BAB V KESIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil penelitian dan pembahasan yang sudah dilakukan, maka dapat diambil kesimpulan sebagai berikut:

1. Cara implementasi *honeypot* tanpa mengurangi keamanan jaringan secara nirkabel dapat dilakukan dengan memisahkan jaringan *honeypot* dan keseluruhan jaringan lain melalui pengaturan *router* (*Dual SSID/Guest Network*). Pengaturan IP statis dan *local management* untuk mengakses pengaturan *router* dapat membantu memperkuat keamanan *router*.
2. Instalasi *honeypot Dionaea* pada *Raspberry Pi* dapat dilakukan dengan *script* instalasi sudah dibuat secara otomatis sesuai dengan alamat IP yang ditentukan. Instalasi ini dibantu dengan layanan *Modern HoneyPot Network* (MHN) dengan tambahan sedikit modifikasi pada *script* agar *honeypot Dionaea* dapat di-instal pada *Raspberry Pi*.
3. Simulasi serangan *malware* pada *honeypot* dapat dilakukan dengan menggunakan *Metasploit* pada komputer penyerang. *Honeypot Dionaea* pada *Raspberry Pi* dapat mendeteksi serangan *malware* dan eksploitasi kelemahan sistem operasi/program dengan tingkat keberhasilan 85.33%, selama *server* MHN tetap berjalan.

5.2 Saran

Adapun beberapa saran yang dapat dikembangkan pada penelitian selanjutnya adalah sebagai berikut:

1. Jaringan dengan sistem *honeypot* dapat ditingkatkan keamanannya dengan menggunakan *router* yang mendukung fitur VLAN (*Virtual Local Area Network*) untuk memisahkan jaringan *honeypot* dengan jaringan komputer lain.
2. Penambahan alat *Raspberry Pi* atau komputer lain sebagai sensor *honeypot* lain (*Kippo, Snort, Conpot, dll.*) dapat meningkatkan keamanan jaringan.
3. Jika ada perangkat *router* tambahan, menambahkan *hardware firewall* sebelum jaringan komputer utama dapat meningkatkan keamanan komputer secara signifikan. Apabila mobilitas perangkat bukan kendala, disarankan menggunakan *switch* dan *firewall* tambahan menggunakan *ethernet port*.