ANALISIS SIMULASI KEAMANAN SIBER YANG DILAKUKAN DI BSSN

LAPORAN MBKM MAGANG

RAISYA PUTRI VIRNANDA
00000081024

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2025

ANALISIS SIMULASI KEAMANAN SIBER YANG DILAKUKAN DI BSSN

LAPORAN MBKM MAGANG

RAISYA PUTRI VIRNANDA
00000081024

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA

TANGERANG
2025

HALAMAN PERNYATAAN ORISINALITAS TIDAK PLAGIAT

Dengan ini saya,

Nama	:	Raisya Putri Virnanda
NIM	:	00000081024
Program Studi	:	Informatika

Menyatakan dengan sesungguhnya bahwa Laporan MBKM Magang saya yang berjudul:

Analisis Simulasi Keamanan Siber yang Dilakukan di BSSN

merupakan hasil karya saya sendiri, bukan merupakan hasil plagiat, dan tidak pula dituliskan oleh orang lain; Semua sumber, baik yang dikutip maupun dirujuk, telah saya cantumkan dan nyatakan dengan benar pada bagian Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan karya ilmiah, saya bersedia menerima konsekuensi untuk dinyatakan TIDAK LULUS. Saya juga bersedia menanggung segala konsekuensi hukum yang berkaitan dengan tindak plagiarisme ini sebagai kesalahan saya pribadi dan bukan tanggung jawab Universitas Multimedia Nusantara.

Tangerang, 19 Juni 2025

(Raisya Putri Virnanda)

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH MAHASISWA

Yang bertanda tangan di bawah ini:

Nama	:	Raisya Putri Virnanda
NIM	:	00000081024
Program Studi	:	Informatika
Jenjang	:	S1
Jenis Karya	:	Laporan MBKM Magang

Menyatakan dengan sesungguhnya bahwa:

☑ Saya bersedia memberikan izin sepenuhnya kepada Universitas Multimedia Nusantara untuk mempublikasikan hasil karya ilmiah saya di repositori Knowledge Center, sehingga dapat diakses oleh Civitas Akademika/Publik. Saya menyatakan bahwa karya ilmiah yang saya buat tidak mengandung data yang bersifat konfidensial dan saya juga tidak akan mencabut kembali izin yang telah saya berikan dengan alasan apapun.

☐ Saya tidak bersedia karena dalam proses pengajuan untuk diterbitkan ke jurnal/konferensi nasional/internasional (dibuktikan dengan *letter of acceptance*)**.

Tangerang, 19 Juni 2025

Yang menyatakan

Raisya Putri Virnanda

** Jika tidak bisa membuktikan LoA jurnal/HKI selama enam bulan ke depan, saya bersedia mengizinkan penuh karya ilmiah saya untuk diunggah ke KC UMN dan menjadi hak institusi UMN.

Halaman Persembahan / Motto

”Plans are useless, but planning is indispensable.”

Dwight D. Eisenhower

KATA PENGANTAR

Puji dan syukur saya panjatkan kehadirat Allah SWT atas rahmat, karunia, dan bimbingan-Nya sehingga laporan magang ini dapat diselesaikan dengan baik. Laporan ini disusun sebagai salah satu bentuk pertanggungjawaban akademik dalam pelaksanaan program magang yang merupakan salah satu syarat kelulusan untuk mendapatkan gelar Sarjana Komputer di Program Studi Informatika, Universitas Multimedia Nusantara. Melalui kegiatan magang ini, saya memperoleh pengalaman langsung dalam menerapkan ilmu yang telah dipelajari, khususnya di bidang keamanan siber. Harapan dari penyusunan laporan ini adalah agar dapat memberikan gambaran menyeluruh mengenai proses pembelajaran dan kontribusi yang diberikan selama masa magang, serta menjadi dokumentasi yang bermanfaat ke depannya. Oleh karena itu, saya mengungkapkan banyak terima kasih kepada:

1. Bapak Dr. Ir. Andrey Andoko, M.Sc., selaku Rektor Universitas Multimedia Nusantara.
2. Bapak Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Bapak Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, selaku Ketua Program Studi Informatika Universitas Multimedia Nusantara.
4. Ibu Alethea Suryadibrata, S.Kom., M.Eng., sebagai Pembimbing magang yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi atas terselesainya laporan magang ini.
5. Kepala Biro Hukum Sestama Sekretariat Utama BSSN dan Kepala Pusdatik yang telah memberikan kesempatan berharga bagi saya untuk mengikuti program kerja magang.
6. Ketua tim Manajemen Risiko dan Keberlangsungan TIK beserta seluruh tim yang telah mendampingi dan membimbing selama melaksanakan program kerja magang.
7. Orang Tua dan keluarga saya yang telah memberikan bantuan dukungan material dan moral, sehingga penulis dapat menyelesaikan laporan magang ini.

8. Pihak-pihak lain yang tidak dapat disebutkan satu per satu yang ikut membantu dalam menyelesaikan laporan magang ini.

Tangerang, 19 Juni 2025

Raisya Putri Virnanda

ANALISIS SIMULASI KEAMANAN SIBER YANG DILAKUKAN DI BSSN

Raisya Putri Virnanda

ABSTRAK

Pengalaman magang di Badan Siber dan Sandi Negara (BSSN) yang bertujuan untuk memahami penerapan prinsip keamanan siber, mengidentifikasi metode serangan, serta meningkatkan keterampilan dalam menggunakan alat keamanan. Kegiatan utama meliputi analisis dan simulasi berbagai ancaman siber seperti SQL Injection dengan SQLMap, digital forensik pada sistem Linux, audit log menggunakan auditd, *penetration testing* aplikasi, dan server hardening Windows Server 2019 sesuai standar CIS Benchmark. Metode yang digunakan adalah observasi, studi kasus, praktik simulasi serangan, dan pengujian keamanan. Hasil menunjukkan bahwa SQLMap efektif mendeteksi kerentanan SQL Injection, audit log membantu melacak aktivitas mencurigakan, dan hardening berhasil meningkatkan keamanan sistem operasi. Simulasi forensik memberikan gambaran alur serangan dan deteksi indikator kompromi (IoC). Pengujian keamanan aplikasi berhasil mengidentifikasi kerentanan seperti *File Disclosure* dan *Unrestricted File Upload*. Secara keseluruhan, magang ini memberikan pengalaman langsung dalam menghadapi ancaman siber dan meningkatkan kemampuan teknis dalam bidang keamanan siber.

Kata kunci: Analisis, Digital Forensik, Keamanan Siber, Pengujian Keamanan Aplikasi, Simulasi Serangan

AN ANALYSIS OF CYBERSECURITY SIMULATION ACTIVITIES AT BSSN

Raisya Putri Virnanda

ABSTRACT

An internship experience at the National Cyber and Cryptography Agency (BSSN), aimed at understanding cybersecurity principles, identifying attack methods, and enhancing skills in using security tools. Key activities included analysis and simulation of cyber threats such as SQL Injection using SQLMap, digital forensics on Linux systems, log auditing with auditd, penetration testing of BSSN applications, and server hardening of Windows Server 2019 following CIS Benchmark standards. The methods used were observation, case studies, simulation practices, and security testing. The results showed that SQLMap effectively detected SQL Injection vulnerabilities, audit logs assisted in tracking suspicious activities, and hardening improved operating system security. Forensic simulations provided insight into attack patterns and detection of indicators of compromise (IoC). Application security testing identified vulnerabilities such as File Disclosure and Unrestricted File Upload. In general, the internship provided hands-on experience in addressing cyber threats and enhanced technical competencies in the field of cybersecurity.

***Keywords**: Analysis, Application Security Testing, Attack Simulation, Cybersecurity, Digital Forensics*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN