ANALISIS KEAMANAN PORTAL AKADEMIK MENGGUNAKAN METODE *PENETRATION TESTING* UNTUK PENCEGAHAN SERANGAN SIBER (STUDI KASUS: https://situ2.unpas.ac.id/)

TUGAS AKHIR

Disusun sebagai salah satu syarat untuk kelulusan
Program Strata 1, Program Studi Teknik Informatika,
Universitas Pasundan Bandung

oleh :

Ibnu Rusdianto
NPM : 20.304.0012

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG

AGUSTUS 2024

LEMBAR PENGESAHAN
LAPORAN TUGAS AKHIR

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari dan tanggal sidang sesuai berita acara sidang, tugas akhir dari:

Nama : Ibnu Rusdianto
Nrp. : 20.304.0012

Dengan judul :

" ANALISIS KEAMANAN PORTAL AKADEMIK MENGGUNAKAN METODE *PENETRATION TESTING* UNTUK PENCEGAHAN SERANGAN SIBER (STUDI KASUS: https://situ2.unpas.ac.id/)"

Bandung, 12 Agustus 2024
Menyetujui ,
Pembimbing Utama

(Doddy Ferdiansyah, S.T., M.T)

ABSTRAK

Portal akademik merupakan salah satu sasaran utama bagi para penyerang untuk mencuri data sensitif, mengganggu layanan, atau melakukan aksi merusak lainnya. Universitas Pasundan (UNPAS) sebagai lembaga pendidikan tidak luput dari risiko serangan siber. Universitas Pasundan memiliki portal akademik yang vital bagi kegiatan akademik dan administratif, seperti pendaftaran, penjadwalan, dan pengelolaan data mahasiswa. Namun, keamanan portal ini rentan terhadap serangan siber yang dapat merusak integritas dan kerahasiaan informasi. Penelitian ini bertujuan untuk menganalisis keamanan portal akademik UNPAS menggunakan metode Penetration Testing guna mencegah serangan siber. Metode ini melibatkan simulasi serangan nyata untuk mengidentifikasi kelemahan sistem.

Penelitian ini berfokus untuk analisis keamanan serangan siber menggunakan metode Penetration Testing. Penetration testing merupakan proses evaluasi terhadap sistem komputer atau jaringan untuk mengidentifikasi kelemahan keamanan yang mungkin dapat dieksploitasi oleh penyerang. Langkah-langkah yang digunakan yaitu information gathering, threat modeling, vulnerability analysis, reporting.

Hasil dari penelitian ini yaitu berupa laporan analisis kerentanan pada portal akademik UNPAS, seperti kelemahan dalam konfigurasi server dan kurangnya pembaruan perangkat lunak, sehingga pengelola dapat meningkatkan keamanan agar meminimalisir dari serangan siber di masa mendatang.

Kata Kunci: Serangan Siber, Penetration Testing, Portal Akademik, Unpas, Website.

ABSTRACT

The academic portal is one of the main targets for hackers to steal sensitive data, disrupt services, or perform other malicious actions. Universitas Pasundan (UNPAS) as an educational institution is not immune to the risk of cyber attacks. Universitas Pasundan has a vital academic portal for academic and administrative activities such as registration, scheduling, and student data management. However, the security of this portal is vulnerable to cyber attacks that can compromise the integrity and confidentiality of information. This research aims to analyze the security of the UNPAS academic portal using the Penetration Testing method to prevent cyber attacks. The Penetration Testing method involves simulating real attacks to identify security vulnerabilities.

This research focuses on analyzing the security of cyber attacks using the Penetration Testing method. Penetration testing is an evaluation process for computer systems or networks to identify potential security vulnerabilities that can be exploited by attackers. The steps used are information gathering, threat modeling, vulnerability analysis, and reporting.

The results of the research are in the form of an analysis report on the vulnerabilities of the UNPAS academic portal, such as server configuration weaknesses and outdated software, allowing administrators to improve security to minimize the risk of future cyber attacks.

Keywords: Cyber Attack, Penetration Testing, Academic Portal, Unpas, Website.

DAFTAR ISI

BAB 1
PENDAHULUAN

Bab 1 terdiri dari penjelasan mengenai usulan penelitian yang dilakukan dalam pengerjaan tugas akhir. Di dalamnya berisi latar belakang masalah, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi pengerjaan tugas akhir, dan sistematika penulisan laporan tugas akhir.

1.1 Latar Belakang

Dalam era digital yang semakin berkembang pesat, portal akademik (https://situ2.unpas.ac.id/) berperan sebagai pintu gerbang utama yang menghubungkan berbagai informasi penting terkait dengan kegiatan akademis, administratif, dan personal mahasiswa serta staf pengajar. Namun, dengan meningkatnya kompleksitas sistem teknologi informasi dan seringnya terjadi ancaman keamanan dalam bentuk serangan siber, penting bagi institusi pendidikan untuk mengamankan portal akademik mereka dengan metode yang tepat.

Meucci dan Matteo menjelaskan bahwa *Penetration testing* adalah teknik umum yang digunakan untuk menguji keamanan jaringan. Pada dasarnya *penetration testing* adalah pengujian aplikasi yang aktif untuk menemukan kerentanan keamanan, tanpa mengetahui cara kerja aplikasi tersebut. Pelaku *penetration testing* bertindak sebagai penyerang dan berupaya untuk menemukan dan mengeksploitasi kerentanan [HID21].

Studi ini bertujuan untuk melakukan analisis mendalam terhadap keamanan portal akademik di Fakultas Teknik Universitas Pasundan melalui penerapan metode *penetration testing*. Dengan mengidentifikasi dan mengevaluasi potensi celah keamanan serta kerentanan yang ada dalam sistem, penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam tentang risiko keamanan yang mungkin dihadapi oleh portal akademik ini.

Dengan demikian, analisis keamanan portal akademik menggunakan metode *penetration testing* ini diharapkan dapat menjadi landasan bagi pengembangan strategi pencegahan serangan siber yang lebih efektif, khususnya dalam konteks Fakultas Teknik Universitas Pasundan, yang pada akhirnya dapat meningkatkan keamanan sistem informasi akademik secara keseluruhan.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya dapat disimpulkan, maka :

a. Bagaimana tingkat efektivitas sistem keamanan yang ada pada portal akademik tersebut terhadap serangan siber?
b. Bagaimana penggunaan metode *penetration testing* dapat membantu dalam menganilisis potensi serangan siber pada portal akademik Fakultas Teknik Universitas Pasundan.

1.3 Tujuan Tugas Akhir

Tujuan dari penulisan tugas akhir:

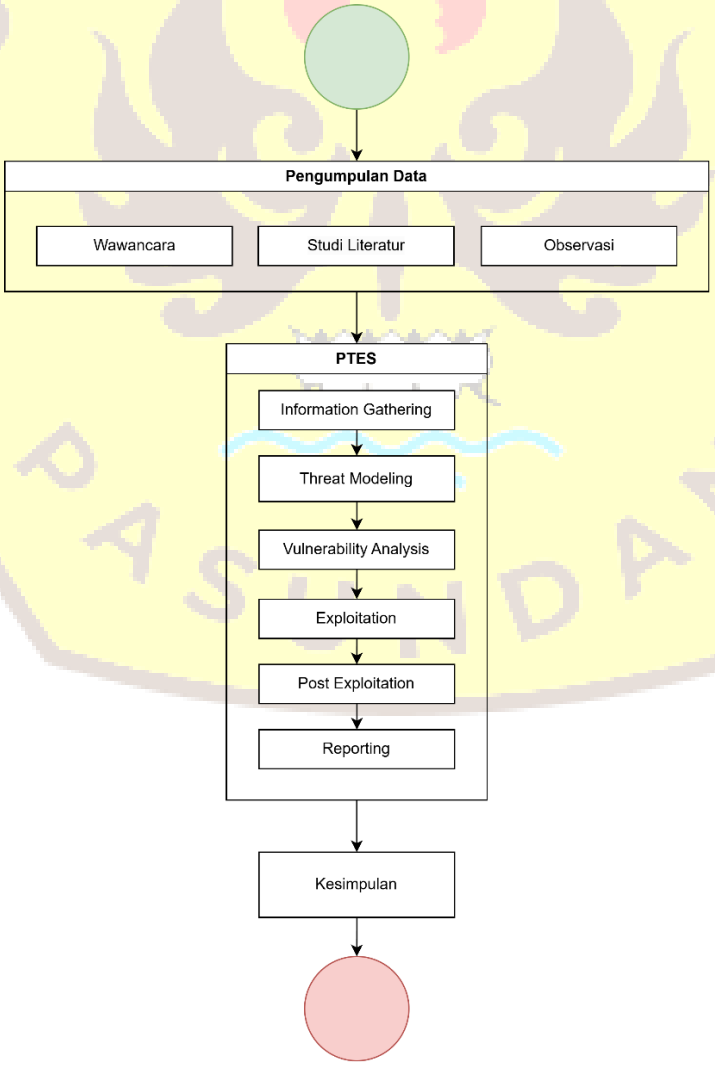
a. Menganalisis keamanan portal akademik termasuk penilaian terhadap risiko serangan peretasan, potensi pencurian data, dan kemungkinan penyalahgunaan.
b. Melakukan *penetration testing* untuk menemukan dan merekomendasikan perbaikan celah keamanan dalam website sebelum dimanfaatkan oleh penyerang siber.

1.4 Lingkup Tugas Akhir

Lingkup dari tugas akhir ini adalah sebagai berikut:

a. Penelitian ini berfokus pada analisis keamanan portal akademik dari serangan siber.
b. Hasil akhir dari penelitian ini yaitu melakukan uji coba secara aktif menggunakan metode penetration testing untuk menguji keamanan portal akademik.

1.5 Metodologi Tugas Akhir



Gambar 1. 1 Metodologi Tugas Akhir

1.6 Sistematika Penulisan Tugas Akhir

Sistematika penulisan yang menjelaskan mengenai bab-bab pada laporan tugas akhir :

BAB 1 : PENDAHULUAN

Pada bab ini terdapat latar belakang masalah, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi tugas akhir dan sistematika penulisan tugas akhir.

BAB 2 : LANDASAN TEORI DAN PENELITIAN TERDAHULU

Bab ini berisikan terkait teori-teori yang mendukung penelitian penulis, berupa literatur yang valid dan penelitian terdahulu yang dapat berhubungan dengan penelitian ini sehingga bisa membantu dalam menyelesaikan masalah yang ada.

BAB 3 : SKEMA PENELITIAN

Bab ini berisi penjelasan alur penelitian, analisis permasalahan, analisis manfaat tugas akhir, kerangka pemikiran teoritis dan lokasi penelitian.

BAB 4 : ANALISIS DAN PERANCANGAN

Bab ini berisi tentang analisis dari sistem yang meliputi analisis objek penelitian, analisis kebutuhan, dan perancangan pengujian yang akan digunakan untuk pengujian pada target.

BAB 5 : PENGUJIAN DAN HASIL

Bab ini berisi tentang pengujian dan hasil pengujian menggunakan Penetration Testing dan Threat Modeling dalam perancangan pengujian target.

BAB 6 : KESIMPULAN DAN SARAN

Bab ini berisikan penjelasan mengenai kesimpulan dan saran penelitian Tugas Akhir terhadap pengujian keamanan pada *website* yang telah dicapai/dilakukan.

DAFTAR PUSTAKA

[FAR22] Farizy, S., & Eriana, E. S. (2022). Keamanan Sistem Informasi.

[HER07] Heru, B., Benny, B., Defendy, D., & Hento, W. (2007). Keamanan jaringan menggunakan unified threat management pada server berbasiskan linux. *CommIT (Communication and Information Technology) Journal*, *1*(1), 48-59.

[LUT21] Luthfah, D. (2021). Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law). *terAs Law Review: Jurnal Hukum Humaniter dan HAM*, *3*(1), 11-22.

[MUH22] Muhyidin, Y., Totohendarto, M. H., & Undamayanti, E. (2022). Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking. *Jurnal Teknologika*, *12*(1), 80-89.

[INV23] invicti.com. 2023. Web-vulnerability-Scanner. Diakses pada 03 Januari 2024, dari https://www.invicti.com/web-vulnerability-scanner/

[KIM20] Kim, J. (2020). *Burp suite: Automating web vulnerability scanning* (Master's thesis, Utica College).

[ALF20] Al Fajar, F. (2020). Analisis Keamanan Aplikasi Web Prodi Teknik Informatika Uika Menggunakan Acunetix Web Vulnerability. Jurnal Inovatif: Inovasi Teknologi Informasi dan Informatika, 3(2), 110-120.

[RAH21] Rahmawita, M. T. (2021). Analisis Kualitas Layanan Portal Akademik Terhadap Kepuasan Mahasiswa Menggunakan Metode E-Servqual Pada FKIP Universitas Riau. *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi*, *7*(2), 145-151.

[COM22] comparitech.com. 21 Oktober 2022. Threat Modeling Guide. Diakses pada 06 April 2024, dari https://www.comparitech.com/net-admin/threat-modeling-guide/.

[ENW24] en.wikipedia.org. 9 Februari 2024. Threat Modeling. Diakses pada 06 April 2024, dari https://en.wikipedia.org/wiki/Threat_model.

[ACU23] Acunetix.com. 5 September 2023. Acunetix Web Security Blog. Diakses 06 April 2024, dari https://www.acunetix.com/blog/.

[ENW23] en.wikipedia.org. 22 Agustus 2023. Nmap. Diakses 06 april 2024, dari https://id.wikipedia.org/wiki/Nmap

[POR24] Portswigger.net. 10 April 2024. Burp Suite documentation – contents. Diakses 12 april 2024, dari https://portswigger.net/burp/documentation/contents.

[NVD23] Nvd.nist.gov. 17 april 2023. CVE-2023-29197 Detail. Diakses 06 april 2024, dari https://nvd.nist.gov/vuln/detail/CVE-2023-29197.