BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Cloud computing menjadi model infrastruktur baru dengan banyak keunggulan dibandingkan arsitektur *on-premise*, seperti layanan *on-demand*, elastisitas, dan *configurable computing resources* [1] [2]. Keunggulan *cloud computing* pada sisi bisnis dalam menekan biaya operasional yang begitu signifikan dan kenyamanan tanpa perlu mengelola infrastruktur membuat tren penggunaan cloud berkembang sangat pesat. Banyak organisasi, startup dan perusahaan besar bermigrasi ke penyedia *cloud* [3]. Berdasarkan data statistik Gartner, model *Infrastructure as a Service* (IaaS) akan menjadi segmen pasar yang tumbuh paling cepat dengan perkiraan pertumbuhan 24% [4]. Tim analis Forbes memprediksi penggunaan *resource* 41% dari beban kerja server perusahaan dijalankan di platform *public cloud* pada tahun 2020, 83% dari adopsi teknologi perusahaan mengimplementasikan cloud pada tahun 2020, 20% lainnya akan menerapkan *private cloud*, dan 22% bergantung pada *hybrid cloud* [5].

Amazon Web Services (AWS) merupakan salah satu *cloud provider* yang memimpin pasar *public cloud* dengan adopsi layanannya mencapai 47%. Pada 2020, metric pengguna *service publik cloud* AWS masih dominan dan menjadi *market leader* dengan porsi *market share* mencapai 47.5%, diikuti Microsoft Azure 29.4% dan *Google Cloud Platform* 3.95% [6]. AWS adalah salah satu provider besar dalam layanan *public cloud* yang menyediakan layanan seperti PaaS dan IaaS. Salah satu *Infrastructure as a Service* (IaaS) milik AWS dengan penggunaan terbanyak adalah *Elastic Cloud Computing* (EC2). Amazon EC2 *service* mengijinkan user untuk membuat *virtual machine* dengan spesifikasi dan berbagai konfigurasi yang bisa disesuaikan dengan keinginan. Pengguna dapat memonitor penggunaan *resource*, dan dipermudahnya managemen *resource* seperti *clone, pause, shutdown, delete* dan apapun yang pengguna inginkan [7]. Gambar 1.1 memperlihatkan *market share* dari tiap provider *public cloud*.

Gambar 1.1 Public Cloud Market Share [28]

Potensi kejahatan yang melibatkan layanan *cloud* karena penerapan *cloud* yang sudah sangat masif [8], terutama pada penggunaan layanan *cloud* dari provider AWS. Selain itu, ada tantangan dan kesenjangan penelitian di bidang cloud forensic menjadikan penulis tergerak mengangkat topik tersebut dengan membahas teknik investigasi yang bisa diterapkan pada lingkungan *cloud* IaaS dengan studi kasus layanan AWS EC2.

Terkait proses dan teknik investigasi pada layanan *cloud* IaaS, peneliti menggunakan gabungan teknik antara lain *network forensic, disk/file system forensic* dan *live forensic*. Hasil akhir dari penelitian ini adalah pengungkapan kasus skenario hacking yang sudah peneliti buat di environment AWS melalui berbagai artefak penting yang sudah diperoleh dari 3 teknik investigasi.

1.2 Rumusan Masalah

Merujuk uraian latar belakang diatas, maka dibuat rumusan permasalahan antara lain :

a. Apakah prosedur metodologi NIST dapat diterapkan dalam proses investigasi *cloud forensic* di *environment Amazon Web Service*?
b. Bagaimana mekanisme akuisisi investigasi *network, live*, dan *filesystem forensic* untuk mendapatkan bukti digital dan mengungkap aktivitas hacking EC2 *instance*?

c. Bagaimana hasil investigasi dari 3 metode analisis (*network, live, filesystem*) dalam mengungkap skenario serangan hacking pada EC2 *instance*?

1.3 Batasan Masalah

Agar penelitian lebih terarah dan sesuai dengan rumusan masalah yang telah dipaparkan sebelumnya, maka peneliti membuat batasan masalah. Adapun batasan masalah yang ditetapkan adalah sebagai berikut :

a. Analisis tidak dilakukan pada sisi IAM *(Identity and Access Management)*
b. Penelitian menggunakan skenario serangan pada EC2 *instance* (*compromised system*) yang digunakan sebagai acuan investigasi dan terbatas pada pembuktian serangan.
c. Analisis pada penelitian ini tidak mendalam, hanya terbatas pada skenario sederhana dengan tujuan mengenalkan tahapan forensik dan metode analisis yang bisa diterapkan pada *cloud environment*.
d. Sistem operasi yang digunakan pada EC2 *instance* adalah Ubuntu 16.04, dalam hal ini dijadikan sebagai *instance victim* atau target serangan.
e. Menggunakan teknik *disk analysis*, mengakuisisi *volume disk* EC2 dengan cara melakukan *snapshot* (duplikasi) ke *instance* baru. Hasil *snapshot* akan dianalisis dengan beberapa *file system analysis tool*dan perangkat analisis nondaring lainnya.
f. Menggunakan teknik *live forensic*, untuk mengakuisisi memori, dilakukan secara remote menggunakan *margarita shotgun tool*. Proses remote akuisisi berjalan pada EC2 *instance* lain yang sudah dipersiapkan sebelumnya, *image memory* hasil akuisisi juga akan tersimpan pada instance ini. Proses analisis *memory image* menggunakan *volatility*.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah sebelumnya maka tujuan yang ingin dicapai dari penelitian adalah :

a. Mengimplementasikan teknik disk forensic, live forensic, dan network forensic untuk melakukan investigasi skenario serangan pada pada EC2

Instance. Penelitian ini memperlihatkan secara rinci proses investigasi mulai dari akuisisi barang bukti.

b. Mencari dan menemukan artefak yang bisa dijadikan bukti pada RAM, *traffic log* dan disk EC2 instance.
c. Mengetahui karakteristik bukti digital pada artefak tiap-tiap teknik forensik.
d. Mengetahui perbandingan temuan dan pembuktian bukti digital yang didapat dari ketiga teknik forensik.

1.5 Manfaat Penelitian

Manfaat yang diharapkan pada penelitian ini berdasarkan latar belakang, rumusan masalah, batasan masalah dan tujuan adalah sebagai berikut :

a. Memberikan gambaran bagaimana melakukan investigasi secara remote pada studi kasus *cloud environment*.
b. Menjadi referensi implementasi teknik *disk forensic*, *live forensic*, dan *network forensic* untuk investigasi *cloud forensic*.
c. Memberikan gambaran karakteristik bukti digital pada artefak hasil penerapan teknik-teknik *digital forensic* untuk kegiatan *cloud forensic*.
d. Menjadi referensi akademisi dan melengkapi penelitian sebelumnya terkait proses *cloud environment investigation* khususnya pada platform AWS dengan tujuan mengembangkan penelitian forensika digital di Indonesia.

1.6 Sistematika Penulisan

Tujuan sistematika penulisan berisikan garis besar atau gambaran secara umum laporan penelitian ini sehingga mempermudah pemahaman alur isi. Adapun garis besar isi laporan skripsi sebagai berikut :

Bab I Pendahuluan, tahapan ini merupakan bab awal yang menjelaskan tentang latar belakang masalah penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

Bab II Landasan Teori, bab ini menjelaskan tinjauan pustaka dari penelitian terkait dan membahas beberapa teori terkait forensika digital, standar operasional prosedur, bukti digital, *indicator of compromise* (ioc), *network forensic*, *live*

forensic, disk forensic, SIFT Workstation, infrastructure as a service (iaas), beberapa layanan AWS, dan tool yang digunakan dalam proses investigasi.

Bab III Metodologi Penelitian, bab ini berisikan gambaran umum tentang alur proses penelitian, prosedur dan mekanisme metode analisis yang diterapkan pada skenario kasus penelitian dan skenario kasus yang diterapkan pada penelitian.

Bab IV Pembahasan, pada tahapan ini membahas implementasi skenario kasus, implementasi investigasi dan hasil analisis berbagai artefak yang dapat ditemukan menggunakan beberapa metode analisis. Bab ini juga menyampaikan rangkuman pembahasan secara teknis dari hasil analisis.

Bab V Penutup, bab ini menjelaskan tahapan terakhir yang dilakukan peneliti dan memuat kesimpulan dari keseluruhan uraian dari bab-bab sebelumnya. Tahapan ini juga memaparkan kekurangan serta saran untuk pengembangan penelitian berikutnya.

Daftar Pustaka, berisi referensi terkait dengan penelitian ini, baik melalui ebook, publikasi jurnal, dan artikel situs yang dapat menunjang proses penelitian.