BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam zaman digital ini, keamanan siber menjadi hal yang penting untuk mengantisipasi terjadinya serangan-serangan atau insiden yang berada di luar ekspektasi, seperti serangan siber atau bencana alam. Hal ini akan menjadi sebuah bencana/insiden siber ketika data yang tersimpan merupakan data yang sensitif bagi seseorang atau bahkan suatu lembaga yang bertanggungjawab pada jutaan individu. Pada tanggal 12 Maret 2023, data BPJS masyarakat Indonesia ditemukan terunggah dalam forum *"Breached"*, di mana data tersebut mengandung NIK (Nomor Induk Kependudukan), nama, email, nomor ponsel, alamat, tempat tanggal lahir, jenis kelamin, pekerjaan, tempat bekerja, dll. (Wamad Sudirman 2023). Hal ini menunjukkan pentingnya untuk memikirkan pengamanan data agar tidak mudah bocor sehingga tidak diakses oleh pihak-pihak yang tidak berkepentingan.

Menurut National Institute of Standards and Technology (NIST) dalam (Mell and Timothy 2011), *Cloud Computing* adalah sebuah *model* yang menyediakan akses yang nyaman (*on-demand* dan dapat diakses kapan pun dan di mana pun) terhadap sejumlah sumber daya komputasi yang dapat dikonfigurasi serta dapat disediakan dan dilepaskan dengan mudah dengan interaksi dengan *Service Provider* yang minim. Saat ini, *Cloud Computing* merupakan salah satu topik yang sedang banyak dibicarakan dalam dunia penelitian dan industri (Alouffi et al. 2021b). Hal ini dikarenakan kemampuannya dalam menyediakan daya

komputasi dan penyimpanan melalui internet untuk membantu bisnis mengembangkan aplikasi/sistem dengan menyewa jasa layanan komputasi sesuai kebutuhan (Joshi et al. 2023). *Cloud Computing* dapat diartikan sebagai sebuah teknologi yang memungkinkan individu atau bisnis untuk mengakses dan menggunakan sumber daya komputasi dan penyimpanan data sesuai yang dibutuhkan melalui internet. Dalam kata lain, *"The Network is the Computer"* (Baars and Spruit 2012). Hal ini memungkinkan pengguna untuk memperoleh sumber daya komputasi dan penyimpanan data tanpa memiliki atau mengatur perangkat keras secara fisik.

Cloud Computing tentunya merupakan teknologi yang mampu membantu bisnis/penelitian, namun salah satu hal yang perlu dipertimbangkan sebelum mengadopsi sistem Cloud adalah keamanan karena dengan memindahkan/mengalokasikan sistem kita di Cloud, sistem kita menjadi dapat diakses oleh siapa pun melalui internet dan membuatnya lebih rentan terhadap serangan-serangan siber. Cloud Service Provider (CSP) besar seperti Google Cloud, Microsoft Azure, dan AWS sudah memiliki solusi untuk mengamankan sistem *customer* mereka di Cloud (Padhy, Patra, and Satapathy 2011), namun peran untuk mengamankan data *customer* juga bergantung dengan konfigurasi yang dilakukan oleh *customer* saat menggunakan layanan-layanan di CSP tersebut (Google Cloud 2023). Maka penting sekali untuk memastikan konfigurasi dari sistem yang dialokasikan di Cloud sesuai dengan kebutuhan keamanan. Hal ini penting karena ditemukan oleh (Zuo, Lin, and Zhang 2019b), bahwa kesalahan konfigurasi

merupakan salah satu isu terbesar dalam keamanan sistem di lingkungan Cloud. Namun bagaimana cara agar kita dapat memastikan keamanan dari sistem?

Penetration Testing menurut NIST (Singhal, Winograd, and Scarfone 2007), merupakan sebuah metode pengujian pada komponen tertentu ataupun keseluruhan dari sebuah aplikasi untuk memastikan *vulnerability* (kerentanan) di dalam atau antar komponen dapat dieksploitasi untuk mengkompromisasi sebuah aplikasi, data aplikasi tersebut, ataupun sumber daya dari lingkungan aplikasi tersebut. *Penetration Testing* merupakan sebuah proses untuk verifikasi keamanan dari sebuah sistem dengan melakukan sejumlah simulasi dari berbagai serangan siber terhadap sistem tersebut sebelum terjadi sebuah insiden siber. Dalam lingkungan Cloud, *Penetration Testing* menjadi hal yang sangat penting untuk meningkatkan keamanan dari sebuah sistem pada *Public* dan *Private Cloud* dengan 1) mencari *vulnerability* dan risiko dalam sistem, 2) memastikan keamanan sistem sudah mengikuti standar industri, 3) dan meningkatkan kemampuan tim/perusahaan untuk menanggapi ketika terjadi sebuah insiden siber (Varghese 2024). Ditambahkan oleh (Varghese 2024) bahwa titik fokus saat menjalankan *Penetration Testing* di lingkungan Cloud dapat dibagi menjadi 3 kategori utama, yaitu 1) *Cloud Application Security* (*API Security, IAM Configuration, Web Vulnerabilities, Cloud Misconfigurations*), 2) *Cloud Infrastructure Security* (*Virtual Machine, Container, Firewall, Storage* and *Data Management for Data Access*, *Access Control, Image Security, Runtime Protection*, Orchestration Platform *Configurations*, dan *Patch Levels*), dan 3) *Cloud Compliance/Governance* (*Data Access*, Metode Penyimpanan, *Monitoring System Logs* yang sesuai dengan standar industri).

Cukup banyak hal yang bisa dan perlu dilakukan dalam proses *Penetration Testing* di lingkungan Cloud untuk verifikasi keamanan dari sistem tersebut, maka diperlukan sebuah standar/framework untuk melakukan *Penetration Testing* di lingkungan Cloud dengan efektif.

Ada beberapa standar *Penetration Testing* di lingkungan Cloud, seperti OWASP (Open Worldwide Application Security Project) Cloud-Native Application Security Top 10, CSA Cloud Control Matrix, NIST SP 800-53 Rev 5, dan Payment Card Industry Data Security Standard (PCI DSS) (Varghese 2024). Masing-masing framework memiliki fokus untuk menjadi panduan dalam mengamankan sistem/aplikasi dari isu-isu siber terkini.

Peneliti menemukan beberapa penelitian yang sudah mencoba membahas topik ini. Dalam penelitian (Al-Khannak and Nehal 2023a), peneliti melakukan sejumlah eksperimen dalam melakukan simulasi serangan-serangan siber pada aplikasi web yang berisiko tinggi berdasarkan OWASP Top 10, seperti XSS, Command Injection, dan Unrestricted File Uploads pada sebuah aplikasi web Damn Vulnerable Web Application (DVWA) yang di host sebuah *Virtual Machine* (VM) di lingkungan Amazon Web Services (AWS) Cloud. Namun penelitian tersebut lebih fokus terhadap keamanan dari aplikasi web tersebut dibanding keamanan dari infrastruktur yang menjalankannya, di mana hal tersebut merupakan salah satu fokus dari *Penetration Testing* aplikasi web berbasis Cloud.

Penelitian lain yang serupa adalah (Denis, Zena, and Hayajneh 2016) di mana peneliti melakukan eksperimen untuk serangan-serangan siber seperti Man-in-the-Middle (MITM), Hacking Remote PC dengan Port Scanner, Traffic Sniffing,

Hacking Phone Bluetooth, Hacking WPA-Protected WiFi, dan Spying. Namun penelitian tersebut tidak dilakukan berdasarkan standar/framework *Penetration Testing* seperti OWASP Top 10, NIST, OSSTMM, ISSAF, ataupun PTES. Penelitian tersebut juga tidak dilakukan pada sistem berbasis Cloud.

Penelitian-penelitian (Alhamed and Rahman 2008; Singh, Jeong, and Park 2016; Hasan and Meva 2018) membahas mengenai *vulnerability* dan serangan-serangan umum yang terjadi pada sistem-sistem Cloud maupun Non-Cloud berdasarkan sumber-sumber bereputasi termasuk OWASP Top 10 sekaligus menyertakan metode dan *tools* yang umum digunakan untuk serangan-serangan siber tersebut. Namun penelitian-penelitian tersebut tidak melakukan eksperimen untuk mendemonstrasikan isu-isu siber yang disebutkan.

Dari studi literatur yang dilakukan oleh peneliti mengenai topik *Penetration Testing* di lingkungan Cloud, peneliti menyadari kurangnya penelitian yang melakukan eksperimen dari isu-isu keamanan siber aplikasi web berbasis Cloud terkhususnya yang berdasarkan standar/*framework Penetration Testing* yang bereputasi dan terkini seperti NIST, OWASP Top 10, OSSTMM, CSA, ISSAF, dan PTES. Dengan meningkatnya penggunaan Cloud dalam bisnis dan penelitian, peneliti melihat pentingnya untuk proses *Penetration Testing* yang efektif pada sistem-sistem berbasis Cloud agar dapat diamankan dari isu-isu/serangan-serangan siber terkini sebelum terjadinya insiden siber.

Dalam penelitian ini, peneliti akan fokus dalam bereksperimen dengan melakukan *Penetration Testing* Aplikasi Web yang dijalankan di sebuah Infrastruktur Cloud Computing yang diimplementasikan dalam lingkungan Google

Cloud (GCPGoat) berdasarkan metodologi *Penetration Testing "Four-Stage Penetration Testing Methodology"* (ditunjukkan dalam Gambar 2.1) yang tertera dalam NIST SP 800-115 (Scarfone et al. 2008a) untuk mendemonstrasikan isu-isu keamanan di lingkungan Cloud terkini yang dibahas dalam *"Top Threats to Cloud Computing 2024"* (CSA 2024c) (ditunjukkan dalam Gambar 2.2). Kemudian peneliti juga akan menyediakan solusi teknis dan non-teknis untuk memitigasi *vulnerability* yang ditemukan dengan memberikan rekomendasi mitigasi berdasarkan sumber bereputasi (NIST, OWASP, dan CSA) dan layanan-layanan keamanan yang sudah disediakan oleh Cloud Service Provider (CSP) Google Cloud.

Keberhasilan dari simulasi masing-masing isu teratas dalam CSA *"Top Threats to Cloud Computing 2024"* ditentukan dari keberhasilan serangan yang dijalankan untuk mengeksploitasi masing-masing isu yang ditemukan dalam Infrastruktur GCPGoat (Gambar 3.4). Hal ini mengutip penjelasan NIST dalam publikasi *"Technical Guide to Information Security Testing and Assessment"* (Scarfone et al. 2008a) di mana sebuah isu akan berhasil diverifikasi dengan keberhasilan serangan yang dilakukan untuk mengeksploitasi isu tersebut.

Walaupun penelitian akan sebagian besar dijalankan pada lingkungan Google Cloud, peneliti berharap hasil dari penelitian ini tetap dapat 1) membuat perusahaan dan penelitian untuk waspada terhadap pengamanan sistem dan data yang mereka alokasikan saat mengadopsi teknologi Cloud, 2) mengarahkan perusahaan dan penelitian dalam mengamankan sumber daya tersebut berdasarkan standar dari sumber yang bereputasi seperti NIST, OWASP, dan CSA, dan 3) melihat besarnya

sebuah risiko yang ditimbulkan oleh sekumpulan kesalahan kecil/sederhana dalam lingkungan Cloud.

1.2 Rumusan Masalah

Rumusan masalah yang akan dibahas dalam penelitian ini adalah sebagai berikut:

Bagaimana cara melakukan simulasi isu keamanan Cloud dalam CSA *"Top Threats to Cloud Computing 2024"* pada aplikasi web berbasis Cloud menggunakan metodologi NIST *"Four-Stage Penetration Testing"*?

1.3 Batasan Masalah

Dalam penelitian ini, diperlukan beberapa batasan yang digunakan sebagai acuan dalam pelaksanaan penelitian untuk memberikan arah yang jelas dalam pengembangannya. Batasan-batasan yang terdapat dalam penelitian adalah sebagai berikut:

1) *Penetration Testing* akan memanfaatkan Kali Linux dengan *tools* Open Source.
2) *Penetration Testing* akan dijalankan mengikuti metodologi *"Four-Stage Penetration Testing Methodology"* oleh NIST (Scarfone et al. 2008a) (Gambar 2.1).
3) *Penetration Testing* akan fokus dalam mengidentifikasi isu-isu keamanan yang jatuh ke tanggung jawab *customer* di Google Cloud berdasarkan model *"shared responsibility and shared fate"* di Google Cloud (Gambar 2.3).
4) *Penetration Testing* akan fokus dalam mengidentifikasi isu-isu keamanan

lingkungan Cloud yang dijelaskan dalam publikasi CSA berjudul *"Top Threats to Cloud Computing 2024"* (CSA 2024c), khususnya 4 isu keamanan teratas, yaitu: 1) *Misconfiguration and Inadequate Change Control*, 2) *Identity and Access Management*, 3) *Insecure Interfaces and APIs*, dan 4) *Inadequate Cloud Security Strategy*.

5) *Penetration Testing* akan dilakukan pada sebuah Google Cloud Platform (GCP) Project yang menjalankan aplikasi bernama GCPGoat (Litesh 2023), sebuah Infrastruktur *Cloud Computing* yang diimplementasikan dalam lingkungan Google Cloud yang menjalankan sebuah aplikasi web berbentuk blog yang memanfaatkan sejumlah layanan Google Cloud dengan konfigurasi yang dapat dieksploitasi.

6) Rekomendasi Mitigasi yang diberikan dari hasil *Penetration Testing* GCPGoat akan melibatkan pemanfaatan layanan-layanan keamanan yang disediakan oleh Google Cloud dan *best practices* dari standar-standar bereputasi yang bersumber dari OWASP, NIST, dan CSA.

7) Keberhasilan dari simulasi masing-masing isu keamanan Cloud teratas dalam publikasi CSA *"Top Threats To Cloud Computing 2024"* akan ditentukan dari keberhasilan serangan yang digunakan untuk mengeksploitasi masing-masing isu yang ditemukan dalam Infrastruktur GCPGoat.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mensimulasikan isu keamanan Cloud berdasarkan CSA *"Top Threats to Cloud Computing 2024"* pada aplikasi web berbasis Cloud dengan melakukan *Penetration Testing* yang mengikuti metodologi *"Four-Stage Penetration Testing"* dari NIST.

1.5 Metodologi

Untuk menyelesaikan masalah pada penelitian ini, metode-metode yang digunakan adalah:

Penelitian akan dilakukan secara bertahap:

1) Penelitian akan dimulai dengan Studi Pustaka untuk mempelajari keterampilan untuk melakukan *Penetration Testing* pada Aplikasi Web berbasis Cloud menggunakan *tools* Open Source sekaligus mendalami pengetahuan mengenai Google Cloud untuk menambahkan wawasan ketika melakukan pengujian serta merancang rekomendasi berdasarkan hasil penelitian.
2) Peneliti akan menjalankan *Penetration Testing* berdasarkan NIST *"Four-Stage Penetration Testing Methodology"* seperti yang ditunjukkan pada Gambar 2.1 terhadap infrastruktur GCPGoat.
3) Peneliti akan mengaitkan penemuan selama *Penetration Testing* dengan 4 isu keamanan Cloud teratas yang disebutkan dalam publikasi CSA *"Top Threats to Cloud Computing 2024"* (CSA 2024c)

4) Peneliti akan memberikan strategi dan rekomendasi pengamanan teknis maupun non-teknis berdasarkan hasil dari *Penetration Testing* yang dilakukan selama penelitian dengan melibatkan pemanfaatan layanan keamanan Google Cloud dan *best practices* dari standar-standar bereputasi (seperti OWASP, NIST, dan CSA).

1.6 Sistematika Penulisan

Laporan tugas akhir ini disusun dengan menggunakan sistematika penulisan yang dapat dijelaskan sebagai berikut:

BAB I PENDAHULUAN

Bab ini dimulai dengan penjelasan mengenai latar belakang penelitian yang berjudul "Simulasi Keamanan Cloud: CSA Top Threats 2024 pada Aplikasi Web Berbasis Cloud dengan Penetration Testing". Kemudian dalam bab ini juga dibahas penentuan rumusan dan batasan masalah serta penjelasan tujuan penelitian dan metodologi yang digunakan pada penelitian ini. Pada akhir bab ini dijelaskan mengenai sistematika penulisan yang digunakan.

BAB II LANDASAN TEORI

Bab ini berisi tentang teori-teori yang digunakan sebagai acuan dalam merancang dan mengembangkan tugas akhir meliputi *Cloud Computing*, *Penetration Testing*, NIST *"Four-Stage Penetration Testing"*, CSA *"Top Threats to Cloud Computing 2024"*, dan Google Cloud.

BAB III ANALISA DAN PERANCANGAN SISTEM

Bab ketiga berisi tentang penjelasan mengenai infrastruktur sistem yang dilakukan *Penetration Testing*, termasuk proses membangun infrastruktur tersebut, layanan Google Cloud yang digunakan, dan gambaran lingkungan Cloud tersebut. Selain itu, bagian ini juga menjelaskan Web Service "XSS Server" yang dibuat oleh peneliti yang akan digunakan dalam proses *Penetration Testing*, termasuk cara kerja, infrastruktur, *source code*, dan proses *deploy* Web Service tersebut. Penjelasan cara kerja akan didukung dengan penjelasan dari NIST dan divisualisasikan.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini berisikan penjelasan mengenai implementasi simulasi proses mengidentifikasi isu-isu keamanan Cloud teratas berdasarkan CSA dalam publikasi *"Top Threats to Cloud Computing"* (CSA 2024b). Simulasi tersebut akan mengikuti metodologi *"Four-Stage Penetration Testing"* milik NIST. Penjelasan akan dimulai dengan menunjukkan garis besar dari proses *Penetration Testing* serta *tools* dan teknik yang digunakan selama implementasi dan pengujian tersebut.

BAB V KESIMPULAN DAN SARAN

Bab lima ini merupakan bab terakhir yang berisikan kesimpulan yang diperoleh dari pengujian yang telah dilakukan serta saran untuk pengembangan atau pendalaman lebih lanjut.