Nusantara Hasana Journal
Volume 6 No. 3 (Agustus 2026), Page: 187-199
E-ISSN: 2798-1428

SISTEM OTOMATISASI RECONNAISSANCE MENGGUNAKAN MODEL OSINT UNTUK MENINGKATKAN KEAMANAN SISTEM INFORMASI PADA UNIVERSITAS MUHAMMADIYAH MAKASSAR

Automated Reconnaissance System Using Osint Model To Enhance Information System Security At Muhammadiyah University Of Makassar

Muh. Fikri Haekal[1], Muhammad Faisal[2], Muhyiddin A.M. Hayat[3]

[1,2,3]Universitas Muhammadiyah Makassar, Indonesia

[1]Email: 105841100821@student.unismuh.ac.id
[2]Email: muhfaisal@unismuh.ac.id
[3]Email: muhyiddin@unismuh.ac.id

Abstract
The development of digital technology provides opportunities to develop more interactive learning media through the integration of cybersecurity systems. However, applications that integrate automated reconnaissance with Open-Source Intelligence (OSINT) models are still challenging to implement, especially in terms of system integration and device limitations. This study aims to develop an automated reconnaissance system based on OSINT to identify exposed digital assets at Muhammadiyah University of Makassar. The application was developed using Python and Flask framework, with various OSINT modules integrated including WHOIS lookup, DNS analysis, port scanning, subdomain enumeration, vulnerability scanning, social OSINT, dark web intelligence, and Google dorking. The system was evaluated using Black Box Testing and functional testing methods. Black Box Testing results showed that most main functions operated according to designed scenarios, although several functions were partially successful due to OCR image quality and system integration limitations. The developed application can function as proactive security monitoring media for universities, providing essential technical instruments for IT administrators to map potential data breaches early, enabling proactive mitigation steps and strengthening information system security posture.
Keywords: *Automated Reconnaissance, OSINT, Cybersecurity, Information Security, Vulnerability Assessment.*

Abstrak
Perkembangan teknologi digital memberikan peluang untuk mengembangkan sistem keamanan siber yang lebih proaktif melalui integrasi sistem reconnaissance otomatis. Penelitian ini bertujuan mengembangkan sistem otomatisasi reconnaissance berbasis Open-Source Intelligence (OSINT) untuk mengidentifikasi aset digital yang terekspos pada Universitas Muhammadiyah Makassar. Aplikasi dikembangkan menggunakan Python dan framework Flask, dengan berbagai modul OSINT yang diintegrasikan meliputi WHOIS lookup, analisis DNS, pemindaian port, enumerasi subdomain, vulnerability scanning, social OSINT, dark web intelligence, dan Google dorking. Sistem dievaluasi menggunakan Black Box Testing dan metode pengujian fungsional. Hasil Black Box Testing menunjukkan bahwa sebagian besar fungsi utama aplikasi dapat berjalan sesuai dengan skenario yang dirancang, meskipun beberapa fungsi memperoleh status berhasil sebagian akibat kualitas OCR dan keterbatasan integrasi sistem. Aplikasi yang dikembangkan dapat digunakan sebagai media pemantauan keamanan proaktif bagi universitas, menyediakan instrumen teknis yang esensial bagi administrator TI untuk memetakan potensi kebocoran data secara

Nusantara Hasana Journal
Volume 6 No. 3 (Agustus 2026), Page: 187-199
E-ISSN: 2798-1428

dini, sehingga langkah-langkah mitigasi dan penguatan postur keamanan sistem informasi dapat diterapkan secara proaktif.
Kata Kunci: *Reconnaissance Otomatis, OSINT, Keamanan Siber, Keamanan Informasi, Penilaian Kerentanan.*

PENDAHULUAN

Dalam era transformasi digital yang semakin pesat, ancaman terhadap sistem informasi menjadi semakin kompleks dan sulit diprediksi (Prasetyo et al., 2023). Perguruan tinggi seperti Universitas Muhammadiyah Makassar memanfaatkan teknologi informasi untuk mendukung operasional akademik, manajemen, serta layanan publik. Namun, meningkatnya ketergantungan terhadap sistem digital menjadikan institusi pendidikan semakin rentan terhadap berbagai serangan siber seperti phishing, data leakage, hingga reconnaissance attack yang dilakukan secara tersembunyi oleh pihak tak bertanggung jawab.

Insiden kebocoran data berskala nasional yang terjadi di Indonesia, seperti peretasan pada Pusat Data Nasional (PDN) di tahun 2024, membuktikan bahwa kelemahan infrastruktur sistemik dan kelalaian manusia masih menjadi tantangan utama dalam tata kelola keamanan siber (Bua et al., 2025). Untuk menghadapi dinamika ancaman yang terus berkembang ini, perlindungan data tidak hanya bertumpu pada satu aspek, melainkan membutuhkan perbaikan menyeluruh. Oleh karena itu, institusi perlu mulai menerapkan kebijakan pertahanan berbasis ancaman (threat-based defense policies) yang secara spesifik memprioritaskan alokasi sumber daya pada celah keamanan berisiko tinggi demi meningkatkan efektivitas keamanan nasional dan organisasional (Sarjito, 2024).

Tahapan awal dalam serangan siber yang dikenal sebagai reconnaissance atau pengintaian merupakan upaya sistematis untuk mengumpulkan sebanyak mungkin informasi dari target dengan tujuan memahami arsitektur jaringan, aplikasi, maupun kerentanan yang ada. Salah satu metode yang paling umum digunakan dalam tahap reconnaissance adalah Open Source Intelligence (OSINT), yaitu pendekatan pengumpulan data dari sumber-sumber publik yang terbuka dan sah seperti media sosial, mesin pencari, data DNS, metadata dokumen, hingga forum daring (Saraswathi et al., 2022).

Meskipun OSINT dapat digunakan secara sah dan bermanfaat dalam konteks pertahanan digital, ia juga berpotensi menjadi alat serangan yang sangat efektif jika digunakan secara tidak etis. Dalam konteks korporasi maupun institusi publik seperti universitas, data yang terbuka sering kali menjadi pintu masuk serangan melalui teknik rekayasa sosial (social engineering) atau eksploitasi layanan terbuka (Bizouarn et al., 2023).

Dalam hal mengatasi ancaman serangan siber modern, pengembangan sistem otomatisasi reconnaissance menjadi salah satu strategi utama dalam keamanan siber modern. Sistem otomatisasi memungkinkan organisasi untuk secara aktif dan otomatis memetakan serta memantau data-data yang terekspos secara publik. Dalam implementasinya, sistem otomatis ini tidak hanya melakukan pengumpulan data dari domain, metadata, dan DNS, tetapi juga menyimpan dan mengatur hasilnya secara terstruktur sebagai bahan evaluasi keamanan internal (Saraswathi et al., 2022).

Nusantara Hasana Journal
Volume 6 No. 3 (Agustus 2026), Page: 187-199
E-ISSN: 2798-1428

Pada lingkungan perguruan tinggi, sistem informasi seperti portal akademik, sistem keuangan, layanan surat menyurat digital, serta data profil mahasiswa dan dosen merupakan aset yang sangat penting. Jika data tersebut terekspos secara tidak sengaja di layanan terbuka, dapat menimbulkan konsekuensi serius baik dari sisi reputasi maupun hukum. Oleh karena itu, penerapan sistem otomatisasi reconnaissance berbasis OSINT dapat berfungsi sebagai mekanisme pertahanan dini yang mendeteksi kebocoran informasi sejak awal (Bizouarn et al., 2023).

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengembangkan sistem otomatisasi reconnaissance berbasis OSINT dengan antarmuka dashboard yang dapat secara berkala dan terstruktur memindai eksposur aset digital milik Universitas Muhammadiyah Makassar, guna mendukung evaluasi postur keamanan siber secara proaktif dan berkelanjutan.

METODE

Lokasi dan Waktu Penelitian

Penelitian ini dilaksanakan di Universitas Muhammadiyah Makassar, yang beralamat di Jalan Sultan Alauddin No. 259, Kota Makassar, Sulawesi Selatan. Pemilihan lokasi ini didasarkan pada relevansi objek penelitian, mengingat Universitas Muhammadiyah Makassar merupakan institusi pendidikan tinggi yang secara aktif mengadopsi sistem informasi digital dalam mendukung layanan akademik dan administratif. Penelitian dilaksanakan selama kurang lebih empat bulan, dimulai pada minggu kedua bulan Mei 2025 dan berakhir pada akhir Agustus 2025.

Alat dan Bahan

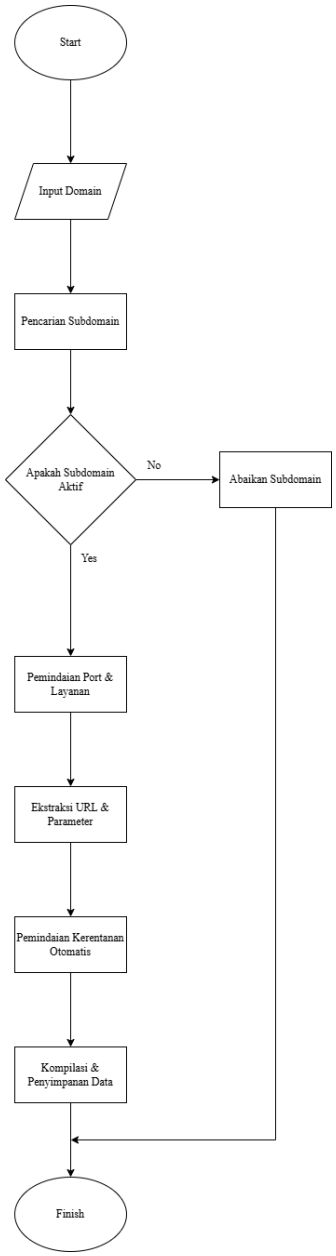
Penelitian ini menggunakan perangkat keras berupa laptop dengan spesifikasi Intel Core i7 CPU 2.20GHz (16 CPUs) dan RAM 8 GB. Perangkat lunak yang digunakan meliputi Python sebagai bahasa pemrograman utama, Terminal untuk eksekusi perintah, berbagai tools OSINT untuk pengumpulan data, dan Kali Linux sebagai sistem operasi pengembangan.

Perancangan Sistem

Sistem dirancang sebagai aplikasi web berbasis dashboard yang mengintegrasikan berbagai modul OSINT. Fungsi-fungsi intelijen dipisahkan ke dalam skrip utility seperti WHOIS, DNS, ports, subdomains, dan vulnerability scanner. Untuk proses pemindaian yang membutuhkan kapabilitas jaringan tingkat lanjut, sistem secara otomatis melakukan pemanggilan eksekusi subprocess terhadap binary utilitas keamanan spesifik seperti Nmap dan Nuclei yang terpasang pada sistem operasi host.

Sistem ini dirancang secara modular agar setiap komponen dapat dijalankan secara independen dan mudah dikembangkan di masa mendatang. Pendekatan modular ini memungkinkan integrasi dan pengujian dilakukan per tahap, seperti hanya menjalankan enumerasi pasif tanpa melanjutkan ke tahap pemindaian kerentanan. Alur logika sistem yang dirancang, ditampilkan melalui flowchart sistem otomatisasi reconnaissance pada Gambar 1:

Nusantara Hasana Journal
Volume 6 No. 3 (Agustus 2026), Page: 187-199
E-ISSN: 2798-1428



Gambar 1. Flowchart Sistem

Perancangan Arsitektur Sistem

Arsitektur sistem dibangun dengan mengadopsi pola pengembangan aplikasi web modern yang memisahkan logika presentasi, pemrosesan, dan penyimpanan data. Menggunakan framework Flask, sistem ini mengimplementasikan struktur routing yang dinamis untuk mengelola permintaan pengguna melalui antarmuka dashboard. Persistensi data dalam arsitektur ini dikelola oleh sistem manajemen basis data SQLite yang ditempatkan pada direktori instance.

Teknologi dan Tools yang Digunakan

Lingkungan pengembangan sistem ini menggunakan Kali Linux sebagai sistem operasi utama. Bahasa pemrograman Python versi 3.8 ke atas dipilih sebagai mesin penggerak utama. Pada lapisan aplikasi web, framework Flask digunakan

Nusantara Hasana Journal
Volume 6 No. 3 (Agustus 2026), Page: 187-199
E-ISSN: 2798-1428

bersama dengan Jinja2 templates untuk membangun antarmuka dashboard yang interaktif. Dari sisi penyimpanan, SQLite dipilih karena efisiensi kinerjanya dalam menangani basis data lokal tanpa memerlukan konfigurasi server basis data yang rumit.

Integrasi utilitas pihak ketiga menjadi komponen krusial dalam memperluas jangkauan deteksi sistem. Sistem memanfaatkan Nmap sebagai utilitas pemindaian jaringan tingkat lanjut untuk memetakan port dan layanan yang aktif pada target. Selain itu, Nuclei diintegrasikan sebagai mesin pemindai kerentanan berbasis template untuk mengidentifikasi celah keamanan spesifik secara otomatis.

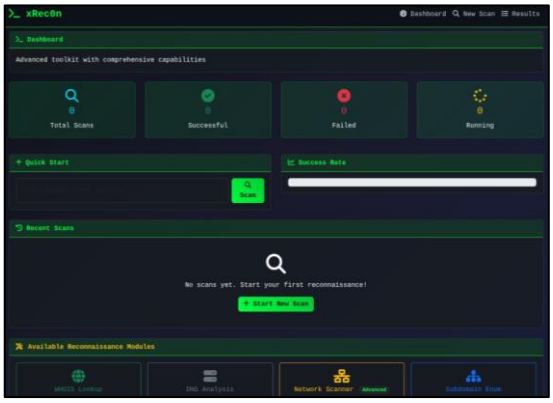
Teknik Pengujian

Pengujian dilakukan setelah seluruh fitur aplikasi selesai diimplementasikan. Penelitian menggunakan metode Black Box Testing untuk menguji fungsi aplikasi berdasarkan masukan (input) dan keluaran (output) tanpa memperhatikan struktur internal kode program. Pengujian dilakukan terhadap fitur-fitur utama aplikasi, meliputi navigasi antarmuka, AR dan kamera, NPC Guru Virtual, animasi, chat, voice interaction, STT, TTS, AI/Gemini, pemindaian materi, OCR, MediaPipe, quiz, dan fungsi pendukung lainnya.

HASIL DAN PEMBAHASAN

Hasil Pengembangan Aplikasi

Penelitian ini menghasilkan sistem otomatisasi reconnaissance berbasis web dashboard yang dikembangkan menggunakan Python dan Flask framework. Aplikasi dirancang sebagai media pemantauan keamanan proaktif dengan mengintegrasikan berbagai teknik OSINT dalam satu platform terpusat. Melalui dashboard tersebut, pengguna dapat memilih jenis analisis, memasukkan target, menjalankan proses reconnaissance, serta melihat hasil pemrosesan secara terpusat. Tampilan dashboard utama sistem ditunjukkan pada Gambar 2.



Gambar 2. Tampilan Dashboard Sistem

Implementasi Sistem Berbasis Dashboard

Sistem yang dikembangkan diimplementasikan dalam bentuk web application dengan dashboard sebagai antarmuka utama yang berfungsi sebagai pusat kendali seluruh proses reconnaissance. Dashboard dirancang untuk memberikan gambaran awal mengenai kondisi sistem, termasuk ringkasan aktivitas pemindaian, status proses yang sedang berjalan, serta akses ke modul-modul analisis yang tersedia.

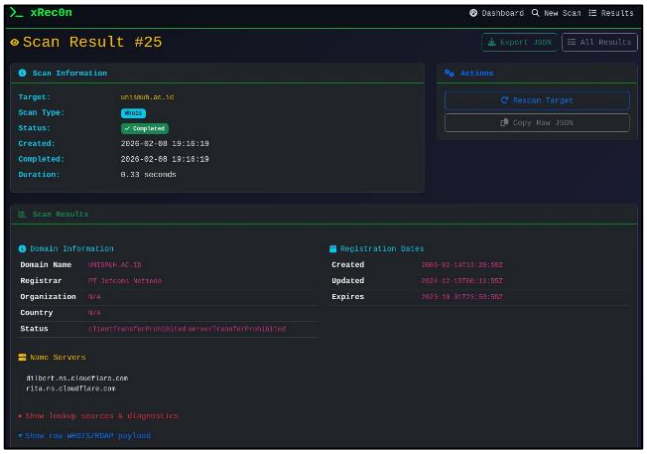
Nusantara Hasana Journal
Volume 6 No. 3 (Agustus 2026), Page: 187-199
E-ISSN: 2798-1428

Fitur dan Fungsi Sistem

Sistem otomatisasi reconnaissance yang dikembangkan memiliki arsitektur modular yang mengintegrasikan berbagai teknik Open-Source Intelligence (OSINT) ke dalam satu platform dashboard terpusat. Berikut adalah penjabaran dari masing-masing fitur dan fungsi modul yang tersedia pada sistem:

1. Modul WHOIS Lookup

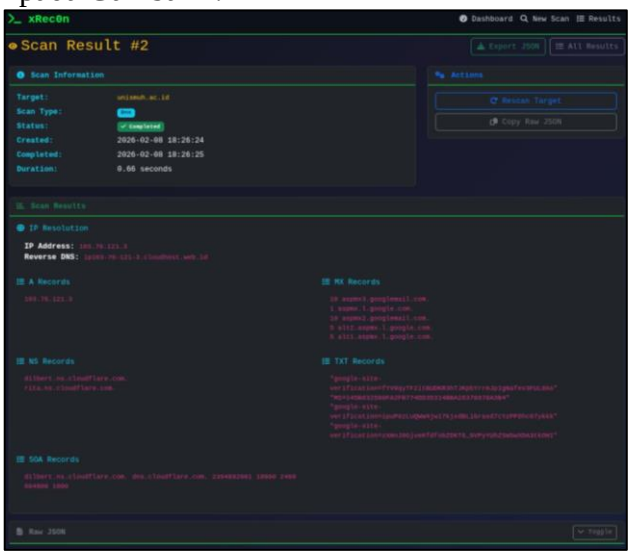
Fitur ini berfungsi untuk mengekstrak informasi legal dan administratif terkait kepemilikan sebuah domain. Sistem secara otomatis mengambil data pendaftaran, termasuk nama registrar, tanggal pembuatan (creation date), tanggal kedaluwarsa (expiry date), detail kontak organisasi, serta name server yang digunakan oleh target. Tampilan hasil proses WHOIS Lookup pada sistem ditunjukkan pada Gambar 3.



Gambar 3. Tampilan Hasil WHOIS Lookup pada Sistem

2. Modul DNS Analysis

Modul Domain Name System (DNS) Analysis bertujuan untuk memetakan topologi jaringan target melalui kueri rekaman DNS. Modul ini akan mengidentifikasi records penting seperti A (pemetaan IP), MX (Mail Exchange), dan TXT (sering memuat konfigurasi keamanan seperti SPF/DKIM). Hasil analisis DNS ditampilkan pada Gambar 4.

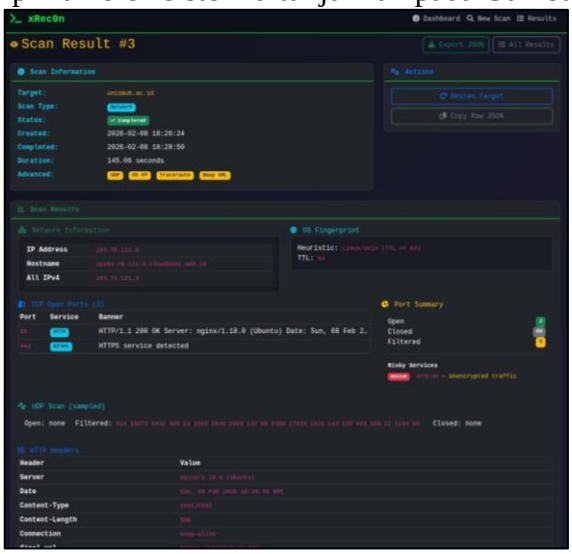


Gambar 4. Tampilan Hasil Analisis DNS pada Domain

Nusantara Hasana Journal
Volume 6 No. 3 (Agustus 2026), Page: 187-199
E-ISSN: 2798-1428

3. Modul Network Scanner

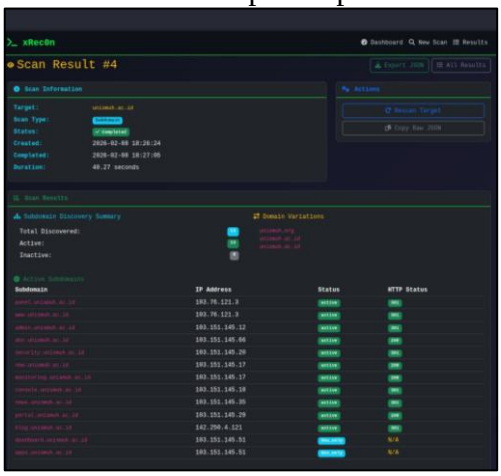
Fitur pemindai jaringan (Network Scanner) diintegrasikan untuk mendeteksi ketersediaan port yang terbuka pada target, sekaligus mengidentifikasi jenis layanan (services) yang beroperasi di balik port tersebut. Hasil pemindaian jaringan yang ditampilkan oleh sistem ditunjukkan pada Gambar 5.



Gambar 5. Tampilan Hasil Network Scanning

4. Modul Subdomain Enumeration

Subdomain Enumeration adalah modul krusial yang melakukan pencarian ekstensif terhadap subdomain yang berafiliasi dengan domain utama institusi. Modul ini menelusuri aset tersembunyi yang mungkin tidak dipublikasikan secara resmi, seperti portal pengembangan (development/staging), dashboard administrasi internal, atau basis data yang secara tidak sengaja dapat diakses melalui internet. Hasil proses enumerasi subdomain ditampilkan pada Gambar 6.



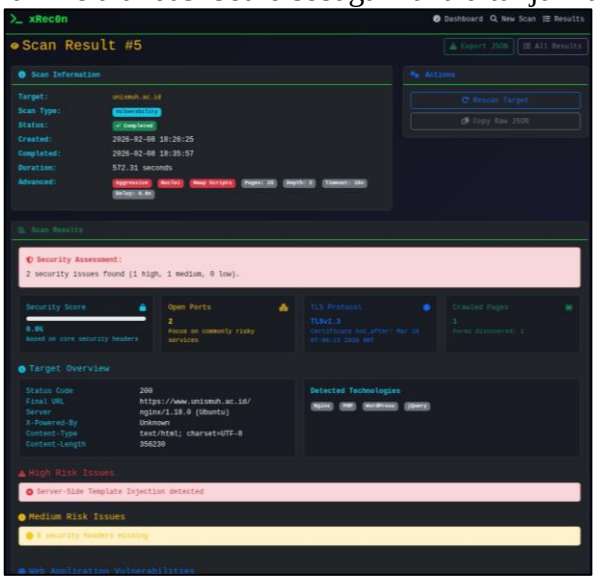
Gambar 6. Tampilan Hasil Subdomain Enumeration

5. Modul Vulnerability Scan

Fitur Vulnerability Scan bekerja dengan membandingkan parameter target terhadap basis data kerentanan yang telah diketahui seperti format Common Vulnerabilities and Exposures. Modul ini secara otomatis mengeksekusi pemeriksaan pasif terhadap kerangka kerja aplikasi, versi server web, maupun

Nusantara Hasana Journal
Volume 6 No. 3 (Agustus 2026), Page: 187-199
E-ISSN: 2798-1428

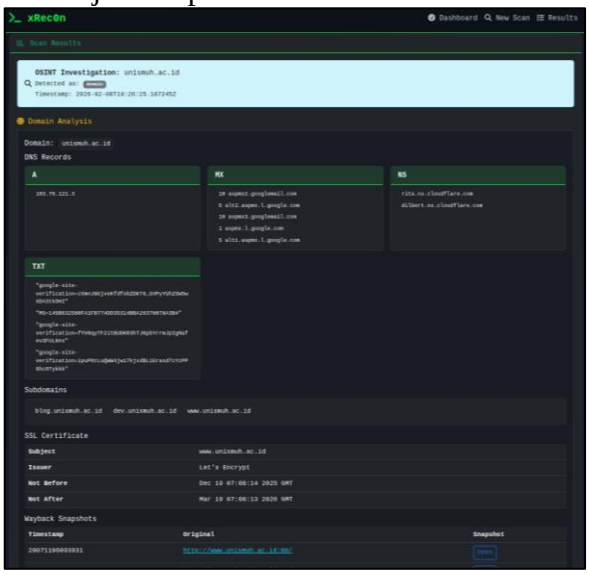
miskonfigurasi keamanan pada header HTTP/HTTPS. Hasil proses vulnerability scanning ditampilkan melalui dashboard sebagaimana ditunjukkan pada Gambar 7.



Gambar 7. Tampilan Hasil Vulnerability Scanning

6. Modul Social OSINT

Fungsi Social OSINT dirancang untuk mengekstrak jejak digital dan keterpaparan informasi dari target melalui berbagai platform media sosial dan repositori publik. Informasi seperti alamat email staf, struktur organisasi, atau repositori kode yang bocor dapat dihimpun secara otomatis. Tampilan hasil Social OSINT pada sistem ditunjukkan pada Gambar 8.

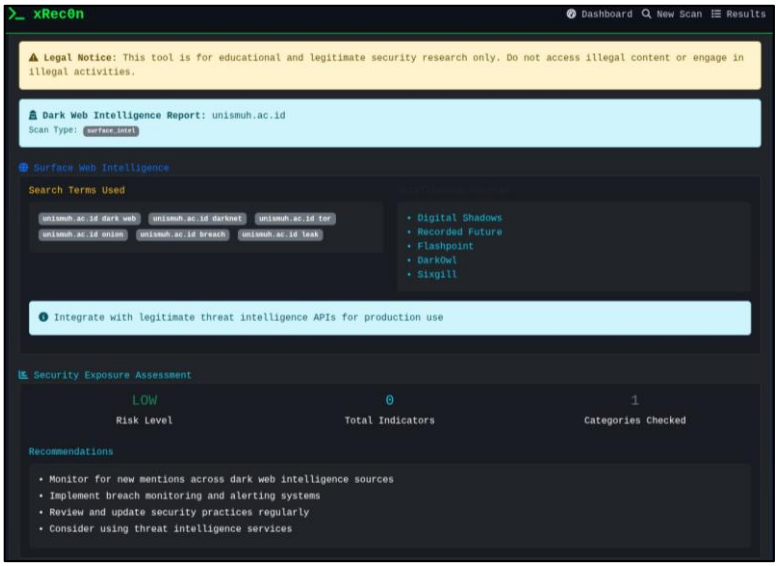


Gambar 8. Tampilan Hasil Social OSINT

7. Modul Dark Web Intelligence

Modul intelijen Dark Web beroperasi untuk memverifikasi apakah terdapat indikator kompromi (Indicator of Compromise / IoC) terkait entitas target di pasar gelap internet atau forum kebocoran data. Hasil proses Dark Web Intelligence ditampilkan pada Gambar 9.

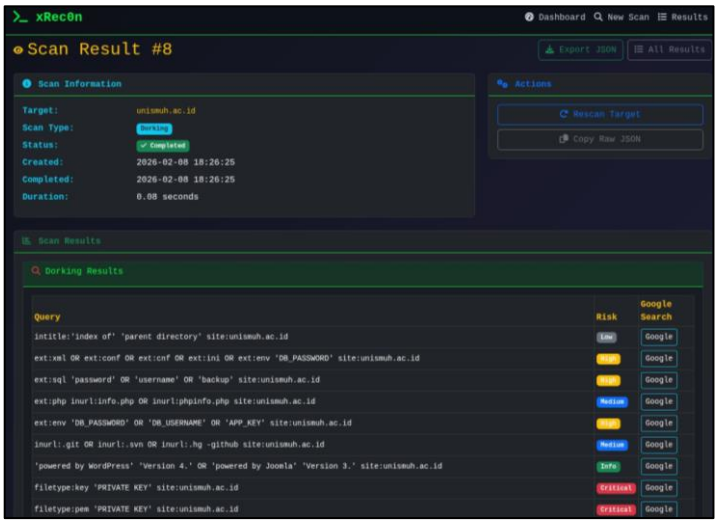
Nusantara Hasana Journal
Volume 6 No. 3 (Agustus 2026), Page: 187-199
E-ISSN: 2798-1428



Gambar 9. Tampilan Hasil Dark Web Intelligence

8. Modul Google Dorking

Fitur Dorking Intelligence mengotomatisasi kueri mesin pencari tingkat lanjut (advanced search operators) untuk menemukan anomali pengindeksan oleh mesin pencari. Modul ini secara proaktif mencari halaman masuk (login page), direktori yang terbuka bebas (directory traversal), dokumen konfigurasi sensitif, atau kunci privat (seperti PRIVATE KEY) yang secara tidak sengaja terindeks secara publik oleh layanan mesin pencari. Tampilan hasil Google Dorking ditunjukkan pada Gambar 10.

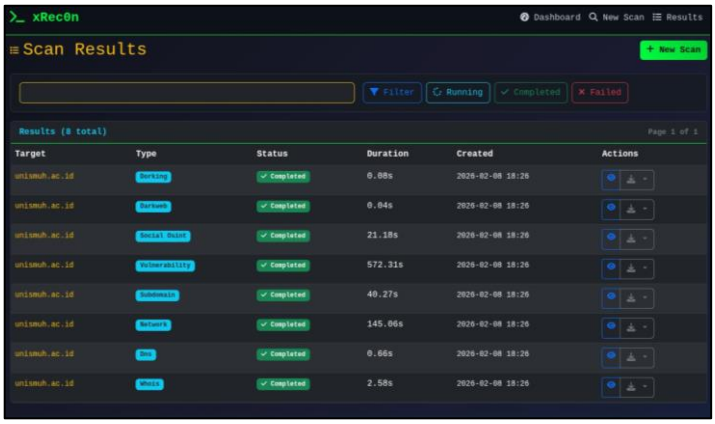


Gambar 10. Tampilan Hasil Google Dorking

Hasil Pengujian Sistem

Pengujian Black Box Testing dilakukan untuk mengetahui apakah fungsi aplikasi dapat berjalan sesuai dengan rancangan. Hasil pengujian menunjukkan bahwa sebagian besar fungsi utama aplikasi dapat berjalan sesuai dengan skenario yang dirancang, meskipun beberapa fungsi memperoleh status berhasil sebagian akibat kualitas gambar pada proses OCR dan keterbatasan implementasi MediaPipe. Tampilan fungsi ekspor hasil ditunjukkan pada Gambar 11.

Nusantara Hasana Journal
Volume 6 No. 3 (Agustus 2026), Page: 187-199
E-ISSN: 2798-1428



Gambar 11. Tampilan Fungsi Ekspor Hasil Reconnaissance

Tabel 1. Ringkasan Hasil Black Box Testing

No.	Fitur yang Diuji	Status
1	Menjalankan aplikasi	Berhasil
2	Navigasi UI	Berhasil
3	Dashboard display	Berhasil
4	WHOIS Lookup	Berhasil
5	DNS Analysis	Berhasil
6	Network Scanner	Berhasil
7	Subdomain Enumeration	Berhasil
8	Vulnerability Scan	Berhasil
9	Social OSINT	Berhasil
10	Dark Web Intelligence	Berhasil
11	Google Dorking	Berhasil
12	Export JSON	Berhasil
13	Database Storage	Berhasil
14	Integrasi sistem	Berhasil Sebagian
15	Keluar sesi	Berhasil

PEMBAHASAN

1. Integrasi Teknologi

Hasil pengembangan menunjukkan bahwa berbagai modul OSINT dapat diintegrasikan dalam satu aplikasi pembelajaran. Integrasi tersebut memberikan beberapa bentuk interaksi kepada pengguna untuk memperoleh informasi keamanan yang komprehensif. Sistem ini menjadikan reconnaissance tidak hanya

Nusantara Hasana Journal
Volume 6 No. 3 (Agustus 2026), Page: 187-199
E-ISSN: 2798-1428

sebagai proses manual yang memakan waktu, tetapi sebagai sistem otomatis yang terstruktur.

2. Sistem Otomatisasi

Sistem otomatisasi yang dikembangkan berhasil mentransformasi proses reconnaissance yang sebelumnya bergantung pada eksekusi manual melalui Command-Line Interface (CLI) menjadi sebuah alur kerja otomatis yang jauh lebih cepat, efisien, dan terstruktur. Pendekatan operasional utama yang diadopsi dalam arsitektur ini adalah pemindaian pasif (passive reconnaissance), di mana pemetaan permukaan serangan (attack surface) dijalankan secara etis dan non-intrusif.

3. Implementasi Dashboard

Dashboard yang dikembangkan tidak hanya berfungsi sebagai media kontrol, tetapi juga sebagai sarana visualisasi hasil reconnaissance. Sistem membantu pengguna memahami profil digital target secara lebih terstruktur dan komprehensif. Kehadiran platform pemantauan terpadu ini pada akhirnya menyediakan instrumen teknis yang esensial bagi administrator teknologi informasi universitas untuk memetakan potensi kebocoran data secara dini.

4. Analisis Hasil Pengujian

Hasil Black Box Testing menunjukkan bahwa sebagian besar fungsi utama aplikasi berjalan sesuai dengan rancangan. Dari 15 skenario pengujian, sebagian besar fitur memperoleh status berhasil, dengan beberapa fitur memperoleh status berhasil sebagian terutama pada integrasi sistem yang kompleks. Secara fungsional aplikasi telah mampu menjalankan komponen utama yang dirancang, tetapi masih terdapat beberapa kondisi teknis yang memengaruhi hasil penggunaan.

KESIMPULAN

Penelitian ini telah berhasil merancang dan membangun sebuah prototipe sistem otomatisasi reconnaissance berbasis Open-Source Intelligence (OSINT) yang diimplementasikan dalam bentuk aplikasi web terintegrasi dengan antarmuka dashboard. Pengembangan sistem ini secara langsung menjawab kebutuhan akan metode identifikasi paparan aset digital pada Universitas Muhammadiyah Makassar, dengan mentransformasi proses pengumpulan data intelijen yang sebelumnya bergantung pada eksekusi manual melalui Command-Line Interface (CLI) menjadi sebuah alur kerja otomatis yang jauh lebih cepat, efisien, dan terstruktur.

Keberhasilan fungsional dari sistem tersebut berakar pada pemilihan perangkat (tools) dan teknologi yang terbukti paling sesuai untuk mendukung proses otomatisasi pengintaian di lingkungan perguruan tinggi. Hasil pengujian menunjukkan bahwa kerangka kerja operasional yang paling efektif adalah pengintegrasian berbagai modul utilitas keamanan open-source yang dieksekusi secara asinkron, yang mencakup WHOIS lookup, analisis topologi Domain Name System (DNS), pemindaian ketersediaan port, enumerasi subdomain, vulnerability scanner, ekstraksi jejak digital (Social OSINT), pemantauan intelijen Dark Web, hingga otomatisasi Google Dorking.

Meskipun sistem otomatisasi reconnaissance ini telah beroperasi dengan baik sebagai instrumen pendeteksi dini, masih terdapat beberapa ruang pengembangan yang dapat disempurnakan pada penelitian di masa mendatang. Salah satu rekomendasi utama dari aspek teknis adalah pengembangan fitur sistem

Nusantara Hasana Journal
Volume 6 No. 3 (Agustus 2026), Page: 187-199
E-ISSN: 2798-1428

peringatan dini (alerting system) secara real-time. Pengintegrasian aplikasi ini dengan platform notifikasi seperti email maupun bot Telegram akan memungkinkan administrator sistem menerima pemberitahuan seketika apabila terdeteksi anomali, kerentanan kritis, atau subdomain baru yang tiba-tiba terekspos ke publik.

DAFTAR PUSTAKA

Al-amien, M. F. (2025). Risiko Keamanan TI Akibat Kelalaian Mahasiswa Non-IT dalam Keamanan Siber: Tinjauan Etis dan Solusi Preventif. *Research Gate*. https://doi.org/10.13140/RG.2.2.14416.62723

Bizouarn, K. M., Abdulnabi, M., & Tan, J. (2023). OSINT and AI: A Powerful Combination for Company Vulnerability Detection. *2023 IEEE 21st Student Conference on Research and Development, SCOReD 2023*, 246–250. https://doi.org/10.1109/SCOReD60679.2023.10563226

Bua, I. T., & Idris, N. I. (2025). Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024. *Desentralisasi: Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan*, 2(2), 100–114. https://doi.org/10.62383/desentralisasi.v2i2.653

Devireddy, I. R., Samual, J., & Machap, K. (2026). OSINT Toolkit for Reconnaissance phase of Penetration Testing. *Journal of Applied Technology and Innovation*, 8(1), 40–44. https://doi.org/10.65136/jati.v8i1.63

Gao, P., Liu, X., Choi, E., Ma, S., Yang, X., & Song, D. (2024). ThreatKG: An AI-Powered System for Automated Open-Source Cyber Threat Intelligence Gathering and Management. *LAMPS 2024 - Proceedings of the 1st ACM Workshop on Large AI Systems and Models with Privacy and Safety Analysis*. https://doi.org/10.1145/3689217.3690613

Hoffman, F. (2025). Rebranding second-generation open-source intelligence: "It's not your father's OSINT". *Intelligence Journal*, 26(3), 61–74.

Khan, S., & Wallom, D. (2022). A system for organizing, collecting, and presenting open-source intelligence. *Journal of Data, Information and Management*, 4(2), 107–117. https://doi.org/10.1007/s42488-022-00068-4

Ningrum, F. A. S., Riwanto, Y., Pratiwi, I. Y. R., & Fikri, M. A. (2024). Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks KAMI. *Jurnal Informatika Polinema*, 10(3), 437–444. https://doi.org/10.33795/jip.v10i3.5154

Prasetyo, D., Sebayang, N., & Dillianto, B. (2023). Pemanfaatan Open Source Intelligence dalam Membantu Tugas TNI untuk Melindungi Pertahanan Negara. *JIIP - Jurnal Ilmiah Ilmu Pendidikan*, 6(10), 7963–7966. https://doi.org/10.54371/jiip.v6i10.3016

Rahman, M. R., Hezaveh, R. M., & Williams, L. (2023). What Are the Attackers Doing Now? Automating Cyberthreat Intelligence Extraction from Text on Pace with the Changing Threat Landscape: A Survey. *ACM Computing Surveys*, 55(12), 1–35. https://doi.org/10.1145/3571726

Ramadhan, R. A., Aresta, R. M., & Hariyadi, D. (2020). Sudomy: Information Gathering Tools for Subdomain Enumeration and Analysis. *IOP*

Conference Series: Materials Science and Engineering, 771(1). https://doi.org/10.1088/1757-899X/771/1/012019

Santa, K., Radjakore, E., Lahutung, R. A., Pangalila, R. P., & Deil, T. V. (2025). Ethical Hacking Sebagai Strategi Keamanan Cyber di Era Digital: Studi Pustaka dan Implementasi Dasar. *Jurnal Ilmiah Teknik Informatika Dan Komunikasi*, 5(2), 548–553. https://doi.org/10.55606/juitik.v5i2.1183

Santoso, J. T. (2023). *Teknologi Keamanan Siber (Cyber Security)*. Penerbit Yayasan Prima Agus Teknik.

Saraswathi, V. R., Ahmed, I. S., Reddy, S. M., Akshay, S., Reddy, V. M., & Reddy, S. M. (2022). Automation of Recon Process for Ethical Hackers. *2022 International Conference for Advancement in Technology, ICONAT 2022*. https://doi.org/10.1109/ICONAT53423.2022.9726077

Sarjito, A. (2024). The Impact of Intelligence Gathering, Risk Analysis, and Scenario Planning on Defense Policy Formulation. *International Journal Administration, Business & Organization*, 5(3), 27–46. https://doi.org/10.61242/ijabo.24.396

Shoffa, I. M. (2025). Parenting Era Digital: Pemanfaatan Open Source Intelligence untuk Meningkatkan Literasi Audio Visual Anak. *Jurnal Pendidikan*, 3(4), 4853–4856.

Stamme, M. I. W. (2025). The Best Disinfectant: The Value of Transparency in Information Operations. *Intelligence and National Security*, 16(1).

Szymoniak, S., Foks, K., & Pyrkosz-Dziubczyk, A. (2025). Application of OSINT Methods in Ensuring Cybersecurity. *IPSI Transactions on Internet Research*, 21(2), 38. https://doi.org/10.58245/ipsi.tir.2502.05