# PENGUJIAN KERENTANAN KEAMANAN PADA SISTEM JARINGAN KOMPUTER MENGGUNAKAN METODE VULNERABILITY ASSESSMENT PADA KANTOR SEKRETARIAT YAYASAN MASJID AGUNG SUNGAILIAT

**SKRIPSI**


Oleh :

HANDAL ZULFANTO
1911500132


**PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFROMASI INSTITUT SAINS DAN BISNIS ATMA LUHUR**

**PANGKALPINANG**

**2023**

## LEMBAR PERNYATAAN

| | |
|---|---|
| NIM | : 1911500132 |
| Nama | : Handal Zulfanto |
| Judul Skripsi | : PENGUJIAN KERENTANAN KEAMANAN PADA SISTEM JARINGAN KOMPUTER MENGGUNAKAN METODE *VULNERABILITY ASSESSMENT* PADA KANTOR SEKRETARIAT YAYASAN MASJID AGUNG SUNGAILIAT |

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang, 20 April 2023


(Handal Zulfanto)

**LEMBAR PENGESAHAN SKRIPSI**

PENGUJIAN KERENTANAN KEAMANAN PADA SISTEM JARINGAN KOMPUTER MENGGUNAKAN METODE VULNERABILITY ASSESSMENT PADA KANTOR SEKRETARIAT YAYASAN MASJID AGUNG SUNGAILIAT

Yang dipersiapkan dan disusun oleh

**HANDAL ZULFANTO**
**1911500132**

Telah dipertahankan di depan Dewan Penguji
Pada tanggal 24 Juli 2023

**Susunan Dewan Penguji**
**Anggota**

**Harrizki Arie Pradana,S.Kom., M.T**
**NIDN. 0213048601**

**Dosen Pembimbing**

**Eza Budi Perkasa, M.Kom**
**NIDN. 0201089201**

**Kaprodi Teknik informatika**

**Chandra Kirana. M.Kom**
**NIDN. 0228108501**

**Ketua Penguji**

**Dian Novianto, M.Kom**
**NIDN. 0209119001**

Skripsi ini telah diterima dan sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 4 Agustus 2023

**DEKAN FAKULTAS TEKNOLOGI INFORMASI**
**ISB ATMA LUHUR**

**Ellya Helmud, M.Kom**
**NIDN. 0201027901**

## KATA PENGANTAR

Puji syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang strata satu (S1) pada Jurusan Sistem Informasi ISB ATMA LUHUR.

Penulis menyadari bahwa laporan skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa proposal skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia
2. Bapak dan Ibu tercinta yang telah mendukung penulis baik spirit maupun materi.
3. Bapak Drs. Djaetun Hs yang telah mendirikan Atma Luhur.
4. Bapak Prof. Dr. Moedjiono, M,Sc selaku Rektor ISB Atma Luhur.
5. Bapak Ellya Helmud, M.Kom selaku Dekan FTI ISB Atma Luhur.
6. Bapak Chandra Kirana, M. Kom Selaku Kaprodi Teknik Informatika.
7. Bapak Eza Budi Perkasa, M.Kom selaku dosen pembimbing.
8. Saudara dan sahabat-sahabatku terutama teman-teman angkatan 2019 yang telah memberikan dukungan moral untuk terus meyelesaikan skripsi ini.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta TaufikNya, Amin.

Pangkalpinang, 27 Maret 2023

Penulis

## ABSTRACT

*Testing security vulnerabilities on computer network systems using the Vulnerability Assessment method is an important step in maintaining system security and protecting sensitive data from potentially harmful attacks. This method involves identifying, evaluating, and mitigating existing vulnerabilities in network systems to reduce security risks that can be exploited by unauthorized parties. This study aims to analyze the processes and steps involved in testing security vulnerabilities in computer network systems using the Vulnerability Assessment method. Through a qualitative approach, this research collects data through literature, observation, and interviews with security experts. So that it can overcome problems or constraints on the current system. The results of the research show that testing security vulnerabilities using the Vulnerability Assessment method involves steps such as vulnerability identification, risk evaluation, mitigation recommendations, and mitigation effectiveness evaluation. Tools like Nessus, Nmap, and Wireshark are used to identify vulnerabilities and the proxy routers used to prevent port scans on Nmap provide the necessary information for proper mitigation. The results of this research can be used as a practical guide for organizations and security professionals who want to perform vulnerability testing on their network systems. This guide provides detailed steps and practical recommendations for identifying and evaluating security vulnerabilities.*



*Keywords* : *Testing security, Vulnerability Assessment, Nessus, Nmap, Wireshark*

# ABSTRAK

Pengujian kerentanan keamanan pada sistem jaringan komputer menggunakan metode *Vulnerability Assessment* adalah langkah penting dalam menjaga keamanan sistem dan melindungi data sensitif dari serangan yang berpotensi merugikan. Metode ini melibatkan identifikasi, evaluasi, dan mitigasi kerentanan yang ada dalam sistem jaringan guna mengurangi risiko keamanan yang dapat dieksploitasi oleh pihak yang tidak berwenang. Penelitian ini bertujuan untuk menganalisis proses dan langkah-langkah yang terlibat dalam pengujian kerentanan keamanan pada sistem jaringan komputer menggunakan metode *Vulnerability Assessment*. Melalui pendekatan kualitatif, penelitian ini mengumpulkan data melalui studi pustaka, observasi, dan wawancara dengan ahli keamanan.Sehingga dapat mengatasi permasalahan atau kendala pada sistem yang berjalan saat ini. Hasil penelitian menunjukkan bahwa pengujian kerentanan keamanan menggunakan metode Vulnerability Assessment melibatkan langkah-langkah seperti identifikasi kerentanan, evaluasi risiko,rekomendasi mitigasi, dan evaluasi efektivitas mitigasi. Alat-alat seperti Nessus, Nmap, dan Wireshark digunakan untuk mengidentifikasi kerentanan dan *router mikrotik* digunakan untuk mencegah *port scan* pada Nmap menyediakan informasi yang diperlukan untuk mitigasi yang tepat. Hasil penelitian ini dapat digunakan sebagai panduan praktis bagi organisasi dan profesional keamanan yang ingin melakukan pengujian kerentanan pada sistem jaringan mereka. Panduan ini memberikan langkah- langkah yang terperinci dan rekomendasi praktis untuk mengidentifikasi, mengevaluasikerentanan keamanan.



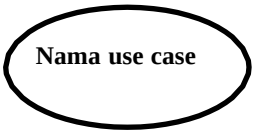
Kata Kunci : Pengujian, *Vulnerability Assessment*, Nessus, Nmap, Wireshark

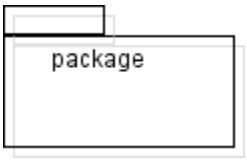
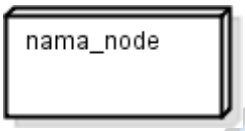
# DAFTAR ISI

# DAFTAR GAMBAR

# DAFTAR TABEL

# DAFTAR SIMBOL

| Simbol Use Case | Deskripsi |
|---|---|
| Use Case<br>  <br> | Fungsionalitas yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau aktor, biasanyadinyatakan dengan menggunakan kata kerja diawal nama*use case*. |
| Aktor/*actor*<br>  | Merupakan orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat itusendiri. |
| Asosiasi<br> | Menunjukkan *use case* memiliki interaksi dengan aktor. |
| Extensi<br><<entend>> | Relasi *use case* tambahan kesebuah *use case* dimana *usecase* yang ditambahkan dapat berdiri sendiri walau tanpa *use case* tambahan itu. |
| Generalisasi<br> | Menunjukkan hubungan generalisasi-spesialisasi (umum-khusus) antara dua buah *use case* dimana fungsi yang satulebih umum dari lainnya. |
| *Include*<br><<include>> | *Include* berarti *use case* yang ditambahkan akan selalu dipanggil saat *use case* tambahan dijalankan. |

| Simbol Deployment | Deskripsi |
|---|---|
| *Package*<br>  | Package merupakan sebuah bungkusan dari satu atau lebih |
| *Node*<br>  | Biasanya mencangkup pada perangkat keras (hardware), perangkat lunak yang tidak dibuat sendiri (*software)*, jika didalam *node* disertakan komponen untuk mengkonsistenkan rancangan maka komponen yang telah didefinisikan sebelumnya pada diagram komponen. |
| Kebergantugan/<br>*dependency*<br>  | Kertergantungan antar *node*, arah panah mengarah pada *node* yang dipakai. |
| *Link*<br> | Relasi antar *node* |