BAB V
PENUTUP

5.1 Kesimpulan

Setelah penelitian investigasi cloud iaas studi kasus compromised GCP VM selesai dilakukan, maka didapat kesimpulan sebagai berikut :

1. Penggunaan metodologi NIST dalam tahapan investigasi yang dilakukan memperoleh alur penelitian secara sistematis, dan dapat dijadikan acuan dalam penelitian
2. Aktivitas hacking yang penulis buat dalam rancangan simulasi berhasil dianalisis dan dijabarkan alurnya dengan menganalisis bukti terkait menggunakan kolaborasi gabungan 3 metode investigasi dan sumber, yaitu network forensic (flow logs), live forensic dan disk & file system forensic (disk image) dengan bantuan berbagai tool forensik.
3. Untuk akuisisi bukti digital disk image peneliti memperoleh dengan memanfaatkan fitur snapshot. Untuk akuisisi memory RAM peneliti menggunakan tool avml sebagai memory dump. Sedangkan perolehan bukti artefak jaringan peneliti peroleh berdasarkan log inbound / outbound dari bantuan service GCP Flow Logs.

5.2 Saran

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

1. Skenario serangan pada penelitian ini tidak melibatkan post exploitation, sehingga artefak masih terbatas pada aktivitas exploitation saja.
2. Penelitian ini tidak melakukan pendekatan rule based scanner untuk disk image dalam mencari artefak IOC terkait malware. Sehingga untuk penelitian selanjutnya diharapkan bisa membuat skenario dengan kondisi

serangan malware ataupun malicious file menggunakan tool scanning seperti LOKI, Yara.

3. Pendekatan metode analisis dan tool yang digunakan pada environment GCP khususnya VM belum tentu sukses dilakukan pada platform lain. Sehingga perlu adanya petunjuk sebagai acuan prosedur.
4. Karena terbatasnya skenario serangan dan minimnya artefak yang bisa ditinggalkan, maka pada penelitian ini khususnya proses disk forensic tidak melakukan file carving. Penerapan file carving sendiri sangat diperlukan untuk memperoleh lebih banyak data data yang dihapus oleh attacker, khususnya jika attacker melakukan file wiping untuk menghilangkan jejak.