *data breach database* haveibeenpwned, sebanyak 38,5% *password* tergolong *leaked* dan 61,5% *password* tergolong *safe*.

5.2 Saran

Saran yang dapat diberikan untuk penelitian selanjutnya adalah sebagai berikut.

1. Berdasarkan kegagalan terhadap 10 responden yang diakibatkan oleh antivirus dan folder ganda, program dapat dikembangkan untuk dapat melewati antivirus dan dapat memilih folder yang di dalamnya terdapat *file* "key3.db" atau "key4.db" dan "logins.json".
2. Berdasarkan kegagalan terhadap 1 responden yang diakibatkan oleh *layout keyboard* yang berbeda, program dapat dikembangkan untuk dapat menyesuaikan dengan *layout keyboard* yang terdapat pada komputer target.
3. Malware yang telah dibuat dapat dikembangkan untuk melakukan *attack* pada sistem operasi yang berbeda.