



Judul:

Analisis Rancangan Mesin Pembayaran dengan Sidik Jari

Sub Judul:

**Analisis Uji Sistem Keamanan Jaringan Web dan Database
Server pada Mesin Pembayaran**

SKRIPSI

Muhammad Nazel Djibran

1807422010

PROGRAM STUDI TEKNIK MULTIMEDIA JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2022



Judul:

Analisis Rancangan Mesin Pembayaran dengan Sidik Jari

Sub Judul:

**Analisis Uji Sistem Keamanan Jaringan Web dan Database
Server pada Mesin Pembayaran**

SKRIPSI

**Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan
untuk Memperoleh Diploma Empat Politeknik**

Muhammad Nazel Djibran

1807422010

**PROGRAM STUDI TEKNIK MULTIMEDIA JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA**

2022



SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Muhammad Nazel Djibran
NIM : 1807422010
Jurusan/Program Studi : TIK/TMJ
Judul Skripsi : Analisis Uji Sistem Keamanan Jaringan Web dan Database Server pada Mesin Pembayaran.

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya sendiri, bebas dari peniruan terhadap karya orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

**POLITEKNIK
NEGERI
JAKARTA**

Depok,

Yang membuat pernyataan



(Muhammad Nazel Djibran)

NIM 1807422010

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama : Muhammad Nazel Djibran
 NIM : 1807422010
 Program Studi : Teknik Multimedia dan Jaringan
 Judul Skripsi : Analisis Uji Sistem Keamanan Jaringan Web dan Database Server pada Mesin Pembayaran.

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Senin, Tanggal 8, Bulan Agustus, Tahun 2022, dan dinyatakan **LULUS**.

Disahkan oleh

Pembimbing I : AsepKurniawan, S. Pd., M. Kom.
 Penguji I : Defiana Arnaldy, S.Tp., M.Si.
 Penguji II : Indra Hermawan, S.Kom., M.Kom.
 Penguji III : Fachroni Arbi Murad, S.Kom., M.Kom.

**POLITEKNIK
NEGERI
JAKARTA**

Mengetahui :

Jurusan Teknik Informatika dan Komputer

Ketua

Mauldy Laya, S.Kom., M.Kom.

NIP. 197802112009121003



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritis atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Puji syukur penulis panjatkan atas kehadiran Allah SWT, karena berkat rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan perkuliahan dan skripsi ini dengan baik. Selama menjalani masa perkuliahan dan pelaksanaan penelitian skripsi, tentu banyak dukungan, bimbingan, dan saran dari berbagai pihak. Oleh karena itu, penulis mengucapkan Terima Kasih kepada :

1. Bapak Asep Kurniawan, S. Pd., M. Kom. Selaku pembimbing skripsi yang telah membimbing penulis dan memberi masukan yang sangat membantu penulis dalam menyelesaikan skripsi ini.
2. Ayahanda Warkah Noval (Alm) dan Ibunda Elis Herwati yang telah memberikan Do'a terbaiknya kepada penulis dan telah memberikan dukungan dan membantu menyelesaikan skripsi ini dan menyelesaikan pendidikan di akhir perkuliahan.
3. Andri dan gilbert sebagai teman satu kelompok skripsi yang saling mendukung satu sama lain untuk menyelesaikan semuanya bersama-sama.
4. Laily, Debby, Alfana, Amin, Boy, Imam, Kepin berterima kasih sebanyak banyaknya yang sekemudian ada untuk penulis dari dulu sampai sekarang dan dari susah hingga senang.

Penulis menyadari bahwa dalam proses penyusunan dan penelitian Tugas Akhir/Skripsi ini masih terdapat banyak kekurangan, maka dari itu penulis meminta saran serta kritik yang membangun kepada para pembaca agar penulis dapat memperbaiki dan menyempurnakan penelitian ini. Penulis berharap laporan ini dapat membawa manfaat baik bagi penulis serta pembaca, dan Tuhan Yang Maha Esa yang akan membalas semua kebaikan kepada pihak yang telah membantu penulis menyelesaikan penyusunan dan penelitian Tugas Akhir/Skripsi.

Depok, 11 Juli 2022

Penulis.



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah,
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI
SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan di bawah ini:

Nama : Muhammad Nazel Djibran
NIM : 1807422010
Jurusan/Program Studi : TIK/TMJ

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta hak bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

Analisis Uji Sistem Keamanan Jaringan Web dan Database Server pada Mesin Pembayaran

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalih media kan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Depok,

Yang membuat pernyataan

(Muhammad Nazel Djibran)

NIM 1807422010



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritis atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Judul:

Analisis Rancangan Mesin Pembayaran dengan Sidik Jari.

Sub Judul:

**Analisis Uji Sistem Keamanan Jaringan Web dan Database Server pada
Mesin Pembayaran**

ABSTRAK

Analisis rancangan mesin pembayaran dengan sidik jari, analisis pada penulisan ini adalah dengan tujuan setiap alat yang digunakan terutama yang bersangkutan dengan transaksi data bahkan sampai di dunia keuangan akan sangat menghawatirkan jika sampai terjadinya kejadian kejahatan terutama kejahatan cyber.

Dengan adanya permasalahan tersebut, maka dikembangkan sistem keamanan dan pertahanan. Perlu adanya antisipasi untuk mengamankan aset-aset penting. kemudian dilakukannya pengetesan keamanan tersebut apakah mampu menangani segala macam bentuk kejahatan cyber yang membahayakan pengguna teknologi terkhusus di dunia keuangan dan membantu menemukan celah yang bisa digunakan oleh seorang hacker dalam melakukan penyerangannya yang bisa diantisipasi oleh administrator.

Hasil yang diperoleh dari penelitian in adalah analisis sistem keamanan jaringan web dan database pada mesin pembayaran yang telah melakukan beberapa pengetesan pencarian celah keamanan sehingga mendapatkan hasil akhir yaitu mendapatkan informasi seputar celah keamanan web yang kemungkinan bisa dilakukannya kejahatan cyber.

Kata kunci: *vulnerability, scanning, penetration, exploitation*



DAFTAR ISI

SURAT PERNYATAAN BEBAS PLAGIARISME	iii
LEMBAR PENGESAHAN	iv
KATA PENGANTAR	v
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI.....	vi
ABSTRAK.....	vii
DAFTAR ISI	8
DAFTAR GAMBAR.....	10
DAFTAR TABEL	12
BAB I PENDAHULUAN	13
1.1 Latar Belakang.....	13
1.2 Perumusan Masalah.....	15
1.3 Batasan Masalah.....	15
1.4 Tujuan dan Manfaat.....	15
1.5 Sistematika Penulisan.....	16
BAB II TINJAUAN PUSTAKA	17
2.1 Keamanan Jaringan.....	17
2.2 Keamanan <i>Website</i>	17
2.3 Keamanan <i>Databases</i>	18
2.4 <i>Vulnerability Assessment</i>	18
2.5 <i>Vulnerability Scanner</i>	18
2.6 <i>Web Vulnerability</i>	19
2.6 <i>Information Gathering</i>	19
2.7 <i>Penetration Tessting</i>	20

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

2.8 Pentesting Tools	22
2.6 Penelitian Sejenis.....	28
BAB III PERENCANAAN DAN REALISASI ATAU RANCANG BANGUN	33
3.1 Rancangan Penelitian	33
3.2 Tahapan Penelitian	34
3.3 Objek Penelitian	34
BAB IV	35
HASIL DAN PEMBAHASAN	35
4.1 Analisis Kebutuhan.....	35
4.2 Perancangan Sistem.....	35
4.2.1 <i>Pre-Engagement Interaction</i>	36
4.2.2 <i>Information Gathering</i>	37
4.3 Implementasi Sistem.....	40
4.4 Pengujian	42
4.5 Analisis Data / Evaluasi.....	51
BAB V	53
KESIMPULAN DAN SARAN	53
5.1 Kesimpulan.....	53
5.2 Saran	54
DAFTAR PUSTAKA.....	55
LAMPIRAN	58



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

DAFTAR GAMBAR

Gambar 2.1 Metode Black Box.....	21
Gambar 2.2 Metode White Box	21
Gambar 2.3 Metode Grey Box.....	22
Gambar 2.4 VMware.....	22
Gambar 2.5 Kali Linux	23
Gambar 2.6 NMAP	24
Gambar 2.7 Acunetix Web Vulnerability Scanner	25
Gambar 2.8 Vega	25
Gambar 2.9 Sqlninja.....	26
Gambar 2.10 Burpsuite	27
Gambar 2.11 Wireshark	27
Gambar 2.12 Simbol flowchart.....	30
Gambar 3.1 Bagan alur Rancangan Penelitian Kuantitatif	33
Gambar 3.2 Tahapan Rancangan Penelitian	34
Gambar 4.1 Skema pentest.....	36
Gambar 4.2 <i>Flowchart pre-engagement interaction</i>	37
Gambar 4.3 <i>Flowchart information gathering</i>	38
Gambar 4.4 <i>Flowchart vulnerability analysis</i>	39
Gambar 4.5 <i>Flowchart exploitation</i>	40
Gambar 4.6 <i>Flowchart PTES</i>	41
Gambar 4.7 <i>Whois</i>	43
Gambar 4.8 <i>Nmap</i>	44
Gambar 4.9 Hasil <i>acunetix web vulnerability</i>	45



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Gambar 4.10 Hasil <i>acunetix web vulnerability</i>	46
Gambar 4.11 Hasil vega.....	46
Gambar 4.12 Hasil vega.....	47
Gambar 4.14 konfigurasi sqlninja.....	48
Gambar 4.15 Hasil sqlninja.....	48
Gambar 4.16 Langkah akses burpsuite	49
Gambar 4.17 <i>Scanning payloads</i> pada burpsuite	49
Gambar 4.18 Hasil <i>scanning</i> akses halaman <i>login website</i>	50
Gambar 4.20 Hasil DoS dilihat dari Wireshark	51





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

DAFTAR TABEL

Tabel 2.1 Penelitian sejenis.....	31
Tabel 4.1 Hasil <i>whois</i>	43
Tabel 4.2 Hasil <i>Nmap</i>	44
Tabel 4.3 Hasil analisis kerentanan dan solusi.....	51



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

BAB I PENDAHULUAN

1.1 Latar Belakang

Dengan perkembangan zaman dan teknologi yang sangat pesat, metode pembayaran pun mengalami berbagai inovasi. Salah satu yang saat ini mulai digunakan oleh masyarakat adalah *cashless*. *Cashless* adalah sistem pembayaran tanpa uang tunai, sesuai dengan arti secara harfiah yang berarti tidak atau tanpa menggunakan uang tunai. *Cashless* mengacu pada pembayaran yang berbentuk digital. Sistem pembayaran *cashless* juga sudah diterapkan di Indonesia. Banyak masyarakat yang juga sudah menggunakan dan memilih metode pembayaran *cashless* (Astuti dan Hastuti, 2020).

Terdapat faktor-faktor yang memunculkan sistem pembayaran *cashless* seperti biaya penerbitan, perawatan, dan distribusi. Selain itu ada pula faktor kesadaran akan potensi kecurangan dan kejahatan yang semakin marak. Kejahatan yang dimaksud bisa diakibatkan karena uang fisik seperti beredarnya uang palsu. Keberadaan *cashless* juga mempermudah tugas pemerintah dalam mengelola dan mengawasi transaksi dari kegiatan ekonomi masyarakatnya. Terlebih, laporan-laporan transaksi dan perdagangan ekonomi bisa diakses dengan menggunakan laporan elektronik. Transaksi dengan menggunakan sistem *cashless* tidak melibatkan perpindahan uang secara fisik, sehingga hal ini akan mengurangi kemungkinan terjadinya korupsi dan kolusi di antara pihak-pihak yang melakukan transaksi. Terutama transaksi yang berkaitan dengan pelayanan publik (Endaru, 2021).

Penggunaan *cashless* juga memiliki beberapa kekurangan dan kerentanan keamanan data dari sisi *database* pada bank atau media penyimpanan keuangan lainnya serta dari sisi metode alat pembayaran. Berkembangnya zaman banyak sekali media penyimpanan atau *database* yang bisa digunakan dan diakses dalam penggunaan pekerjaan, salah satunya *cloud computing*. *Cloud computing* salah satu media *database* yang sudah marak dipakai di zaman sekarang karena beberapa kelengkapan fitur dan efisiensi dalam penggunaannya.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Cloud computing adalah salah satu dari teknologi jaringan yang sedang berkembang pesat saat ini, hal ini dikarenakan *cloud computing* memiliki kelebihan dapat meningkatkan fleksibilitas dan kapabilitas dari proses komputer secara dinamis tanpa perlu mengeluarkan dana besar untuk membuat infrastruktur baru. Hal ini juga akan memperkecil keluarnya biaya, *cloud computing* dapat memberikan kenyamanan akses bagi para penggunanya, serta dapat secepatnya dirilis dengan interaksi yang minimal dengan para penyedia layanan (Sasongko, 2011).

Pada penggunaan perangkat metode pembayaran, pastinya semua perangkat sudah terintegrasi dengan internet untuk melakukan transaksi data salah satunya pembayaran. Salah satu penerapan dari internet adalah adanya *Internet of Things* (IoT). Konsep dari *Internet of Things* adalah menghubungkan perangkat dan fasilitas dengan berbagai jaringan untuk menyediakan layanan yang efisien dan aman bagi semua pengguna dan aplikasi, kapan saja dan di mana saja. Dengan adanya konsep baru ini tentunya *Internet of Things* menjadi target utama dalam kejahatan *cyber* terutama dalam segi *User Interface* salah satunya yaitu *Website* (Artiyasa, 2020).

Keamanan sebuah *Website* merupakan hal yang penting, karena untuk melindungi informasi yang ada. Karena, meski dapat di akses banyak orang, dalam sebuah *website* juga terdapat informasi penting yang harus dijaga seperti data pengguna, informasi pribadi, dan sebagainya. Jika keamanan suatu *website* tidak diperhatikan, *vulnerability* atau kerentanan tersebut digunakan oleh pihak tidak bertanggung jawab untuk mengambil keuntungan. *Vulnerability* adalah salah satu point kelemahan di mana suatu sistem rentan terhadap serangan. Terdapat beberapa jenis kerentanan yang dapat terjadi, untuk itu perlu dilakukan pencarian celah kerentanan dengan melakukan *vulnerability scanning*. *Vulnerability scanning* adalah aplikasi yang menjalankan pemindai keamanan dan penilaian kerentanan, metode ini memanfaatkan beberapa *tools* pengujian yang ada pada Kali Linux (Dimas, 2019).



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

1.2 Perumusan Masalah

Berdasarkan latar belakang permasalahan yang telah diuraikan di atas, dapat diambil perumusan masalahnya yaitu:

- a. Bagaimana menemukan celah kerentanan dan kelemahan pada server web dan database?
- b. Bagaimana melakukan pengujian kerentanan yang ditemukan pada server server web dan database?
- c. Bagaimana melakukan analisis sistem keamanan yang dilakukan pengetesan server web dan database?

1.3 Batasan Masalah

Berdasarkan rumusan yang telah diutarakan, maka batasan masalah yang ditentukan dalam penelitian adalah sebagai berikut:

- a. Server yang di analisa adalah web server dan database server.
- b. Pengujian yang dilakukan pada penelitian ini dengan *vulnerability analysis* dan *penetration testing*.
- c. *Tools* yang digunakan untuk kebutuhan *vulnerability analysis web* yaitu *Vega, Acunetix Web Vulnerability Scanner, SQL Ninja, Burpsuite, Wireshark*

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari penelitian ini adalah:

- a. Menemukan celah kerentanan dan kelemahan pada server server web dan database
- b. Melakukan pengujian kerentanan yang ditemukan pada server server web dan database
- c. Melakukan analisis sistem keamanan yang dilakukan pengetesan server server web dan database



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

1.4.2 Manfaat

Manfaat dari penelitian ini adalah mengetahui celah keamanan *web server* apakah *server* rentan terhadap serangan dan mengetahui langkah dan pencegahan berdasarkan hasil analisis.

1.5 Sistematika Penulisan

Sistematika penulisan dalam proposal ini, disusun sebagai berikut:

1. BAB I PENDAHULUAN

Bab ini berisi pembahasan tentang latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat serta sistematika penulisan.

2. BAB II TINJAUAN PUSTAKA

Bab ini berisi pembahasan mengenai materi/teori yang mendukung dan membantu proyek yang dibuat pada proposal.

3. BAB III PERANCANGAN DAN REALISASI ATAU RANCANG BANGUN

Bab ini berisi pembahasan rangkaian dari metode penelitian yaitu rancangan penelitian, tahapan penelitian, dan objek penelitian.

4. BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi tentang hasil dari penelitian dan beberapa pembahasan dari hasil yang di dapatkan yaitu analisis kebutuhan, perancangan sistem, implementasi sistem, pengujian, dan analisis data.

5. BAB V KESIMPULAN DAN SARAN

Bab terakhir ini menjelaskan tentang hasil dari penelitian yang akan dianalisis dan menjadikan kesimpulan dari penulisan ini serta saran dari hasil analisis penelitian pada penulisan ini.

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisis pengujian *pentest* ini yang menggunakan target server mendapatkan beberapa kesimpulan dari rumusan masalah pada analisis kali ini:

- a. Celah kerentanan dan kelemahan ditemukan dengan cara pengujian testing terhadap server yang menggunakan *tools* Vega dan Acunetix Web Vulnerability Scanner, hasil yang didapatkan dengan analisa yang diberikan oleh kedua *tools* tersebut memiliki kerentanan dan celah yang cukup tinggi dengan poin-poin celah kerentanan yang diberikan oleh kedua *tools* sehingga didapatkan hasil analisa kelemahan dengan tingkat level yang diberikan oleh kedua *tools*.
- b. Pengujian cara menemukan celah pada web dan database server adalah melakukan *scanning* terhadap kedua server tersebut dengan menggunakan Vega dan Acunetix Web Vulnerability Scanner untuk langkah menemukan kerentanan pada web server dengan target *scanning* IP web server yang sudah diketahui dan dilakukan pengujian penyerangan pada celah kerentanan yang dimiliki web server, dan *scanning* pengujian database server digunakannya *tools* Sqlninja dan dari hasil yang diberikan oleh *tools* tersebut tidak ditemukan kerentanan pada database server yang artinya aman dari serangan dengan langkah pengujian ditargetkannya IP database server untuk sasaran pengujian.
- c. Analisis yang dilakukan untuk menilai hasil analisis keamanan dan kerentanan yang didapatkan adalah dengan menyimpulkan hasil dari *tools* yang digunakan untuk melakukan pengujian hingga menemukan kerentanan dari Vega, Acunetix Web Vulnerability Scanner, dan Sqlninja sampai dilakukannya tahapan *exploit* untuk melakukan pengujian penyerangan pada web server yang memiliki

kerentanan dan di akhir memberikan solusi untuk celah kerentanan yang dimiliki oleh web server untuk mencegah penyerangan oleh orang yang tidak bertanggung jawab.

5.2 Saran

Pada penelitian ini, penulis dalam hasil analisis keamanan dan kerentanan *web* dan *database* terdapat beberapa faktor yang masih belum terjangkau dalam melakukan *pentest* secara meluas, sehingga penulis berharap pada penelitian ini selanjutnya bisa dikembangkan kembali dari hasil proses *pentest* ini dan dapat dilakukan analisis dari berbagai aspek dalam penilaian keamanan dan kerentanan secara lengkap.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta





DAFTAR PUSTAKA

- Arnaldy, D., Perdana, A, R., (2019) 'Implementation and Analysis of Penetration Techniques Using the Man-In-The-Middle Attack', *Internasional Conference of Computer and Informatics Engineering (IC2IE)*, pp188-192
- Budiman, I., Saori, S., Anwar, R, N., Fitriani, Yuga, M., (2021) 'ANALISIS PENGENDALIAN MUTU DI BIDANG INDUSTRI MAKANAN'. *Jurnal Inovasi Penelitian*, 1(10), pp2185-2190
- Fachri, F., Fadil, A., Riadi, I., (2021) 'Analisis Keamanan Webserver Menggunakan Penetration Test', *Jurnal Informatika*, 8(2), pp. 183-190
- Fauzan, F. Y., Syukhri., (2021) 'Analisis metode web security PTES (Penetration Testing Execution adn Standart) pada aplikasi E-Learning Universitas Negeri Padang', *Jurnal Vocational Teknik Elektronika dan Informatika*, 9(2), pp.105-110
- Hidayatulloh, S., Saptadji, D., (2021) 'Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)', *Jurnal Algoritma*, 19(1), pp. 77-86
- Kholiq, A., Khoirunnisa, D., (2019) 'Analisis keamanan wireless local area network (WLAN) dengan metode penetratation testing execution standard (PTES)', *Jurnal ilmiah Fakultas Teknik*, 15(1), pp. 46-55
- Lika, S., Halim, R. D. P., Verdian, I., (2018) 'Analisa serangan SQL Injeksi menggunakan SQLMAP', *Jurnal Sistem dan Teknologi Informasi*, 4(2), pp. 88-94.
- Nugroho, A. B., Mandala, S., (2019) 'Study the best PenTest Algorithm for Blind SQL Injection Attacks', *Intl Journal on ICT*, 5(2), pp.1-10
- Orisa, M., Ardita, M., (2021) 'Vulnerability assesment untuk meningkatkan kualitas keamanan web', *Jurnal MNEMONIC*, 4(1), pp.16-19

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

- Pohan, Y. A., Yunus, Y., Sumijan., (2021) ‘Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar’, *Jurnal Sistim Informasi dan Teknologi*, 3(1), pp1-6
- Sanjaya, I. G. A. S., Sasmita, G. M. A., Arsa, D. M. S., (2019) ‘Evaluasi keamanan website lembaga X mekemudiani penetratioin testing menggunakan framework ISSAF’, *Jurnal Ilmiah Merpati*, 8(2), pp.113-124
- Singasatia, D., Totohendarto, M. H., Saputro, J., (2018) ‘ Penetration Testing untuk menguji kerentanan pada sistem informasi akademik di sekolah tinggi teknologi XYZ’, *Jurnal Sekolah Tinggi Teknologi Wastukencana*, 12(5), pp. 121-128
- Sinha. S, (2018) ‘Beginning Ethical Hacking with Kali Linux’, *Library of congress*, 978-1-4842-3891-2, pp. 46-426.
- Subandi, K., Sugara, V. I., (2021) ‘Analisa Serangan Vulnerabilites Terhadap Server Selama Periode WFH di Masa Pandemi Covid-19 Sebagai Prosedur Mitigasi’, *Jurnal Semnastek*, 007, pp. 2407-1846
- Susilo, G., (2018) ‘Keamanan basis data pada sistem informasi di era global’. *Transformasi jurnal informasi & pengembangan iptek*, 12(2), pp.78—87
- Syarifudin, I. (2018) ‘Pentesting dan analisis keamanan web paud dikmas’, *Jurnal pentesting dan analisis keamanan*, 4(5), pp.2-7
- Tarigan, B. V., Kusyanti, A., Yahya, W., (2018) ‘Analisis Perbandingan Pentetration Testing Tool untuk aplikasi Web’, *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 1(3), pp.206-214
- Wibowo, F., Harjono., Wicaksosno, A. P., (2019) ‘Uji vulnerability pada website jurnal ilmiah universitas muhamadiyah purwokerto menggunakan OpenVAS dan Acunetix WVS’, *Jurnal Informatika*, 6(2), pp. 212-218



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Yunanri, W., Riadi, I., Yudhana, A., (2018) ‘Analisis Deteksi Bulnerability pada Web Server Open Jurnal System Menggunakan OWASP Scanner’, *JURTI*, 2(1), pp.2579-8790

