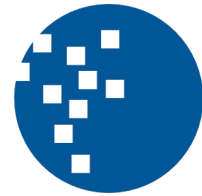


**IMPLEMENTASI PENETRATION TESTING PADA PORTAL LAYANAN
PNS KOTA MAGELANG**



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

MAGANG

Fierly Felicio Febriansa
00000056185

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2024

**IMPLEMENTASI PENETRATION TESTING PADA PORTAL LAYANAN
PNS KOTA MAGELANG**



UMN

**UNIVERSITAS
MULTIMEDIA
NUSANTARA**

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA**

TANGERANG

2024

HALAMAN PERNYATAAN TIDAK PLAGIAT

Dengan ini saya,

Nama : Fierly Felicio Febriansa
NIM : 00000056185
Program Studi : Informatika

Menyatakan dengan sesungguhnya bahwa Laporan Magang saya yang berjudul:
Implementasi Penetration Testing pada Portal Layanan PNS Kota Magelang

merupakan hasil karya saya sendiri, bukan merupakan hasil plagiat, dan tidak pula dituliskan oleh orang lain; Semua sumber, baik yang dikutip maupun dirujuk, telah saya cantumkan dan nyatakan dengan benar pada bagian Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan karya ilmiah, saya bersedia menerima konsekuensi untuk dinyatakan TIDAK LULUS. Saya juga bersedia menanggung segala konsekuensi hukum yang berkaitan dengan tindak plagiarisme ini sebagai kesalahan saya pribadi dan bukan tanggung jawab Universitas Multimedia Nusantara.

Tangerang, 31-05-2024



(Fierly Felicio Febriansa)

HALAMAN PENGESAHAN

Magang dengan judul

**IMPLEMENTASI PENETRATION TESTING PADA PORTAL LAYANAN
PNS KOTA MAGELANG**

oleh

Nama : Fierly Felicio Febriansa
NIM : 00000056185
Program Studi : Informatika
Fakultas : Fakultas Teknik dan Informatika

Telah diujikan pada hari Selasa, 11-05-2024
Pukul 11.00 s/s 12.00 dan dinyatakan
LULUS

Dengan susunan penguji sebagai berikut

Dosen Pembimbing

Penguji

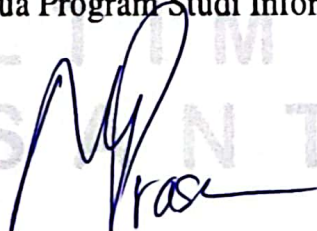


(Dr. Maria Irmina Prasetyowati,
S.Kom., M.T.)
NIDN: 0725057201



(Alethea Suryadibrata, S.Kom., M.Eng.)
NIDN: 0322099201

Pj. Ketua Program Studi Informatika,



(Dr. Eng. Niki Prastomo, S.T., M.Sc.)
NIDN: 0419128203

**HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK
KEPENTINGAN AKADEMIS**

Yang bertanda tangan di bawah ini:

Nama : Fierly Felicio Febriansa

NIM : 00000056185

Program Studi : Informatika

Jenjang : S1

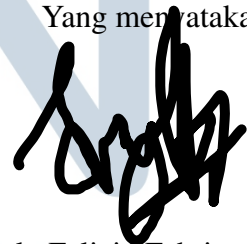
Jenis Karya : Magang

Menyatakan dengan sesungguhnya bahwa:

- Saya bersedia memberikan izin sepenuhnya kepada Universitas Multimedia Nusantara untuk mempublikasikan hasil karya ilmiah saya di repositori Knowledge Center, sehingga dapat diakses oleh Civitas Akademika/Publik. Saya menyatakan bahwa karya ilmiah yang saya buat tidak mengandung data yang bersifat konfidensial dan saya juga tidak akan mencabut kembali izin yang telah saya berikan dengan alasan apapun.
- Saya tidak bersedia karena dalam proses pengajuan untuk diterbitkan ke jurnal/konferensi nasional/internasional (dibuktikan dengan *letter of acceptance*)**.

Tangerang, 31-05-2024

Yang menyatakan



Fierly Felicio Febriansa

U M M N
UNIVERSITAS
MULTIMEDIA
NUSANTARA

** Jika tidak bisa membuktikan LoA jurnal/HKI selama enam bulan ke depan, saya bersedia mengizinkan penuh karya ilmiah saya untuk diunggah ke KC UMN dan menjadi hak institusi UMN.

Halaman Persembahan / Motto

"A good name is to be more desired than great wealth, Favor is better than silver and gold."

Proverbs 22:1 (NASB)



UMMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

KATA PENGANTAR

Puji Syukur atas berkat dan rahmat kepada Tuhan Yang Maha Esa, atas selesainya penulisan laporan Magang ini dengan judul: Implementasi Penetration Testing pada Portal Layanan PNS Kota Magelang dilakukan untuk memenuhi salah satu syarat untuk mencapai gelar Sarjana Komputer Jurusan Informatika Pada Fakultas Teknik dan Informatika Universitas Multimedia Nusantara. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan laporan magang ini, sangatlah sulit bagi saya untuk menyelesaikan laporan magang ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Dr. Ninok Leksono, selaku Rektor Universitas Multimedia Nusantara.
2. Bapak Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Bapak Dr.Eng. Niki Prastomo,S.T.,M.Sc., selaku Ketua Program Studi Informatika Universitas Multimedia Nusantara.
4. Ibu Dr.Maria Irminda Prasetyowati, S.Kom., M.T.. sebagai Pembimbing Magang yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi atas terselesainya laporan magang ini.
5. Kepada Pak Bagus Setiawan, S.Mat., selaku mentor yang telah memberikan arahan dalam mengerjakan tugas.
6. Orang Tua dan keluarga saya yang telah memberikan bantuan dukungan material dan moral, sehingga penulis dapat menyelesaikan laporan magang ini.

Semoga laporan magang ini bermanfaat, baik sebagai sumber informasi maupun sumber inspirasi, bagi para pembaca.

Tangerang, 31-01-2024



Fierly Felicio

Implementasi Penetration Testing pada Portal Layanan PNS Kota Magelang

Fierly Felicio Febriansa

ABSTRAK

Keamanan siber pada web dan jaringan menjadi semakin krusial seiring dengan meningkatnya ketergantungan terhadap teknologi digital di berbagai sektor, termasuk bisnis, pemerintahan, dan kehidupan sehari-hari. Serangan siber yang semakin canggih dan beragam, seperti peretasan, malware, phishing, dan serangan DDoS, mengancam integritas, kerahasiaan, dan ketersediaan data yang disimpan dan diproses oleh sistem informasi. Keamanan siber yang efektif melibatkan implementasi protokol keamanan yang kuat, penggunaan enkripsi, pembaruan perangkat lunak secara berkala, serta edukasi pengguna mengenai praktik keamanan terbaik. Dengan melindungi web dan jaringan dari ancaman siber, organisasi dapat mencegah kerugian finansial, kerusakan reputasi, dan pelanggaran hukum yang mungkin timbul akibat kebocoran data. Oleh karena itu, investasi dalam keamanan siber bukan hanya sebagai langkah defensif, tetapi juga sebagai strategi proaktif untuk memastikan kontinuitas operasional dan kepercayaan pengguna.

Kata kunci: Ancaman siber, Integritas data, Keamanan siber, dan Strategi proaktif



Implementation of Penetration Testing on the Civil Servant Service Portal of Magelang City

Fierly Felicio Febriansa

ABSTRACT

Cybersecurity on the web and network has become increasingly crucial as reliance on digital technology grows across various sectors, including business, government, and daily life. Sophisticated and diverse cyber attacks, such as hacking, malware, phishing, and DDoS attacks, threaten the integrity, confidentiality, and availability of data stored and processed by information systems. Effective cybersecurity involves implementing strong security protocols, using encryption, regularly updating software, and educating users on best security practices. By protecting the web and network from cyber threats, organizations can prevent financial losses, reputational damage, and legal violations that may arise from data breaches. Therefore, investing in cybersecurity is not only a defensive measure but also a proactive strategy to ensure operational continuity and user trust.

Keywords: *Cybersecurity, Cyber threats, Data integrity, Proactive strategy*



DAFTAR ISI

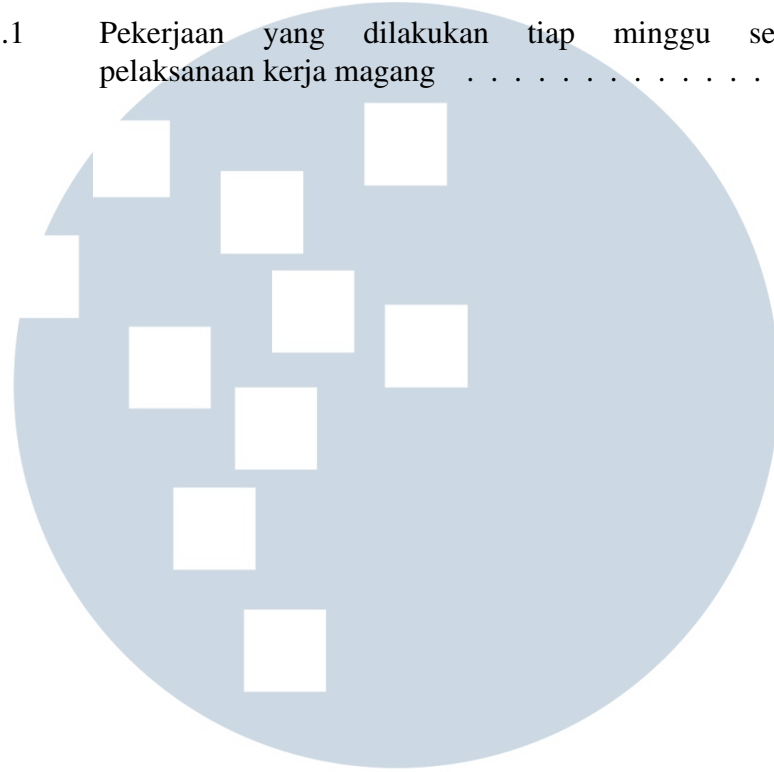
HALAMAN JUDUL	i
PERNYATAAN TIDAK MELAKUKAN PLAGIAT	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERSETUJUAN PUBLIKASI ILMIAH	v
HALAMAN PERSEMBAHAN/MOTO	vi
KATA PENGANTAR	vii
ABSTRAK	viii
ABSTRACT	ix
DAFTAR ISI	x
DAFTAR GAMBAR	xi
DAFTAR TABEL	xii
DAFTAR KODE	xiii
DAFTAR LAMPIRAN	xiv
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Maksud dan Tujuan Kerja Magang	2
1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang	3
BAB 2 GAMBARAN UMUM PERUSAHAAN	4
2.1 Sejarah Singkat Perusahaan	4
2.2 Visi dan Misi Perusahaan	4
2.3 Struktur Organisasi Perusahaan	5
BAB 3 PELAKSANAAN KERJA MAGANG	6
3.1 Kedudukan dan Organisasi	6
3.2 Tugas yang Dilakukan	6
3.3 Uraian Pelaksanaan Magang	7
3.4 Kegiatan dan Implementasi	9
3.4.1 Mengunduh 5 Aplikasi Virtualisasi	9
3.4.2 Meretas dan Mendeskripsi <i>Password</i>	12
3.4.3 Mencari Kerentanan pada Web dan Jaringan	16
3.4.4 Mengenal Aplikasi <i>Honeypot</i> untuk Mendeteksi Malware	19
3.4.5 Memulihkan <i>file</i> dan Membuat <i>Publicapp</i> dan <i>Privateapp</i>	21
3.4.6 Mengatur IP dan IPV4 dan mengenal TCP/UDP	24
3.4.7 Mendeteksi jaringan yang mencurigakan	26
3.4.8 Mengenal <i>Certificate Authority</i> dan <i>Public Key infrastructure</i>	28
3.4.9 Memulihkan <i>file</i> PDF,MP4,JPG, dan <i>folder</i>	29
3.4.10 <i>IT Policy</i>	32
3.4.11 Implementasi Pentest	33
3.5 Kendala dan Solusi yang Ditemukan	35
BAB 4 SIMPULAN DAN SARAN	36
4.1 Simpulan	36
4.2 Saran	36
DAFTAR PUSTAKA	37

DAFTAR GAMBAR

Gambar 3.1	tampilan awal VmWare	9
Gambar 3.2	tampilan awal Virtual Box	10
Gambar 3.3	tampilan awal XenServer	11
Gambar 3.4	tampilan awal Proxmox	11
Gambar 3.5	tampilan awal OpenStack	12
Gambar 3.6	Aplikasi Abel <i>and</i> Cain	13
Gambar 3.7	Tampilan awal aplikasi Abel <i>and</i> Cain	14
Gambar 3.8	Jika sudah terdeskripsi <i>password</i>	14
Gambar 3.9	Tampilan awal Hydra	15
Gambar 3.10	Meretas <i>password</i> dengan Hydra	15
Gambar 3.11	Tampilan Sqlmap	15
Gambar 3.12	Tampilan <i>database</i>	16
Gambar 3.13	Tampilan <i>password</i> dan <i>username</i>	16
Gambar 3.14	Membuka Arachni	17
Gambar 3.15	Tampilan <i>Login</i>	17
Gambar 3.16	Tampilan awal Arachni	17
Gambar 3.17	Tampilan <i>login</i>	18
Gambar 3.18	Tampilan awal OpenVas	19
Gambar 3.19	GRMWDKE ISO	20
Gambar 3.20	Aplikasi GhostGUI	20
Gambar 3.21	Tampilan awal GhostGUI jika sudah mendeteksi Malware	21
Gambar 3.22	Membuat cadangan <i>file</i>	21
Gambar 3.23	<i>Private key</i>	22
Gambar 3.24	<i>Public key</i>	23
Gambar 3.25	<i>folder</i> download	23
Gambar 3.26	Sudah terdaftar	23
Gambar 3.27	mengatur <i>router, switch</i> dan VLAN	24
Gambar 3.28	konfigurasi IP	25
Gambar 3.29	mengatur IPV4 <i>address, subnet</i> dan <i>default gateway</i>	25
Gambar 3.30	aplikasi Rufus	27
Gambar 3.31	Kismet	27
Gambar 3.32	<i>Certificate Authority</i>	28
Gambar 3.33	Sertifikat pada <i>folder</i> yang telah dibuat	29
Gambar 3.34	aplikasi <i>recovery</i>	30
Gambar 3.35	Tskrecovery	30
Gambar 3.36	Foremost	31
Gambar 3.37	FTK <i>Imager</i>	31
Gambar 3.38	Autopsy	32
Gambar 3.39	Dmde	32
Gambar 3.40	Deteksi protokol SSL dan masa tenggang	34
Gambar 3.41	<i>brute force</i> nama <i>directory</i>	35

DAFTAR TABEL

Tabel 3.1	Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang	8
-----------	--	---



UMMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR KODE



UMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR LAMPIRAN

Lampiran 1	MBKM-01 Cover Letter MBKM Internship Track 1	38
Lampiran 2	MBKM-02 MBKM Internship Track 1 Card	39
Lampiran 3	MBKM-03 Daily Task - Internship Track 1	40
Lampiran 4	MBKM-03 Daily Task - Internship Track 1	41
Lampiran 5	MBKM-03 Daily Task - Internship Track 1	42
Lampiran 6	MBKM-03 Daily Task - Internship Track 1	43
Lampiran 7	MBKM-03 Daily Task - Internship Track 1	44
Lampiran 8	MBKM-03 Daily Task - Internship Track 1	45
Lampiran 9	MBKM-03 Daily Task - Internship Track 1	46
Lampiran 10	MBKM-03 Daily Task - Internship Track 1	47
Lampiran 11	MBKM-03 Daily Task - Internship Track 1	48
Lampiran 12	MBKM-03 Daily Task - Internship Track 1	49
Lampiran 13	MBKM-03 Daily Task - Internship Track 1	50
Lampiran 14	MBKM-03 Daily Task - Internship Track 1	51
Lampiran 15	MBKM-03 Daily Task - Internship Track 1	52
Lampiran 16	MBKM-03 Daily Task - Internship Track 1	53
Lampiran 17	MBKM-03 Daily Task - Internship Track 1	54
Lampiran 18	MBKM-03 Daily Task - Internship Track 1	55
Lampiran 19	MBKM-03 Daily Task - Internship Track 1	56
Lampiran 20	MBKM-03 Daily Task - Internship Track 1	57
Lampiran 21	MBKM-03 Daily Task - Internship Track 1	58
Lampiran 22	MBKM-03 Daily Task - Internship Track 1	59
Lampiran 23	MBKM-03 Daily Task - Internship Track 1	60
Lampiran 24	MBKM-04 Verification Form of Internship Report MBKM Internship Track 1	61
Lampiran 25	Form Bimbingan	62
Lampiran 26	Lampiran Turnitin	63

