BAB I
PENDAHULUAN

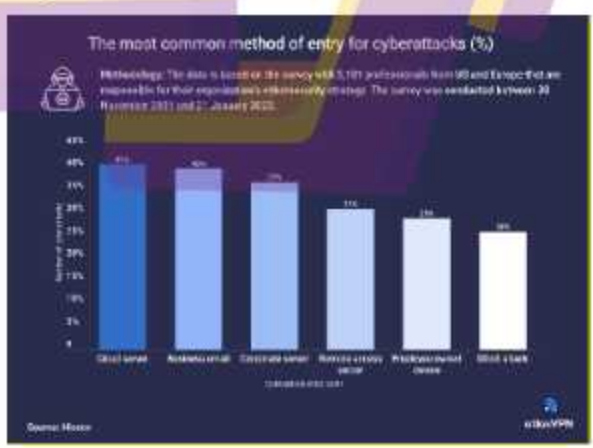
1.1 Latar Belakang

Cloud computing menjadi terobosan dan platform dengan pertumbuhan konsumen sangat pesat sekali. Komputasi awan telah memikat banyak minat penelitian ilmiah karena banyak manfaatnya dan masa depan yang menjanjikan. Selain itu, biaya rendah layanannya telah berkontribusi pada popularitas mereka yang semakin meningkat di kalangan individu, perusahaan, dan pemerintah. Komputasi awan telah secara dramatis meningkatkan utilitas praktis komputer. Cloud computing saat ini sudah banyak digunakan di bidang keuangan, manajemen bisnis, telekomunikasi, transportasi, pendidikan, iot, pemerintahan, perawatan kesehatan, dan bidang lain dalam kehidupan kita sehari-hari. Ini juga memungkinkan pengguna untuk berkomunikasi secara efisien, berbagi perangkat lunak, perangkat keras, serta sumber daya data melalui protokol jaringan.

Cloud Computing menjadi semakin menarik bagi organisasi dan individu sebagai platform untuk komputasi di mana-mana, sesuai permintaan, berdaya tinggi, dan berbiaya rendah. Tidak mengherankan, manfaat dan peluang cloud tidak hanya menarik pengguna yang sah, tetapi juga penjahat dunia maya. Ini memperburuk kemungkinan aktivitas ilegal skala besar (misalnya, penyimpanan dan distribusi materi terlarang, penyebaran infrastruktur botnet, dan kampanye phishing), memfasilitasi model bisnis baru, seperti kejahatan sebagai layanan dan "awan gelap", dan memungkinkan bentuk serangan baru dan penyalahgunaan data. Realitas ini menimbulkan banyak tantangan bagi pemangku kepentingan yang berbeda dalam hal mencegah (aspek keamanan) dan bereaksi (aspek forensik) terhadap aktivitas ilegal tersebut. Berikut detail pertumbuhan penggunaan teknologi cloud computing saat ini yang diperlihatkan pada gambar 1.1.

Gambar 1.1 Public Cloud Market Share

Potensi kejahatan yang melibatkan layanan cloud karena penerapan cloud yang sudah sangat masif, terutama pada penggunaan layanan cloud dari provider Google Cloud. 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 Google Cloud VM. Gambar 1.2 adalah data survey pada tahun 2021- 2022 dimana metode yang paling umum dilalui untuk melancarkan serangan siber adalah melalui cloud server.



Gambar 1.2 Data Survey metode penyerangan siber

Terkait proses dan teknik investigasi pada layanan cloud IaaS, peneliti menggunakan gabungan teknik antara lain network forensic, live forensic dan disk/file system forensic. Hasil akhir dari penelitian ini adalah pengungkapan kasus skenario hacking yang sudah peneliti buat di environment Google Cloud melalui berbagai artefak penting yang sudah diperoleh dari 3 teknik investigasi. Penggunaan tools foresik digital juga mendukung keberhasilan dari sebuah proses investigasi[1].

1.2 Rumusan Masalah

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

1. Apakah prosedur metodologi NIST dapat diterapkan dalam proses investigasi *Cloud Forensic* di *Environment Google Cloud Platform*?
2. Bagaimana mekanisme akuisisi investigasi live, network dan disk forensic untuk mendapatkan bukti digital dan mengungkap aktivitas hacking Google Cloud VM?
3. Bagaimana hasil investigasi dari 3 metode analisis (*live, network* dan *disk forensic*) dalam mengungkapkan skenario serangan hacking pada *Google Cloud VM*?

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 :

1. Analisis tidak dilakukan pada sisi IAM (*Identify and Access Management*)
2. Penelitian menggunakan skenario serangan pada Google Cloud VM (*infected system*) yang digunakan sebagai acuan investigasi dan terbatas pada pembuktian serangan.
3. 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*.

4. Sistem operasi yang digunakan pada *Google Cloud VM* adalah Ubuntu 20.04, dalam hal ini dijadikan sebagai VM target.
5. Menggunakan teknik disk analysis, mengakuisisi volume disk VM dengan cara melakukan snapshot (duplikasi) ke VM baru. Hasil snapshot akan dianalisis dengan beberapa *file system analysis tool* dan perangkat analisis non daring lainnya

1.4 Tujuan Penelitian

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

1. Mengimplementasikan teknik *live forensic*, *disk forensic* dan *network forensic* untuk melakukan investigasi skenario serangan pada pada *Google Cloud VM*. Penelitian ini memperlihatkan secara rinci proses investigasi mulai dari akuisisi barang bukti.
2. Mencari dan menemukan artefak yang bisa dijadikan bukti pada *traffic log* dan disk *Google Cloud VM*.
3. Mengetahui karakteristik bukti digital pada artefak tiap-tiap teknik forensik.
4. 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 :

1. Memberikan gambaran bagaimana melakukan investigasi secara remote pada studi kasus cloud environment.
2. Menjadi referensi implementasi teknik *live forensic*, *disk forensic* dan *network forensic* untuk investigasi *cloud forensic*.
3. Memberikan gambaran karakteristik bukti digital pada artefak hasil penerapan teknik-teknik digital *forensic* untuk kegiatan *cloud forensic*.
4. Menjadi referensi akademisi dan melengkapi penelitian sebelumnya terkait proses cloud environment investigation khususnya pada *platform Google*

Cloud 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 forensik 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 GCP, 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.