ISSN: 2477-5126
e-ISSN: 2548-9356

Pengumpulan Informasi pada Situs Web Dengan Menyusun Kerangka Kerja Keamanan Siber NIST

Dega Surono Wibowo[1*)], M.Nishom[2], Taufiq Abidin[3]
[1,2,3]Jurusan Teknik Informatika, Politeknik Harapan Bersama, Tegal
[1,2,3]Jln. Mataram No.9, Margadana, Kota Tegal, 52147, Indonesia
email: [1]dega.wibowo@poltektegal.ac.id, [2]m.nishom.dosen@gmail.com, [2]taufiq.abidin@poltektegal.ac.id

Abstract *— In the current era, the rapid development of websites has made them one of the most significant modern information media. Website creation is not only focused on the design and information presented, but also focuses on security aspects. The presence of security on a website is very important, considering the need to protect the data and information contained therein. Information Gathering is one method used to test a website's security. This information gathering is the earliest stage to obtain ownership and other sensitive information. This research aims to conduct security testing of the oase.poltektegal.ac.id website using tools in the form of penetration testing software; then, the testing results are entered into the cybersecurity framework issued by N.I.S.T. The test results obtained and adjusted to N.I.S.T. Cybersecurity are that the oase.poltektegal.ac.id website has vulnerabilities in the form of CVE-2003-1418 (apache webserver vulnerability), CVE-2005-3299 (PHP vulnerability), CVE-2010-4344 (Buffer Overflow Vulnerability), CVE-2007-6750 (XSS). The solution to this vulnerability is updating the software and closing unused ports. These results will be used as a benchmark in creating or improving similar websites to increase awareness and vigilance in achieving cyber resilience.*

Keywords *– Information Gathering, N.I.S.T. Cybersecurity Framework, Website*

Abstrak **– Pada era saat ini, perkembangan pesat website menjadikannya sebagai salah satu media informasi modern yang sangat signifikan. Pembuatan website tidak hanya terfokus pada desain dan informasi yang disajikan, melainkan juga menitikberatkan pada aspek keamanan. Kehadiran keamanan dalam sebuah website menjadi sangat penting, mengingat perlunya melindungi data dan informasi yang terdapat di dalamnya. Information Gathering merupakan salah satu metode yang dilakukan untuk pengujian keamanan suatu website, information gathering ini merupakan tahapan yang paling awal dengan tujuan untuk mendapatkan informasi kepemilikan dan informasi sensitive lainnya. Tujuan penelitian ini adalah melakukan pengujian keamanan website oase.poltektegal.ac.id menggunakan tools yang berupa perangkat lunak penetration testing, kemudian hasil dari pengujian dimasukkan kedalam kerangka cybersecurity yang dikeluarkan NIST. Hasil pengujian yang didapat dan sudah disesuaikan dengan NIST Cybersecurity adalah website oase.poltektegal.ac.id memiliki kerentanan yang berupa CVE-2003-1418 (kerentanan webserver apache), CVE-2005-3299 (kerentanan PHP), CVE-2010-4344 (Kerentanan Buffer Overflow), CVE-2007-6750 (XSS). Solusi dari kerentanan tersebut adalah dengan cara memperbaharui perangkat lunak dan melakukan penutupan port yang tidak terpakai. Berdasarkan hasil tersebut akan digunakan sebagai patokan dalam pembuatan atau perbaikan website yang serupa supaya dapat menambah aspek kesadaran dan kewaspadaan dalam mencapai ketahanan siber.**

Kata Kunci *– Information Gathering, N.I.S.T. Cybersecurity Framework, Website*

*) **penulis korespondensi**: Dega Surono Wibowo
Email: dega.wibowo@poltektegal.ac.id

I. PENDAHULUAN

Pengolahan data mengubahnya menjadi informasi yang bermakna, memberikan nilai tambah bagi penerimanya. Informasi ini menjadi landasan bagi pengambilan keputusan, memungkinkan penerima informasi untuk menggunakannya secara efektif. Di sisi lain, data adalah representasi faktual yang dapat dimodifikasi dalam berbagai bentuk seperti gambar, kata, atau angka. Karena prosedur penggunaan dan tujuan tertentu, data dapat menjadi sangat sensitive, terutama ketika bersifat rahasia

Keamanan informasi pada suatu situs web memiliki signifikansi yang sangat besar. Pentingnya keamanan ini tidak dapat diabaikan, terutama oleh para pengembang situs web. Jika langkah-langkah keamanan tidak diimplementasikan dengan baik oleh pembuat situs web, potensi risiko muncul, seperti peretasan yang dapat mengakses data krusial atau merusak tata letak dan konten situs web secara tidak sah. Oleh karena itu, langkah-langkah perlindungan yang kuat perlu diterapkan untuk menjaga keamanan informasi dan integritas suatu situs web.

Saat ini, peretas tidak hanya mengincar instansi pemerintah seperti yang terjadi pada tahun 2019, tetapi juga telah melancarkan serangan terhadap instansi pendidikan. Pemantauan dan identifikasi Badan Siber dan Sandi Negara menunjukkan bahwa pada tahun 2020, serangan terhadap instansi pendidikan mencapai 38%. Sebagai upaya preventif terhadap potensi serangan siber di lembaga pendidikan, langkah-langkah analisis keamanan informasi terhadap sistem-sistem yang terpasang menjadi suatu keharusan. Dengan demikian, tindakan ini menjadi langkah proaktif dalam melindungi keamanan dan integritas data di lingkungan pendidikan dari ancaman peretasan yang semakin meningkat.

Tahap Information Gathering merupakan langkah komprehensif dalam mengidentifikasi target, yang mencakup informasi seperti sistem operasi, topologi jaringan, alamat IP, port yang terbuka, dan DNS yang digunakan. Selain itu, tahap ini juga memungkinkan untuk mengidentifikasi pemilik suatu website [1]. Dalam proses asesmen keamanan, seringkali celah-celah kritis dapat ditemukan pada tahap awal, yaitu Information Gathering [2] [3]. Fenomena ini dapat disebabkan oleh kesalahan dalam pengembangan sistem, yang dikenal sebagai Misconfiguration [4]. Oleh karena itu,

kesalahan dalam mengelola konfigurasi sistem pada tahap awal ini dapat menjadi pintu masuk bagi ancaman keamanan yang lebih serius

NIST Cybersecurity Framework dianggap sebagai praktik terbaik untuk membangun kerangka kerja ketahanan siber. Kerangka kerja ini terstruktur dalam lima komponen utama, dimulai dari identifikasi, proteksi, deteksi, respon, hingga pemulihan. Setiap bagian utama memberikan perspektif holistik yang menyeluruh terhadap rangkaian langkah-langkah dalam mitigasi risiko keamanan siber. Dengan menyusun ke lima aspek ini, organisasi dapat mencapai pendekatan yang komprehensif dan terstruktur dalam menghadapi tantangan dan ancaman dalam dunia siber, mencakup segala aspek dari pengenalan risiko hingga pemulihan setelah terjadinya insiden [5]. Penerapan keamanan siber NIST memberikan kewenangan kepada pengelola website untuk melakukan identifikasi dan manajemen risiko keamanan siber dengan memberikan penilaian terhadap setiap ancaman yang ada. Dengan menggunakan kerangka kerja ini, pengelola dapat secara sistematis mengevaluasi potensi risiko keamanan, memberikan nilai terhadap tingkat ancaman, dan mengembangkan strategi perlindungan yang sesuai. Pendekatan ini memberikan alat yang efektif bagi pengelola website untuk merancang langkah-langkah keamanan yang tepat dan mengurangi risiko potensial yang dapat mengancam integritas dan keamanan sistem [6].

Penelitian ini akan mengimplementasikan tahap information gathering guna mendapatkan laporan komprehensif yang mencakup seluruh aspek pada sistem. Selanjutnya, dilakukan penyesuaian agar sesuai dengan standar yang telah ditetapkan oleh NIST Cybersecurity Framework. Penyesuaian ini melibatkan integrasi aspek-aspek resistensi terhadap serangan siber dan ketahanan siber, seperti kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Dengan demikian, penelitian ini bertujuan untuk mengoptimalkan kerangka kerja keamanan siber berdasarkan pedoman NIST, sehingga sistem dapat lebih efektif dalam melindungi informasi dan menjaga keberlanjutan operasionalnya melawan berbagai ancaman siber.

Website yang menjadi subjek penelitian ini adalah oase.poltektegal.ac.id, sebuah platform yang digunakan untuk pengolahan nilai mahasiswa. Kehadiran website ini memiliki signifikansi penting dalam konteks akademis, oleh karena itu, penyesuaian berdasarkan pedoman NIST Cybersecurity Framework menjadi langkah krusial. Dengan menerapkan standar keamanan dari NIST, diharapkan website ini akan menjadi lebih tangguh terhadap potensi serangan siber yang mungkin dilakukan oleh peretas di masa mendatang. Upaya penyesuaian tersebut bertujuan untuk memperkuat tingkat keamanan, menjaga integritas data, dan memastikan ketersediaan sistem, sehingga website dapat beroperasi secara aman dan efisien.

II. PENELITIAN YANG TERKAIT

Tahap Information Gathering menjadi langkah komprehensif dalam mengenali target dengan tujuan memperoleh berbagai informasi, termasuk status atau tipe jaringan, jenis sistem operasi yang sedang digunakan, rentang alamat IP yang dipakai, port yang terbuka, dan server DNS yang tengah aktif. Pentingnya tahap ini tidak hanya terbatas pada pengungkapan teknis tetapi juga bisa memungkinkan identifikasi kepemilikan suatu sistem. Dengan menggali informasi ini secara mendalam, pihak yang melakukan Information Gathering dapat memahami dengan lebih baik lanskap teknologi suatu entitas, yang kemudian dapat digunakan untuk berbagai tujuan analisis, keamanan, dan pengambilan keputusan [1].

Data yang diperoleh menjadi elemen krusial sebagai pendukung tahap asesmen berikutnya. Alat bantu dalam proses Information Gathering telah melimpah dan tersedia di berbagai sistem operasi, khususnya yang dirancang untuk kegiatan pengujian keamanan informasi atau layanan jasa pengujian keamanan situs web. Dengan memanfaatkan informasi-informasi yang terkumpul ini, tim keamanan dapat memperoleh wawasan yang mendalam terkait dengan konfigurasi dan kelemahan potensial dalam sistem yang dievaluasi. Hal ini menjadi pondasi yang kokoh untuk menghadapi tahapan analisis keamanan dan memastikan bahwa langkah-langkah selanjutnya dalam asesmen dapat dilakukan dengan lebih terarah dan efisien [7]. Meskipun alat bantu yang ada mungkin tidak sepenuhnya memenuhi kebutuhan analis atau penguji keamanan siber secara menyeluruh, inilah yang mendorong pengembangan aplikasi Sudomy. Aplikasi ini dirancang untuk memberikan dukungan yang lebih komprehensif pada tahapan Information Gathering dengan menerapkan metode hybrid scan. Pendekatan hybrid scan yang diimplementasikan oleh Sudomy diharapkan dapat memberikan keunggulan dalam melengkapi kelemahan yang mungkin dimiliki oleh alat bantu yang sudah ada. Dengan demikian, aplikasi ini bertujuan untuk memperkaya pengalaman analis keamanan siber, memberikan alat yang lebih efektif, dan meningkatkan kemampuan dalam mengidentifikasi dan mengelola informasi yang diperlukan selama proses Information Gathering [8].

Penelitian ini bertujuan untuk mengidentifikasi kelemahan keamanan pada website Lembaga X melalui penerapan metode penetration testing dengan menggunakan Framework ISSAF. Framework ISSAF mencakup sembilan aspek penilaian yang melibatkan Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Privilege Escalation, Enumerating Further, Compromise Remote User/Sites, Maintaining Access, dan Covering Tracks. Sebanyak 18 celah keamanan berhasil diidentifikasi pada website Lembaga X sebagai hasil dari penelitian ini. Rekomendasi telah disusun untuk meningkatkan tingkat keamanan pada website Lembaga X, sebagai upaya proaktif untuk mengatasi dan mencegah potensi risiko yang teridentifikasi selama proses penetration testing [9].

Penelitian ini bertujuan untuk mengidentifikasi kerentanan pada website Universitas ARS dan melakukan uji serta analisis untuk mengevaluasi kondisi kerentanan tersebut dengan menggunakan standar keamanan dari OWASP. Metode penelitian mengadopsi parameter keamanan yang

dijelaskan dalam OWASP Top-10 2017. Hasil dari seluruh pengujian kerentanan menunjukkan bahwa website Universitas ARS memiliki tingkat keamanan yang sangat baik. Website ini memenuhi ketiga aspek keamanan informasi, serta menunjukkan keamanan yang solid pada web server dan perangkat lunak sistem informasi akademik yang digunakan [10].

Aplikasi yang diimplementasikan dalam fase asesmen melibatkan penggunaan Sudomy. Sudomy merupakan aplikasi yang dirancang dengan mengadopsi metode active scan dan passive scan, berfungsi sebagai alat pendukung dalam pengujian keamanan informasi pada tahapan Information Gathering dan Network Mapping. Beberapa fitur utama Sudomy mencakup pemeriksaan Host pada subdomain aktif, pengumpulan informasi HTTP status code response, konversi dari daftar subdomain ke Resolver IP, pemindaian port dari Resolver IP, pengecekan potensi serangan Subdomain Take-Over, pengambilan tangkapan layar melalui daftar domain, serangan DNS Bruteforce Subdomain, dan penyajian laporan interaktif. Walaupun Sudomy memiliki keunggulan dalam fitur-fiturnya, kelemahannya terletak pada penggunaan antarmuka berbasis teks atau CLI (Command Line Interface), yang belum mendukung antarmuka grafis untuk memudahkan pengguna [11].

Aplikasi Bangkolo, yang diterapkan dalam tahap Identifikasi Kerentanan, memadukan keunggulan Nmap sebagai aplikasi berbasis Command Line Interface (CLI) dengan kerangka pengembangan multiplatform berbasis Javascript, yakni ElectronJS. Melalui pengintegrasian ini, aplikasi Bangkolo menghasilkan antarmuka pengguna berbasis GUI (Graphical User Interface). Dengan demikian, aplikasi ini menyajikan kemudahan penggunaan dan visualisasi data yang lebih intuitif, menjembatani kesenjangan antara kinerja unggul aplikasi CLI dan kemudahan penggunaan GUI, yang memperkaya pengalaman pengguna dalam mengidentifikasi kerentanan pada suatu sistem [12].

Penelitian ini mengusulkan pengembangan aplikasi Sudomy yang berbasis grafis dengan menerapkan metode HybridApps, yang mengintegrasikan teknologi native dari Command Line Interface (CLI) dan teknologi web sebagai antarmuka grafis. Meskipun aplikasi ini memiliki antarmuka grafis, fitur dan fungsi secara menyeluruh tetap mengadopsi Sudomy. Pengembangan aplikasi menggunakan metode HybridApps menggabungkan kelebihan dari teknologi CLI dan teknologi web, menciptakan platform tunggal yang menggabungkan kemudahan penggunaan aplikasi berbasis grafis dengan keunggulan fungsionalitas Sudomy. Hasil dari penelitian ini adalah aplikasi Information Gathering yang berbasis grafis, memberikan kemudahan penggunaan dalam proses pengujian keamanan sistem dan jaringan komputer [13].

Dalam penelitian ini, analisis keamanan informasi dilakukan menggunakan perangkat lunak dengan lisensi Free Open Source Software, yaitu Sudomy dan OWASP ZAP. Pemanfaatan kedua perangkat lunak ini menghasilkan analisis mendalam terhadap potensi celah keamanan yang mungkin ada pada sistem informasi yang diimplementasikan di Universitas Duta Bangsa. Dengan pendekatan ini, penelitian dapat memberikan wawasan yang komprehensif terkait dengan keamanan sistem informasi, melibatkan penggunaan alat-alat yang didukung oleh sumber terbuka untuk menganalisis dan mengidentifikasi potensi risiko serta kerentanan dalam lingkungan universitas tersebut [14].

Penelitian ini melakukan analisis terhadap serangan web phishing yang dilakukan oleh phiser, yang melibatkan penggunaan fitur fake login. Dalam proses ini, berhasil diperoleh file capture Wireshark dari web phishing yang menggunakan protokol HTTPS. Analisis mendalam dilakukan terhadap pendekripsian fitur keamanan yang terkandung dalam protokol HTTPS, termasuk URL phishing, sistem Domain Name System (DNS) yang dimanfaatkan oleh pelaku, alamat IP server, alamat IP tujuan, identitas penyerang, dan informasi email yang digunakan oleh phiser untuk menjalankan tindakan kejahatannya dan memperoleh akun valid dari korban [15].

Analisis terhadap sistem keamanan jaringan dilaksanakan menggunakan Framework NIST (National Institute of Standards Technology), suatu kerangka kerja yang dirancang khusus untuk perhitungan kualitatif berdasarkan analisis sistem keamanan. Pada penelitian risiko keamanan jaringan di sebuah perusahaan perbankan, menggunakan NIST SP800-30, berhasil mengidentifikasi beberapa temuan. Ditemukan bahwa sistem keamanan jaringan yang telah beroperasi selama ini menghadapi risiko rendah terkait dengan backdoor, sedangkan risiko pada packet sniffing, spoofing, dan rootkit berada pada tingkat sedang. Selain itu, temuan menunjukkan bahwa risiko yang terkait dengan DDoS memiliki tingkat risiko yang tinggi pada sistem keamanan jaringan perusahaan tersebut [16].

Penelitian ini memanfaatkan dua alat forensik, yaitu Wondershare dr. Fone for Android dan Oxygen Forensics Suite 2014, untuk mendapatkan bukti digital berupa data kontak, log panggilan, dan pesan yang telah dihapus pada smartphone Android. Proses analisis bukti digital ini dilakukan dengan menerapkan metode National Institute of Standards and Technology (NIST). Hasil penelitian menunjukkan bahwa Wondershare dr. Fone for Android berhasil mengembalikan data terhapus dengan tingkat keberhasilan sebesar 30%, sedangkan Oxygen Forensics Suite 2014 mencapai tingkat keberhasilan sebesar 73%. Dari temuan ini, dapat disimpulkan bahwa bukti digital hasil pemulihan dengan Oxygen Forensics Suite 2014 dapat diandalkan sebagai barang bukti yang valid dalam konteks persidangan [17].

Berdasarkan tinjauan pustaka yang telah disampaikan, peneliti memutuskan untuk melakukan penelitian dengan mengintegrasikan hasil dari tahap Information Gathering ke dalam kerangka kerja NIST Cybersecurity. Tujuannya adalah menciptakan patokan kerangka kerja yang memiliki ketangguhan terhadap serangan siber. Dengan demikian, penelitian ini bertujuan untuk memanfaatkan panduan dan standar keamanan yang diperoleh dari NIST Cybersecurity Framework sebagai landasan untuk memperkuat kerangka keamanan yang sudah ada dan menjadikannya lebih resisten terhadap potensi serangan siber.

III. METODE PENELITIAN

Dalam kerangka penelitian ini, metodologi yang diadopsi secara umum mengintegrasikan dua pendekatan utama. Pertama, menggunakan pendekatan proses forensik untuk mendapatkan informasi melalui observasi yang terfokus pada website yang menjadi objek penelitian. Kedua, menggunakan

ISSN: 2477-5126
e-ISSN: 2548-9356

studi pustaka sebagai sumber referensi teoritis dan landasan penelitian untuk mendukung analisis dan pemahaman tema yang menjadi fokus penelitian. Kombinasi kedua pendekatan ini memberikan gambaran yang komprehensif dalam pelaksanaan kegiatan penelitian ini, sebagaimana tergambarkan pada Gbr. 1.

Gbr. 1 N.I.S.T. Cybersecurity Framework (NIST-CSF)

A. Metode Pendekatan Proses Forensic

Tahapan-tahapan yang diterapkan dalam proses forensik terdiri dari beberapa langkah kunci. Pertama, tahap Identifikasi (Identify) di mana data didokumentasikan dan dikategorikan secara fundamental. Tahap kedua adalah Melindungi (Protect), yang melibatkan pengembangan perlindungan untuk semua layanan yang krusial. Selanjutnya, tahap Mendeteksi (Detect) fokus pada identifikasi peristiwa ancaman keamanan dan risiko. Tahap keempat adalah Merespon (Respond), yang melibatkan perencanaan respons secepat mungkin untuk menanggulangi serangan. Terakhir, tahap Memulihkan (Recover) mencakup perencanaan jangka panjang untuk pemulihan aset yang mungkin hilang dalam insiden tersebut. Setiap tahapan ini merupakan langkah kunci dalam proses forensik untuk menanggapi dan merespons kejadian keamanan.

B. Metode Pengumpulan Data

Dalam penyusunan penelitian ini, kegiatan pengumpulan data dilakukan melalui berbagai metode. Pertama, dengan memeriksa bahan-bahan tertulis seperti buku dan melakukan browsing melalui internet, yang sering disebut sebagai Library Research. Selanjutnya, peneliti memperoleh data yang relevan melalui observasi, baik secara virtual maupun nonvirtual. Pada observasi virtual, peneliti mengunjungi website oase.poltektegal.ac.id, sementara pada observasi nonvirtual, kunjungan langsung dilakukan ke Unit Pelaksana Teknis Sistem Informasi. Kombinasi metode ini memastikan keragaman dan kelengkapan data yang diperoleh, memberikan landasan yang kokoh untuk penelitian ini.

IV. HASIL DAN PEMBAHASAN

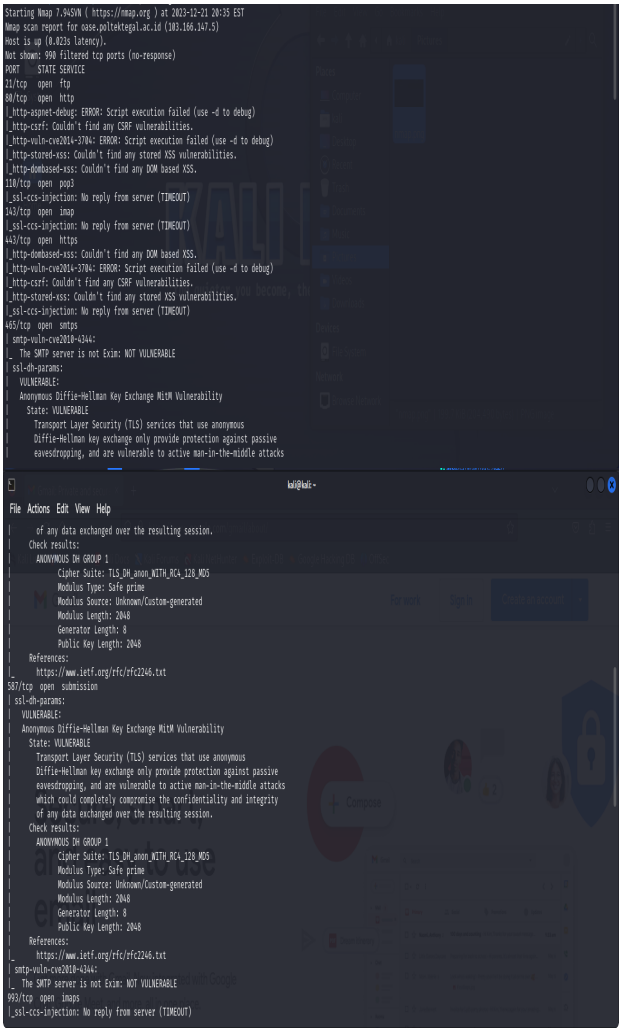
A. Pengecekan Server

Untuk melakukan pengecekan server, menggunakan aplikasi nikto dengan perintah nikto -h oase.poltektegal.ac.id -ssl seperti terlihat pada Gbr. 2.

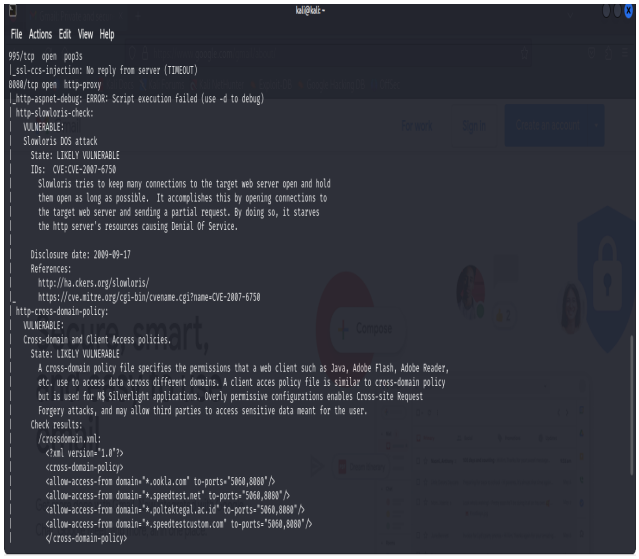
Gbr. 2 Pengecekan Server dengan nikto

B. IP PORT

Untuk melakukan scan IP PORT menggunakan aplikasi nmap dengan perintah nmap -sV -sS -p- --script vuln 103.166.147.5 seperti terlihat pada Gbr. 3.



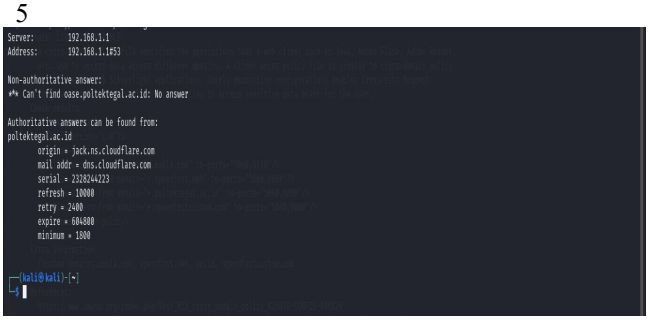
ISSN: 2477-5126
e-ISSN: 2548-9356



Gbr. 4. Pengecekan IP PORT menggunakan nmap

C. NSLOOKUP

Melakukan pengecekan DNS Server dengan menggunakan perintah nslookup, dapat dilihat pada Gbr. 5



Gbr. 5. Pengecekan DNS Server menggunakan nslookup

Dari hasil pemeriksaan server, port IP, dan NSlookup, beberapa kerentanan berhasil diidentifikasi yang sesuai dengan kerangka kerja keamanan NIST Cybersecurity yaitu :

CVE-2003-1418 merupakan sebuah kerentanan pada web server Apache yang memungkinkan potensi serangan jarak jauh (remote access). Kerentanan ini memungkinkan penyerang untuk mengakses informasi sensitif melalui header Etag, yang menampilkan nomor inode atau multipart MIME boundary untuk menampilkan Child process IDs (PID).

CVE-2005-3299 merupakan sebuah kerentanan pada penyertaan file PHP di file grab_globals.lib.php pada versi phpMyAdmin 2.6.4 dan 2.6.4-pl1. Kerentanan ini memungkinkan penyerang jarak jauh untuk menyisipkan file lokal melalui parameter $__redirect, yang pada gilirannya memungkinkan penggunaan subform array.

CVE-2010-4344 merupakan sebuah kerentanan berupa buffer overflow berbasis heap yang terdapat pada fungsi string_vformat dalam file string.c. Kerentanan ini memungkinkan serangan jarak jauh dengan kemampuan eksekusi kode arbiter selama sesi SMTP.

CVE-2007-6750 adalah sebuah kerentanan yang memungkinkan serangan jarak jauh dan dapat menyebabkan penolakan layanan dengan cara mematikan daemon melalui permintaan HTTP parsial. Umumnya, kerentanan ini terkait dengan kekurangan modul mod_reqtimeout,

Referensi, saran, solusi, dan alat untuk memperbaiki kerentanan tersebut dapat ditemukan dengan melakukan patch pada masing-masing celah keamanan. Patch ini umumnya disediakan oleh vendor perangkat lunak yang bersangkutan, dan diterapkan sebagai upaya untuk mengatasi kelemahan keamanan yang teridentifikasi. Menggunakan patch-patch yang diberikan oleh vendor merupakan praktik umum dalam menjaga dan meningkatkan keamanan sistem, sehingga perangkat lunak yang digunakan dapat tetap aman dari potensi risiko keamanan.

V. KESIMPULAN

Secara komprehensif, pengumpulan informasi memiliki peran penting dalam memberikan kontribusi berharga untuk peningkatan NIST Cybersecurity Framework. Melalui pendekatan ini, diharapkan bahwa ketahanan siber dapat diperkuat dan resistensi terhadap serangan siber dapat dibangun. Menyimak situasi saat ini, terdapat potensi kerentanan pada website oase.poltektegal.ac.id terhadap serangan siber. Oleh karena itu, disarankan agar UPT Sistem Informasi merespons dengan konsisten melakukan pembaruan perangkat lunak guna meningkatkan tingkat keamanan dan mengurangi risiko terhadap serangan siber yang mungkin terjadi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan bantuan dan dukungan terkait dengan penelitian ini, termasuk fasilitas penelitian, dana hibah, dan kontribusi lainnya.

DAFTAR PUSTAKA

[1] M. Zeeshan, S. Un Nisa, T. Majeed, N. Nasir and S. Anayat, "Vulnerability Assessment and Penetration Testing: A proactive approach towards Network and Information Security," *International Journal of Digital Information and Wireless Communications,* pp. 124-142, 2017.

[2] H. H. R, E. N. L and H. R, "Analisis Uji Penetrasi Menggunakan ISSAF," *Hacking Digit, Forensics Expo,* pp. 32-40, 2017.

[3] R. B, Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1B, Open Information Systems Security Group, 2006.

[4] R. Sahtyawan, "PENERAPAN ZERO ENTRY HACKING DIDALAM SECURITY MISCONFIGURATION PADA VAPT (VULNERABILITY ASSESSMENT AND PENETRATION TESTING)," *JURNAL OF INFORMATION SYSTEM MANAGEMENT,* vol. 1, pp. 18-22, 2019.

[5] "https://www.nist.gov/cyberframework," 2023. [Online].

[6] M. Antunes, M. Maximiano, R. Gomes and D. Pinto, "Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal," *Journal Of Cybersecurity Privacy,* pp. 219-238, 2021.

[7] M. Denis, C. Zena and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies. 2016

ISSN: 2477-5126
e-ISSN: 2548-9356

IEEE Long Island Systems," *Applications and Technology Conference, LISAT 2016.,* 2016.

[8] M. Riasetiawan, A. Wisnuaji, D. Hariyadi and T. Febrianto, "PENGEMBANGAN APLIKASI INFORMATION GATHERING MENGGUNAKAN METODE HYBRID SCAN BERBASIS GRAPHICAL USER INTERFACE," *CyberSecurity dan Forensik Digital,* vol. 4, pp. 44-48, 2021.

[9] I. G. A. S. SANJAYA, G. M. A. SASMITA and D. M. S. ARSA, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi),* vol. 8, pp. 113-124, 2020.

[10] S. H. d. D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *Jurnal Algoritma,* vol. 18, no. 1, pp. 77-86, 2021.

[11] R. A. Ramadhan, R. M. Aresta and D. Hariyadi, "Sudomy: Information Gathering Tools for Subdomain Enumeration and Analysis," *IOP Conference Series: Materials Science and Engineering,* 2020.

[12] D. Hariyadi, F. and H. Wijayanto, "BANGKOLO: APLIKASI VULNERABILITY IDENTIFICATION BERBASIS HYBRID APPS," *CyberSecurity dan Forensik Digital,* pp. 39-44, 2020.

[13] C. B. Setiawan, D. Hariyadi, A. Sholeh and A. Wisnuaji, "Pengembangan Aplikasi Information Gathering Berbasis HybridApps," *INTEK,* vol. 5, pp. 22-28, 2022.

[14] D. Hariyadi and F. E. Nastiti, "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta," *Jurnal Komtika (Komputasi dan Informatika),* vol. 5, pp. 35-42, 2021.

[15] A. Nofiyan and M. Mushlihudin, "Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST)," *Jurnal Sarjana Teknik Informatika,* vol. 8, pp. 11-23, 2020.

[16] f. panjaitan and A. Aprilo, "ANALISIS MANAJEMEN RISIKO KEAMANAN JARINGAN MENGGUNAKAN FRAMEWORK NIST," *Jurnal Ilmiah Matik ,* vol. 24, pp. 71-81, 2022.

[17] r. Umar and S. Sahiruddin, "METODE NIST UNTUK ANALISIS FORENSIK BUKTI DIGITAL PADA PERANGKAT ANDROID," *SEMINAR NASIONAL MULTI DISIPLIN ILMU DAN CALL FOR PAPERS /,* 2019.