

**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 INFOMASI 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

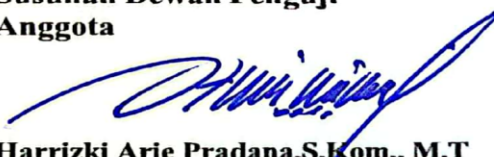
**PENGUJIAN KERENTANAN KEAMANAN PADA SISTEM
JARINGAN KOMPUTER MENGGUNAKAN METODE
VULNERABILITY ASSESSMENT PADA KANTOR
SEKRETARIAT YAYASAN MASJID AGUNG SUNGAILIAT**

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
SUN ATMA LUHUR**


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

KATA PENGANTAR

Puji syukur Alhamdulillah kehadiran 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, mengevaluasi kerentanan keamanan.

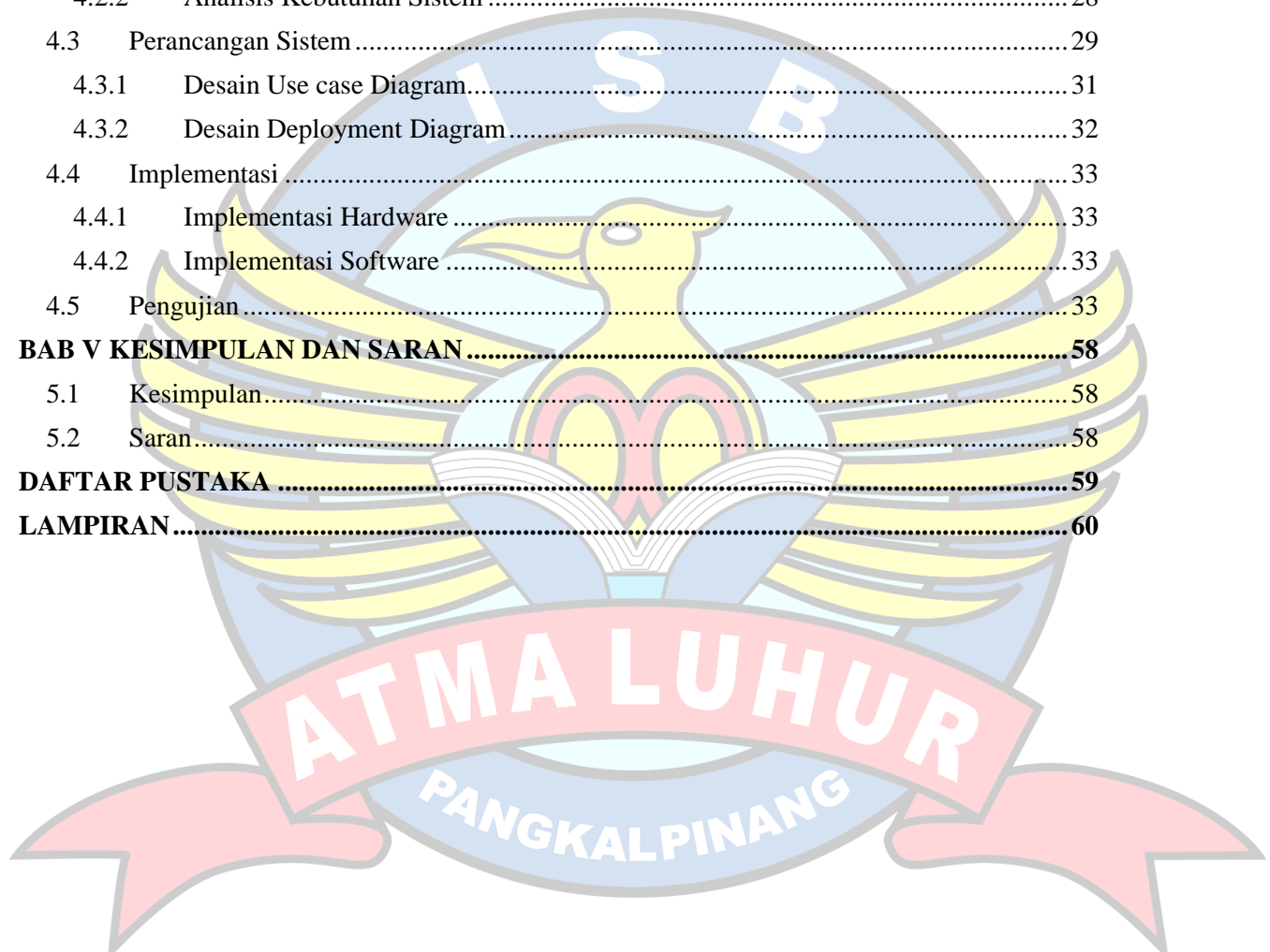
Kata Kunci : Pengujian, *Vulnerability Assessment*, Nessus, Nmap, Wireshark



DAFTAR ISI

LEMBAR PERNYATAAN	i
LEMBAR PERSETUJUAN SIDANG	ii
KATA PENGANTAR	iii
ABSTRACT	iv
ABSTRAK	v
DAFTAR ISI	vi
DAFTAR GAMBAR	viii
DAFTAR TABEL	x
DAFTAR SIMBOL	xi
BAB I PENDAHULUAN	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah	4
1.4 Tujuan dan Manfaat Penelitian	4
1.5 Sistematika Penulisan Laporan	5
BAB II LANDASAN TEORI	7
2.1 Model NDLC (Network Development Life Cycle)	7
2.2 Tahapan atau fase model NDLC (Network Development Life Cycle).....	7
2.3 Nessus.....	9
2.4 Nmap (Network Mapper).....	9
2.5 Web Application Scanner	10
2.6 Password Cracking Tools	10
2.7 Wire Shark.....	11
2.8 UML (Unified Modelling Language).....	11
2.9 Use Case Diagram	11
2.10 Deployment Diagram.....	11
2.11 Astah Community	12
2.12 Cisco Packet Tracer	12
2.13 Penelitian Terdahulu.....	13
BAB III METODOLOGI PENELITIAN	17
3.1 Model Penelitian.....	17
3.2 Teknik Pengumpulan Data.....	18
3.3.2 Teknik Pengumpulan Data Sekunder	19
3.3 Alat Bantu Pengembangan Sistem	19

BAB IV HASIL DAN PEMBAHASAN.....	22
4.1 Profil Kantor.....	22
4.1.1 Latar Belakang Kantor Sekretariat Yayasan Masjid Agung.....	22
4.1.2 Visi dan Misi Kantor Sekretariat Yayasan Masjid Agung.....	23
4.1.3 Struktur Organisasi	24
4.1.4 Jabatan Tugas dan Wewenang.....	24
4.2 Analisis Masalah.....	26
4.2.1 Solusi Pemecahan Masalah	27
4.2.2 Analisis Kebutuhan Sistem	28
4.3 Perancangan Sistem.....	29
4.3.1 Desain Use case Diagram.....	31
4.3.2 Desain Deployment Diagram.....	32
4.4 Implementasi	33
4.4.1 Implementasi Hardware	33
4.4.2 Implementasi Software	33
4.5 Pengujian.....	33
BAB V KESIMPULAN DAN SARAN.....	58
5.1 Kesimpulan.....	58
5.2 Saran.....	58
DAFTAR PUSTAKA	59
LAMPIRAN.....	60



DAFTAR GAMBAR

Gambar 2.1 Metode NDLC	7
Gambar 4.1 Struktur Organisasi	24
Gambar 4.2 Topologi sistem yang sedang berjalan.....	29
Gambar 4.3 Topologi sistem menggunakan <i>Mikrotik</i>	29
Gambar 4.4 Diagram Activity usulan.....	29
Gambar 4.5 Use Case Diagram yang diusulkan	30
Gambar 4.6 Use Case Diagram Pengujian	30
Gambar 4.7 Deployment diagram Sistem yang diusulkan	31
Gambar 4.8 Halaman Login Nessus	33
Gambar 4.9 Tampilan <i>Fitur Basic Network Scan</i>	33
Gambar 4.10 Tampilan <i>Scans IP Kantor Sekretariat</i>	34
Gambar 4.11 <i>Scan Host discovery</i>	34
Gambar 4.12 <i>Scan Host discovery All Ports</i>	35
Gambar 4.13 Perbedaan Scan	35
Gambar 4.14 Hasil Pemindaian kerentanan	36
Gambar 4.15 Presentase Hasil Pemindaian Kerentanan.....	36
Gambar 4.16 Hasil Kerentanan dengan skor tertinggi	37
Gambar 4.17 <i>Scan Zenmap Nmap GUI</i>	39
Gambar 4.18 <i>Scan IP local host</i>	40
Gambar 4.19 Hasil Scan Port Zenmap.....	40
Gambar 4.20 Hasil Port Scanning 10 kali Zenmap	41
Gambar 4.21 Host Details.....	42
Gambar 4.22 Hasil <i>port scan IP Domain</i>	43
Gambar 4.23 <i>Interface Network</i> pada wifi	43
Gambar 4.24 Penggunaan Wifi Kantor	45
Gambar 4.25 Proses Capturing from Wifi	46
Gambar 4.26 Stop Capturing from Wifi	46
Gambar 4.27 Hasil monitoring jaringan http.....	47
Gambar 4.28 Analisis data <i>Tcp Stream</i>	48
Gambar 4.29 Hasil dari Analisis Data.....	49
Gambar 4.30 <i>Filter New Firewall Rule</i>	50
Gambar 4.31 <i>Filter New Firewall Rule Action</i>	51
Gambar 4.32 <i>tcp firewall rule Apply</i>	51

Gambar 4.33 <i>Filter New Firewall Rule udp</i>	52
Gambar 4.34 <i>Filter New Rule Chain Input tcp</i>	53
Gambar 4.35 <i>Filter New Rule Chain Input udp</i>	53
Gambar 4.36 <i>Blocking port-scan</i>	54
Gambar 4.37 <i>Action Drop</i>	54
Gambar 4.38 <i>Blocking port scan Input</i>	56
Gambar 4.39 <i>Testing port scan Nmap</i>	57
Gambar 4.40 <i>Filter Rule Blocking</i>	57

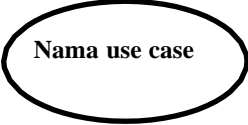





DAFTAR TABEL

Tabel 2.13	Peneltian Terdahulu.....	13
------------	--------------------------	----



DAFTAR SIMBOL

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

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