IDENTIFIKASI KERENTANAN JARINGAN MENGGUNAKAN METODE *PENETRATION TESTING*

(Kasus: PT. Berlian Anugerah Transportasi Surabaya)

Tugas Akhir

Diajukan untuk memenuhi persyaratan mencapai derajat Sarjana Sistem Informasi

Albertus Hari Gunadi

NPM: 201710965

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ATMA JAYA YOGYAKARTA

2024

HALAMAN PENGESAHAN

Tugas Akhir Berjudul

IDENTIFIKASI KERENTANAN JARINGAN MENGGUNAKAN METODE PENETRATION TESTING (Kasus: PT. Berlian Anugerah Transportasi)

yang disusun oleh
Albertus Hari Gunadi
20171096
dinyatakan telah memenuhi syarat pada tanggal 18 Juli 2024

		Keterangan
Dosen Pembimbing 1	: Dr. Fl. Sapty Rahayu, S.T., M.Kom.	Telah Menyetujui
Dosen Pembimbing 2	: Elisabeth Marsella, S.S., M.Li.	Telah Menyetujui
Tim Penguji		
Penguji 1	: Dr. Fl. Sapty Rahayu, S.T., M.Kom.	Telah Menyetujui
Penguji 2	: Yohanes Priadi Wibisono, S.T., M.M.	Telah Menyetujui
Penguji 3	: Putri Nastiti, S.Kom., M.Eng.	Telah Menyetujui

Yogyakarta, 18 Juni 2024
Universitas Atma Jaya Yogyakarta
Teknologi Industri
Dekan

ttd.

Dr. Ir. Parama Kartika Dewa SP., S.T., M.T.

Dokumen ini merupakan dokumen resmi UAJY yang tidak memerlukan tanda tangan karena dihasilkan secara elektronik oleh Sistem Bimbingan UAJY. UAJY bertanggung jawab penuh atas informasi yang tertera di dalam dokumen ini

LEMBAR PENYATAAN

Orisinalitas & Publikasi Ilmiah

Saya yang bertanda tangan di bawah ini:

Nama Lengkap	: Albertus Hari Gunadi
NPM	: 201710965
Program Studi	: Sistem Informasi
Fakultas	: Teknologi Industri
Judul Penelitian	: Identifikasi Kerentanan Jaringan Menggunakan Metode Penetration Testing (Kasus: PT. Berlian Anugerah Transportasi Surabaya)

Menyatakan dengan ini:

1. Skripsi ini adalah benar merupakan hasil karya sendiri dan tidak merupakan salinan sebagian atau keseluruhan dari karya orang lain.
2. Memberikan kepada Universitas Atma Jaya Yogyakarta, berupa Hak Bebas Royalti non eksklusif (*Non-Exclusive-Royalty-Free Right*) atas Penelitian ini,
3. dan berhak menyimpan, mengelola dalam pangkalan data, mendistribusikan, serta menampilkan untuk kepentingan akademis, tanpa perlu meminta izin selama tetap mencantumkan nama penulis.
4. Bersedia menanggung secara pribadi segala bentuk tuntutan hukum yang mengikuti atas pelanggaran Hak Cipta dalam pembuatan Skripsi ini.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 25 Agustus 2023

Yang menyatakan,

Albertus Hari Gunadi

201710965

LEMBAR PENYATAAN

Persetujuan dari Instansi Asal Peneltian

(Jika penelitian membutuhkan akses data organisasi eksternal)

Saya yang bertanda tangan di bawah ini:

Nama Lengkap Pembimbing	: Nama Lengkap Pembimbing Lapangan
Jabatan	: Jabatan Pembimbing Lapangan
Departemen	:

Menyatakan dengan ini:

Nama Lengkap	: Albertus Hari Gunadi
NPM	: 201710965
Program Studi	: Sistem Informasi
Fakultas	: Teknologi Industri
Judul Penelitian	: Identifikasi Kerentanan Jaringan Menggunakan Metode Penetration Testing (Kasus: PT. Berlian Anugerah Transportasi Surabaya)

1. Penelitian telah selesai dilaksanakan pada perusahaan, dan telah diaplikasikan pada sistem terkait.
2. Perusahaan telah melakukan sidang internal berupa kelayakan penelitian ini dan akan mencantumkan lembar penilaian secara tertutup kepada pihak universitas sebagai bagian dari nilai akhir mahasiswa

3. Memberikan kepada perusahaan berupa Hak Bebas Royalti non eksklusif (*Non-Exclusive-Royalty-Free Right*) atas Penelitian ini, dan berhak menyimpan, mengelola dalam pangkalan data, tanpa perlu meminta izin selama tetap mencantumkan nama penulis.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Kota, Tanggal Bulan Tahun

Yang menyatakan,

Nama Pembimbing Lapangan

Jabatan

PRAKATA

Puji syukur kehadirat Allah yang senantiasa melimpahkan rahmat, anugerah, dan panduan-Nya kepada penulis sehingga dapat menyelesaikan Tugas Akhir ini dengan baik. Penyusunan Tugas Akhir ini bertujuan sebagai persyaratan untuk meraih gelar sarjana Sistem Informasi dari Program Studi Sistem Informasi Fakultas Teknologi Industri Universitas Atma Jaya Yogyakarta

Penulis mengakui bahwa dalam penyusunan Tugas Akhir ini, kerjasama dari berbagai individu baik secara langsung maupun tidak langsung memiliki peran yang besar. Pada kesempatan ini penulis ingin mengungkapkan rasa terima kasih kepada:

1. Allah yang senantiasa melimpahkan rahmat, nikmat, dan semangat-Nya kepada penulis.
2. Keluarga yang selalu memberikan segala dukungan positif.
3. Dr. Fl. Sapty Rahayu, S.T., M.Kom, selaku Dosen Pembimbing I yang telah meluangkan banyak waktu, tenaga, bantuan untuk memberikan bimbingan dan memberikan masukan sehingga Tugas Akhir ini dapat terselesaikan.
4. Ibu Elisabeth Marsella, S.S., M.Li., selaku Dosen Pembimbing II yang telah meluangkan banyak waktu, tenaga, bantuan untuk memberikan bimbingan dan memberikan masukan sehingga Tugas Akhir ini dapat terselesaikan.
5. Seluruh Dosen dan Staff Fakultas Teknologi Industri Universitas Atma Jaya Yogyakarta yang pernah mengajar dan membimbing penulis selama kuliah di Program Studi Sistem Informasi.
6. Teman-teman terkasih yang selalu mendukung serta menemani dalam suka dan duka

7. Seluruh staf PT. Berlian Anugerah Transportasi Surabaya
8. Semua yang tidak dapat disebutkan satu persatu yang telah memberikan semangat, motivasi, doa, kebersamaan selama penulis menjalani masa perkuliahan.

Demikian Tugas Akhir ini penulis susun dengan segenap usaha dan kemampuan. Penulis memahami bahwa penyusunan Tugas Akhir ini masih memiliki keterbatasan, dan penulis berharap kepada semua pihak agar menyampaikan kritik maupun saran untuk memperbaiki dan menyempurnakan Tugas Akhir ini. Akhir kata penulis berharap agar Tugas Akhir ini dapat memberikan manfaat bagi semua pihak

INTI SARI

Keamanan jaringan merupakan aspek krusial dalam menjaga integritas, kerahasiaan, dan ketersediaan data dalam suatu organisasi. Salah satu metode yang efektif untuk mengidentifikasi dan mengukur kerentanan dalam jaringan adalah *penetration testing*. Penelitian ini bertujuan untuk mengidentifikasi kerentanan yang terdapat pada jaringan suatu organisasi dengan menggunakan metode *penetration testing*.

Penelitian ini menggunakan pendekatan eksploratif dengan beberapa tahapan uji penetrasi, yaitu pengumpulan informasi, penetration testing dan report. Tools yang digunakan dalam penelitian ini antara lain Advanced IP Scanner untuk memindai ip, Nmap untuk memindai *port*, dan Wireshark untuk menganalisis lalu lintas jaringan. Hasil dari *penetration testing* ini diharapkan dapat mengidentifikasi celah-celah keamanan yang ada serta memberikan rekomendasi perbaikan untuk meningkatkan keamanan jaringan.

Dari hasil penelitian, ditemukan beberapa kerentanan yang signifikan pada jaringan, antara lain kelemahan pada konfigurasi firewall, sistem autentikasi yang lemah, dan adanya celah pada perangkat lunak yang digunakan. Rekomendasi yang diberikan mencakup perbaikan konfigurasi keamanan, kebijakan penerapan kata sandi yang kuat, dan pembaruan perangkat lunak. Dengan adanya kerentanan ini, organisasi dapat mengambil langkah proaktif untuk memperbaiki sistem keamanan jaringan mereka, sehingga dapat meminimalkan risiko terhadap serangan siber di masa mendatang.

ABSTRACT

Network security is a crucial aspect in maintaining the integrity, confidentiality and availability of data in an organization. One effective method for identifying and measuring vulnerabilities in a network is penetration testing. This research aims to identify vulnerabilities that exist in an organization's network using the penetration testing method.

This research uses an exploratory approach with several stages of penetration testing, namely information gathering, penetration testing and reporting. The tools used in this research include Advanced IP Scanner to scan IP, Nmap to scan ports, and Wireshark to analyze network traffic. The results of this penetration testing are expected to be able to identify existing security gaps and provide recommendations for improvements to improve network security.

From the research results, several significant vulnerabilities were found in the network, including weaknesses in the firewall configuration, a weak authentication system, and gaps in the software used. Recommendations include security configuration improvements, strong password enforcement policies, and software updates. Given these vulnerabilities, organizations can take proactive steps to improve their network security systems, thereby minimizing the risk of future cyber attacks

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL