Jurnal Transformasi Pendidikan Vol. 6, No. 3
https://ejurnals.com/ojs/index.php/jtp Juli 2025

PENERAPAN PENETRATION TESTING PADA WEBSITE LAPORAN HARIAN POLDA ACEH MENGGUNAKAN METODE NIST

Gadis Tri Wandinil[1], Raihan Islamadina[2]
[1,2]Universitas Islam Negeri Ar-Raniry
210212007@student.ar-raniry.ac.id

ABSTRAK

Penelitian ini mengusulkan penerapan penetration testing pada website "Laporan Harian Polda Aceh" menerapkan metodologi Institut Standar dan Teknologi Nasional (NIST)sebagai upaya untuk meningkatkan sistem keamanan aplikasi web yang digunakan oleh instansi kepolisian. Penelitian dilakukan dengan pendekatan kualitatif yang melibatkan studi pustaka, analisis dokumen, serta simulasi pengujian secara praktis menggunakan alat-alat keamanan seperti OWASP ZAP. Dalam penelitian ini, tahap-tahap pengujian meliputi perencanaan dan persiapan, pengumpulan informasi, pemindaian dan identifikasi kerentanan, eksploitasi, evaluasi pascapenetrasi, serta penyusunan laporan. Setiap tahap dilakukan secara sistematis sesuai pedoman NIST SP 800-115 untuk mengidentifikasi dan mengklasifikasikan celah keamanan yang terdapat dalam aplikasi "Laporan Harian Polda Aceh". Hasil penelitian menunjukkan bahwa website tersebut rentan terhadap berbagai ancaman siber, seperti pencurian data dan eksploitasi kerentanan sistem, yang berpotensi mengganggu operasional dan integritas data. Dengan menerapkan metode NIST, proses pengujian tidak hanya berhasil menemukan kerentanan kritis, tetapi juga memberikan rekomendasi perbaikan yang komprehensif guna meningkatkan standar keamanan sistem. Diharapkan lembaga pemerintah lainnya dapat menggunakan temuan ini sebagai panduan. mengimplementasikan sistem keamanan informasi yang lebih robust guna melindungi data penting dan menjaga kontinuitas layanan.

Kata Kunci: Penetration Testing, Metode NIST, Keamanan Aplikasi Web, Laporan Harian Polda Aceh, Kerentanan Siber, Evaluasi Risiko.

ABSTRACT

This study proposes the implementation of penetration testing on the "Laporan Harian Polda Aceh" website utilizing the National Institute of Standards and Technology (NIST) approach in an attempt to improve the police department's online application's security system.The research is conducted through a qualitative approach involving literature review, document analysis, and practical simulation of security testing using tools such as OWASP ZAP. In this research, the testing process encompasses planning and preparation, information gathering,

vulnerability scanning and identification, exploitation, post-penetration evaluation, and report compilation. Each phase is executed systematically in accordance with the guidelines provided by NIST SP 800-115 to identify and classify vulnerabilities present in the "Laporan Harian Polda Aceh" application. The results indicate that the website is susceptible to various cyber threats, including data breaches and system vulnerability exploits, which could potentially disrupt operations and compromise data integrity. By employing the NIST method, the testing process not only successfully uncovers critical vulnerabilities but also provides comprehensive recommendations for enhancing the system's security standards. These findings are expected to serve as a reference for other governmental institutions in implementing more robust information security systems to protect vital data and ensure service continuity

Keywords: *Penetration Testing, NIST Method, Web Application Security, Laporan Harian Polda Aceh, Cyber Vulnerabilities, Risk Assessment.*

A. PENDAHULUAN

Di era abad 21, kemajuan teknologi telah memudahkan di seluruh aspek kehidupan, meskipun tampak mudah, sebenarnya tersimpan potensi ancaman siber yang semakin canggih dan terstruktur. Peningkatan interaksi digital diikuti dengan meningkatnya risiko serangan yang dapat mengancam integritas data dan operasional sistem informasi. Pentingnya perlindungan data dan keamanan siber bagi instansi pemerintah Indonesia ditunjukkan dengan peraturan seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE).

Polda Aceh, sebagai salah satu instansi yang memiliki peran strategis dalam menjaga keamanan dan kesatuan negara, telah mengembangkan aplikasi web "Laporan Harian Polda Aceh" untuk mendukung kinerja personel di berbagai satuan kerja. Aplikasi ini digunakan secara rutin oleh seluruh Polres dan Satker di wilayah Aceh untuk mengirim dan menerima laporan kegiatan. Namun, tingginya potensi serangan siber yang menargetkan aplikasi ini mengindikasikan bahwa masih terdapat celah keamanan yang perlu segera diatasi guna mencegah pencurian data dan serangan lainnya.

Penetration Testing (Pentest) ialah metode efektif dalam mengevaluasi dan meningkatkan keamanan aplikasi web dengan mensimulasikan serangan dari pihak yang berwenang. Metode ini, yang meliputi pengumpulan informasi, identifikasi kerentanan, eksploitasi kelemahan, hingga pelaporan temuan, didasarkan pada teori-teori keamanan siber dan praktik ilmiah dalam ilmu komputer. Penerapan metode NIST, sebagaimana dijelaskan

dalam NIST Special Publication 800-115, menawarkan pendekatan yang komprehensif dan terstandarisasi dalam pelaksanaan uji penetrasi. Oleh karena itu, penelitian ini mengusulkan simulasi penetration testing pada aplikasi "Laporan Harian Polda Aceh" menggunakan metode NIST sebagai upaya untuk mengidentifikasi celah keamanan serta memberikan rekomendasi perbaikan guna meningkatkan standar keamanan sistem secara menyeluruh.

B. KAJIAN PUSTAKA

Deskripsi Teori

Kajian pustaka ini menyajikan landasan teori yang menjadi dasar penelitian mengenai penerapan penetration testing pada aplikasi web "Laporan Harian Polda Aceh". Teori-teori yang dikaji mencakup aspek hukum, faktor kerentanan, metodologi penetration testing, standar NIST, dan konteks operasional aplikasi yang menjadi objek penelitian.

1. Dasar Hukum

Meningkatnya frekuensi serangan siber baik di dalam negeri maupun internasional menjadikan keamanan sistem informasi sebagai prioritas utama. Undang-undang seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah pada tahun 2016, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), dan Undang-Undang Nomor 71 Tahun 2019 tentang Perlindungan Data Pribadi menegaskan kewajiban administrator sistem untuk menjamin keamanan dan integritas data. Aturan-aturan ini memberikan landasan hukum yang kuat untuk menetapkan persyaratan keamanan dan mendisiplinkan mereka yang melanggar tugas keamanan informasi.

2. Faktor Kerentanan

Pentingnya menjaga ketersediaan, kerahasiaan, dan integritas data didukung oleh teori keamanan siber (CIA Triad). STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) adalah model ancaman lainnya.digunakan untuk mengidentifikasi potensi risiko yang mungkin terjadi. Faktor kerentanan pada aplikasi web umumnya disebabkan oleh kesalahan pengkodean, penggunaan perangkat lunak usang, kurangnya pembaruan sistem, dan ketidakpatuhan terhadap praktik keamanan terbaik, yang secara kolektif meningkatkan risiko serangan siber.

3. Penetration Testing (Pen Testing)

Penetration Testing merupakan metode pengujian keamanan yang mensimulasikan serangan oleh pihak yang tidak berwenang untuk mengidentifikasi celah dan kelemahan dalam sistem atau aplikasi. Proses ini melibatkan beberapa tahap, antara lain pengumpulan informasi, pemindaian kerentanan, eksploitasi, dan pelaporan temuan. Metode ini sangat penting untuk mengukur efektivitas kontrol keamanan yang ada dan memberikan rekomendasi perbaikan yang diperlukan guna menjaga integritas dan ketersediaan sistem.

4. NIST

Teori keamanan siber (CIA Triad) mendukung pentingnya menjaga ketersediaan, kerahasiaan, dan integritas data. Model ancaman lainnya disebut STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Pedoman NIST SP 800-115 menyediakan kerangka kerja terstruktur untuk melaksanakan penetration testing secara sistematis, mulai dari perencanaan, pelaksanaan, hingga analisis dan pelaporan hasil. Standar NIST sangat relevan untuk instansi pemerintah karena pendekatannya yang komprehensif, terstandarisasi, dan terbukti efektif dalam mengidentifikasi kerentanan.

5. Aplikasi Laporan Harian Polda Aceh

Aplikasi Laporan Harian Polda Aceh merupakan sistem informasi yang dirancang untuk memudahkan proses pelaporan kegiatan oleh Polres dan Satker di wilayah Aceh. Aplikasi ini menjadi tulang punggung komunikasi dan evaluasi kinerja operasional, sehingga keamanannya sangat krusial. Rentannya aplikasi terhadap serangan siber menuntut penerapan metode pengujian keamanan seperti penetration testing agar dapat mengidentifikasi celah yang ada dan mengimplementasikan perbaikan yang diperlukan untuk menjaga integritas data dan kontinuitas layanan.

Proses Penerapan Penetration Testing

Proses penerapan penetration testing pada aplikasi web "Laporan Harian Polda Aceh" melibatkan serangkaian langkah sistematis yang dirancang untuk mendeteksi dan mengatasi kerentanan. Proses tersebut meliputi:

1. Menetapkan ruang lingkup pengujian, memperoleh izin dari pihak berwenang, dan mempersiapkan sumber daya, termasuk tim penguji dan alat yang akan digunakan.

2. Mengidentifikasi data sistem, alamat IP, konfigurasi jaringan, dan informasi terkait lainnya melalui teknik OSINT dan pemetaan jaringan.
3. Menggunakan alat seperti Nmap, Nessus, atau OWASP ZAP untuk mendeteksi port terbuka, layanan yang berjalan, serta celah keamanan yang ada.
4. Melakukan simulasi serangan untuk mengeksploitasi kelemahan yang ditemukan, dengan tujuan menguji efektivitas kontrol keamanan yang ada.
5. Menyusun laporan komprehensif yang mencakup temuan, dampak potensial, serta rekomendasi perbaikan, diikuti dengan evaluasi pascapenetrasi untuk memastikan sistem kembali ke kondisi semula.

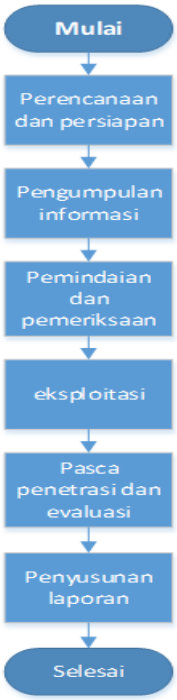
Hipotesis

Berdasarkan uraian teori dan proses di atas, hipotesis penelitian ini adalah:

Setelah penerapan penetration testing pada aplikasi "Laporan Harian Polda Aceh" menggunakan metode NIST, ditemukan adanya celah keamanan yang perlu segera ditindaklanjuti untuk meningkatkan standar keamanan dan mencegah serangan siber lebih lanjut

C. METODE PENELITIAN

Berikut merupakan diagram dari alur penelitian:



Gambar 1 flowchart alir

Penelitian ini menggunakan pendekatan kualitatif untuk mengevaluasi keamanan aplikasi "Laporan Harian Polda Aceh" melalui penerapan penetration testing dengan acuan standar NIST SP 800-115. Proses penelitian diringkas dalam beberapa langkah sistematis sebagai berikut:

Perencanaan dan Persiapan:

1. Menetapkan tujuan uji penetrasi dan menentukan ruang lingkup aplikasi yang akan diuji.
2. Mendapatkan izin tertulis dari pihak berwenang dan menentukan tim penguji yang kompeten untuk melakukan pengujian.
3. Pengumpulan Informasi
4. Mengumpulkan data awal mengenai target, seperti alamat IP, struktur jaringan, dan informasi relevan lainnya.
5. Menggunakan teknik *Black Box* dan alat pemindaian untuk mengidentifikasi informasi yang dapat mendukung tahap pengujian.

Pemindaian dan Penilaian

1) Melakukan pemindaian untuk mendeteksi port terbuka, layanan aktif, dan komponen sistem lainnya menggunakan alat seperti Nmap dan Nessus.
2) Menganalisis temuan pemindaian untuk menilai keparahan serta potensi dampak kerentanan terhadap sistem.

Eksploitasi

1. Mensimulasikan serangan dengan mengeksploitasi celah yang ditemukan untuk menguji efektivitas kontrol keamanan.
2. Menggunakan teknik eksploitasi manual maupun otomatis guna memperoleh akses yang tidak sah sebagai indikasi kelemahan sistem.

Pascapenetrasi dan Evaluasi

1) Menganalisis hasil eksploitasi dan mengevaluasi akses yang berhasil diperoleh selama pengujian.
2) Mengembalikan sistem ke kondisi semula dengan menghapus semua jejak yang tertinggal selama proses uji penetrasi.

Penyusunan Laporan

1. Menyusun laporan komprehensif yang mendokumentasikan seluruh temuan, mencakup deskripsi kerentanan, teknik eksploitasi yang digunakan, dampak yang mungkin terjadi, dan rekomendasi perbaikan.
2. Laporan ini digunakan sebagai dasar untuk pengembangan kebijakan keamanan dan perbaikan sistem di lingkungan instansi.

Akumulasi Data

Data diperoleh melalui proses pengujian yang mengikuti langkah-langkah standar dalam NIST SP 800-115, di mana alat-alat seperti Nmap, Nessus, dan OWASP ZAP digunakan untuk memetakan jaringan, memindai kerentanan, dan melakukan eksploitasi. Seluruh informasi yang dikumpulkan, mulai dari konfigurasi sistem hingga temuan eksploitasi, dianalisis secara kualitatif guna mengidentifikasi serta memprioritaskan celah keamanan berdasarkan risiko dan potensi dampaknya terhadap operasional aplikasi.

Pendekatan kualitatif dalam penelitian ini memungkinkan pemahaman mendalam terhadap konteks di balik kerentanan yang ditemukan, serta memberikan insight tentang faktor-faktor teknis dan organisasi yang mempengaruhi keamanan sistem. Metode ini juga menyediakan fleksibilitas untuk menyesuaikan strategi pengujian seiring dengan munculnya temuan baru, sehingga hasil penelitian dapat memberikan rekomendasi perbaikan yang komprehensif dan aplikatif

D. HASIL DAN PEMBAHASAN

1. Planning

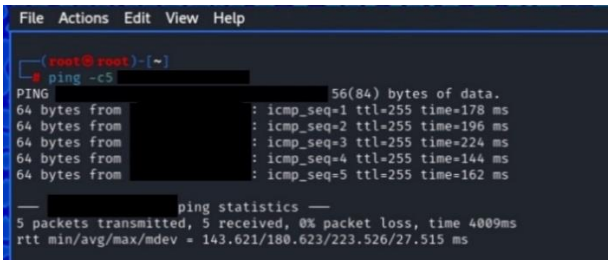
Pada tahapan ini membahas mengenai ruang lingkup penelitian, hardware yang digunakan pada penelitian, software yang digunakan pada penelitian serta teknik yang digunakan pada saat penelitian

2. Discovery

a. Information Gathring

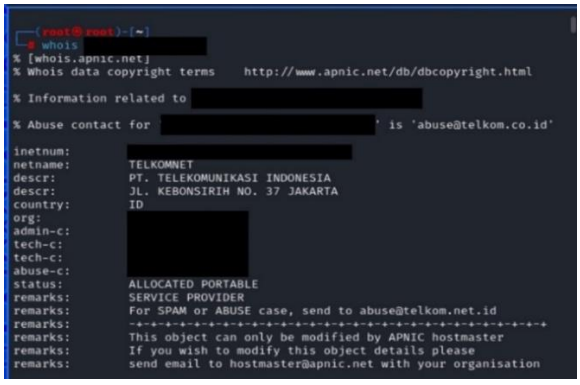
Pengumpulan Data pada metode ini dilakukan untuk mendapatkan informasi dari sample penelitian. Teknik yang digunakan adalah teknik Black Box, perintah ping -c5 "Ip

Adrees" merupakan langkah awal yang harus dijalankan untuk melihat kecepatan sistem informasi dalam mengirim paket data, seperti pada gambar 4.1.



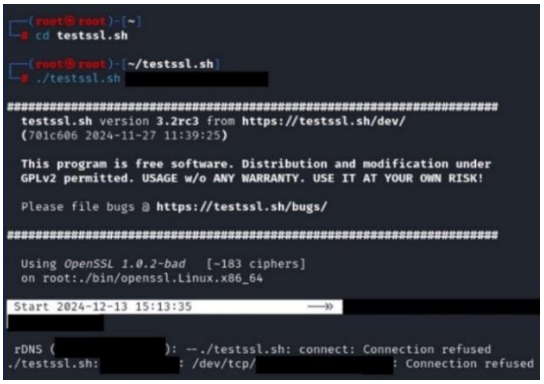
Gambar 4.1 Hasil *nmap* pada *DNS*

Hasil ping yang layak adalah kurang dari 100 milidetik (ms), yang merupakan waktu respons host. Durasi dalam detik paket data berada di jaringan dikenal sebagai time to live (TTL). Jalankan perintah whois “IP Address” untuk mendapatkan informasi sistem yang lebih detail, seperti terlihat pada gambar di bawah ini., seperti pada gambar 4.2.



Gambar 4.2 Hasil *Whois* Pada *IP Address*.

Output perintah ini berhasil menampilkan informasi aplikasi yang komprehensif. Perintah cd testssl.sh harus dijalankan selanjutnya, diikuti dengan perintah./testssl.sh "Alamat IP", Seperti pada gambar 4.3

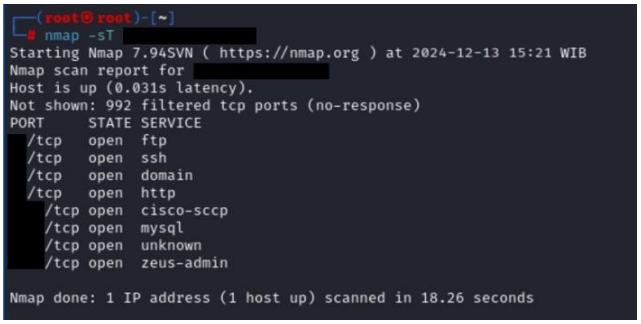


Gambar 4.2 Hasil *Testssl* Pada *IP Addres*.

Sesuai gambar, aplikasi online tersebut tidak memiliki SSL atau TLS yang merupakan standar keamanan jaringan sistem informasi.

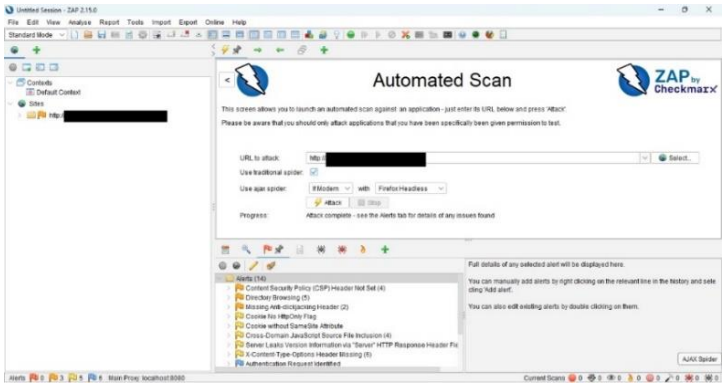
b. Vulnerability Scanning

Pada titik ini, nmap digunakan untuk memindai program. Di sini, perintah *nmap -sT "IP Address"* digunakan untuk melihat port terbuka aplikasi web, seperti yang ditunjukkan pada gambar di bawah.



Gambar 4.3 Hasil *nmap* Pada *IP Addres*.

Langkah selanjutnya adalah melakukan scanning menggunakan *framework Zap*, seperti terlihat pada gambar di bawah ini, setelah hasil scan dari nmap tool menunjukkan bahwa beberapa port di server terbuka.



Gambar 4.4 Proses *Scanning* menggunakan *Zap*.

Aplikasi online memiliki beberapa kerentanan, seperti yang ditunjukkan oleh temuan pemindaian kerangka kerja OWASP Zap, yang mengungkapkan beberapa tingkatan kerentanan. Hasil pemindaian dengan framework OWASP Zap adalah sebagai berikut.

Table 4.2 Hasil Proses *scanning* berdasarkan level

Risk Level	Number of Allert
High	0
Medium	3
Low	5
Informational	6

Berikut merupakan detail dari penjelasan Scanning menggunakan framework Zap.

Table 4.2 Hasil *Vulenerability Scanning Zap*

No	***Allert***	***Description***	***Risk Level***	***Solution***
1.	*Absence of Anti-CSRF Tokens*	CSRF biasanya digunakan untuk memanfaatkan hak istimewa korban untuk melakukan operasi terhadap situs target. Namun, penyerang dapat bekerja di dalam kebijakan asal yang sama karena XSS dapat digunakan sebagai platform untuk CSRF, sehingga	*Medium*	Fase: Arsitektur dan Desain memanfaatkan perpustakaan atau kerangka kerja yang telah terbukti dapat menghilangkan cacat ini atau menawarkan kerangka kerja yang memudahkan untuk

		meningkatkan kemungkinan kebocoran informasi.		menghindarinya. Gunakan paket anti-CSRF seperti OWASP CSRFGuard, misalnya.
2.	*Header for Content Security Policy (CSP) Not Set*	Salah satu lapis keamanan tambahan adalah Content Security Policy (CSP). CSP mendeteksi dan memerangi berbagai jenis intrusion, seperti Cross Site Scripting (XSS) dan data injection attacks. Attacks seperti ini dapat digunakan untuk hal-hal seperti pencurian data, kegagalan website, atau penyebaran malware. *CSP memberi pemilik situs web kemampuan untuk mendeklarasikan sumber konten menggunakan serangkaian header HTTP standar. Browser dapat memuat beberapa jenis konten di situs web, termasuk JavaScript, CSS, bingkai HTML, font, gambar, dan objek yang dapat disematkan, termasuk video, file audio, ActiveX, dan applet Java.*	*Medium*	Periksa apakah server web, server aplikasi, penyeimbang beban, dan komponen lainnya telah menetapkan tajuk Keamanan Kebijakan Konten.
3.	*Directory Browsing*	dimungkinkan untuk melihat daftar direktori. Daftar direktori dapat mengungkapkan skrip tersembunyi, termasuk file, file sumber cadangan, dll. Yang dapat diakses untuk membaca informasi sensitif.	*Medium*	Jika diperlukan, matikan penjelajahan direktori. Pastikan tidak ada file dalam daftar yang berbahaya.

4	*missing Anti-clickjacking Header*	Karena Kebijakan Keamanan Konten tidak melindungi terhadap serangan "ClickJacking", solusinya harus menggabungkannya menggunakan X-Frame-Options atau direktif "frame-ancestors".	*Medium*	Saat ini, browser web kontemporer mendukung Protokol Keamanan Konten dan Opsi X-Frame HTTP. Pastikan salah satu dari keduanya dipilih pada setiap halaman yang ditampilkan situs web atau aplikasi Anda. Anda harus menggunakan DENY jika Anda tidak ingin halaman dibingkai sama sekali, namun Anda dapat menggunakan SAMEORIGIN jika Anda mengantisipasi halaman tersebut dibingkai secara eksklusif oleh halaman di server Anda (misalnya, sebagai bagian dari FRAMESET). Sebagai alternatif, pertimbangkan untuk menerapkan pedoman “Kerangka Leluhur” kebijakan keamanan.
5.	*Version information is distributed by the server via the "server"*	Informasi versi dibocorkan oleh server web/aplikasi melalui Header Respons HTTP "server". Peretas dapat dengan mudah	*Low*	Verifikasi bahwa penyeimbang beban, server web, server aplikasi, dan perangkat keras lainnya telah diatur

	HTTP Response Header.	menemukan kerentanan lain di server web/aplikasi Anda.		untuk menampilkan informasi umum atau menyembunyikan header "server".
6.	*There are no X-Content-Type-Options. Heading*	Opsi untuk X-Content-Type Opsi "nosniff" tidak dipilih untuk header Hanti-MIME-sniffing. Hal ini memungkinkan isi respons diendus MIME oleh versi Chrome dan Internet Explorer yang lebih lama, yang dapat mengakibatkan isi respons ditafsirkan sebagai Hilang dan muncul sebagai jenis konten yang berbeda dari yang dinyatakan.Versi *Firefox* saat ini (awal 2014) dan lama akan menggunakan tipe konten yang dideklarasikan (jika ada yang disetel) daripada melakukan sniffing MIME	*Low*	Opsi untuk X-Content-Type Opsi "nosniff" tidak dipilih untuk header Hanti-MIME-sniffing. Hal ini memungkinkan isi respons diendus MIME oleh versi Chrome dan Internet Explorer yang lebih lama, yang dapat mengakibatkan isi respons ditafsirkan sebagai Hilang dan muncul sebagai jenis konten yang berbeda dari yang dikatakan. atau yang mana aplikasi web atau server web mungkin menginstruksikan untuk tidak digunakan untuk mengendus MIME
7.	*Get for POST*	GET juga diterima untuk permintaan yang awalnya dianggap sebagai POST. Meskipun ini bukan merupakan risiko keamanan, masalah ini dapat mempermudah serangan lainnya. Hal ini menunjukkan bahwa jika POST awal rentan terhadap Cross-Site Scripting (XSS), maka XSS yang lebih	*Information*	Pastikan hanya POST yang diterima jika POST diharapkan

		sederhana (berbasis GET) juga layak dilakukan.		
8.	*Information Disclosure-Suspicious comments*	Tampaknya pernyataan yang tidak jelas berisi informasi yang mungkin berguna bagi penyerang. Catatan: Konten secara keseluruhan, bukan hanya komentar, bertentangan dengan kecocokan yang dibuat dalam blok skrip atau file.	*Information*	Hapus semua komentar yang berisi informasi yang dapat membantu penyerang dalam menyelesaikan masalah buruk apa pun yang mereka kemukakan
9.	*Fuzzer, a User Agent*	Carilah variasi tanggapan berdasarkan agen pengguna yang ambigu. Lihat kode hash isi pesan dan kode status di samping pesan asli.	*Information*	Gunakan *Monitor Header* HTTP, Analisis Log Server, dan Validasi Agen Pengguna.

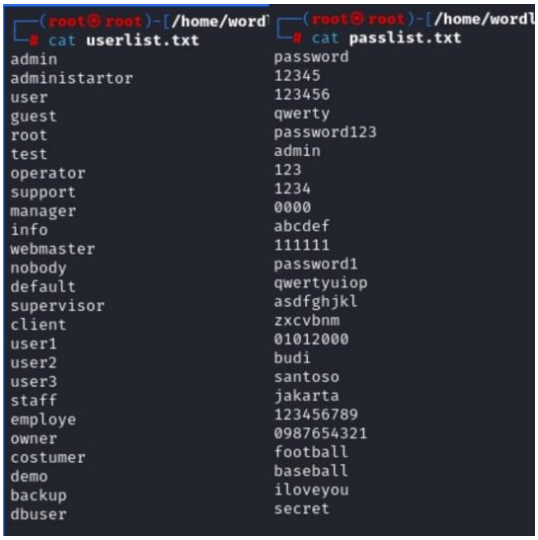
Menurut temuan pemindaian *fremwork Zap*, sebagian besar kerentanan yang ditemukan disebabkan oleh kesalahan dalam pemrograman atau perlindungan desain yang memengaruhi keamanan situs web. Hal ini mungkin terjadi karena kurangnya kesadaran keamanan selama tahap desain.

3. Attack

Langkah-langkah utama metode NIST SP 800-115 untuk Fase primer dalam proses NIST SP 800-115 untuk melakukan pengujian penetrasi pada data Discovery termasuk dalam fase ini. Berikut adalah beberapa potensi serangan. Langkah ini melibatkan melakukan pengujian penetrasi terhadap temuan dari Discovery. Serangan berikut tersedia untuk digunakan`:

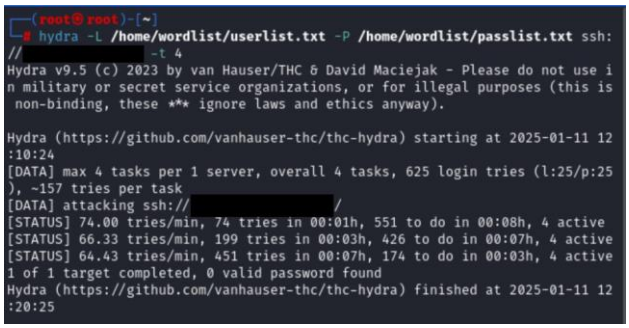
1) *Brute For Attack*

Saat mencoba melakukan serangan brute force attack, haruslah membut user dan password acak yang umum digunakan seperti gambar dibawah 4.5.



Gambar 4.5 *Wordlist User* dan Password Umum

Selanjutnya untuk melakukan serangan tersebut gunakan Hydra pada saat melakukan serangan, lalu jalankan perintah seperti yang terlihat pada gambar di 4.6.



Gambar 4.6 Serangan Brute For Attack.

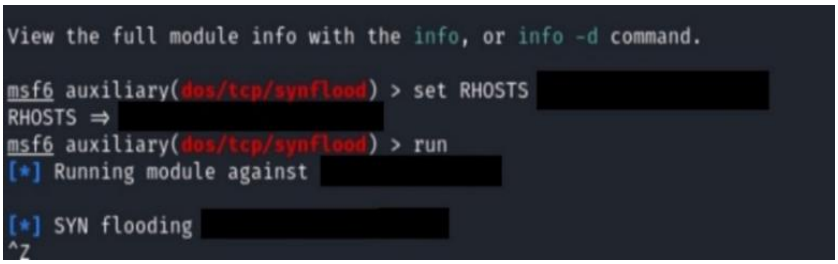
Dari hasil serangan tidak ada hasil sah yang dicapai, yang menunjukkan 0 kata sandi valid diambil. Oleh karena itu, menggunakan SSH untuk menguji login brute force tidaklah rentan.

2) *Denial of Service Synflood*

Untuk memanfaatkan Denial of Service (DoS), gunakan eksploitasi Synflood DoS. DoS Serangan yang dikenal sebagai "synflood" terjadi ketika jaringan dibanjiri dengan lalu lintas palsu. Ini menyiratkan bahwa sistem akan dirugikan dan tidak dapat berfungsi dengan baik karena jaringan atau server yang disusupi tidak akan mampu menyediakan lalu lintas. Pengujian ini menggunakan framework Metasploit untuk meniru serangan Synflood DoS dan menggunakan Wirshark untuk memantau data lalu lintas jaringan selama proses eksploitasi

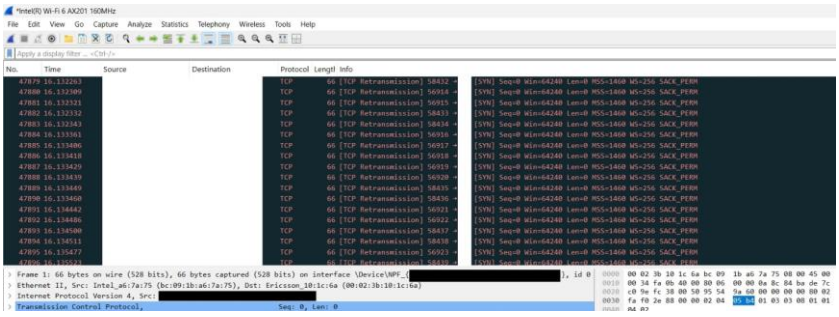
DoS. Perintah digunakan terlebih dahulu, diikuti oleh ux/dos/tcp/synflood, dan opsi ditampilkan di akhir.

Gambar 4.7 Modul serangan Denial of Service Synflood.



Gambar 4.8 Serangan *Denial of Service Synflood*

Serangan telah diimplementasikan seperti yang ditunjukkan pada gambar 4.7. Selanjutnya Wireshark diperlukan untuk mencatat aktivitas paket data grafik di seperti pada gambar 4.8.



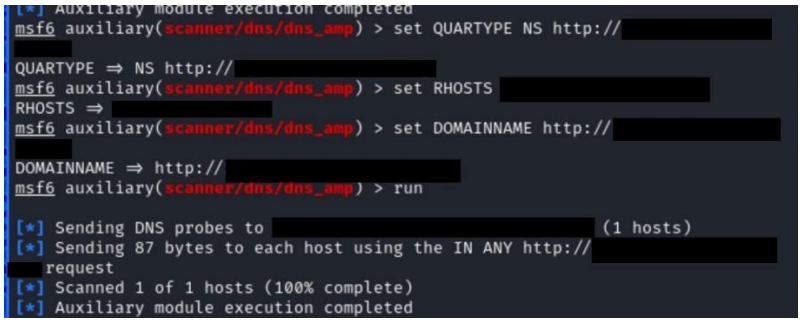
Gambar 4.9 Serangan *Denial of Service Synflood.*

Tampilan Wireshark menunjukkan bahwa sistem sedang sibuk karena lalu lintas jaringan yang sangat padat. TCP dapat dieksploitasi dengan mengirimkan paket SYN dan memalsukan

alamat IP, yang menyebabkan server mengklarifikasi koneksi namun tidak pernah membuatnya. Akibatnya kapasitas server terlampaui oleh proses yang berjalan di dalamnya.

3) Amplification of DNS Server Requests

Peretasan amplifikasi DNS mengubah kueri langsung menjadi muatan yang lebih besar untuk melumpuhkan server DNS sebagai bagian dari serangan Penolakan Layanan Terdistribusi (DDoS).Setelah menampilkan opsi dengan perintah bantu/scanner/dns/dns_amp, konfigurasikan menggunakan perintah modul yang tersedia seperti yang pada gambar 4.8 di bawah.



Gambar 4.10 Serangan *Distributed Denial of Service.*

Ini telah secara efektif menyusup ke modul DNS Amp, sesuai dengan hasil eksploitasi. Mengirimkan 87 *bytes* permintaan untuk menguji paket menunjukkan efek amplifikasi DNS.

E. KESIMPULAN

Dari hasil pengujian pada Aplikasi Web Sistem Evaluasi Data Bidang Tik Polda Aceh berhasil ditemukannya kerentanan-kerentanan yang terdapat pada Aplikasi Web tersebut seperti:

1. Aplikasi web menggunakan alamat IP server sebagai DNS sehingga memungkinkan penyerang mengakses situs lain di server. Aplikasi web tidak boleh menyertakan alamat IP dalam DNS-nya.
2. Server web tidak menerapkan Secure Sockets Layer (SSL) atau Transport Layer Security (TLS), dua protokol keamanan yang digunakan untuk melindungi interaksi internet. Karena Type X Option Header tidak ditentukan, penyerang dapat membaca data pribadi dari respons aplikasi web. Untuk lebih mengamankan aplikasi web, disarankan untuk mengonfigurasi Type X Option Header..
3. Banyak kesalahan pemrograman atau desain yang tidak aman dapat mengakibatkan kerentanan yang dapat mengungkapkan detail tentang kerentanan lainnya. Tindakan terbaik adalah memperbaiki kelemahan pemrograman dan mempertimbangkan dampak yang timbul dari desain yang tidak aman atau kesalahan pemrograman.CSP tidak dikonfigurasi sehingga dapat

mengakibatkan perusakan situs dan penyebaran malware, Sebaiknya mengkonfigurasi CSP pada aplikasi web tersebut agar dapat meminimalisir serangan malware.

4. Ubuntu Server masih menggunakan versi lama, Sebaiknya diupgrade ke versi Ubuntu Server yang lebih baru agar aplikasi web lebih terproteksi.
5. Untuk menangani serangan DoS.

- Sebaiknya server menggunkan Firewall untuk menghindari serangan,
- Melakukan Blocking terhadap IP yang terliht mencurigakan,
- Nonaktifkan layanan UDP (User Diagram Protocol) dan tolak paket data.
- Memanfaatkan perangkat lunak antivirus seperti Kapersky yang dapat mencegah pelanggaran data.
- Menggunakan firewall untuk memfilter pertanyaan gema ICMP.Untuk menangani serangan DDoS
- Sebaiknya Menggunakan Firewall yang kuat,
- Sebaiknya Menggunakan Load Blancer untuk mendistribusikan beban jaringan secara merata ke beberapa server.
- Sebaiknya memasang Sertifikasi SSL sebagai standar keamanan suatu sistem informasi.
- Sebaiknya dilakukan perbaikan untuk meningkatkan keamanan sistem baik pada Aplikasi Web maupun Server agar sistem infrmasi tersebut lebih terproteksi.

Metode NIST SP 800-115 membahas Information Gathring, Vulnerability Scanning dan Reporting, metode NIST SP 800-115 terdapat fase Attack yang bertujuan mencoba melakukan serangan terhadap sistem informasi yang menjadi sample. Dan jika ingin lebih detail dalam melakukan percobaan penetrasi sebaiknya menggunkan metode NIST 800-115.

DAFTAR PUSTAKA

Wasis Wardana, Ahmad Almaarif, Adityas Widjajarto,Telkom University, Indonesia, "VULNERABILITY ASSESSMENT AND PENETRATION TESTING ON THE XYZ WEBSITE USING NIST 800-115 STANDARD", Jurnal Ilmiah Indonesia p–ISSN: 2541-0849 e-ISSN: 2548-1398 Vol. 7, Special Issue No. 1, Januari 2022.

Doddy Ferdiansyah Universitas Pasundan, Sali Alas Majapahit Universitas Pasundan, Miftahul Fadli Muttaqin Universitas Pasundan, "Rancangan Infrastruktur Virtual Lab Untuk

Mendukung Praktikum Keamanan Informasi Berdasarkan National Institute of Standards and Technology (NIST)", 2023-12-06, Published by APTIKOM SUMSEL.

IM RAAZI, "Analisis Penilaian Keamanan Server Terhadap Sistem Informasi Manajemen Kepegawaian Dengan Metode NIST SP 800-115 Pada Universitas Islam Negeri Ar-raniry Banda Aceh", 02 januari 2023, repository.ar-raniry.ac.id.

M. Rozali and M. Dayan Sinaga, "DIAGNOSIS KEAMANAN WEB MENGGUNAKAN METODE UJI PENETRASI WEBSITE SEKOLAH Web Security Diagnosis Using School Website Penetration Test Method," JID (Jurnal Info Digit., vol. 2, no. 1, pp. 248–262, 2024, [Online]. Available: http://kti.potensi-utama.ac.id/index.php/JID

DZAKI ANMARIS HARAHAP, " ANALISIS UJI PENETRASI PADA SISTEM MANAJEMEN DATA SUMBER TERBUKA CKAN MENGGUNAKAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY SPECIAL PUBLICATION (NIST SP 800-115)", Jakarta 7 juli 2023. epository.upnvj.ac.id

Doddy Ferdiansyah, Sali Alas Majapahit, Miftahul Fadli Muttaqin,Universitas Pasundan, "Rancangan Infrastruktur Virtual Lab Untuk Mendukung Praktikum Keamanan Informasi Berdasarkan National Institute of Standards and Technology (NIST)", 2023-12-06, Vol. 4 No. 3 (2023): Journal of Information Technology Ampera.

[Achmad Iqbal Yuladi Universitas Amikom Yogyakarta, Rini Indrayani Universitas Muhammadiyah Palopo, "Analisis dan Perbandingan Tools Forensik menggunakan Metode NIST dalam Penanganan Kasus Kejahatan Siber", 2023-12-12,Vol 9 No 2 (2023): Desember, 2023.

DA Purnama, C Sulfadriman, "Penerapan NIST Cybersecurity dalam Analisis Resiko Keamanan Sistem Informasi Website", 2023 - elibrary.undipa.ac.id

Megia Nofita Universitas Atma Jaya Yogyakarta, Danny Sebastian Universitas Kristen Duta Wacana, "Technology Acceptance Models pada Teknologi Digital: Survey Paper", 23-05-2022,Vol. 2 No. 2 (2022): Desember 2022.

Fujiama Diapoldo Silalahi, "KEAMANAN CYBER (CYBER SECURITY)", 2022-08-23,2022: Penerbit Yayasan Prima Agus Teknik.

Rian Dwi Hapsari, Kuncoro Galih Pambayun, Institut Pemerintahan Dalam Negeri,"ANCAMAN CYBERCRIME DI INDONESIA Sebuah Tinjauan Pustaka Sistematis", 26-10-2023 , Jurnal Konstituen Vol.5 (1), April 2023: 1-17.

Dita Septasari, "The Cyber Security and The Challenge of Society 5.0 Era in Indonesia", Aug 21, 2023,Vol. 5 No. 2 (2023): Aisyah Journal Of Informatics and Electrical Engineering.

Rifqi Galuh Putra,Achmad Fauzi,Ery Teguh Prasetyo,Salza Rio Pratama,Indah Deya Ramadhan,Febriyanti Febriyanti, Siti Nurlela,Universitas Bhayangkara Jakarta Raya, "Pentingnya Manajemen Security di Era Digitalisasi", 2023-06-02, Vol. 2 No. 1 (2023): Jurnal Ilmu Multidisplin .

D SULISDYANTORO,"IDENTIFIKASI BUKTI DIGITAL WHATSAPP PADA SMARTPHONE ANDROID DENGAN MENGGUNAKAN METODE ANDROID BACKUP APPLICATION PACKAGE KIT (APK) DOWNGRADE", 19 Aug 2022 ,repository.mercubuana.ac.id.

SS Anelia, J Jayanta, B Hananto, "Uji Penetrasi Server Universitas PQR Menggunakan Metode National Institute of Standards and Technology (NIST SP 800-115)",2021, repository.upnvj.ac.id.