# ABSTRACT

Christian Kasih Pratama Setiawan (01082210008)

**Cloud Security Simulation: CSA Top Threats 2024 on Cloud-Native Web Applications through Penetration Testing**

(xxiii + 290 pages: 169 figures; 16 tables, 1 appendices)

In today's digital era, cybersecurity is important to anticipate attacks and incidents that may occur beyond our expectations. Security should be considered in any information system, including those that benefit from *Cloud Computing* technology, which has lately been popular in the research and industrial world. Security in using Cloud technology is important because moving our system to the Cloud will make it accessible to anyone over the Internet, which increases the *attack surface*. CSA's publication titled *"Top Threats to Cloud Computing 2024"*, that misconfigurations given by the *customer* towards their Cloud resources are the most concerning issue in 2024. This shows the importance of ensuring our Cloud resources are given appropriate configurations that follow the best security standards and practices from trusted sources like NIST, OWASP, or CSA.

*Penetration Testing* is a method for identifying security weaknesses in a system by simulating a real cyber-attack. Much can be done in *Penetration Testing*, so assessors should follow a standard/framework to improve results. This research focuses on simulating the top Cloud security issues based on CSA's *"Top Threats to Cloud Computing 2024"* by following NIST's *"Four-Stage Penetration Testing"* framework. The assessment will be done on a web application running on a Cloud Computing Infrastructure, GCPGoat.

This research successfully identified and simulated the top 4 cloud security issues described in *"Top Threats to Cloud Computing 2024"* by performing successful attacks that exploits each issue on the assessed infrastructure (GCPGoat). It also includes technical and non-technical recommendations to secure the infrastructure. Hopefully, this research can improve the awareness of those interested in adopting Cloud technology regarding the security of their digital assets, showing that a set of small mistakes can lead to huge losses.

Reference: 243 (1999 – 2024)

# ABSTRAK

Christian Kasih Pratama Setiawan (01082210008)

**Simulasi Keamanan Cloud: CSA Top Threats 2024 pada Aplikasi Web Berbasis Cloud dengan Penetration Testing**

(xxiii + 290 halaman: 169 gambar; 16 tabel; 1 lampiran)

Dalam zaman digital ini, keamanan siber menjadi hal yang penting untuk mengantisipasi terjadinya serangan-serangan atau insiden yang berada di luar ekspektasi. Keamanan siber sebaiknya diperhatikan dalam sistem informasi apa pun, termasuk yang memanfaatkan teknologi *Cloud Computing*, yang merupakan salah satu topik yang sedang banyak dibicarakan dalam dunia penelitian dan industri. Keamanan dalam pemanfaatan teknologi Cloud penting karena pemindahan sistem ke Cloud akan membuat sistem dapat diakses oleh siapa pun melalui Internet, meningkatkan kerentannya terhadap serangan-serangan siber. Dalam publikasi CSA berjudul "Top Threats to *Cloud Computing 2024"*, kesalahan konfigurasi *customer* terhadap sumber daya Cloud merupakan isu keamanan yang paling perlu diperhatikan dalam tahun 2024. Hal ini menunjukkan pentingnya untuk memastikan konfigurasi dalam lingkungan Cloud sudah mengikuti standar keamanan dan *best practices* dari sumber-sumber terpercaya, seperti NIST, OWASP, dan CSA.

*Penetration Testing* merupakan sebuah metode untuk mengidentifikasi kelemahan keamanan sebuah sistem dengan mensimulasikan sebuah serangan siber. Ada banyak sekali hal yang dapat dilakukan dalam melakukan *Penetration Testing*, maka penting bagi para penguji untuk mengikuti sebuah standar/*framework* untuk meningkatkan hasil dari pengujian tersebut. Dalam penelitian ini, peneliti akan fokus dalam mensimulasikan isu-isu keamanan terutama dalam lingkungan Cloud berdasarkan *"Top Threats to Cloud Computing 2024"* oleh CSA dengan mengikuti *framework "Four-Stage Penetration Testing"* oleh NIST. Pengujian tersebut akan dilakukan terhadap aplikasi web yang dijalankan di sebuah Infrastruktur Cloud Computing, GCPGoat.

Hasil dari penelitian ini berhasil mengidentifikasi dan mensimulasikan 4 isu-isu keamanan teratas dalam *"Top Threats to Cloud Computing 2024"* dengan melakukan serangan yang berhasil mengeksploitasi masing-masing isu dari infrastruktur yang diuji (GCPGoat). Peneliti juga menyertakan rekomendasi-rekomendasi teknis maupun non-teknis untuk meningkatkan keamanan infrastruktur tersebut. Peneliti berharap hasil penelitian ini dapat meningkatkan kesadaran pihak-pihak yang tertarik mengadopsi teknologi Cloud untuk memperhatikan keamanan dari aset digital mereka, menunjukkan bahwa kumpulan kesalahan kecil dapat menyebabkan kerugian besar.

Referensi: 243 (1999 – 2024)