BAB V
PENUTUP

5.1 Kesimpulan

Setelah penelitian investigasi cloud iaas studi kasus *compromised* AWS EC2 selesai dilakukan, maka didapat kesimpulan sebagai berikut :

a) Penggunaan metodologi NIST dalam tahapan investigasi yang dilakukan memperoleh alur penelitian secara sistematis, dan dapat dijadikan acuan dalam penelitian

b) Aktifitas *hacking (exploitation* dan *post exploitation)* yang penulis buat dalam rancangan simulasi berhasil dianalisis dan dijabarkan alurnya dengan menganalisis bukti terkait menggunakan kolaborasi gabungan 3 metode investigasi dan sumber, yaitu *live forensic (memori image), network forensic (flow logs)* dan *disk & file system forensic (disk image)* dengan bantuan berbagai tool forensik.

c) Proses akuisisi memori *image* berbeda *server (instance)* dapat dilakukan secara *remote* tanpa *install agent* dengan memanfaatkan tool *margarita shotgun*. Untuk akusisi bukti digital *disk image* peneliti memperoleh dengan memanfaatkan fitur *snapshot*. Sedangkan perolehan bukti artefak jaringan peneliti peroleh berdasarkan log *inbound / outbound* dari bantuan *service* AWS *Flow Logs*.

d) Tahap analisis memori image pada penelitian ini tidak mendalam, hanya sebatas pembuktian *ip attacker* yang melakukan *listening connection* dan beberapa informasi pendukung artefak *filesystem timeline* bahwa attacker tidak sampai menanam malware apapun pada sistem.

e) Ketika proses penelitian berjalan, peneliti menemukan tantangan yang benar-benar menarik dari sisi *cloud environment*, yaitu AMI *instance* terupdate secara sendirinya setelah kondisi instance di *reboot*. Terupdatenya AMI ini tentu juga mengubah versi kernel dari sistem.

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 :

a) Skenario serangan *post exploitation* pada penelitian ini tidak melibatkan malware, sehingga artefak masih terbatas pada aktivitas penetration testing.
b) 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
c) Banyaknya artefak potensial yang bisa investigator dapat dan diinvestigasi pada *cloud environment* dari banyaknya cloud service (WAF, IAM) akan memberikan perspektif lebih baik dan *insight* lebih mendalam dalam proses investigasi.
d) Pendekatan metode analisis dan tool yang digunakan pada environment AWS IAAS khususnya EC2 belum tentu sukses dilakukan pada platform lain. Sehingga perlu adanya petunjuk sebagai acuan prosedur.
e) Analisis *flow logs* dan berbagai artefak berkaitan dengan data traffic *inbound/ outbound* akan lebih powerfull dan efektif menggunakan tool visualisasi seperti ELK untuk mempermudah memahami pattern traffic secara cepat dan tepat.
f) Analisis flow logs pada penelitian ini tidak memanfaatkan *service amazon CloudWatch. Amazon CloudWatch* sendiri menyediakan informasi waktu paket data tercatat, sehingga akurasi dari pengambilan keputusan seperti kapan awal mula terjadi penyerangan pertama kali lebih cepat terdeteksi hanya dengan memanfaatkan data traffic.
g) 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.