BAB V
PENUTUP

1.1 Kesimpulan

Berdasarkan hasil penelitian dengan menggunakan metode Live Network Forensics, investigator dapat dengan cepat mendeteksi suatu serangan dan mengidentifikasi penyerang. Data-data yang diperlukan untuk proses investigasi antara lain, tanggal terjadi serangan, waktu terjadi serangan, MAC Address penyerang, IP Address penyerang, MAC Address Victim dan IP Address Victim dapat tersaji dengan cepat dan tepat, sehingga dapat membantu investigator dalam pengambilan keputusan terhadap serangan yang terjadi. Penelitian juga diharapkan dapat memberikan rekomendasi tools yang digunakan terutama pada software dalam mendeteksi dan mengidentifikasi serangan dan penyerang. Penelitian kedepan juga meneliti cara menangani dan pencegahan dari serangan ARP Spoofing. Setelah penelitian investigasi cloud iaas studi kasus ARP Poisoning selesai dilakukan, maka didapat kesimpulan sebagai berikut :

a. Penggunaan metodologi forensik dalam tahapan investigasi yang dilakukan memperoleh alur penelitian secara sistematis, dan dapat dijadikan acuan dalam penelitian.
b. Aktivitas hacking Man in The Middle Attack yang penulis buat dalam rancangan simulasi berhasil dianalisis dan dijabarkan alurnya dengan menganalisis bukti terkait menggunakan network forensic dengan bantuan berbagai tool forensik.
c. Ketika proses penelitian berjalan, peneliti menemukan tantangan yang benar- benar menarik dari sisi ARP Poisoning, yaitu begitu mudahnya attacker mengganti ganti MAC Address maupun IP Address. Sehingga dalam kenyataan lapangan investigator perlu mencocokkan kejadian serangan dengan data lain seperti timeline record CCTV untuk menangkap pelaku.

1.2 Saran

Pada penelitian ini masih didapat beberapa kekurangan, sehingga harapan peneliti dalam waktu yang akan datang penelitian seputar network forensic masih dapat terus dikembangkan. Berikut beberapa saran untuk penelitian kedepannya antara lain:

a. Tahap analisis network forensic pada penelitian ini tidak mendalam, hanya sebatas pembuktian ARP Poisonning yang melakukan login spoofing dan dns redirect.
b. Skenario serangan ARP Poisoning pada penelitian ini tidak sampai menghilangkan atau mempersulit jejak serangan dengan cara rotasi MAC danIP Address.
c. Penelitian ini tidak melakukan pendekatan rule based scanner untuk barang bukti. Sehingga proses analisa benar benar masih manual. Harapan nantinya penerapan machine learning bisa diimplementasikan untuk membantu investigator.
d. Penelitian selanjutnya diharapkan bisa membuat skenario dengan kondisi serangan malware.
e. Analisis paket jaringan dan berbagai artefak berkaitan dengan data traffic inbound/ outbound akan lebih powerfull dan efektif menggunakan tool visualisasi seperti ELK untuk mempermudah memahami pattern traffic secaracepat dan tepat.
f. Sebaiknya dengan adanya penelitian selanjutnya diharapkan serangan ARP Poisoning dapat diatasi tidak hanya proses pendeteksian saja akan tetapi dapat dilakukan tindakan pencegahan maupun pemblokiran.