

BAB V PENUTUP

5.1 Kesimpulan

Berdasarkan proses hasil dan pembahasan dari proses *network forensic* dan *static forensic* terhadap serangan *ARP Poisoning* menggunakan tahapan yang ada pada metode NIST SP 800-86, maka dapat ditarik kesimpulan antara lain:

1. Mengetahui pola serangan *ARP Poisoning* yaitu pola pertama, *Attacker* menargetkan website dengan protokol *HTTP*, karena saat terjadi serangan website masih bisa diakses oleh *victim*. Sedangkan website dengan protokol *HTTPS* akan menampilkan *alert* "Your Connection not Private" karena sistem mendeteksi kemungkinan adanya serangan yang terjadi saat itu dan waktu serangan masih berlangsung *victim* tidak bisa mengakses website *HTTPS* yang lain. Pola kedua, *attacker* menduplikasi *IP Address* dari router.
2. Hasil dari *static forensic* menampilkan informasi dari *attacker* (penyerang) antara lain *IP Address attacker* (192.168.100.16), *Mac Address attacker* (9C:AD:97:7B:05:1D), dan waktu serangan terjadi (Senin, 3 Juli 2023 - 12:05:48). Informasi *IP* dan *Mac Address* akan dilakukan pemblokiran untuk tindakan pencegahan.

5.2 Saran

1. Penelitian selanjutnya diharapkan dapat lebih banyak menggunakan alat-alat pengujian serangan seperti *arp spoof*, *Netcut*, *KickThemOut*, *Bettercap* dan masing-masing serangan tadi terdapat satu file *capture pcap* dengan tujuan pengembangan analisis jaringan pada setiap serangan.
2. Penelitian selanjutnya diharapkan menggunakan perbandingan *framework* dalam proses forensik NIST dengan *NIJ*.
3. Penelitian selanjutnya diharapkan dapat mencegah serangan *Man In The Middle* secara jangka panjang.