BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari rangkaian penelitian yang sudah dilakukan diatas yang meliputi konfigurasi dan implementasi IDS, hingga dampak serangan *cryptojacking* dapat disimpulkan sebagai berikut :

1. Waktu yang dibutuhkan *snort* untuk mendeteksi serangan cryptojacking adalah 2.15 detik, waktu deteksi setiap konfigurasi serangan tentu tidak sama.
2. Dengan menggunakan IDS *snort* serangan *cryptojacking* dapat terdeteksi sesuai dengan 2 variabel yaitu *rule* dari *snort* dan pemakaian sumber daya komputer korban yang tinggi.
3. Perbandingan penggunaan sumber daya komputer sebelum dan ketika mengakses website cryptojacking memiliki selisih 20% untuk penggunaan RAM dan batterai, khusus untuk penggunaan CPU mempunyai selisih cukup besar yaitu 30-50%.
4. Perangkat komputer yang digunakan dalam pengujian hanya bertahan dalam waktu 50%.

5.2 Saran

Peneltiian cryptojacking akan selalu mengalami perubahan dimasa depan, entah dalam bentuk format serangan ataupun jenis sisipan pada website, berikut beberapa saran yang diberikan penulis terkait penelitian tentang cryptojacking :

1. Di sarankan untuk menggunakan tools lain yang lebih dapat diandalkan.
2. Menambahkan notifikasi kepada pengguna ketika serangan sedang dilancarkan

3. Menggabungkan dengan sistem lain seperti Machine Learning untuk dapat mengetahui pola serangan dan mengukur dampak serangan secara lebih akurat.
4. Membuat penelitian lintas platform.

Penelitian yang dilakukan tentang cryptojacking tentu masih sangat luas untuk selalu dijelajahi, kedepannya penulis berharap akan terus bermunculan penelitian tentang cryptojacking.