BAB V
SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil pengujian dan pembahasan yang telah diuraikan dapat ditarik kesimpulan sebagai berikut:

1. Dalam penelitian penyerangan DNS *spoofing* peneliti tidak dapat menjebol *wifi.id* di lokasi mana pun karena keamanan jaringan *wifi* menggunakan *mikrotik.*
2. *Wifi.id* menggunakan IP *address* kelas A dimana bila melakukan *scaning* IP *host* dibutuhkan waktu yang lama dan sedikit rumit menentukan target dibandinngkan dengan IP *address* kelas B
3. Apabila attacker melakukan DNS *spoofing* pada target atau pengguna *internet* maka *attacker* akan memberikan alamat palsu kepada para korbannya sehingga korbannya mengalami kebingungan karena *website* yang diaksesnya tidak dapat terhubung dengan internet.
4. Solusi untuk menanggulangi DNS *spoofing* adalah gunakan *firewall* pada setiap *host* dan *setting router* dengan *mikrotik*, *cisco*, dll agar bisa dibatasi penyerangan terjadi.

5.2 Saran

Saran dalam penelitian ini merupakan hal yang bertujuan untuk adanya perbaikan atau pengembangan keamanan DNS *spoofing* pada jaringan *free hospot* di Kota Batam, adapun saran sebagai berikut:

1. Untuk kedepannya DNS *spoofing* dapat dicegah dengan *tools* yang lebih modern dan mudah dipahami oleh *user* yang belum paham.
2. Untuk kedepannya bisa menggunakan DNS *server* yang lebih bagus untuk menghindari serangan DNS *spoofing*.
3. Bila diperlukan, aktifkan fitur *security* pada *access point* untuk meningkatkan keamanan jaringan.
4. Manfaatkan dan berdayakan kemajuan teknologi informasi dan komunikasi dengan bijak dan untuk kebaikan dan kemajuan hidup antar umat manusia, jangan lupa ambil yang baiknya dan buang yang buruknya.
5. Jangan pernah berhenti untuk belajar tentang *cybercrime* khususnya DNS *spoofing*