Analisa Kerentanan dan Sistem Keamanan *Website* Politeknik Negeri Lhokseumawe Menggunakan *Network Forensic Tools*

Muhammad Farhan[1], Aswandi[2], Ilham Safar[3]

[1,3] Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA

[1]farhanmuhammad1503@gmail.com
[2]aswandi@pnl.ac.id
[3]ilham_safar@pnl.ac.id

Abstrak— **Penelitian ini dilatarbelakangi dengan adanya serangan yang terjadi pada *website* xyz.ac.id pada tahun 2010 dan 2018, yang mengakibatkan perubahan tampilan situs (defacing). Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan yang ada pada *website* Politeknik Negeri Lhokseumawe dan Mendeteksi dan Menganalisis Serangan yang Pernah Terjadi pada *Website* xyz.ac.id Menggunakan Network Forensik Tools. Metode yang digunakan melibatkan *network forensic tools* dan analisis kerentanan. Hasil penelitian menunjukkan adanya 9 port terbuka dan 17 kerentanan yang terdeteksi, yang dibagi menjadi 1 kerentanan *high*, 7 kerentanan *medium*, 5 kerentanan *low*, dan 4 kerentanan informational. Kerentanan tersebut mencakup Hash Disclosure - Mac OSX salted SHA-1, Absence of Anti-CSRF Tokens dan Vulnerable JS Library. Selain itu, penelitian ini menemukan bukti dua serangan yang mengubah tampilan halaman situs web, yang terdeteksi melalui zona-h. Meskipun analisis menggunakan Wireshark tidak memberikan indikasi mencurigakan terhadap situs web tersebut. Dengan menggabungkan analisis kerentanan dan alat-alat Forensik Jaringan, diharapkan risiko serangan siber dapat ditekan, sehingga keamanan dan kerahasiaan informasi pada situs web Politeknik Negeri Lhokseumawe. Dengan menggunakan Network Forensik Tools, mampu membantu dalam menganalisa kerentanan dan memonitor keamanan *website website* di Politeknik Negeri Lhokseumawe.**

Kata kunci **:** Zone-h*, Website, Network forensic toosl, Wireshark*

Abstract— **This research was motivated by attacks that occurred on xyz.ac.id *website*s in 2010 and 2018, which resulted in changes in site appearance (defacing). This study aims to identify and analyze vulnerabilities that exist on the Lhokseumawe State Polytechnic *website* and Detect and Analyze Attacks that have occurred on xyz.ac.id *website* using Network Forensics Tools. The methods used involve network forensic tools and vulnerability analysis. The results showed that there were 9 open ports and 17 vulnerabilities detected, which were divided into 1 high vulnerability, 7 medium vulnerabilities, 5 low vulnerabilities, and 4 informational vulnerabilities. These vulnerabilities include Hash Disclosure - Mac OSX salted SHA-1, Absence of Anti-CSRF Tokens and Vulnerable JS Library. In addition, the study found evidence of two attacks that altered the appearance of *website* pages, which were detected through the h-zone. Although the analysis using Wireshark did not give any suspicious indication of the *website*. By combining vulnerability analysis and Network Forensics tools, it is hoped that the risk of cyber attacks can be suppressed, so that the security and confidentiality of information on the Lhokseumawe State Polytechnic *website*. By using Network Forensics Tools, it is able to assist in analyzing vulnerabilities and monitoring the security of *website*s at the Lhokseumawe State Polytechnic.**

Keywords : Zone-h*, Website, Network forensic tools, Wireshark*

I. Pendahuluan

Era digital saat ini membawa perubahan yang signifikan dalam berbagai aspek kehidupan, termasuk informasi dan komunikasi. Internet dan situs web adalah sarana utama untuk mentransmisikan dan mengakses informasi. Keamanan *website* adalah serangkaian tindakan dan langkah-langkah yang dijalankan guna memberikan perlindungan yang kuat terhadap situs web dari berbagai resiko dan ancaman siber yang dapat mengancam integritas dan keberlangsungan fungsionalnya. Ancaman-ancaman ini meliputi serangan peretas yang berusaha merusak sistem, pencurian data sensitif, gangguan layanan yang dapat menghentikan akses pengguna, dan juga eksploitasi kerentanan dalam perangkat lunak yang digunakan oleh situs web[1].

Analisis kerentanan adalah tahap penting dalam konteks keamanan siber yang bertujuan untuk mengidentifikasi dan mengevaluasi potensi celah atau kerentanan dalam sistem komputer, perangkat lunak, atau infrastruktur IT. Proses ini dilakukan oleh para ahli keamanan

dengan menggunakan berbagai metode dan alat guna mengungkap titik-titik masuk yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab, seperti peretas, yang mungkin memiliki niat untuk merusak, mencuri informasi, atau mengganggu operasi normal entitas digital[2].

Ancaman keamanan dapat timbul baik melalui upaya peretasan jaringan dari pihak luar maupun akibat kelalaian dari pihak yang memiliki data sensitif. Beberapa jenis ancaman umum dalam keamanan jaringan meliputi phishing, social engineering, ransomware, dan malware[3]. Untuk mendukung analisis kerentanan, berbagai metode seperti Footprinting, yang berkaitan dengan pengumpulan informasi terperinci tentang target, serta teknik seperti Vulnerability scanning, yang membantu mengidentifikasi kerentanan pada sistem atau aplikasi[4].

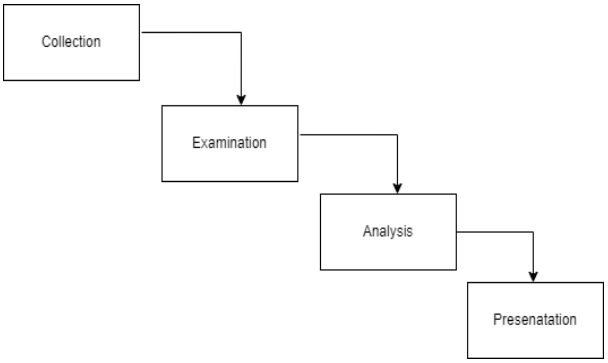
Keamanan Jaringan atau Cyber Security adalah suatu kegiatan yang dilakukan oleh sistem dalam rangka menjaga, melindungi sistem dan jaringan komputer dari suatu serangan ilegal dari seseorang[5].

Network forensics tools merupakan *tools* digunakan untuk mendeteksi, mencegah, dan menyelidiki serangan jaringan, merupakan alat penting dalam menjaga keamanan siber dan menjadi landasan bagi penelitian dan penulisan jurnal[6]. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan dalam sistem keamanan *website* Politeknik Negeri Lhokseumawe dan mengevaluasi tingkat kerentanan yang mungkin ada dalam sistem *website* tersebut, termasuk potensi titik masuk yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Hasil dari penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam tentang keamanan *website* dan menyediakan rekomendasi serta solusi yang dapat diterapkan untuk memperkuat keamanan *website* Politeknik Negeri Lhokseumawe, dengan tujuan menjaga kerahasiaan serta integritas informasi yang disimpan dalam situs web tersebut.

II. Metodologi Penelitian

Metode penelitian yang digunakan pada penelitian ini adalah metode *Network Forensic Tools*. *Network Forensic Toosl* adalah tools yang digunakan untuk melakukan analisis dan pemeriksaan terhadap aktivitas dalam jaringan. Tujuan utama dari penggunaan *tools* ini adalah untuk mendeteksi, menganalisis, serta memberikan respons terhadap insiden keamanan yang terjadi dalam jaringan tersebut[6].

1. Model *Investigasi Digital Forensik*

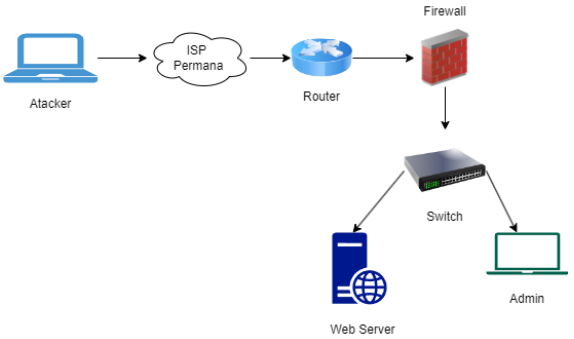


Gambar 1. Model *Investigasi Digital Forensik*

Penjelasan dari model investigasi forensik :

a. Pengumpulan (Collection) Pada tahap ini, data yang relevan dikumpulkan dari berbagai sumber seperti sistem komputer, perangkat seluler, server, atau jaringan
b. Pemeriksaan (Examination) Setelah data terkumpul, tahap pemeriksaan dilakukan. Ini melibatkan proses analisis terhadap data yang dikumpulkan untuk mengidentifikasi informasi penting, jejak aktivitas mencurigakan, dan bukti lainnya yang relevan dengan investigasi.
c. Analisis (Analysis) Dalam tahap analisis, hasil dari pemeriksaan dianalisis lebih lanjut untuk mendapatkan wawasan yang lebih dalam tentang kronologi peristiwa, cara serangan dilakukan, serta dampak yang dihasilkan.
d. Presentasi (Presentation) Pada tahap akhir, temuan dari analisis dijelaskan dalam bentuk laporan forensik.

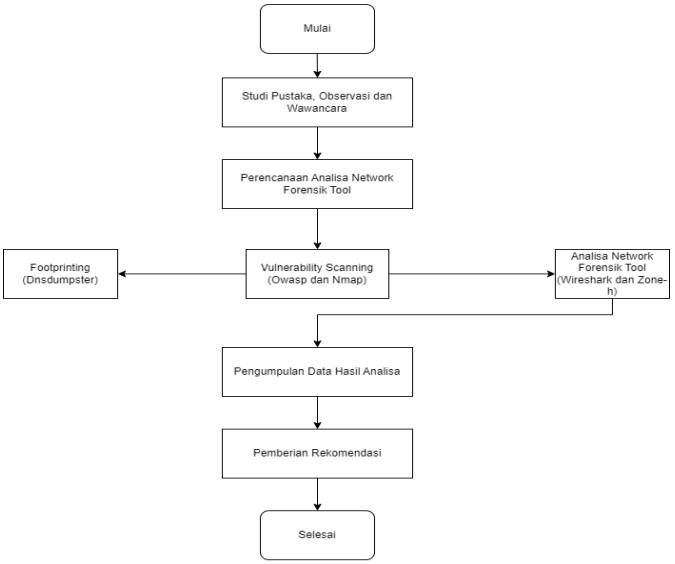
2. Arsitektur Jaringan



Gambar 2. *Arsitektur Jaringan*

Pada rancangan arsitektur sistem gambar 2 dimana *attacker* menggunakan jaringan WiFi yang ada di lingkungan kampus menggunakan layanan dari penyedia internet yang bernama Permana kemudian mencoba menganalisa *website* kampus politeknik negeri lhokseumawe menggunakan *network forensic tools*.

Adapun tahapan penelitian dapat dilihat pada Gambar 3.



Gambar 3. Metde Penelitian

Penjelasan dari tahapan-tahapan metode penelitian :

a. Studi Pustaka pada tahap ini peneliti mencari landasan teori untuk materi *Footprinting* dan *vulnerability scanning* yang dilakukan dengan cara mempelajari referensi dari buku, jurnal, maupun mencari literatur di internet yang berkaitan dengan masalah laboratorium komputer
b. Observasi yang dilakukan dalam tahap penelitian ini dengan cara mengunjungi *website* kampus.
c. Wawancara dalam tahap ini wawancara dilakukan dengan cara mengunjungi kepala unit pelaksana teknis (UPT) Politeknik Negeri Lhokseumawe
d. Footprinting merupakan tahap pengumpulan informasi yang dilakukan pada target, informasi yang didapat berupa sistem operasi apa yang dipakai, alamat IP dan *website* yang digunakan.
e. Vulnerability Scanning pada tahapan ini peneliti mencari kerentanan dan celah keamanan yang ada pada *website* tersebut.
f. Analisa Network Forensik pada tahapan ini dilakukan analisis forensik untuk mengidentifikasi jejak digital atau bukti lain dari aktivitas yang mencurigakan atau ilegal pada jaringan.
g. Pengumpulan data hasil analisa pada tahapan ini dilakukan pengumpulan data hasil analisa yang didapatkan pada saat mencari kerentanan dan celah keamanan yang ada pada *website*.
h. Pemberian Rekomendasi pada tahapan ini dilakukan pemberian rekomendasi pada kerentanan yang ditemukan pada *website*

III. HASIL DAN PEMBAHASAN

Proses yang dilakukan untuk menemukan kerentanan dan sistem keamanan website Politeknik Negeri Lhokseumawe. Pada proses mencari celah kerentanan website Politeknik Negeri Lhokseumawe menggunakan OWASP dan untuk tools network forensik menggunakan wireshark dan juga Zone.h.

1. Footprinting

Pada tahap ini, dilakukan penggalian informasi lebih mendalam tentang suatu situs web[4]. Proses ini melibatkan pencarian detail informasi yang terdapat di dalam situs web menggunakan DNSdumpster. Hasil informasi *website* menggunakan DNSdumpster dapat dilihat pada Gambar 4.

Gambar 4. Hasil Scanning Menggunakan DNSdumpster

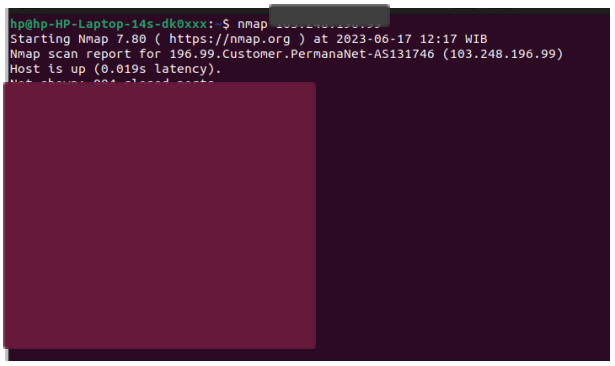
Berdasarkan hasil gambar 4 merupakan hasil dari footprinting yang dilakukan menggunakan DNSdumpster untuk mencari informasi mengenai *website* xyz.ac.id. Dengan memasukan domain dari *website* xyz.ac.id informasi yang didapatkan seperti pada gambar 4 Dalam informasi yang diberikan, terdapat beberapa rincian yang terkait dengan web dan infrastruktur yang digunakan. Untuk layanan HTTP (web server), digunakan Apache dengan versi 2.4.52, yang berjalan pada sistem operasi Windows 64-bit. Selain itu, ada juga OpenSSL versi 1.1.1m yang digunakan untuk keamanan, serta PHP versi 7.4.27 yang berperan sebagai bahasa pemrograman server-side. Sementara itu, layanan FTP (file transfer protocol) menggunakan ProFTPD versi 1.3.5rc3 dan dijalankan pada sistem operasi Debian. Terdapat pula informasi mengenai alamat IP "::ffff:103.248.196.99", yang kemungkinan adalah alamat IPv6 yang merujuk pada alamat IPv4 "103.248.196.99". Selain itu, web tersebut juga digunakan PHP versi 7.4.27, Apache versi 2.4.52, dan framework CodeIgniter.

2. Mencari Celah Kerentanan

Celah Kerentanan adalah proses identifikasi kerentanan atau celah keamanan pada suatu sistem atau aplikasi dengan menggunakan software khusus yang disebut sebagai vulnerability scanner[7].

a. NMAP

Nmap merupakan tools open source yang digunakan untuk melakukan scanning dan mendeteksi port-port yang terbuka pada jaringan[8]. Gambar 5 merupakan port yang terbuka pada website xyz.ac.id

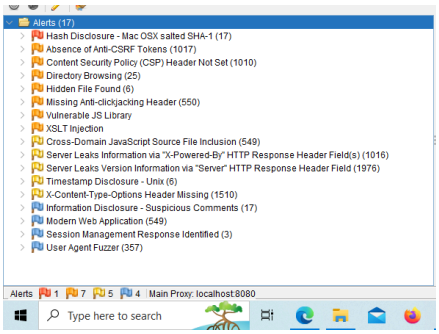


Gambar 5. Hasil Scan Menggunakan NMAP

Saat melakukan pemindaian port menggunakan Nmap, dapat dilihat pada Gambar 5 yaiut terdapat dua status yang muncul dalam hasil pemindaian, yaitu terdapat 8 port dengan status terbuka dan 7 port dengan status filtered

b. OWASP ZAP

OWASP merupakan komunitas global yang berfokus pada peningkatan keamanan website, Gambar 6 merupakan kerentanan yang terdeteksi pada website xyz.ac.id



Gambar 6. Hasil Scan Menggunakan OWASP ZAP

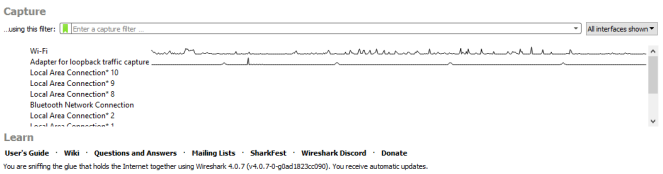
Ketika melakukan pemindaian menggunakan OWASP (Open Web Application Security Project), menunjukkan adanya 17 macam alerts yang memiliki level high, level medium, level low dan level informational.

3. *Network Forensik*

Network forensics adalah cabang forensik digital yang berfokus pada analisis dan investigasi kejadian yang terjadi dalam jaringan komputer.

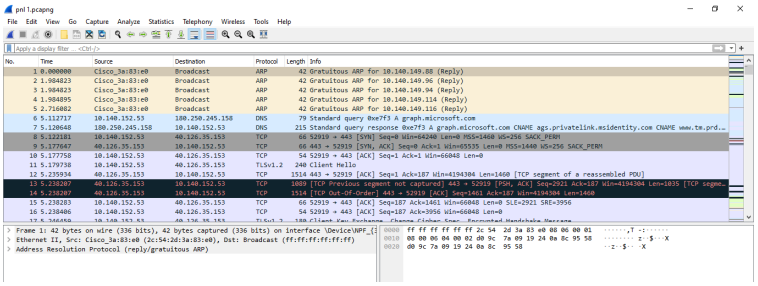
a. Wireshark

Wireshark adalah sebuah perangkat lunak analisis paket. Aplikasi ini digunakan untuk tujuan perbaikan jaringan dan analisis[9].



Gambar 7 Capture Wireshark

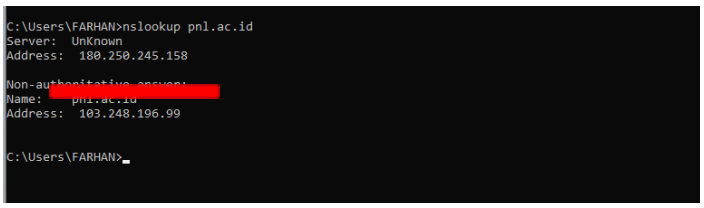
Pada Gambar 7, terdapat beberapa antarmuka yang tercantum dalam perangkat lunak Wireshark. Antarmuka ini merupakan daftar jalur yang tersedia pada perangkat untuk menghubungkannya ke jaringan internet. terlihat adanya garis-garis yang menyerupai diagram elektronik. Jika terdapat gelombang-gelombang pada garis tersebut, dapat dipastikan bahwa terdapat aktivitas yang sedang berlangsung. Aktivitas yang dimaksud adalah adanya komunikasi data yang sedang terjadi melalui *interfaces* yang tertera di Wireshark.



Gambar 8 Hasil Capture Website xyz.ac.id

Pada Gambar 8 merupakan tampilan capture jaringan pada website menggunakan perangkat lunak Wireshark, yang merekam aktivitas yang terjadi dalam jaringan.

Sebelum melakukan penyaringan, penulis harus memperoleh alamat IP dari website "xyz.ac.id". Metode untuk mendapatkan informasi ini melibatkan penggunaan terminal, di mana penulis dapat memasukkan perintah "nslookup xyz.ac.id" dan kemudian menekan tombol "Enter" pada keyboard. Hasilnya akan mengungkapkan alamat IP terkait dengan xyz.ac.id, yang nantinya dapat digunakan dalam penyaringan paket.

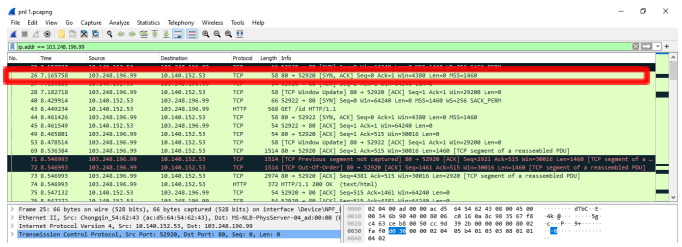


Gambar 9 Ip Address xyz.ac.id

Pada Gambar 9, terdapat penjelasan bahwa angka yang ditandai merupakan alamat IP dari website xyz.ac.id. Setelah mendapatkan informasi alamat IP dari xyz.ac.id, yaitu "103.248.196.99".

Langkah selanjutnya adalah melakukan penyaringan paket menggunakan address bar filter yang terletak di bawah

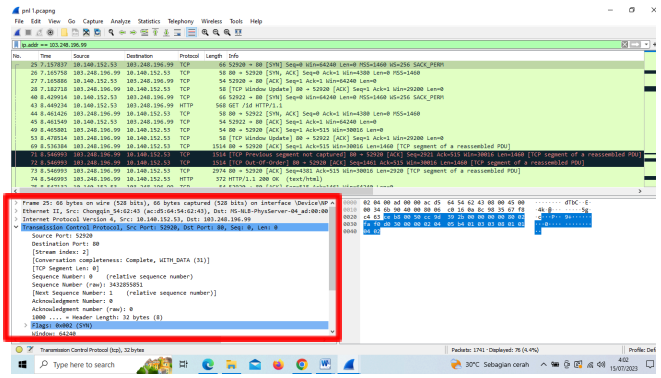
ikon-ikon aplikasi Wireshark. Penulis dapat memasukkan perintah "ip.addr==103.248.196.99" ke dalam address bar filter tersebut, sehingga akan muncul paket-paket yang memiliki alamat IP tersebut.



Gambar 10 Hasil Penyaringan Paket Data xyz.ac.id

Pada Gambar 10, terlihat adanya sejumlah paket data yang melibatkan IP Address 103.248.196.99 baik sebagai Source maupun sebagai Destination. Hal menarik yang dapat diperhatikan adalah adanya pertukaran posisi antara Source dan Destination dalam setiap paket tersebut. Dalam total 76 paket data yang ditampilkan, terdapat 2 jenis protokol yang dominan, yaitu Transmission Control Protocol (TCP) dan Hypertext Transfer Protocol (HTTP). Hal ini tidak mengherankan mengingat TCP merupakan protokol yang umum digunakan dalam koneksi internet.

Untuk melakukan analisis yang lebih mendalam terhadap paket-paket data, fokus perhatian dapat ditujukan pada panel detail data paket. Di panel ini, tersedia informasi yang terperinci mengenai setiap paket data yang terekam, termasuk informasi tentang protokol TCP yang digunakan. Dengan mempelajari detail-detail ini, peneliti dapat memperoleh wawasan yang lebih komprehensif mengenai komunikasi yang terjadi dan mendapatkan pemahaman yang lebih mendalam mengenai karakteristik protokol TCP yang digunakan dalam koneksi tersebut.



Gambar 11 Hasil Penyaringan Paket Data xyz.ac.id

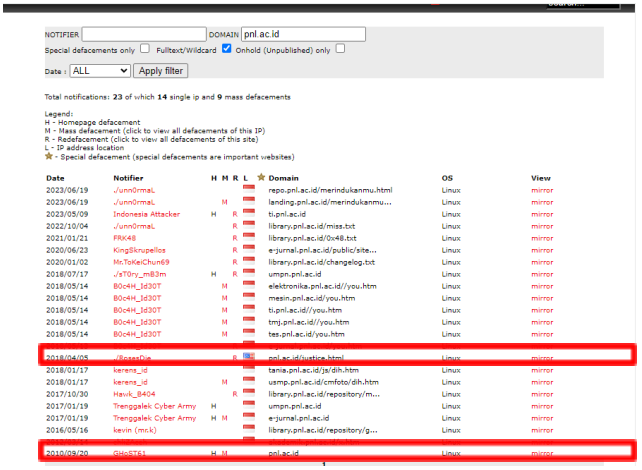
Pada Gambar 11, terlihat detail paket yang menggunakan protokol Transmission Control Protocol (TCP). Dari analisis detail paket data tersebut, peneliti dapat mengidentifikasi dan menganalisis informasi sebagai berikut:

a. Source Port : 52920
   Merupakan port yang digunakan client adalah 52920.
b. Destination Port : 80
   Merupakan port yang digunakan server adalah 80 yaitu http.
c. Flags : 0x002 (SYN)
   Merupakan client yang ingin meminta data dari server.

Dalam melakukan analisis forensik terhadap sebuah website menggunakan aplikasi Wireshark, hasil penelitian yang dilakukan menunjukkan bahwa tidak terdapat adanya indikasi atau bukti yang mencurigakan pada website yang sedang diselidiki. Dengan mengamati secara mendalam paket-paket data yang terekam dalam Wireshark, dapat disimpulkan bahwa seluruh interaksi komunikasi pada website tersebut berjalan dengan lancar dan sesuai dengan standar protokol yang digunakan, tanpa adanya perubahan atau manipulasi yang mencurigakan.

b. Zone-H

Zone-H merupakan platform yang secara khusus fokus pada pelaporan dan dokumentasi serangan defacing pada situs web[10]. Defacing adalah tindakan mengubah tampilan atau konten sebuah situs web secara ilegal oleh pihak yang tidak berwenang. Website Zone-H bertujuan untuk mengumpulkan, mencatat, dan mempublikasikan informasi mengenai serangan defacing yang terjadi di seluruh dunia.



Gambar 12 Hasil Pencarian Serangan Domain Target

Dalam penelitian ini, saat melakukan pencarian menggunakan website Zone-H, dideteksi bahwa website xyz.ac.id telah mengalami serangan defacing sebanyak dua kali. Serangan pertama terjadi pada tahun 2010, sedangkan serangan kedua terjadi pada tahun 2018.

4. Report

Report memberikan rincian tentang kerentanan yang telah terdeteksi, potensi risiko yang terkait, bukti forensik yang diperoleh, serta rekomendasi untuk mengatasi masalah tersebut.

a. Solusi Perbaikan Pada Port Yang Terbuka
   Analisis port yang terbuka pada website xyz.ac.id mengidentifikasi jenis port yang terbuka serta memberikan rekomendasi untuk port tersebut dapat dilihat pada tabel 1 Solusi Perbaikan

TABEL 1
Solusi Perbaikan Port

Port	State	Service	Rekomendasi
1/tcp	Filtered	tcpmux	
21/tcp	Open	ftp	Pastikan untuk memastikan bahwa konfigurasi FTP aman. Gunakan kata sandi yang kuat dan enkripsi data untuk melindungi akses dan transfer file.
22/tcp	Filtered	ssh	
23/tcp	Filtered	telnet	
25/tcp	Filtered	smtp	
53/tcp	Open	domain	Periksa konfigurasi server DNS dan pastikan keamanan serta kendalanya. Pastikan untuk memperbaiki dan mengamankan server DNS agar tidak rentan terhadap serangan DNS spoofing atau serangan DDoS.
80/tcp	Open	http	Periksa keamanan situs web yang berjalan pada port 80. Pastikan menggunakan protokol HTTPS (port 443) untuk mengenkripsi lalu lintas data dan menerapkan langkah-langkah keamanan seperti firewall aplikasi web dan pembaruan rutin pada platform atau CMS yang digunakan.
110/tcp	Open	Pop3	Jika menggunakan protokol POP3 untuk mengelola surel, pastikan menggunakan koneksi yang aman dan menerapkan enkripsi SSL/TLS (port 995) untuk melindungi informasi pengguna.
139/tcp	Filtered	netbios-ssn	
143/tcp	Open	imap	Jika menggunakan protokol IMAP untuk mengelola surel, pastikan penggunaan koneksi yang aman dan terenkripsi menggunakan SSL/TLS (port 993).
443/tcp	Open	https	Pastikan menggunakan sertifikat SSL/TLS yang valid untuk melindungi lalu lintas HTTPS. Periksa pengaturan keamanan server web dan pastikan protokol TLS yang lebih baru dan aman digunakan.
445/tcp	Filtered	Microsoft-ds	
993/tcp	Open	imaps	Pastikan penggunaan koneksi yang aman dan terenkripsi untuk mengakses surel menggunakan protokol IMAP.
995/tcp	Open	Pop3s	Pastikan penggunaan koneksi yang aman dan terenkripsi saat mengakses surel menggunakan protokol POP3.
3007/tcp	Filtered	lotusmtap	
10000/tcp	Open	Snet-sensor-mgmt	

b. Solusi Perbaikan Kerentanan Pada Website

Analisis kerentanan yang terdeteksi pada website xyz.ac.id mengidentifikasi jenis-jenis kerentanan yang ada serta memberikan rekomendasi solusi perbaikan untuk setiap kerentanan tersebut. Informasi detail mengenai kerentanan yang terdeteksi beserta langkah-langkah perbaikan yang direkomendasikan dapat ditemukan dalam Tabel 4.2 Solusi Perbaikan.

TABEL 2
Solusi Perbaikan Port

Nama Vulnerability	Risk Level	Confidence Level	Solusi Perbaikan
Hash Disclosure - Mac OSX salted SHA-1	*High*	*Medium*	Disarankan untuk mengganti algoritma hashing yang digunakan dengan algoritma yang lebih aman, misalnya SHA-256. Selain itu, perlu dilakukan implementasi teknik salt yang lebih kuat.
Absence of Anti-CSRF Tokens	*Medium*	*Low*	Gunakan paket anti-CSRF seperti OWASP CSRFGuard. Dan Pastikan website bebas dari masalah cross-site scripting (XSS),
Content Security Policy (CSP) Header Not Set	*Medium*	*Low*	Pastikan bahwa server web, server aplikasi, penyeimbang beban, dll. dikonfigurasi untuk mengatur header Content-Security-Policy.
Directory Browsing	*Medium*	*High*	Pastikan bahwa server web, server aplikasi, penyeimbang beban, dll. dikonfigurasi untuk mengatur header Content-Security-Policy.
Hidden File Found	Medium	High	Evaluasi dan sesuaikan komponen produksi sesuai kebutuhan. Aktifkan otentikasi, otorisasi, dan batasan akses jika diperlukan.
Missing Anti-clickjacking Header	Medium	Medium	Pastikan mengatur header HTTP Content-Security-Policy atau X-Frame-Options pada semua halaman web.
Vulnerable JS Library	Medium	Medium	Harap perbarui ke versi terbaru dari chart.js.

XSLT Injection	Medium	Medium	Lakukan sanitasi dan analisis terhadap setiap masukan pengguna yang berasal dari klien (client-side)
Cross-Domain JavaScript Source File Inclusion	Low	Medium	Pastikan file sumber JavaScript dimuat hanya dari sumber yang dipercaya, dan sumber tersebut tidak dapat dikendalikan oleh pengguna akhir aplikasi.
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	Medium	Pastikan bahwa server web, server aplikasi, penyeimbang beban, dll. dikonfigurasi untuk menekan header "X-Powered-By".
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	High	Pastikan bahwa server web, server aplikasi, penyeimbang beban, dll. dikonfigurasi untuk menekan header "Server" atau memberikan detail yang umum.
Timestamp Disclosure - Unix	Low	Low	Konfirmasikan secara manual bahwa data timestamp tidak sensitif, dan bahwa data tersebut tidak dapat dikumpulkan untuk mengungkapkan pola yang dapat dieksploitasi.
X-Content-Type-Options Header Missing	Low	Medium	Pastikan server mengatur header Content-Type dengan benar dan header X-Content-Type-Options menjadi 'nosniff' di semua halaman web. Gunakan browser modern yang mematuhi standar dan hindari MIME-sniffing jika memungkinkan.
Information Disclosure - Suspicious Comments	Information	Low	Hapus semua komentar yang mengembalikan informasi yang dapat membantu penyerang, dan perbaiki semua masalah mendasar yang mereka sebutkan.
Modern Web Application	Information	Medium	Ini adalah peringatan informatif dan tidak memerlukan perubahan.
Session Management Response Identified	Information	Medium	Ini adalah peringatan informatif daripada kerentanan, sehingga tidak ada yang perlu diperbaiki
User Agent Fuzzer	Information	Medium	Ini adalah peringatan informatif dan tidak memerlukan perubahan.

c. Bukti Forensik

Pada table 3 bukti forensik di bawah, dapat ditemukan bukti yang mendukung informasi bahwa domain website xyz.ac.id mengalami dampak dari serangan pada tahun 2010 dan 2018. Hasil pencarian domain website xyz.ac.id di platform zona-h secara khusus memperkuat kesimpulan ini. Serangan yang teridentifikasi pada dua insiden tersebut adalah manipulasi tampilan visual pada halaman utama website, yang mengindikasikan bahwa pelaku memiliki tujuan untuk mengubah tampilan yang terlihat oleh pengunjung situs.

TABEL 3
Solusi Perbaikan Port

Tanggal Serangan	Bukti Serangan	Penjelasan
05, Mei, 2018		Pada 05 Mei 2018, by ./RosesDie melakukan penyerangan pada *website* xyz.ac.id dimana merubah tampilan pada *website*
20, September, 2010		Pada 20 September 2010, GHoST61 melakukan penyerangan pada *website* xyz.ac.id dimana merubah tampilan pada *website*

Dengan begitu, membuktikan bahwa website xyz.ac.id rentan terhadap serangan. bahwa domain website ini ditemukan dalam hasil penelusuran zona-h menunjukkan bahwa tindakan mengubah tampilan halaman bukanlah masalah kecil, melainkan menunjukkan bahwa ada celah dalam keamanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Oleh karena itu, sangat penting untuk mengambil langkah-langkah guna memperbaiki dan memperkuat keamanan website xyz.ac.id agar dapat melindungi dari ancaman serupa di masa mendatang.

Selain itu, penting untuk dicatat bahwa menggunakan *Network Forensik Tools* bisa membantu dalam menganalisis kerentanan dan keamanan website di Politeknik Negeri Lhokseumawe. *Network Forensik Tools* dapat membantu mengidentifikasi sumber serangan, bukti serangan, dan memberikan pemahaman lebih dalam tentang bagaimana serangan itu terjadi. Dengan pemahaman yang lebih baik tentang kerentanan yang ada, tindakan pencegahan dapat diambil untuk memperbaiki dan memperkuat keamanan website xyz.ac.id, sehingga melindungi situs ini dari ancaman serangan.

IV. KESIMPULAN

Berdasarkan penelitian yang dilakukan, dapat diperoleh kesimpulan bahwa hasil identifikasi port terbuka pada website xyz.ac.id terdapat 9 port yang terbuka. Hasil identifikasi kerentanan pada website xyz.ac.id terdapat celah kerentanan pada level high yaitu Hash Disclosure - Mac OSX salted SHA-1. Pada Level medium terdapat pada kerentanan

Absence of Anti-CSRF Tokens, Content Security Policy (CSP) Header Not Set, Directory Browsing, Hidden File Found, Missing Anti-clickjacking Header, Vulnerable JS Library dan XSLT Injection. Selanjutnya Level law terdapat pada kerentanan Cross-Domain JavaScript Source File Inclusion, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), Server Leaks Version, Information via "Server" HTTP Response Header Field, Timestamp Disclosure – Unix dan X-Content-Type-Options Header Missing dan Level informational terdapat pada kerentanan Information Disclosure - Suspicious Comments, Modern Web Application, Session Management Response Identified dan User Agent Fuzzer. Ketika melakukan pencarian pada zona-h terhadap website xyz.ac.id, ditemukan dua bukti serangan yang jelas mengindikasikan bahwa serangan tersebut telah mengubah tampilan pada halaman website tersebut. Pada saat melakukan analisis website menggunakan Wireshark, tidak ada tanda-tanda mencurigakan yang ditemukan pada website tersebut.

REFERENSI

[1] L. M. Gultom and M. Harahap, "Analisis Celah Keamanan Website Instansi," vol. 02, pp. 1–7, 2015.

[2] E. I. Alwi and L. B. Ilmawan, "Analisis Keamanan Sistem Informasi Akademik (SIAKAD) Universitas XYZ Menggunakan Metode Vulnerability Assessment," *INFORMAL Informatics J.*, vol. 6, no. 3, p. 131, 2021, doi: 10.19184/isj.v6i3.27053.

[3] A. Ary, "Mengenal 14 Jenis Serangan Siber dan Cara Mencegahnya," *13 april*, 2022. https://www.helios.id/blog/detail/mengenal-14-jenis-serangan-siber-dan-cara-mencegahnya (accessed Mar. 13, 2023).

[4] E. I. Alwi, H. Herdianti, and F. Umar, "Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning," *INFORMAL Informatics J.*, vol. 5, no. 2, p. 43, 2020, doi: 10.19184/isj.v5i2.18941.

[5] A. Hermawan, T. Hartati, and Y. A. Wijaya, "Analisa Keamanan Data melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad," *Jpit*, vol. 7, no. 3, pp. 125–130, 2022.

[6] I. Riad and K. Ade, *Forensik Jaringan dan Cloud*. Yogyakarta: Diandra Kreatif, 2020.

[7] Y. Mulyanto, M. Taufan Asri Zaen, and S. Sihab, "Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest)," *J. Inf. Syst. Res.*, vol. 4, no. 1, pp. 202–209, 2022, doi: 10.47065/josh.v4i1.2335.

[8] M. A. Mu'min, A. Fadlil, and I. Riadi, "Analisis Keamanan Sistem Informasi Akademik Menggunakan Open Web Application Security Project Framework," *J. Media Inform. Budidarma*, vol. 6, no. 3, p. 1468, 2022, doi: 10.30865/mib.v6i3.4099.

[9] U. L. Richard Sharpe, Ed Warnicke, "Wireshark User's Guide." https://www.wireshark.org/docs/wsug_html_chunked/index.html (accessed Mar. 29, 2023).

[10] H. Hermanto and H. Haeruddin, "Peningkatan Sistem Keamanan Website Menggunakan Metode OWASP," *J. Ilmu Komput. dan Bisnis*, vol. 13, no. 1, pp. 94–104, 2022, doi: 10.47927/jikb.v13i1.277.