PENETRATION TESTING PADA WEBSITE UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR (UMKT) DENGAN MENGGUNAKAN METODE PTES

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan mencapai gelar Sarjana Komputer

DISUSUN OLEH:

FITRIA NUR YAQIN

1911102441104

PROGRAM STUDI S1 TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR

SAMARINDA

JULI 2024

Penetration Testing Pada website Universitas Muhammadiyah Kalimantan Timur (UMKT) Dengan Menggunakan Metode PTES

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan mencapai gelar Sarjana Komputer

DISUSUN OLEH:

FITRIA NUR YAQIN

1911102441104

PROGRAM STUDI S1 TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR

SAMARINDA

JULI 2024

HALAMAN PENGESAHAN

HALAMAN PENGESAHAN

PENETRATION TESTING PADA WEBSITE UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR (UMKT) DENGAN MENGGUNAKAN METODE PTES

DISUSUN OLEH :

FITRIA NUR YAQIN

1911102441104

Telah Melaksanakan Ujian skripsi dan dinyatakan lulus,

Pada tanggal : 17 Juli 2024

Menyetujui,

Dosen Pembimbing

Faldi, S.Kom., M.TI
NIDN. 1121079101

Dosen Penguji

M. Taufiq Sumadi, S.Tr.Kom., M. Tr.Kom
NIDN. 1111089501

Ketua Program Studi

Arbansyah, S.Kom., M.Ti
NIDN. 1118019203

PERNYATAAN KEASLIAN SKRIPSI

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan dibawah ini :

Nama : Fitria Nur Yaqin

NIM : 1911102441104

Judul : Penetration Testing Pada Website Universitas Muhammadiyah Kalimantan Timur (UMKT) Dengan Menggunakan Metode PTES

Menyatakan dengan jujur bahwa skripsi ini merupakan hasil penelitian, dan ide saya sendiri, termasuk seluruh teks laporan dan kegiatan pemrograman. Jika saya memasukkan karya orang lain, saya akan dengan jelas menuliskan sumbernya.

Demikian pernyataan ini, saya membuat pernyataan ini dan siap menerima sanksi apa pun sesuai dengan peraturan di Universitas Muhammadiyah Kalimantan Timur.

Samarinda, 17 Juli 2024

Yang membuat pernyataan,

Fitria Nur Yaqin

1911102441104

PRAKATA

Puji syukur ke hadirat Allah SWT, karena atas segala rahmat-Nya penulis dapat menyelesaikan penyusunan Skripsi ini sebagai salah satu syarat untuk menyelesaikan tugas perkuliahan dan sebagai syarat mencapai kelulusan dari Universitas Muhammadiyah Kalimantan Timur Samarinda.

Skripsi ini merupakan hasil dari perjalanan panjang telah penulis tempuh selama masa perkuliahan. Penyusunan skripsi ini tidak terlepas dari dukungan, bimbingan, dan dorongan dari berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Keluarga, yang selalu memberikan dukungan moril dan materil serta menjadi sumber inspirasi dalam setiap langkah hingga saat ini.
2. Bapak Faldi, S.Kom., M.TI selaku dosen pembimbing sekaligus dosen penguji yang telah membantu mengarahkan, dan kesabaran dalam membimbing selama proses penulisan skripsi ini.
3. Bapak Muhammad Taufiq Sumadi, S.Tr.Kom., M.Tr.Kom selaku dosen penguji yang telah memberikan masukan dan arahan dalam revisi skripsi ini.
4. Teman-teman seperjuangan, yang senantiasa memberikan semangat, motivasi, dan dukungan dalam menyelesaikan tugas akhir ini.
5. Pihak Universitas Muhammadiyah Kalimantan Timur Samarinda, yang telah memberikan kesempatan dan sarana pendidikan selama ini.

Penulisan Skripsi ini tidak luput dari kekurangan dan kekhilafan. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun untuk perbaikan di masa mendatang.

Akhir kata, semoga Skripsi ini dapat memberikan manfaat dan kontribusi yang positif bagi perkembangan ilmu pengetahuan dan masyarakat pada umumnya.

ABSTRAK

Penetration testing merupakan proses penting dalam mengidentifikasi dan mengevaluasi kerentanan keamanan pada system informasi, termasuk website. Penelitian ini berfokus pada penetration testing pada website Universitas Muhammadiyah Kalimantan Timur (UMKT) dengan menggunakan metode Penetration Testing Execution Standard (PTES). PTES merupakan framework yang komprehensif dan terstruktur yang mencakup tahap-tahap penting dalam penetration testing pengujian, pengumpulan informasi , analisis ancaman, pengujian kerentanan. Tujuan dari penelitian ini untuk mengidentifikasi kerentanan pada website UMKTdan memberikan rekomendasi untuk perbaikan keamanan. Metode yang di gunakan meliputi pengumpulan data melalui pengujian penetrasi seperti scanning dan eksploitasi. Hasil penelitian menunjukkan bahwa terdapat bebrapa kerentanan yang dapat di eksploitasi untuk mendapatkan akses ke dalam sistem. Pembaruan sistem, peningkatan konfigurasi keamanan dan penerapan untuk menditeksi serta pencegahan serangan. Dengan melakukan penetration testing menggunakan metode PTES, penelitian ini memberikan signifikan dalam meningkatkan keamanan website UMKT dan sekaligus melindungi dari ancaman siber.

Kata Kunci: Penetration Testing,PTES, Keamanan Website, kerentanan, pengujian.

ABSTRACT

Penetration testing is an important process in identifying and evaluating security vulnerabilities in information systems, including websites. This research focuses on penetration testing on the Muhammadiyah University of East Kalimantan (UMKT) website using the Penetration Testing Execution Standard (PTES) method. PTES is a comprehensive and structured framework that includes important stages in penetration testing, information gathering, threat analysis, vulnerability testing. The aim of this research is to identify vulnerabilities on the UMKT website and provide recommendations for improvements to improve security. The methods used include data collection through penetration testing such as scanning and exploitation. The research results show that there are several vulnerabilities that can be exploited to gain access to the system. System updates, security configuration improvements and implementation to detect and prevent attacks. By carrying out penetration testing using the PTES method, this research is significant in improving the security of the UMKT website and at the same time protecting it from cyber threats.

Keywords: Penetration Testing, PTES, Website Security, vulnerabilities.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB 1

PENDAHULUAN

1.1. Latar Belakang

Dengan kemajuan teknologi informasi dan komunikasi saat ini, keamanan data menjadi perhatian yang sangat penting. Keamanan data merupakan masalah kritis mengingat kemajuan teknologi informasi dan komunikasi saat ini. Situs web adalah informasi yang tersedia secara online, dapat diakses oleh siapa saja yang memiliki koneksi internet di mana pun di dunia. Situs web ini terdiri dari teks, grafik, dan suara animasi untuk menjadikannya sumber informasi yang lebih menarik. (Ahmia & Belbachir, 2018). Website merupakan kebutuhan yang sangat penting bagi instansi pendidikan khususnya Universitas Muhammadiyah Kalimantan Timur. Diantara kelebihan website adalah fungsinya sebagai sarana penyampaian informasi, sebagai sarana interaksi dan sebagai titik kontak yang aktif.

Penggunaan internet semakin meningkat setiap tahunnya dalam skala global, termasuk di Indonesia. Dari sisi positifnya internet atau teknologi informasi memang ada manfaatnya, namun sisi negatifnya ternyata internet atau teknologi internet menjadi alat baru yang digunakan oleh orang-orang yang ingin merugikan orang lain. Cybercrime misalnya, merupakan salah satu jenis kekerasan virtual yang melibatkan penggunaan media komputer yang terhubung dengan internet. Namun, dibalik banyaknya keuntungan, ada juga ancaman yang bisa muncul. Berdasarkan data Indonesia Cybercrime Agency tahun 2019-2020 terdapat 2.880 kejadian cybercrime di Indonesia pada juni 2020 yang diinterupsi oleh serangan cyber ransomware Wannarcy (ransomware bsi tahun 2023). Untuk bisnis dan rumah, instansi swasta dan pemerintahan yang disebabkan oleh serangan ini telah terlihat dan menjadi langkah pertama dalam kerja sama keamanan dunia maya(Kiswanto & Thamrin, n.d.).

Sistem keamanan komputer adalah metode untuk mengamankan operasi informasi, aktivitas atau apa yang ada di dalam sistem komputer. Sebuah percobaan ini berguna untuk mengetahui apakah situs web aman dari tindakan penyerang. Salah satu cara untuk

mengetahui apakah suatu sistem aman atau tidak adalah dengan melakukan pengujian penetrasi.

Dapat dikatakan bahwa pengujian penetrasi adalah cara legal dan resmi untuk menemukan dan mengeksploitasi sistem komputer untuk membuat sistem lebih aman. Namun, dalam beberapa kasus, pihak yang tidak bertanggung jawab mengeksploitasi kelemahan dari penetration testing. Itulah mengapa sangat penting untuk mendapatkan ijin dari pihak yang ingin melakukan penetration testing.

Universitas Muhammadiyah Kalimantan Timur adalah Lembaga Pendidikan yang berkomitmen untuk memberikan pelayanan terbaik kepada mahasiswa dan masyarakat umum. Maka dari itu keamanan informasi adalah tanggung jawab yang haus dianggap dengan serius dalam era teknologi yang terus berkembang, serangan siber menjadi ancaman yang semakin nyata dan kompleks. Oleh karena itu saat ini terdapat kekurangan yang perlu di atasi yaitubelum pernah di lakukan uji penetrasi yang sesuai dengan standard Penetration testing Execution Standard(PTES) (Mulyanto et al., 2022). Penetration Testing Execution Standard (PTES) belakangan ini menjadi salah satu framework acuan untuk penetration testing. Meskipun framework ini masih dalam pengembangan, namun menyediakan cara yang sangat terstruktur untuk mengidentifikasi keamanan server. Berdasarkan permasalahan yang dihadapi maka dilakukan penelitian ini yang diharapkan dapat membantu pihak Universitas Muhammadiyah Kalimantan Timur dalam menjaga keamanan website.

1.2. Rumusan Masalah

Pendekatan rumusan masalah adalah analisis keamanan website. Universitas Muhammadiyah Kalimantan Timur(UMKT) dengan menggunakan Metode Penetration Testing Excution Standard(PTES).

1.3. Tujuan Penelitian

Tujuan penelitian ini adalah untuk melakukan uji penetrasi sebagai sarana menilai keamanan sistem website.

1.4. Batasan masalah

Batasan masalah ini tidak menyimpang dari pokok pembahasan penelitian, adapun batasa masalah sebagai berikut.

1. Metode yang di gunakan pada penelitian ini adalah penetration Testing Excution Standard (PTES).
2. Penelitian Ini di lakukan hanya untuk uji penetrasi pada website.

1.5. Manfaat Penelitian

Manfaat dari uji penetrasi kita bisa dapat mengidentifikasi kelemahan pada website server. Hasil dari uji penetrasi akan di jadikan saran maupun rekomendasi untuk perbaikan website.

BAB 2

TINJAUAN PUSTAKA

Pada bab ini penulis menjelaskan penelitian sebelumnya yang menghubungkan penelitian selanjutnya dan juga teori dasar sebagai sistem pendukung penelitan.

2.1. Penelitian Terkait

Pada penyusunan skripsi ini sedikit banyak nya terinspirasi dan mengacu dari penelitian – penelitian yang berkaitan dengan latar belakang masalah pada skripsi ini. Adapun penelitian yang berhubngan dengan skripsi ini antara lain yaitu:

Tabel 2. 1 Penelitian Terkait

Penelitian 1	
Penulis dan Tahun	(Suradji & Chandra, 2014)
Judul	Penetration Testing Sistem Jaringan Komputer Untuk Mengetahui Kerentanan Keamanan Server Dengan Menggunakan Metode Penetration Testing Execuition Standard (PTES) Studi Kasus Rumah Sakit Santa Madiun.
Objek	Keamanan Server Rumah Sakit Sanata Clara Madiun.
Metode	Penetration Testing Execuition Standard (PTES).
Hasil	Dengan menggunakan metode PTES, para peneliti menemukan bahwa server Rumah Sakit Santa Clara memiliki kerentanan signifikan yang dapat digunakan untuk melakukan kejahatan dunia maya. Kerentanan tersebut berasal dari layanan Microsoft Server yang masih penuh dengan bug dan error. Pelaku penyerangan memiliki kemampuan untuk menguasai server, memasang pintu belakang yang memungkinkan akses ke sistem, dan mencuri atau mengubah data yang tersimpan di dalamnya. Meskipun masalah yang ditemukan selama penelitian ini telah diperbaiki, firewall server juga harus

	diaktifkan untuk menghentikan serangan, dan filter jaringan seperti IDS dan IPS harus dipasang untuk memantau dan membatasi akses data ke internet.
Penelitian 2	
Penulis dan Tahun	(Utoro et al., 2020)
Judul	Analisis Keamanan Website E-learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execuition Standard (PTES).
Objek	Keamanan Website E-learning SMKN 1 Cibatu.
Metode	Penetration Testing Execuition Standard (PTES).
Hasil	Metode PTES digunakan dalam penelitian ini untuk mengetahui tingkat kerentanan sistem informasi yang paling berisiko terhadap serangan seperti eavesdropping, cross-site scripting, dan cross-site request forgery, yang dapat menyebabkan kebocoran data yang signifikan. Aplikasi website milik SMKN 1 Cibatu ditemukan rentan.
Penelitian 3	
Penulis dan Tahun	(Fauzan & Syukhri, 2021)
Judul	Analisis Metode Web Security Penetration Testing Execuition Standard (PTES) pada aplikasi E-learning Universitas Negeri Padang.
Objek	Web Security Pada Aplikasi E-learning Universitas Negeri Padang .
Metode	Penetration Testing Execuition Standard (PTES).

Hasil	Kesenjangan keamanan Level 2 atau level menengah pada penelitian ini ditemukan menggunakan pendekatan PTES, artinya serangan apa pun tidak akan berdampak signifikan pada situs web. Selain itu, karena *Secure Socket Layer* digunakan untuk meningkatkan keamanan situs web, eksploitasi *SQL Injection* tidak berhasil.
Penelitian 4	
Penulis dan Tahun	(Adrian & Setiyadi, 2018)
Judul	Analisis Keamanan Jaringan Dengan Menggunakan Metode Penetration Testing Execuition Standard (PTES) DI Dinas Kesehatan Provinsi Jawa Barat.
Objek	Keamanan Jaringan pada Layanan Internet Publik Provinsi Sumatra Selatan.
Metode	Penetration Testing Execuition Standard (PTES).
Hasil	Dinas Kesehatan Provinsi Jawa Barat memiliki sejumlah kerentanan yang perlu diwaspadai oleh Divisi Teknologi Informasi dan Komunikasi organisasinya, berdasarkan hasil penelitian metode PTES. Kerentanan ini membuka banyak kemungkinan kelemahan sistem dalam jaringan, khususnya yang berkaitan dengan keamanan jaringan nirkabel.
Penelitian 5	
Penulis dan tahun	(Pratama & Syamsuar, 2021)
Judul	Analisis Keamanan Jaringan Pada Layanan Internet Publik Menggunakan Metode Penetration Testing Execution Standard (PTES) DPRD Provinsi Sumatra Selatan
Objek	Keamanan Jaringan Pada Layanan Internet Publik Provinsi Sumatra Selatan.

Metode	Penetration Testing Execution Standard (PTES).
Hasil	penelitian ini menunjukkan bahwa DPRD Provinsi Sumatera Selatan merupakan salah satu pusat pemerintahan yang memberikan berbagai pelayanan kepada masyarakat. Setiap karyawan dan anggota staf memiliki akses ke satu jaringan *Wireless Area Network* (WLAN) yang menggunakan satu SSID untuk semua aktivitas berbagi data dalam jaringan. Untuk mengetahui celah keamanan pada jaringan WLAN, penulis melakukan percobaan menggunakan metode Penetration Testing Excuition Standard (PTES) dan empat parameter serangan yaitu *Man-in-the-Middle Attack, ARP Spoofing*, *Bypassing MAC Authentication*, dan *Cracking the* Enkripsi. Periksa pengaturan keamanan jaringan WLAN saat ini. Hasil dari empat parameter penyerangan yang digunakan, tiga di antaranya berhasil diselesaikan.
Penelitian 6	
Penulis dan Tahun	(Ningsih, 2021)
Judul	Analisis Pengujian Kerentanan Situs Pemda XYZ Menggunakan Metode PTES.
Objek	Kerentanan Situs Pemda XYZ Menggunakan Metode PTES.
Metode	Penetration Testing Execution Standard (PTES) .
Hasil	Pada penelitiandi peroleh bahwa pemerintah XYZ telah menggunakan website dan penetration testing adalah metode pengujian kerentanan keamanan yang ada pada sebuah website dan penetration testing pada sebuah website. Pada penelitian ini akan di lakukan *vulnerability assessment* dan

	penetration testing pada situs layanan terpadu pemerintah XYZ menggunakan standar PTES dengan beberapa tools yang di gunakan *Acunetix*, dan Paros Kali Linux. Hasil dari kerentanan yang di peroleh pada website layanan terpadu memiliki jenis kerentanan dan tingkat resiko berbeda-beda sesuai tools yang di gunakan.
Penelitian 7	
Penulis dan Tahun	(Andhika et al., 2022)
Judul	Pengujian Penetrasi Pada Windows 10 Menggunakan Metode Penetration Testing Execuition Standard (PTES).
Objek	Pengujian Penetrasi Pada Windows 10.
Metode	Penetration Testing Execuition Standard (PTES).
Hasil	Penelitian ini menemukan bahwa serangan terhadap keamanan sistem informasi dapat dilihat dari sudut pandang peran komputer atau jaringan komputer sebagai penyedia informasi. Jika seseorang mengambil keuntungan dari kelemahan yang ditemukan demi keuntungannya sendiri dan melemahkan sistem sehingga merugikan lembaga atau perusahaan, maka dampaknya mungkin akan merugikan. Karena masalah yang ada sejak Windows 10 pertama kali diinstal oleh konsumen, ditemukan bahwa Windows 10 mengandung kerentanan yang lebih kritis. Kerentanan ini dapat dieksploitasi karena beberapa layanan tidak dapat diakses oleh publik.

Berdasarkan dari hasil penelitian terkait yang di lakukan pengujian dengan menggunakan metode Penetration Testing Execution Standard (PTES) di peroleh bahwa

pada sistem informasi website atau aplikasi masih memiliki sistem keamanan yang lemah seperti *SQL injection* dan keamanan server. Penelitian terkait menggunakan metode PTES telah dilakukan dalam pengujian keamanan sistem. Dari objek pengujian memiliki perbedaan dari tahapannya hasil dan analisis setiap penelitian tersebut. Analisa dari hasil metode ini akan di gunakan dan di rekomendasikan.

2.2. Kajian Teori

2.2.1. Jaringan Komputer

Jaringan komputer adalah sistem yang menghubungkan beberapa komputer untuk bertukar sumber daya dan data. Kemampuan pengguna dalam berkomunikasi akan difasilitasi oleh komputer dan gadget berjaringan lainnya. Beberapa komputer dan perangkat lainnya dihubungkan melalui media kabel atau nirkabel sehingga membentuk suatu jaringan. Selain menggunakan perangkat keras ini, menyiapkan jaringan komputer biasanya memerlukan instalasi perangkat lunak tertentu. Deteksi perangkat jaringan dilakukan oleh perangkat lunak. Sederhananya, jaringan komputer biasanya terdiri dari komputer host untuk operasi pengguna dan komputer server yang berfungsi sebagai pusat kendali.

2.2.2. Keamanan jaringan Komputer

Keamanan jaringan merupakan salah satu hal penting dalam memonitoring komponen dan mencegah.

a. Confidentiality

Confidentiality yaitu, menuntut hanya pihak yang berwenang yang dapat mengakses informasi atau data.

b. Intergrity

Intergrity yaitu, menuntut pemilik informasi menjadi satu-satunya yang dapat mengubahnya.

c. Availability

Availability yaitu menuntut agar informasi dapat diakses oleh pihak yang berwenang pada waktu yang tepat.

d. Authentication

Authentication yaitu menuntut agar pengirim informasi diidentifikasi secara akurat dan terdapat bukti bahwa identifikasi yang diperoleh adalah asli..

e. Nonrepudiation

Nonrepudiation yaitu menuntut agar informasi dikirim dan diterima tanpa pengirim atau penerima dapat menarik kembali tindakannya.

2.2.3. **Website**

Menurut (Lukmanul hakim, 2004) Halaman web adalah sumber daya online yang menghubungkan dokumen secara lokal dan global. Halaman web dokumen yang ditemukan di situs web. Pengguna dapat berpindah antar halaman (hiperteks) di server yang sama atau di server lain di seluruh dunia dengan menggunakan tautan di situs web. Pengguna yang menggunakan browser seperti *Google Chrome*, *Mozilla Firefox*, dan lainnya dapat melihat dan membaca halaman.

2.2.4. **Webserver**

Mesin yang menyimpan, memproses, dan mengirimkan file halaman web ke browser web disebut server web. Server web terdiri dari perangkat keras dan perangkat lunak yang merespons permintaan dari pengguna web di World Wide Web menggunakan HTTP (Hypertext Transfer Protocol). Halaman yang diminta dimuat dan dikirimkan oleh server web melalui prosedur ini untuk ditampilkan di browser pengguna, seperti *Google Chrome*. Dari segi *hardware*, web server terhubung dengan internet sehingga file atau data dapat dibagikan ke perangkat lain yang terhubung. Apa pun dapat dimasukkan dalam data ini, termasuk foto, lembar gaya CSS, file *JavaScript*, dan file HTML. Perangkat lunak server web, yang mengatur cara pengguna online mengakses file yang disimpan, juga ditempatkan pada perangkat keras ini. Perangkat lunak ini terdiri dari beberapa bagian.

2.2.5. **IP Address (Internet Protocol Address)**

Alamat IP, atau alamat Protokol Internet, adalah pengidentifikasi numerik yang digunakan setiap perangkat komputer yang terhubung ke internet untuk mengidentifikasi dirinya sendiri. Alamat IP sering kali digambarkan sebagai seperangkat pedoman yang mengontrol aktivitas internet dan memfasilitasi penyelesaian tugas online. Alamat IP terdiri dari beberapa digit. Empat adalah ekspresi angka. Ada satu hingga tiga digit di setiap kelompok bilangan bulat. Alamat IP dapat berupa angka antara 0 dan 255. Alamat IP diwakili oleh notasi 192(dot)168(dot)38.1. ID Jaringan dan ID Host adalah dua komponen yang membentuk alamat IP. Bagian alamat IP yang dikenal sebagai ID jaringan menunjukkan lokasi jaringan aktif. Dalam ilustrasi.

2.2.6. **Penetration Testing**

Pengujian penetrasi adalah mengirim atas otoritas yang sah dengan cara mengidentifikasi kerentanan dan memanfaatkannya untuk keuntungan pribadi. Peretasan yang terkontrol dapat digunakan untuk mengetahui tingkat keamanan suatu jaringan. Karena pengujian penetrasi tidak selalu membuktikan adanya kerentanan, pengujian ini cenderung lebih menekankan pada seni daripada ilmu peretasan. Selain itu, pengujian penetrasi yang tidak efektif tidak selalu menjadi penyebab pengujian gagal mengidentifikasi kerentanan.

2.2.7. **Penetration Testing Execuition Standard (PTES)**

Standar Eksekusi Pengujian Penetrasi (PTES) yang baru, yang terdiri dari tujuh komponen utama, diciptakan untuk memberikan perusahaan dan penyedia layanan keamanan kosakata dan ruang lingkup yang konsisten untuk melaksanakan tes penetrasi. menjelaskan tahap awal pengujian penetrasi dan motivasi di baliknya. Hal ini juga mencakup pengumpulan informasi, pemodelan ancaman, dan penelitian kerentanan, eksploitasi, dan pasca-eksploitasi, di mana penguji melakukan pengujian untuk mendapatkan lebih banyak informasi. Terakhir, diakhiri dengan pembuatan laporan yang mendokumentasikan keseluruhan proses.

a. pre-engagement interaction

Pre-engagement interactions bertujuan untuk menyediakan dan menjelaskan sarana atau metode yang di gunakan untuk mendukung dalam Langkah Pre-enggament yang berhasil dari uji penetrasi.

b. Intelligence Gathering

mengumpulkan data untuk tujuan pengujian penetrasi. Informasi umum berikut harus diperoleh: host, alamat IP, dan domain.

c. Threat Modeling

Komponen pemodelan ancaman yang digunakan untuk melakukan pengujian penetrasi.

d. Vulnerability Analysis

pengujian kerentanan melibatkan identifikasi kelemahan dalam sistem dan aplikasi, seperti konfigurasi host dan layanan yang salah atau desain aplikasi yang tidak aman, yang mungkin digunakan penyerang untuk mendapatkan akses ke kerentanan.

e. Exploitation

tujuan dari fase eksploitasi uji penetrasi adalah untuk mendapatkan akses ke sumber daya atau sistem dengan menghindari langkah-langkah keamanan saat ini. Jika fase kerentanan dilaksanakan secara tidak memadai, fase ini perlu dilaksanakan dengan cermat dan dengan perencanaan yang sempurna.

f. Post Exploitation

Menentukan nilai dari sistem yang terekspos dan menjaga kendali sistem agar dapat berfungsi lebih lanjut adalah tujuan dari fase pasca eksploitasi..

g. Reporting

Tahap pelaporan merupakan tahap terakhir dimana masalah penting dari uji penetrasi dicatat dan dilaporkan..

BAB 3

METODOLOGI PENELITIAN

3.1. Subjek dan Objek Penelitian

3.1.1. Subjek Penelitian

Penelitian Ini akan di lakukan pengujian penetrasi testing menggunakan Penetration Testing Execution Standard (PTES) pada website server yang di buat menggunakan virtualbox.

3.1.2. Objek Penelitian

Sistem yang akan diuji pada penelitian ini adalah server pada Universitas Muhammadiyah Kalimantan Timur.

3.2. Metode Penelitian

Penelitian akan dilakukan Penyimpanan data, pengujian penetrasi menggunakan metode PTES serta analisis laporan. Mengenai metode penelitian yang dilakukan dapat dilihat pada gambar di bawah.

Gambar 3. 1 Metode Penelitian

3.2.1. Studi Literatur

Pada tahapan akan di lakukan survey tujuannya Buat menjelaskan tentang teori pendukung yang di gunakan sebagai sebagai bahan penelitian. Literatur ini di peroleh dari buku, artikel penelitian dari internet.

3.2.2. Pengumpulan Data

Pada tahapan akan di lakukan pengumpulan data dengan cara mengumpulkan data target yang akan di uji dengan menggunakan alat yang sudah di tentukan. Pengumpulan data

di lakukan dengan cara mengidentifikasi web server Universitas Muhammadiyah Kalimantan Timur (UMKT).

3.2.3. Analisis Kebutuhan

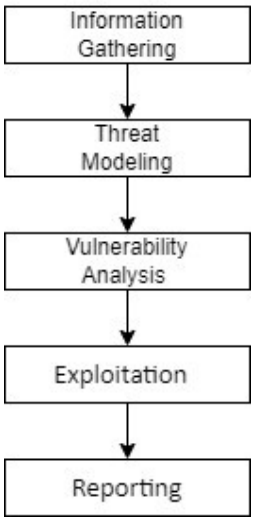
Analisis kebutuhan perangkat untuk melakukan uji penetrasi dan dilihat pada tabel 3.1

Tabel 3. 1 Analisis kebutuhan

No	Perangkat	Spesifikasi
1	Laptop	AMD ryzen 5 355H up to 3.7 Ghz Memory 8GB DDR4
2	Sistem Operasi	Windows 10 dan Linux
3	Vulnerebility Tools	Nessus Vulnerability Scanner, NMAP dan Wireshark.
4	Penetration Tools	PTES

3.2.4. Tahap pengujian

Pengujian akan di lakukan dengan menggunakan Metode PTES tahap pengujian dapat dilihat pada gambar di bawah.



Gambar 3. 2 Tahap Pengujian

Intelligence Gathering: Pada tahap ini, peneliti mengumpulkan data berupa alamat IP, server, jenis domain, dan detail lainnya dari situs web. yang berguna untuk pengujian penetrasi.

Thread Modeling: pada tahap ini peneliti menentukan model ancam yang harus diidentifikasi pada website yang akan di uji penetrasi.

Vulnerability Analysis: pada tahapan ini akan di lakukan proses scanning ini bertujuan untuk menemukan mencari port atau celah keamanan yang ada pada website.

Exploitation: pada tahapan melakukan serangan pada website adapun tool yang digunakan merupakan aplikasi scanner otomatis untuk mengeksplorasi kerentanan yang dapat di gali pada website.

Reporting:pada tahapan ini mendeskripsikan hasil dari uji pengujian penetrasi.

3.2.5. Alur Pengujian

Pada awal pengujian di lakukan mengidentifikasikan kerentanan dengan menggunakan tooll rapid scan lalu akan di lakukan penetrasi testing dan fase terakhir akan di buat laporan tertulis.

3.2.6. Analisis dan laporan

Pada Tahap ini di lakukan analisi dan laporan dari uji penetrasi denganmenggunakan metode PTES. Analisis dan laporan di sajikan dalam bentuk saran atau rekomendasi pada server.

3.3. Jadwal Penelitian

Tabel 3. 2 Jadwal Penelitian

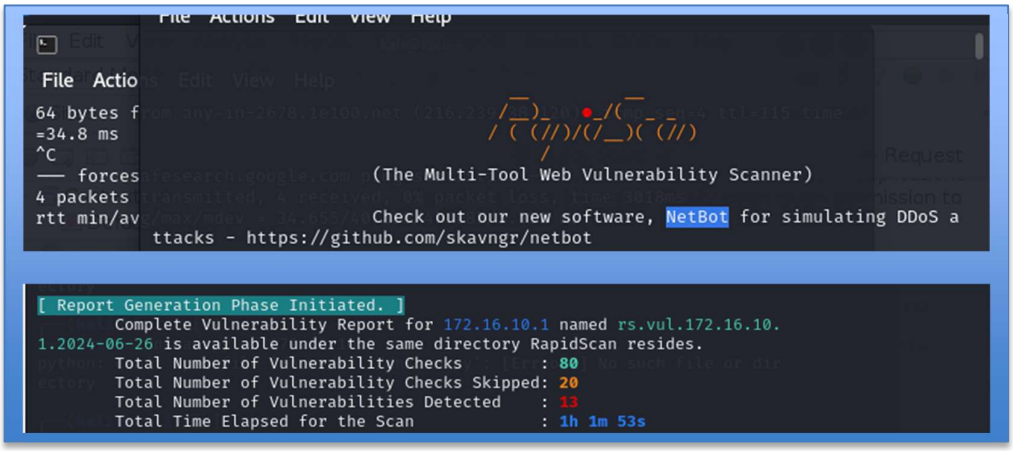
No	Kegiatan		April				Mei				Juni				Juli			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Penulisan Proposal																	
2.	Pengumpulan Data																	
3.	Pengujian Sistem																	
4.	Evaluasi																	
5.	Penulisan Laporan																	

BAB 4

HASIL DAN PEMBAHASAN

4.1. Identifikasi Kerentanan

Teknik pemindaian cepat digunakan dalam penelitian ini untuk menilai tingkat kerentanan pada server web dengan domain server 172.16.10.1. Hasil dari pemindaian cepat adalah sebagai berikut:



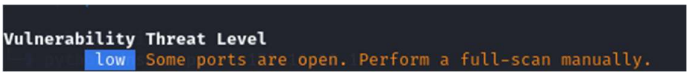
Gambar 4. 1 Identifikasi Kerentanan

Dari hasil scaning pada domain server 172.16.10.1 dengan menggunakan tools rapid scan terdapat 80 pemeriksaan kerentanan di mna kerentanan dilewati sebanyak 20 dan kerentanan terdeteksi 13 dapat lihat pada tabel 4.1.1

Tabel 4. 1 Hasil Identifikasi Kerentanan

NO	Nama	Jumlah Kerentanan
1	*Vulnerability check*	80
2	*Vulnerability check skipped*	20
3	*Vulnerability detected*	13

4.1.1. **Vulnerability Threat Level**



Gambar 4. 2 Vulnerability Threat Level

Vulnerability Threat Level pada Kali Linux merujuk pada tingkat keparahan dan potensi bahaya dari sebuah kerentanan (vulnerability) yang ada dalam sistem atau perangkat lunak tertentu. Kali Linux, sebagai distribusi Linux yang terkenal dalam bidang pengujian penetrasi dan keamanan informasi, memiliki pendekatan untuk mengklasifikasikan tingkat keparahan kerentanan berdasarkan pada sejumlah faktor.

Critical (Kritis): Kerentanan ini memiliki potensi yang sangat tinggi untuk dieksploitasi dan dapat menyebabkan kerusakan yang serius pada sistem atau data. Contohnya adalah kerentanan yang memungkinkan penyerang untuk mendapatkan akses penuh ke sistem tanpa otorisasi.

High (Tinggi): Kerentanan ini memiliki potensi tinggi untuk dieksploitasi, meskipun tidak seberat kerentanan kritis. Contohnya adalah kerentanan yang memungkinkan untuk menjalankan kode berbahaya atau memperoleh akses yang lebih tinggi dari yang seharusnya.

Medium (Sedang): Kerentanan ini memiliki potensi yang signifikan untuk dimanfaatkan oleh penyerang, tetapi sering kali memerlukan kondisi tertentu atau serangan yang lebih rumit untuk dieksploitasi.

Low (Rendah): Kerentanan ini memiliki dampak yang relatif kecil atau hanya mempengaruhi fungsi-fungsi yang terbatas. Contohnya mungkin adalah kerentanan yang memungkinkan pengungkapan informasi sensitif, tetapi tidak langsung mengancam integritas sistem secara keseluruhan.

Info (Informasi): Informasi ini biasanya bukan sebuah kerentanan yang bisa dieksploitasi secara langsung, tetapi memberikan informasi penting kepada peneliti keamanan tentang konfigurasi atau keadaan sistem.

4.1.2. **Vulnerability definition**

Gambar 4. 3 Vulnerability Definition

"vulnerability" (kerentanan) mengacu pada kelemahan atau celah dalam suatu sistem, perangkat lunak, atau jaringan dieksploitasi untuk mendapatkan kesempatan,menyebabkan kerusakan, dapat mengganggu operasi normal dari sistem tersebut. Secara lebih teknis, vulnerability dapat diartikan sebagai kondisi di mana ada celah atau kelemahan dalam desain, implementasi, operasi, atau pengaturan sistem yang memungkinkan penyerang untuk mengeksploitasi sistem tersebut.

Dalam konteks Kali Linux, distribusi ini dikenal sebagai alat utama untuk pengujian penetrasi (penetration testing) dan pengujian keamanan. Oleh karena itu, pengertian vulnerability dalam konteks Kali Linux:

Identifikasi Kerentanan: Proses mencari, mengidentifikasi, dan mengevaluasi kerentanan dalam sistem atau perangkat lunak yang sedang diuji. Alat-alat di Kali Linux seperti scanner kerentanan (vulnerability scanners) membantu dalam menemukan celah-celah keamanan yang ada.

Eksploitasi: Setelah kerentanan teridentifikasi, peneliti keamanan atau praktisi pengujian penetrasi dapat menggunakan Kali Linux untuk mencoba mengeksploitasi kerentanan tersebut. Ini membantu untuk memahami potensi serangan yang dapat dilakukan oleh penyerang dan mengambil tindakan pencegahan yang sesuai.

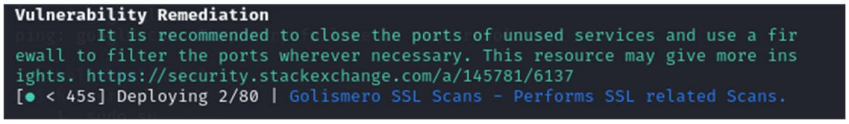
Pemetaan Risiko: Setelah identifikasi dan eksploitasi, Kali Linux dapat digunakan untuk memetakan risiko dari kerentanan yang ditemukan. Ini termasuk menilai potensi dampak, keparahan, dan kemungkinan eksploitasi oleh penyerang.

Pengujian Keamanan: Kali Linux digunakan secara luas untuk melakukan pengujian keamanan secara menyeluruh terhadap sistem dan perangkat lunak guna memastikan bahwa

mereka memiliki lapisan keamanan yang memadai dan mampu menanggulangi potensi serangan.

Dengan demikian, vulnerability definition pada Kali Linux tidak hanya mencakup identifikasi kelemahan, tetapi juga proses eksploitasi dan pengujian keamanan yang komprehensif. Hal ini penting untuk membantu meningkatkan keamanan sistem, mencegah insiden keamanan, dan menjaga integritas data.

4.1.3. **Vulnerability Remediation**



Gambar 4. 4 Vulnerability Remediation

Vulnerability remediation pada Kali Linux mengacu pada proses memperbaiki atau mengurangi risiko yang disebabkan oleh kerentanan yang ditemukan dalam sistem atau perangkat lunak. Ini adalah langkah-langkah yang diambil setelah kerentanan diidentifikasi melalui pengujian penetrasi atau penilaian keamanan menggunakan Kali Linux atau alat-alat lainnya. Berikut adalah beberapa tahapan utama dalam vulnerability remediation:

Pemahaman Kerentanan: Langkah pertama adalah memahami dengan jelas tentang kerentanan apa yang telah ditemukan. Ini meliputi pemahaman mendalam tentang bagaimana kerentanan dapat dieksploitasi, potensi dampaknya terhadap sistem atau data, dan kondisi yang diperlukan untuk mengeksploitasi kerentanan tersebut.

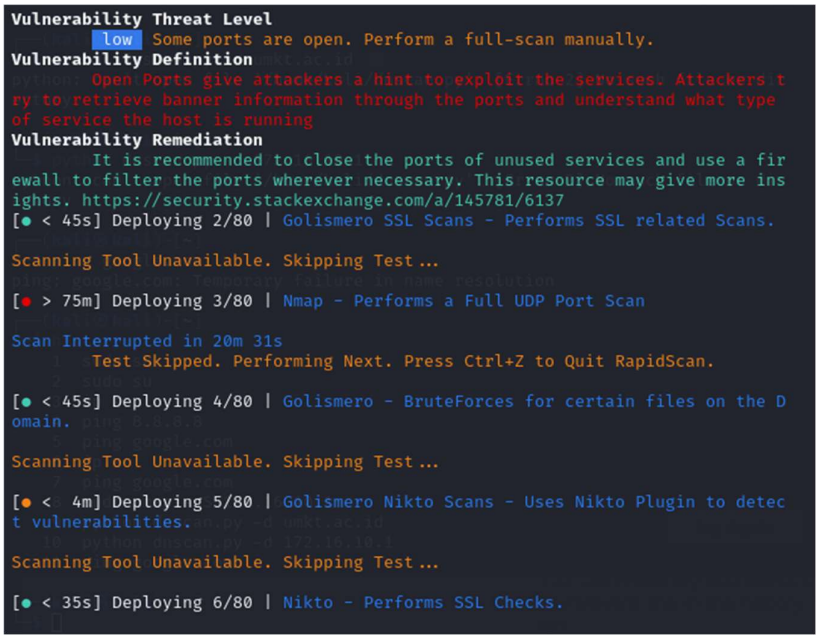
Penilaian Risiko: Setelah pemahaman awal tentang kerentanan, langkah berikutnya adalah menilai risiko yang terkait. Ini melibatkan penilaian tentang seberapa serius kerentanan tersebut dapat dieksploitasi, potensi dampaknya terhadap operasi bisnis atau layanan yang disediakan oleh sistem, dan seberapa mudah atau sulit untuk mengeksploitasi kerentanan tersebut.

Verifikasi: Setelah perbaikan atau mitigasi diterapkan, penting untuk memverifikasi efektivitasnya. Ini melibatkan pengujian ulang menggunakan alat-alat Kali Linux atau skenario

simulasi serangan untuk memastikan bahwa kerentanan telah ditangani dengan efektif dan tidak ada celah keamanan yang tersisa.

Monitoring dan Pemeliharaan: Kerentanan dan ancaman keamanan untuk melakukan pemantauan terus-menerus terhadap sistem dari perangkat lunak, serta menjaga keamanan dengan memperbarui patch dan konfigurasi keamanan secara berkala.

4.1.4. **Port Manual**



Gambar 4. 5 Port Manual

Membuka port secara manual pada proses masuk ke suatu port tertentu pada sebuah perangkat atau server. Ini penting untuk aplikasi atau layanan tertentu yang perlu diakses.

Identifikasi Port yang dibuka: port 10 untuk HTTP, port 172 untuk HTTPS, atau port tertentu dibutuhkan oleh aplikasi atau layanan khusus.

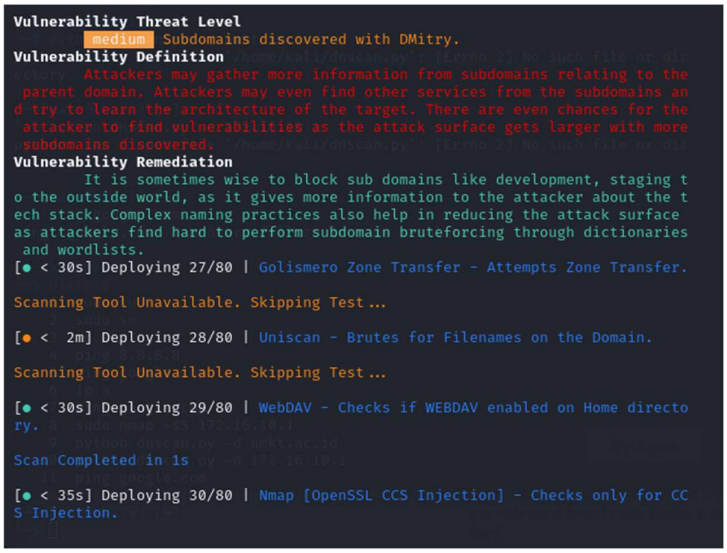
Akses Konfigurasi Firewall: Jika menggunakan firewall di Linux atau Windows Firewall di Windows, akses konfigurasi firewall. Ini biasanya dapat dilakukan melalui terminal atau command promp.

Menyimpan dan Mengaktifkan Perubahan: Setelah aturan firewall ditambahkan, pastikan untuk menyimpan konfigurasi (tergantung pada sistem operasi dan alat manajemen firewall yang Anda gunakan).

Verifikasi Koneksi: Setelah port dibuka, koneksi dari luar jaringan untuk memastikan bahwa port telah terbuka dan dapat diakses.

Pemantauan dan Keamanan: Setelah membuka port, penting untuk memantau yang masuk ke port tersebut dan memastikan bahwa hanya yang diizinkan yang diterima. Pastikan juga untuk mempertimbangkan keamanan dengan menggunakan enkripsi jika diperlukan, atau mengatur akses berdasarkan alamat IP.

4.1.5. **Subdomain**



Gambar 4. 6 Subdomain

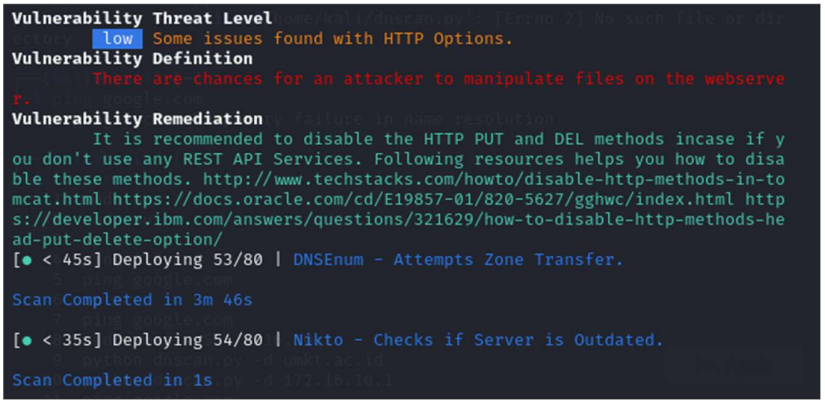
Subdomain pada dasarnya adalah bagian dari domain yang berada di bawah domain utama. Dalam konteks Kali Linux, subdomain dapat berarti beberapa hal tergantung pada konteksnya:

Eksploitasi dan Pemantauan: Setelah subdomain ditemukan, peneliti keamanan dapat menggunakan informasi ini untuk mengidentifikasi dan mengeksploitasi potensi celah

keamanan. Misalnya, subdomain yang tidak terlindungi dengan baik atau tidak diperbarui dapat menjadi titik masuk untuk serangan.

Pengujian Web dan Aplikasi: Subdomain juga sering kali digunakan untuk mengarahkan ke aplikasi atau layanan khusus dalam pengujian web. Dalam pengujian penetrasi web, Kali Linux dapat digunakan untuk melakukan serangan terhadap subdomain yang mungkin memiliki kelemahan keamanan.

4.1.6. **HTTP(Hypertext Transfer Protocol)**



Gambar 4. 7 HTTP(Hypertext Transfer Protocol)

Pada Kali Linux, HTTP (Hypertext Transfer Protocol) digunakan secara luas dalam berbagai konteks, terutama dalam keamanan siber dan pengujian penetrasi. Berikut adalah beberapa aspek penting tentang HTTP dalam konteks Kali Linux:

Penggunaan HTTP di Kali Linux: Pengujian Penetrasi Web: Kali Linux dilengkapi dengan banyak alat untuk pengujian keamanan web yang berhubungan dengan HTTP, seperti Burp Suite, OWASP ZAP, Nikto, dan lainnya.

Eksploitasi dan Pemindaian: Alat-alat seperti Metasploit Framework menggunakan HTTP untuk melakukan eksploitasi dan pemindaian terhadap target.

Analisis Lalu Lintas HTTP: Kali Linux memiliki alat seperti Wireshark dan tcpdump yang dapat digunakan untuk menganalisis HTTP.

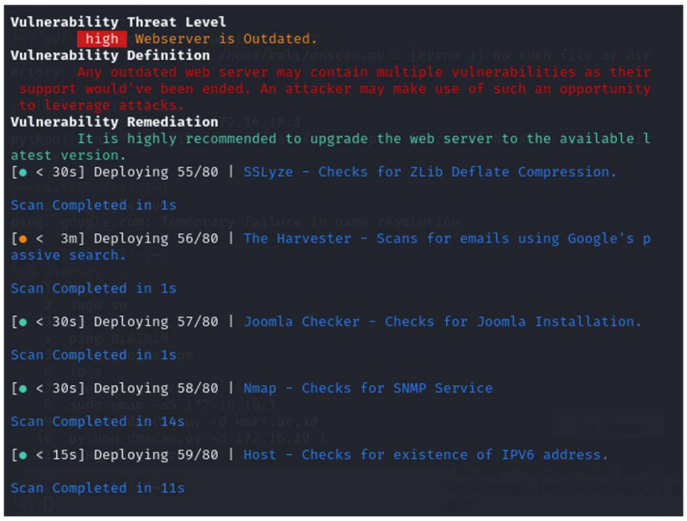
Alat-Alat HTTP di Kali Linux: Burp Suite: Sebuah platform untuk melakukan pengujian keamanan aplikasi web. Ini memungkinkan pengguna untuk menganalisis, memodifikasi, dan mengulang permintaan HTTP.

OWASP ZAP (Zed Attack Proxy): Alat untuk menemukan kerentanan dalam aplikasi web. Ini menyediakan fitur untuk menganalisis dan mengintersepsi lalu lintas HTTP.

Nikto: Scanner server web yang memeriksa server HTTP untuk menemukan berbagai jenis masalah keamanan.

Metasploit Framework: Platform untuk pengembangan dan pelaksanaan exploit. Ini sering digunakan untuk menguji kerentanan yang terkait dengan layanan HTTP.

4.1.7. **Webserver**



Gambar 4. 8 Webserver

Perangkat lunak server web bertugas merespons permintaan HTTP dengan tepat dari klien (seperti browser web), biasanya dalam bentuk halaman web atau data lainnya. Sehubungan dengan Kali Linux, web server sering digunakan untuk berbagai tujuan, termasuk pengujian penetrasi, pengembangan aplikasi web, dan simulasi serangan. Pengujian Penetrasi: Pengujian kerentanan aplikasi web dengan menggunakan server web sebagai target uji. Pengembangan dan Simulasi: Mengembangkan dan menguji aplikasi web lokal sebelum di-deploy ke lingkungan produksi. Simulasi Serangan: Menjalankan server web untuk mensimulasikan skenario serangan terhadap aplikasi web.

4.1.8. **Ipv6(Internet Protocol version)**

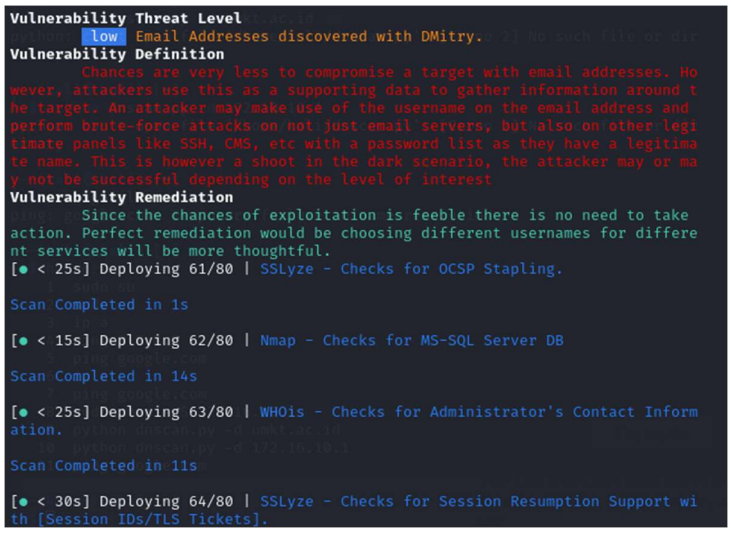
Gambar 4. 9 Ipv6 (Internet Protocol Version)

(Protokol Internet versi 6), iterasi terbaru dari protokol yang dimaksudkan untuk menggantikan IPv4.

Alamat 32-bit digunakan dalam IPv4, sehingga menghasilkan sekitar 4,3 miliar alamat berbeda. Ketika jumlah perangkat yang terhubung ke Internet meningkat, alamat IPv4 semakin sulit didapat. Karena alamat 128-bit digunakan dengan IPv6, ada sekitar 340 undecillion (3,4 x 10^38) alamat unik yang mungkin. memadai untuk kebutuhan sekarang dan masa depan.

IPv6 solusi untuk keterbatasan alamat IPv4, menawarkan ruang alamat yang lebih besar dan fitur-fitur tambahan untuk meningkatkan efisiensi dan keamanan jaringan. Dengan adopsi yang terus meningkat, IPv6 menjadi penting bagi infrastruktur Internet masa depan.

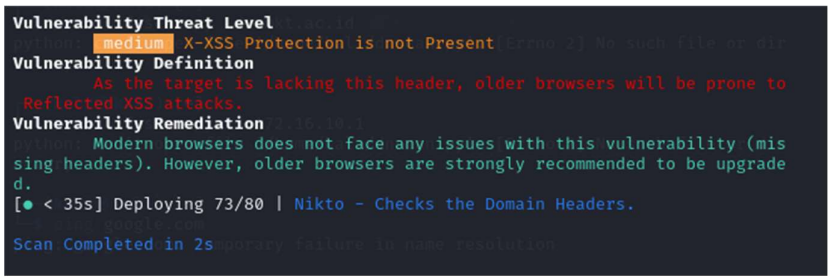
4.1.9. **Email Adress**



Gambar 4. 10 Email Adress

Alamat email (email address) digunakan dalam berbagai konteks, terutama dalam keamanan siber, Di Kali Linux, alamat email digunakan dalam berbagai alat dan konteks untuk tujuan pengujian penetrasi, analisis keamanan, dan administrasi jaringan. Dengan memanfaatkan alat-alat yang tersedia di kali linux, para profesional keamanan dapat menguji dan meningkatkan keamanan email.

4.1.10. **X-Xss Protection**

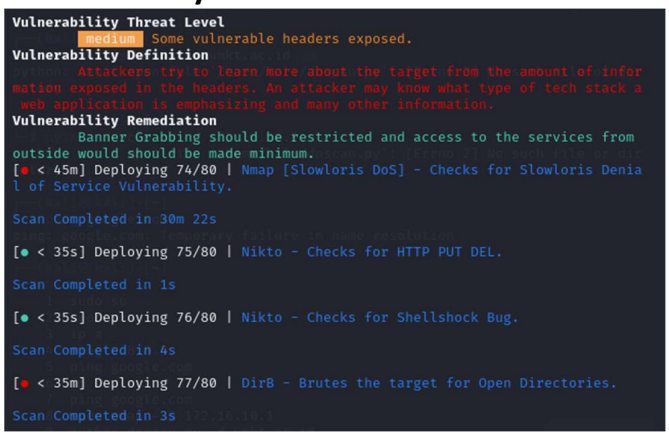


Gambar 4. 11 X-Xss Protection

Dalam konteks keamanan siber, "vulnerable headers" mengacu pada header HTTP yang tidak dikonfigurasi dengan benar atau hilang, yang dapat membuat aplikasi web rentan terhadap berbagai jenis serangan. Di Kali Linux, pengujian header ini merupakan bagian penting dari penilaian keamanan aplikasi web.

Header HTTP komponen dari permintaan dan respons HTTP yang menyediakan informasi tambahan tentang permintaan atau respons tersebut. Header ini dapat digunakan untuk mengontrol perilaku browser dan server.

4.1.11. **Vulnerability Headrs**

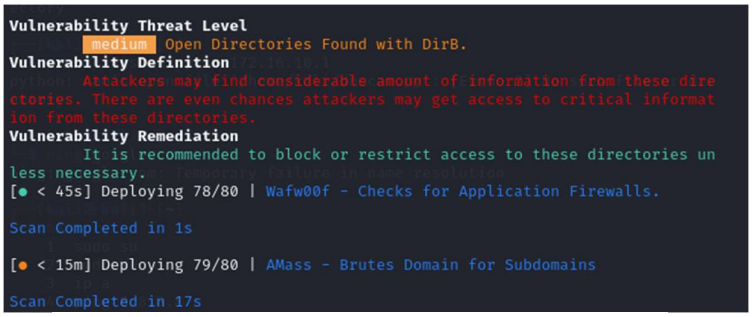


Gambar 4. 12 Vulnerability Headres

Dalam konteks keamanan siber, "vulnerable headers" mengacu pada header HTTP yang tidak dikonfigurasi dengan benar atau hilang, yang dapat membuat aplikasi web rentan terhadap berbagai jenis serangan. Di Kali Linux, pengujian header ini merupakan bagian penting dari penilaian keamanan aplikasi web.

Header HTTP komponen dari permintaan dan respons HTTP yang menyediakan informasi tambahan tentang permintaan atau respons tersebut. Header ini dapat digunakan untuk mengontrol perilaku browser dan server.

4.1.12. **Directories**



Gambar 4. 13 Directories

Direktori struktur fundamental dalam sistem file Linux yang digunakan untuk mengatur dan menyimpan file. Di Kali Linux, seperti di distribusi Linux lainnya, memahami direktori dan hierarki sistem file sangat penting untuk navigasi, manajemen file, dan administrasi sistem.

Direktori Utama pada kali Linux

a. / (Root)

Deskripsi: Direktori root adalah dasar dari hierarki sistem file. Semua file dan direktori lain berada di bawah direktori root.

Penggunaan: Hanya pengguna root yang memiliki izin penuh di direktori ini.

b. /bin

Deskripsi: Berisi program biner penting yang digunakan oleh semua pengguna.

Contoh Isi: Perintah dasar seperti ls, cp, mv, rm.

c. /sbin

Deskripsi: Berisi program biner penting yang biasanya digunakan oleh administrator sistem.

Contoh Isi: Perintah administrasi seperti ifconfig, reboot, shutdown.

d. /etc

Deskripsi: Berisi file konfigurasi sistem.

Contoh Isi: File konfigurasi jaringan (/etc/network), file konfigurasi layanan (/etc/apache2).

e. /home

Deskripsi: Berisi direktori home untuk setiap pengguna.

Contoh Isi: Direktori home untuk pengguna user1 berada di /home/user1.

f. /root

Deskripsi: Direktori home untuk pengguna root.

Penggunaan: Digunakan untuk file pribadi dan konfigurasi root.

g. /var

Deskripsi: Berisi file yang berubah-ubah seperti log, antrian cetak, dan file temporer.

Contoh Isi: Log sistem (/var/log), file email (/var/mail), spool cetak (/var/spool).

h. /tmp

Deskripsi: Berisi file temporer yang dapat dihapus setelah reboot.

Penggunaan: Tempat penyimpanan sementara untuk aplikasi.

i. /usr

Deskripsi: Berisi program dan file yang digunakan oleh pengguna.

Contoh Isi: Program biner (/usr/bin), library (/usr/lib), dokumentasi (/usr/share/doc).

j. /lib

Deskripsi: Berisi library penting yang dibutuhkan oleh program di /bin dan /sbin.

Contoh Isi: Library bersama (/lib/libc.so.6).

k. /opt

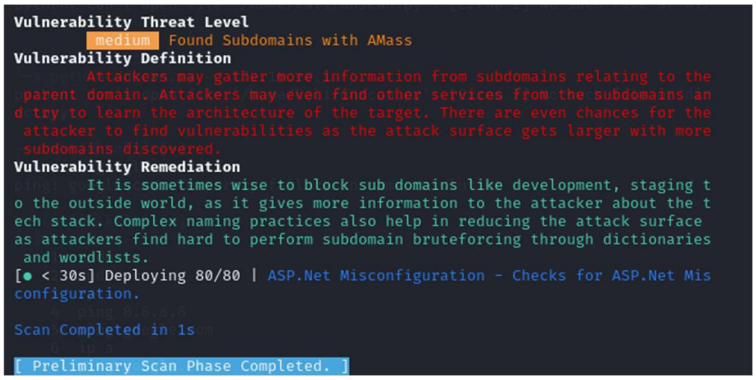
: Berisi paket perangkat lunak tambahan.

Penggunaan: Digunakan untuk aplikasi yang diinstal secara manual.

l. /mnt dan /media

Deskripsi: Berisi titik kait (mount points) untuk sistem file yang di-mount secara sementara, seperti drive USB dan CD-ROM.

4.1.13. **Subdomain With Amas**



Gambar 4. 14 Subdomain With Amas

Amass open-source yang digunakan untuk melakukan pengintaian dan pemetaan subdomain secara pasif dan aktif. Ini sangat berguna bagi profesional keamanan siber dan penguji penetrasi untuk menemukan subdomain tersembunyi yang mungkin tidak diketahui atau tidak dipublikasikan. Berikut adalah penjelasan tentang subdomain dan bagaimana menggunakan AMass untuk melakukan pengintaian subdomain di Kali Linux.

4.2. Tools Yang Di Gunakan Dalam Uji Penetrasi

4.2.1. Rapid Scan

Rapid Scan alat open-source yang tersedia di Kali Linux untuk melakukan pemindaian cepat terhadap situs web guna menemukan berbagai jenis kerentanan. Berikut adalah beberapa fungsi utama dari Rapid Scan Banyak kerentanan, termasuk *SQL Injection*, *Cross-Site Scripting* (XSS), dan kerentanan penyertaan file, dapat ditemukan di aplikasi web populer dengan Rapid Scan.Rapid Scan mengintegrasikan hasil dari berbagai alat keamanan lainnya, sehingga memberikan laporan yang lebih lengkap dan terperinci. Selain memeriksa aplikasi

web, Rapid Scan juga memeriksa konfigurasi server web untuk menemukan kelemahan yang dapat dieksploitasi. Rapid Scan menghasilkan laporan yang dapat disesuaikan berdasarkan kebutuhan pengguna, memungkinkan untuk fokus pada jenis kerentanan tertentu atau bagian spesifik dari aplikasi web.

Rapid Scan dirancang untuk melakukan pemindaian dengan cepat, memungkinkan pengguna untuk dengan cepat mendapatkan wawasan awal tentang status keamanan situs web.Rapid Scan juga memeriksa pengaturan SSL/TLS pada server web untuk memastikan bahwa tidak ada kelemahan dalam implementasi protokol keamanan ini. Rapid Scan dapat dijalankan secara periodik untuk melakukan pemindaian berkala terhadap situs web, memastikan bahwa situs tersebut tetap aman dari kerentanan baru. Rapid Scan sangat berguna bagi profesional keamanan dan administrator jaringan untuk melakukan pemindaian cepat dan efektif terhadap situs web guna mengidentifikasi dan memperbaiki kerentanan.

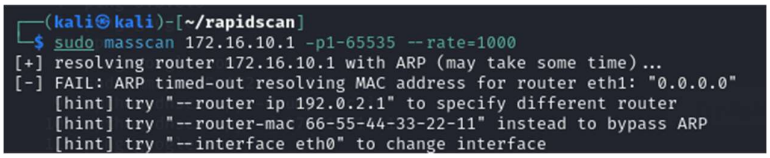
4.2.2. Tahapan yang di gunakan

1. Nmap: Di gunakan Untuk Pemindaian Port:

Gambar 4. 15 Nmap

- -T4 berfungsi untuk meningkatkan kecepatan pemindaian
- -F Fast scan, hanya memindai port yang paling umum di gunakan

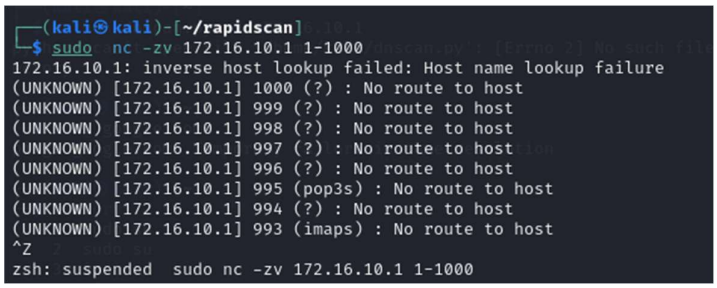
2. Mascan: pemindaian port yang sangat cepat.



Gambar 4. 16 Mascan

- -p1 -65535 berfungsi untuk memindai semua port
- --rate=1000 berfungsi untuk mengatur kecepatan pemindaian (paket perdetik

3. Netcat: Pemindaian Port Sederhana



Gambar 4. 17 Net Cat

- -z berfungsi untuk mode pemindaian , tidak mengirimkan data.
- -v berfungsi untuk mode verbose, memberikan output yang lebih detail.
- 1.1000 berfungsi untuk rentang port yang akan di pindai.

BAB 5

PENUTUP

5.1. Kesimpulan

Dari hasil pengujian menggunakan rapidsacan mendapatkan bahwa hasil scaning server yang berdomain 172.16.10.1 terdapat 13 kerentanan yaitu,*Vulnerability Threat Level*, *Vulnerabilty Definition*, *Vulnerabilty Remediation, Port Manual, Subdomain*, *HTTP (Hypertext Transfer Protocol*), *Webserver*, *Ipv6(Internet Protocol Version 6*), *Email Adress*, *X-Xss Protection*, *Vulnerabilty Headrs,Directories*,*Subdomain With Amas*.

5.2. Saran

Penelitian menyarankan bahwa untuk menentukan kerentanan spesifik pada server web, penelitian lebih lanjut harus dilakukan dengan menggunakan metode Penetration Testing Excution Standard (PTES), seperti yang ditunjukkan oleh kesimpulan di atas.

Daftar Pustaka

Adrian, A., & Setiyadi, A. (2018). Analisis Keamanan Jaringan Dengan Metode Penetration Testing Execution Standard (Ptes) Di Dinas Kesehatan Provinsi Jawa Barat. *Jurnal Unikom Repisitory*, *1*, 1–8.

Ahmia, M., & Belbachir, H. (2018). p, q-Analogue of a linear transformation preserving log-convexity. *Indian Journal of Pure and Applied Mathematics*, *49*(3), 549–557. https://doi.org/10.1007/s13226-018-0284-5

Andhika, D. A., Slamet, & Ningsih, N. (2022). Pengujian Penetrasi pada Windows 10 menggunakan Model Penetration Testing Execution Standard (PTES). *Journal of Technology and Informatics (JoTI)*, *3*(2), 55–61. https://doi.org/10.37802/joti.v3i2.222

Fauzan, F. Y., & Syukhri, S. (2021). Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang. *Voteteknika (Vocational Teknik Elektronika Dan Informatika)*, *9*(2), 105. https://doi.org/10.24036/voteteknika.v9i2.111778

Kiswanto, R. H., & Thamrin, R. M. H. (n.d.). *Edukasi dan Sosialisasi CyberCrime Terhadap Keamanan Data Bagi Kalangan Guru Tingkat Sekolah Menengah Pertama di Kota Jayapura*. 79–84.

Mulyanto, Y., Taufan Asri Zaen, M., & Sihab, S. (2022). Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest). *Journal of Information System Research*, *4*(1), 202–209. https://doi.org/10.47065/josh.v4i1.2335

Ningsih, S. W. (2021). Analisis Pengujian Kerentanan Situs Pemerintahan XYZ dengan PTES. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *8*(3), 1543–1556. https://doi.org/10.35957/jatisi.v8i3.1224

Pratama, A., & Syamsuar, D. (2021). Analisis Keamanan Jaringan Pada Layanan Internet Publik Menggunakan Metode Penetration Testing Execution Standard (Ptes) …. *Bina Darma Conference on …*, 441–446. https://conference.binadarma.ac.id/index.php/BDCCS/article/view/2110

Suradji, E. L. D., & Chandra, D. W. (2014). *Penetration Testing Sistem Jaringan Komputer Untuk Mengetahui Kerentanan Keamanan Server Dengan Menggunakan Metode Penetration Testing*

Execution Standart (PTES) studi kasus Rumah Sakit Santa Clara Madiun.

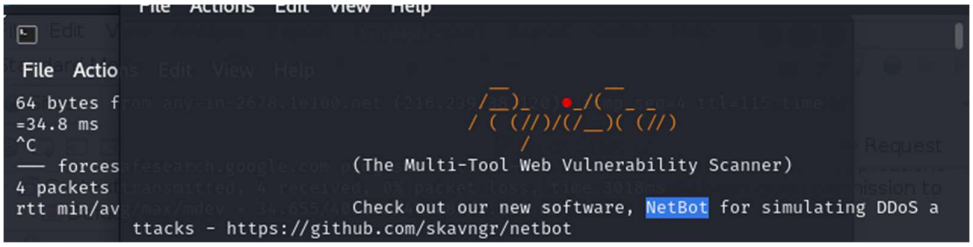
Utoro, S., Nugroho, B. A., Meinawati, M., & Widianto, S. R. (2020). Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard. *Multinetics*, *6*(2), 169–178. https://doi.org/10.32722/multinetics.v6i2.3432

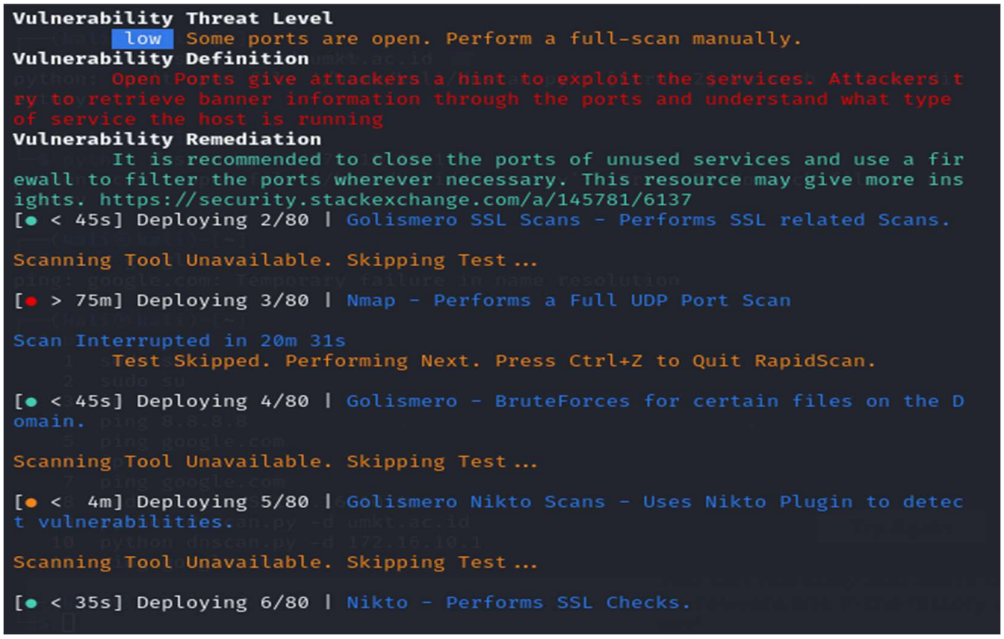
Lampiran

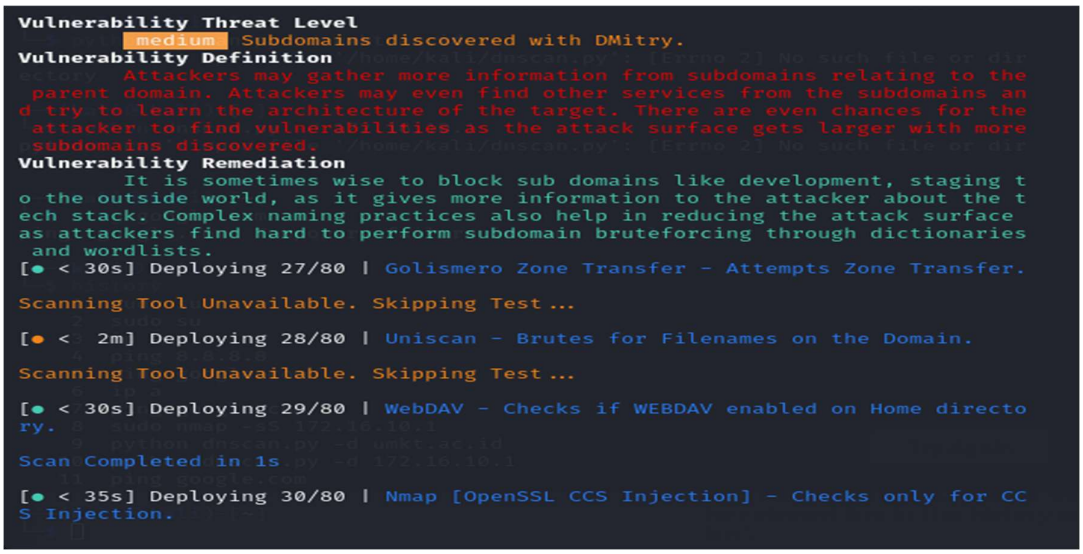
Lampiran 1 Riwayat Hidup

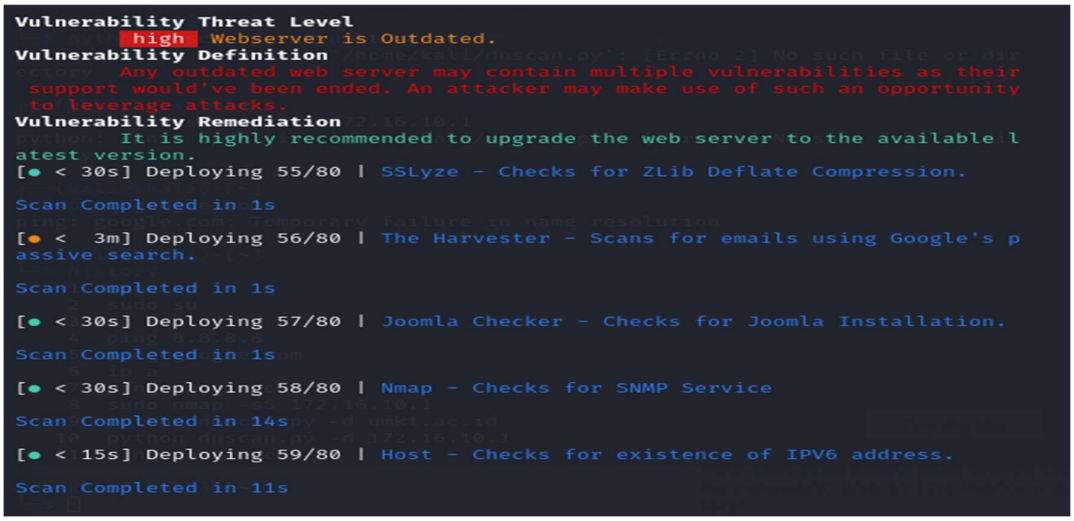
Fitria Nur Yaqin, lahir di Samarinda 13 Desember 2001. Penulis lahir dari Ibu Suparti dan Bapak Normani yang merupakan anak ketiga dari tiga bersaudara. Pada tahun 2007 penulis masuk Sekolah Dasar Negeri 012 Sungai Kunjang dan lulus pada tahun 2013. Pada tahun yang sama melanjutkan Pendidikan di SMPN 25 Samarinda dan lulus pada tahun 2016. Kemudian pada tahun 2016 melanjutkan pendidikan di SMK Negeri 2 Samarinda Jurusan Teknik Listrik dan lulus pada tahun 2019. Pada tahun 2019 Penulis melanjutkan pendidikan perguruan tinggi di Universitas Muhammadiyah Kalimantan Timur dengan melalui jalur mandiri dan di terima pada Program Studi S1 Teknik Informatika.

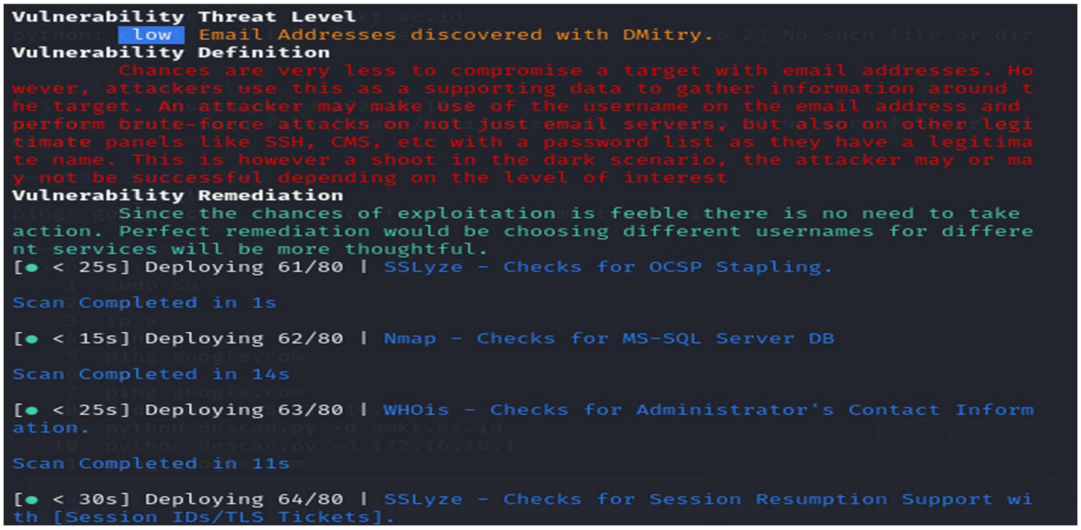
***Lampiran 2 Hasil* Scaning**

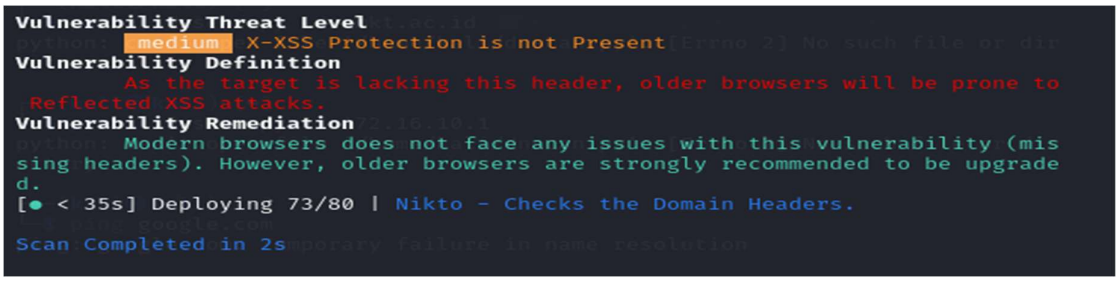


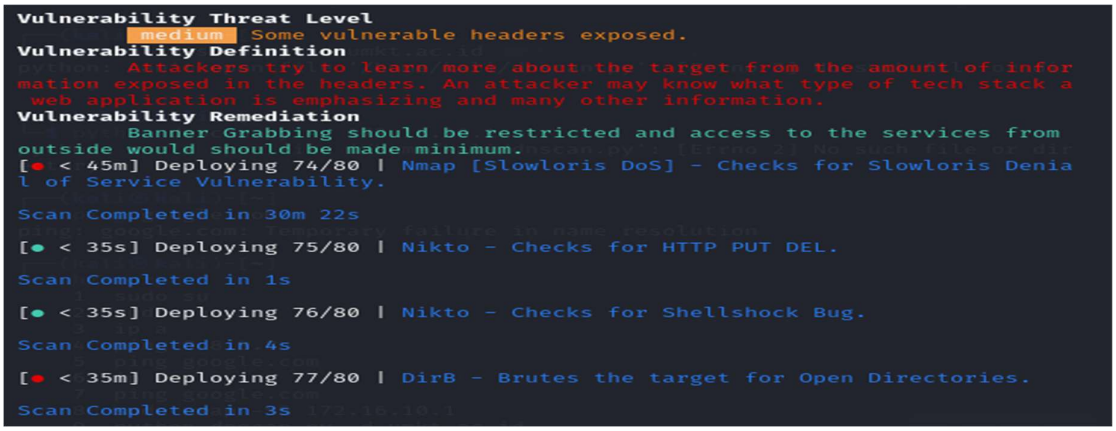



Vulnerability Threat Level
medium Subdomains discovered with DMitry.
Vulnerability Definition
Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances for the attacker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.
Vulnerability Remediation
It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
[● < 30s] Deploying 27/80 | Golismero Zone Transfer - Attempts Zone Transfer.
Scanning Tool Unavailable. Skipping Test ...
[● < 2m] Deploying 28/80 | Uniscan - Brutes for Filenames on the Domain.
Scanning Tool Unavailable. Skipping Test ...
[● < 30s] Deploying 29/80 | WebDAV - Checks if WEBDAV enabled on Home directory.
Scan Completed in 1s
[● < 35s] Deploying 30/80 | Nmap [OpenSSL CCS Injection] - Checks only for CCS Injection.


Vulnerability Threat Level
high Webserver is Outdated.
Vulnerability Definition
Any outdated web server may contain multiple vulnerabilities as their support would've been ended. An attacker may make use of such an opportunity to leverage attacks.
Vulnerability Remediation
It is highly recommended to upgrade the web server to the available latest version.
[● < 30s] Deploying 55/80 | SSLyze - Checks for ZLib Deflate Compression.
Scan Completed in 1s
[● < 3m] Deploying 56/80 | The Harvester - Scans for emails using Google's passive search.
Scan Completed in 1s
[● < 30s] Deploying 57/80 | Joomla Checker - Checks for Joomla Installation.
Scan Completed in 1s
[● < 30s] Deploying 58/80 | Nmap - Checks for SNMP Service
Scan Completed in 14s
[● < 15s] Deploying 59/80 | Host - Checks for existence of IPV6 address.
Scan Completed in 11s


Vulnerability Threat Level
low Email Addresses discovered with DMitry.
Vulnerability Definition
Chances are very less to compromise a target with email addresses. However, attackers use this as a supporting data to gather information around the target. An attacker may make use of the username on the email address and perform brute-force attacks on not just email servers, but also on other legitimate panels like SSH, CMS, etc with a password list as they have a legitimate name. This is however a shoot in the dark scenario, the attacker may or may not be successful depending on the level of interest
Vulnerability Remediation
Since the chances of exploitation is feeble there is no need to take action. Perfect remediation would be choosing different usernames for different services will be more thoughtful.
[● < 25s] Deploying 61/80 | SSLyze - Checks for OCSP Stapling.
Scan Completed in 1s
[● < 15s] Deploying 62/80 | Nmap - Checks for MS-SQL Server DB
Scan Completed in 14s
[● < 25s] Deploying 63/80 | WHOis - Checks for Administrator's Contact Information.
Scan Completed in 11s
[● < 30s] Deploying 64/80 | SSLyze - Checks for Session Resumption Support with [Session IDs/TLS Tickets].


Vulnerability Threat Level
medium X-XSS Protection is not Present
Vulnerability Definition
As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.
Vulnerability Remediation
Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.
[● < 35s] Deploying 73/80 | Nikto - Checks the Domain Headers.
Scan Completed in 2s


Vulnerability Threat Level
medium Some vulnerable headers exposed.
Vulnerability Definition
Attackers try to learn more about the target from the amount of information exposed in the headers. An attacker may know what type of tech stack a web application is emphasizing and many other information.
Vulnerability Remediation
Banner Grabbing should be restricted and access to the services from outside would should be made minimum.
[● < 45m] Deploying 74/80 | Nmap [Slowloris DoS] - Checks for Slowloris Denial of Service Vulnerability.
Scan Completed in 30m 22s
[● < 35s] Deploying 75/80 | Nikto - Checks for HTTP PUT DEL.
Scan Completed in 1s
[● < 35s] Deploying 76/80 | Nikto - Checks for Shellshock Bug.
Scan Completed in 4s
[● < 35m] Deploying 77/80 | DirB - Brutes the target for Open Directories.
Scan Completed in 3s

```
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to restart 'networking.service'.
Authenticating as: kikin
Password:
==== AUTHENTICATION COMPLETE ===
kikin@kikin:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 10
0
    link/ether 08:00:27:d1:48:f3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 80936sec preferred_lft 80936sec
    inet6 fe80::a00:27ff:fed1:48f3/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 10
0
    link/ether 08:00:27:ff:4c:4f brd ff:ff:ff:ff:ff:ff
    inet 172.16.10.1/24 brd 172.16.10.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feff:4c4f/64 scope link
       valid_lft forever preferred_lft forever
kikin@kikin:~$ ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_seq=1 ttl=64 time=5.52 ms
64 bytes from 172.16.10.10: icmp_seq=2 ttl=64 time=0.603 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.603/3.061/5.520/2.458 ms
kikin@kikin:~$ [66787.161746] e1000 0000:00:03.0 enp0s3: Reset adapter

kikin@kikin:~$ _
```

Lampiran 3 Keterangan Melakukan Penelitian

UMKT
Program Studi
Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Muhammadiyah Kalimantan Timur
Berkarakter | Berwawasan | Berkemajuan
Telp. 0541-748511 Fax.0541-766832
Website http://informatika.umkt.ac.id
email: informatika@umkt.ac.id

بسم الله الرحمن الرحيم

Nomor : 056-010/KET/FST.1/A/2024
Lampiran : -
Perihal : **Keterangan Melakukan Penelitian**

Assalamu'alaikum Warrahmatullahi Wabarrakatuh

Puji Syukur kepada Allah Subhanahu wa ta'ala yang senantiasa melimpahkan Rahmat-Nya kepada kita sekalian. Amin.

Dengan surat ini, kami menerangkan bahwa mahasiswa berikut:

Nama : Fitria Nur Yaqin

NIM : 1911102441104

Program Studi : Teknik Informatika

Melakukan penelitian dengan mengembangkan sistem platform MCDM, studi kasus penentuan peminatan jurusan pada Program Studi Teknik Informatika Universitas Muhammadiyah Kalimantan Timur.

Demikian hal ini disampaikan, atas kerjasamanya kami ucapkan terima kasih.

Wassalamu'alaikum Warrahmatullahi Wabarrakatuh

Samarinda, 3 Muharram 1446 H
9 Juli 2024 M

Ketua Program Studi S1 Teknik Informatika

Arbansyah, S.Kom., M.TI
NIDN. 1118019203

Kampus 1 : Jl. Ir. H. Juanda, No.15, Samarinda
Kampus 2 : Jl. Pelita, Pesona Mahakam, Samarinda

Lampiran 4 Lembar Bimbingan Skripsi

LEMBAR BIMBINGAN SKRIPSI

Nama Mahasiswa : Fitria Nur Yaqin
NIM : 1911102441104
Nama Dosen Pembimbing : Faldi, S.Kom., M.TI
Judul Skripsi : Penetration Testing Pada Website Universitas Muhammadiyah Kalimantan Timur (UMKT) Dengan Menggunakan Metode PTES

No	Tanggal	Keterangan	Paraf Dosen
1.	02 Februari 2023	Konsultasi tentang judul penelitian, dan metode yang digunakan	
2.	28 Februari 2023	Konsultasi Penelitian Bab 1	
3.	02 Maret 2023	Konsultasi Mengenai Latar Belakang	
4.	09 Maret 2023	Konsultasi Revisi BAB 1	
5.	13 Maret 2023	Konsultasi Penulisan BAB 2	
6.	19 Maret 2023	Konsultasi Revisi BAB 2 Kajian Teori	
7.	22 April 2023	Konsultasi Penulisan BAB 3	
8.	07 Mei 2023	Konsultasi Perbaikan BAB 1, 2, 3	
9.	17 Juni 2024	Konsultasi Revisi Seminar Hasil	
10.	17 Juli 2024	Konsultasi Perbaikan Seminar Hasil BAB 1,2,3,4,5	
11.	20 Juli 2024	Persetujuan Laporan Skripsi dan melanjutkan membuat Jurnal	

Dosen Pembimbing

Faldi, S.Kom., M.TI
NIDN. 1121079101