

**ANALISIS KERENTANAN MENGGUNAKAN VULNERABILITY  
ASSESSMENT PADA SITUS WEB FAKULTAS TEKNIK DAN  
TEKNOLOGI INFORMASI UNIVERSITAS JENDERAL ACHMAD YANI  
YOGYAKARTA**

**TUGAS AKHIR**

Diajukan sebagai salah satu syarat memperoleh gelar Sarjana  
Program Studi Teknologi Informasi



Disusun oleh:

**DANANG PRIHANTO**  
182104005

**PROGRAM STUDI TEKNOLOGI INFORMASI  
FAKULTAS TEKNIK & TEKNOLOGI INFORMASI  
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA  
2022**

## HALAMAN PENGESAHAN

### TUGAS AKHIR

#### ANALISIS KERENTANAN MENGGUNAKAN VULNERABILITY ASSESSMENT PADA SITUS WEB FAKULTAS TEKNIK DAN TEKNOLOGI INFORMASI UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

Diajukan oleh:

**DANANG PRIHANTO**

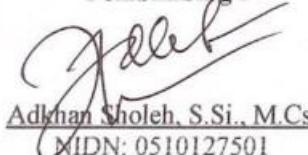
182104005

Telah dipertahankan di depan Dewan Pengaji dan dinyatakan sah  
sebagai salah satu syarat untuk memperoleh gelar Sarjana  
di Fakultas Teknik & Teknologi Informasi  
Universitas Jenderal Achmad Yani Yogyakarta

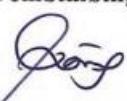
Tanggal: 25 Agustus 2022

Mengesahkan

Pembimbing I

  
Adkhan Sholeh, S.Si., M.Cs.  
NIDN: 0510127501

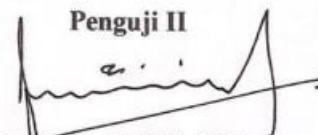
Pembimbing II

  
Chanief Budi Setiawan, S.T., M.Eng.  
NIDN: 0514068101

Pengaji I

  
Alfirna Rizqi Lahitani, S.Kom., M.Eng.  
NIDN: 0506019202

Pengaji II

  
Dedy Hariyadi, S.T., M.Kom.  
NIDN: 0518108001

Ketua Program Studi Teknologi Informasi  
Fakultas Teknik & Teknologi Informasi  
Universitas Jenderal Achmad Yani Yogyakarta



Chanief Budi Setiawan, S.T., M.Eng.

NIP: 2008.13.0021

## **HALAMAN PERNYATAAN**

Saya yang bertanda tangan di bawah ini, adalah mahasiswa Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta,

Nama : Danang Prihanto  
NPM : 182104005  
Program Studi : Teknologi Informasi (S-1)  
Judul Tugas Akhir : Analisis Kerentanan Menggunakan *Vulnerability Assessment* Pada Situs Web Fakultas Teknik Dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta.

Menyatakan bahwa hasil penelitian dengan judul tersebut di atas adalah asli karya saya sendiri dan bukan hasil plagiarisme. Semua referensi dan sumber terkait yang dikutip dalam karya ilmiah ini telah ditulis sesuai kaidah penulisan ilmiah yang berlaku. Dengan ini, saya menyatakan untuk menyerahkan hak cipta penelitian kepada Universitas Jenderal Achmad Yani Yogyakarta guna kepentingan ilmiah.

Demikian surat pernyataan ini dibuat dengan sebenar-benarnya tanpa ada paksaan dari pihak mana pun. Apabila terdapat kekeliruan atau ditemukan adanya pelanggaran akademik di kemudian hari, maka saya bersedia menerima konsekuensi yang berlaku sesuai ketentuan akademik.

Yogyakarta, 07 Agustus 2022



## **KATA PENGANTAR**

Puji syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul: “Analisis Website Vulnerability Menggunakan Metode Vulnerability Assessment Pada Website Fakultas Teknik & Teknologi Informasi (FTTI) di Universitas Jenderal Achmad Yani Yogyakarta”. Penyusunan laporan ini merupakan salah satu persyaratan untuk menyelesaikan studi di Program Studi Teknologi Informasi (S-1) Fakultas Teknik & Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta. Laporan ini dapat diselesaikan atas bimbingan, arahan, dan bantuan dari berbagai pihak. Pada kesempatan ini penulis dengan rendah hati mengucapkan terima kasih dengan setulus-tulusnya kepada:

1. Bapak Aris Wahyu Murdiyanto, S.Kom., M.Cs. selaku Dekan Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
2. Bapak Chanief Budi Setiawan, S.T., M.Eng. selaku Ketua Program Studi Teknologi Informasi (S-1) Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
3. Bapak Adkhan Sholeh, S.Si., M.Cs. dan Bapak Chanief Budi Setiawan, S.T., M.Eng. selaku Dosen Pembimbing Tugas Akhir;
4. Para dosen yang telah memberikan banyak bekal ilmu pengetahuan kepada penulis selama menjadi mahasiswa di Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
5. Ayah, Ibu, dan Adik saya, Alm. Tegar Dwi Santoso, yang telah memberikan dukungan semangat serta doa restu kepada saya, sehingga dapat menyelesaikan studi saya;
6. Reza Aisyah Puri Rahmalia, seseorang yang selalu mendukung, memberikan semangat dan doa kepada saya;
7. Teman-teman seperjuangan yaitu Wahyu Dwi Riyanto, Nanang Widayanto, Heri Gunawan, Bambang Nakulo, Aline Vida Sefara, Nur

Rosid Wakhid Wahyudi dan lainnya yang telah memberikan motivasi dan semangat selama masa kuliah saya.

8. Rekan-rekan mahasiswa Teknologi Informasi (S-1) di Universitas Jenderal Achmad Yani Yogyakarta yang sudah memberi dukungan dan kerja sama selama pembuatan tugas akhir.

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari kata sempurna. Maka dari itu dengan segala kerendahan hati penulis sangat menghargai adanya kritik dan saran yang membangun dari semua pihak yang bersedia meluangkan waktu untuk membaca laporan tugas akhir ini.

Yogyakarta, 28 Juli 2022



Danang Prihanto

## DAFTAR ISI

<b>Halaman Judul .....</b>	<b>i</b>
<b>Halaman Pengesahan.....</b>	<b>ii</b>
<b>Halaman Pernyataan .....</b>	<b>iii</b>
<b>Kata Pengantar .....</b>	<b>iv</b>
<b>Daftar Isi .....</b>	<b>vi</b>
<b>Daftar Tabel.....</b>	<b>viii</b>
<b>Daftar Gambar .....</b>	<b>ix</b>
<b>Daftar Lampiran .....</b>	<b>x</b>
<b>Daftar Singkatan .....</b>	<b>xi</b>
<b>Intisari .....</b>	<b>xii</b>
<b>Abstract .....</b>	<b>xiii</b>
<b>Bab 1 Pendahuluan .....</b>	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Perumusan Masalah .....	2
1.3 Pertanyaan Penelitian .....	2
1.4 Tujuan Penelitian .....	3
1.5 Manfaat Hasil Penelitian .....	3
<b>Bab 2 Tinjauan Pustaka dan Landasan Teori.....</b>	<b>4</b>
2.1 Tinjauan Pustaka .....	4
2.2 Landasan Teori.....	7
2.2.1 <i>Website</i> .....	7
2.2.2 <i>Vulnerability Assessment</i> .....	7
2.2.3 DNSDumpster .....	7
2.2.4 Nmap ( <i>Network Mapper</i> ) dan Zenmap .....	8
2.2.5 Nessus.....	8
2.2.6 CVSS.....	10
2.2.7 WPScan .....	10
<b>Bab 3 Metode Penelitian.....</b>	<b>12</b>
3.1 Bahan dan Alat Penelitian.....	14

3.2 Jalan Penelitian.....	14
3.3 Metode <i>Vulnerability Assessment</i> .....	15
<b>Bab 4 Hasil Penelitian.....</b>	<b>17</b>
4.1 Ringkasan Hasil Penelitian .....	17
4.2 Arsitektur Sistem.....	18
4.3 Testing.....	18
4.3.1 Identifikasi <i>Headers</i> menggunakan DNSdumpster.....	18
4.3.2 Pemindaian pada IP target menggunakan Nmap.....	21
4.3.3 Pemindaian kerentanan menggunakan WPScan .....	22
4.3.4 Pemindaian kerentanan menggunakan Nessus.....	24
4.4 Analisis.....	28
4.4.1 Analisis hasil pemindaian menggunakan Nmap .....	28
4.4.2 Analisis hasil pemindaian menggunakan WPScan .....	29
4.4.3 Analisis hasil pemindaian menggunakan Nessus .....	30
4.5 Pembahasan.....	32
4.5.1 Rekomendasi .....	32
<b>Bab 5 Kesimpulan dan Saran .....</b>	<b>36</b>
5.1 Kesimpulan .....	36
5.2 Saran.....	36
<b>Daftar Pustaka.....</b>	<b>37</b>
<b>Lampiran .....</b>	<b>39</b>

## **DAFTAR TABEL**

<b>Tabel 2.1</b> Literatur Review.....	5
<b>Tabel 2.2</b> Tabel fitur Nessus.....	8
<b>Tabel 2.3</b> Tabel metode WPScan .....	10
<b>Tabel 3.1</b> Tabel alat pemindaian .....	15
<b>Tabel 4.1</b> Daftar fungsi port yang terbuka menggunakan Nmap .....	28
<b>Tabel 4.2</b> Analisis hasil pemindaian ftti.unjaya.ac.id menggunakan WPScan ....	29
<b>Tabel 4.3</b> Tabel ringkasan pengujian menggunakan Nessus.....	30
<b>Tabel 4.4</b> Tabel Rekomendasi perbaikan celah .....	32

## DAFTAR GAMBAR

<b>Gambar 3.1</b> Alur pengujian .....	13
<b>Gambar 4.1</b> Topologi jaringan.....	18
<b>Gambar 4.2</b> Informasi HTTP Headers pada ftti.unjaya.ac.id menggunakan DNSDumpster .....	19
<b>Gambar 4.3</b> Informasi HTTP Headers pada app.ftti.unjaya.ac.id menggunakan DNSDumpster.....	19
<b>Gambar 4.4</b> Informasi HTTP Headers pada elearning.ftti.unjaya.ac.id menggunakan DNSDumpster.....	20
<b>Gambar 4.5</b> Pemindaian Nmap pada ftti.unjaya.ac.id .....	21
<b>Gambar 4.6</b> Pemindaian Nmap pada elearning.ftti.unjaya.ac.id .....	21
<b>Gambar 4.7</b> Pemindaian Nmap pada app.ftti.unjaya.ac.id .....	22
<b>Gambar 4.8</b> Tampilan pertama pemindaian WPScan.....	23
<b>Gambar 4.9</b> Tampilan kedua pemindaian WPScan .....	24
<b>Gambar 4.10</b> Pemindaian ftti.unjaya.ac.id pada Nessus.....	25
<b>Gambar 4.11</b> Pemindaian app.ftti.unjaya.ac.id pada Nessus.....	26
<b>Gambar 4.12</b> Pemindaian elearning.ftti.unjaya.ac.id pada Nessus.....	26
<b>Gambar 4.13</b> Grafik perbandingan kerentanan .....	27

## **DAFTAR LAMPIRAN**

<b>Lampiran 1</b> Surat Ijin Penelitian .....	39
<b>Lampiran 2</b> Jadwal Penelitian .....	40
<b>Lampiran 3</b> Lembar Bimbingan Dosen .....	41
<b>Lampiran 4</b> Hasil Cek Plagiarisme.....	42

## **DAFTAR SINGKATAN**

NSE	Nmap Scripting Engine
API	Application Programming Interface
CVSS	Common Vulnerability Scoring System
CSRF	Cross-Site Request Forgery
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
NDLC	Network Development Life Cycle
OWASP	Open Web Application Security Project
PUSI	Pusat Sistem Informasi
FTTI	Fakultas Teknik dan Teknologi Informasi
WWW	World Wide Web
GOV-CSIRT	Goverment Computer Security Incident Response Team
NASL	Nessus Attack Scripting Laungage
VPR	Vulnerability Priority Rating
FTP	File Transfer Protocol
SSH	Secure Shell
SMTP	Simple mail Transfer Protocol
SQL	Standard Query Language
POP	Post Office Protocol
IMAP	Internet Message Access Protocol
MSA	Mail Submission Agen
BLP	Bloomberg Professional
IP	Internet Protocol
OS	Operating System