BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan informasi merupakan hal yang sangat penting terutama dalam dunia digital seperti saat ini. Informasi yang bersifat privasi tidak boleh sampai tersebar luaskan secara umum karena hanya orang yang berkepentingan saja yang boleh mengaksesnya karena hal ini sudah merusak aspek dalam konsep CIA. Dengan perkembangan zaman, semua informasi tersimpan kedalam sebuah wadah digital digital yang disebut penyimpanan data (*database*) sehingga informasi yang dicari akan dengan mudahnya didapatkan, oleh karena itu pentingnya aspek keamanan perlu diperhatikan untuk menjaga keaslian data tersebut. Penyimpanan data memerlukan sebuah infrastruktur untuk menunjang sumber daya yang dibutuhkan dalam memproses sekumpulan data, sehingga data bisa lebih cepat untuk diakses dan infrastruktur yang digunakan adalah sistem komputer yang menyediakan kebutuhan pengguna atau disebut sebagai *server*. Sistem tersebut terbagi lagi menjadi beberapa jenis layanan, salah satunya adalah komputasi awan yang merupakan teknologi modern serta menyediakan bermacam jenis model layanan seperti Infrastructure as Service (IaaS), Software as Service (SaaS), Platform as Service (PaaS) dan lainnya.

Komputasi awan menjadi model bisnis baru yang juga disediakan oleh perusahan terkemuka seperti Google, Amazon, dan Microsoft. Ketiganya membuat produk masing-masing dengan tujuan menyediakan sumber daya yang diperlukan oleh pengguna dengan cepat, fleksibel dan mudah digunakan. Perusahaan Google membuat layanan awan yang bernama Google Cloud Platform, kemudian Amazon yang awalnya merupakan sebuah *marketplace* juga membuat layanan awan bernama Amazon Web Services dan Microsoft dengan Microsoft Azure. Layanan tersebut juga memiliki berbagai macam produk yang menyesuaikan dengan kebutuhan penggunanya, sehingga pengguna tidak perlu mengkhawatirkan sumber daya yang digunakan seperti bagaimana dalam mengelolanya, maupun merawatnya (*maintenance*), dan pengguna hanya cukup

membayar dari sumber daya yang digunakannya. Dengan adanya komputasi awan bukan berarti semua hal dikelola secara menyeluruh oleh penyedia layanan, melainkan pengguna juga memiliki tanggung jawab yang perlu diperhatikan ketika menggunakan layanan cloud, seperti contohnya data yang tersimpan didalam sebuah cloud merupakan tanggung jawab pengguna karena pengguna hanya menyewa sistem yang disediakan, dan penyedia layanan tidak bertanggung jawab atas data yang ada didalamnya, penyedia hanya memberikan sumber daya fisik yang dapat digunakan dengan mudahnya.

Hal ini membuat pengguna harus mengetahui bagaimana cara mengelola sumber daya yang digunakannya dengan baik, terutama dalam aspek keamanannya. Dari berbagai penyedia layanan, masing-masing diantaranya memiliki kelebihan dan kekurangan dalam berbagai macam aspek sehingga pengguna harus bijak dalam memilih layanan cloud yang akan digunakannya, dengan meninjau dari studi kasus yang akan dihadapi, anggaran yang dibutuhkan, layanan apa saja yang akan digunakan dalam jangka waktu lama maupun rencana perubahan layanan saat ini dengan masa yang mendatang sehingga akan sangat berdampak pada kualitas produk digital yang dibuat dan anggaran yang digunakan dapat semakin mengecil.

Aspek keamanan juga sangat penting ketika menggunakan komputasi awan, teknologi ini memudahkan pengguna untuk melakukan kustomisasi pada layanannya. Bagaimana sebuah layanan yang dibuat dapat disesuaikan dengan kebutuhan penggunanya seperti dapat menyimpan informasi publik seperti gambar, video dan lainnya maupun menyimpannya secara pribadi yang dimana orang lain tidak dapat mengaksesnya. Masalah yang sering dihadapi ketika individu atau organisasi mulai mengadopsi komputasi awan adalah kebocoran data, kurangnya pengetahuan mengenai keamanan cloud menyebabkan terjadinya masalah tersebut sehingga diperlukannya sosialisasi mengenai cara mengamankan komputasi awan pada layanan tertentu seperti Google Cloud Platform, Amazon Web Services, Microsoft Azure, Linode, Digital Ocean dan masih banyak lagi. Penyampaian konsep keamanan yang baik, dapat terimplementasikan ke semua

penyedia layanan cloud karena secara garis besar perbedaannya adalah fitur-fitur yang disediakan atau tidaknya oleh penyedia layanan.

Dari permasalahan diatas, tim Work From Cloud fokus untuk mengadakan *sharing session* mengenai keamanan di bidang cloud dan mengikuti kompetisi dibidang keamanan komputasi awan seperti Cloud Village DEFCON 29 dalam rangka menambah wawasan terutama pada layanan cloud yang banyak digunakan perusahaan seperti Amazon Web Services, Google Cloud Platform dan Alibaba yang menjadi tantangan dalam kompetisi ini.

1.2 Uraian Lomba

Hacker Summer Camp adalah event yang diadakan pada setiap musim panas dimana banyak konferensi keamanan informasi / keamanan siber / Hacker Conferences di Las Vegas, Nevada, USA. Dengan event ini banyak orang memnghabiskan sepanjang minggu di Las Vegas dalam Summer Learning yang mendapat julukan "Hacker Summer Camp". Pada tahun 2021 ada beberapa event yang dapat diikuti dengan acara utama:

- Diana Initiative - July 16-17, 2021 - Virtual - open to all, women focused
- h@cktivitycon is a HackerOne hosted hacker conference
- Black Hat USA - July 31-August 5, 2021 - four days of technical Trainings followed by the two-day main conference featuring Briefings, Arsenal, Business Hall, and more.
- BSidesLV - virtual on July 31 and August 1, 2021
- DEF CON - August 5-8, 2021 Hybrid
- DEF CON Villages
- DC Furs
- Queercon is hosting events on their discord QueerCord
- HOPE - Hackers On Planet Earth - August 13-15, 2021 - In Person NYC

Cloud Village adalah sistem untuk bertemu dengan orang-orang yang tertatik dengan aspek ofensif dan defensif pada cloud. *Cloud Village* adalah pusat bagi

kegiatan seperti seminar, lokakarya, KKP, dan diskusi seputar layanan *cloud. Cloud Village* memberikan pengetahuan tentang cara menjaga cloud stack dengan aman. Event ini ditujukan untuk orang yang ingin memecahkan tantangan pada *cloud* dengan mengikuti alur cerita yang rumit untuk membantu tim menemukan flag.

DEF CON 29 2021 membuka 2 tipe lomba yang dapat diikuti yaitu Red Team Village CyberWraith dan CTF. Pada lomba CTF ada beberapa event yang dapat diikuti yaitu: OOO's DEF CON CTF, Bio Hacking Village CTF, OSINT Search Party CTF, Car Hacking Village CTF, Cloud Village CTF, Crypto and Privacy Village Workshop and CTF, Sea-TF - Hack the Sea Village CTF, ICS Village - CTF, CISA ICS Capture the Flag, IoT Village CTF, A-ISAC CTF @ Aerospace Village, OpenSOC CTF, Red Team Village Capture the Flag (CTF), dan RF Village RFCTF

CTF Cloud Village Defcon 29 adalah event dengan model *joepardy* selama tiga hari dimana tim memiliki banyak tantangan yang diselenggarakan oleh panitia dengan berbagai kategori kesulitan pada lingkungan penyedia layanan cloud seperti AWS, GCP, Azure dan Alibaba. Event ini dapat diikuti sebagai tim atau individu, menggunakan petunjuk yang diberikan guna membantu menemukan flag yang ada.

1.3 Keunikan Event

DEF CON adalah salah satu konvensi hacker tertua yang masih aktif dan salah satu yang terbesar dikalangan event internasional. Setiap tahunnya para peretas berkumpul pada event ini untuk melakukan hal-hal yang menakjubkan dibidang IT khususnya hacking dan keamanan komputer. DEF CON biasanya dihadiri oleh penggiat IT dari seluruh dunia. Event ini memberikan beberapa kompetisi seperti Call For Everything (CFE) dan kompetisi Capture The Flag (CTF).

1.4 Manfaat dan Tujuan Event

Manfaat CTF adalah untuk menguji dan melatih kemampuan dalam bidang kemanan sistem. Capture The Flag (CTF) adalah salah satu jenis kompetisi hacking dimana seseorang atau tim mengharuskan mengambil sebuah file atau informasi yang sudah disembunyikan pada sistem yang dimana disebut dengan istilah "flag". Untuk kompetisi CTF pada DEFCON menggunakan tipe joepardy yang menggunakan server untuk menyimpan soal tantangan dimana soal tersebut berbentuk *web exploitation, forensic, cryptography, steganography*, dll dengan tujuan mencari string atau flag yang disembuntikan pada server.