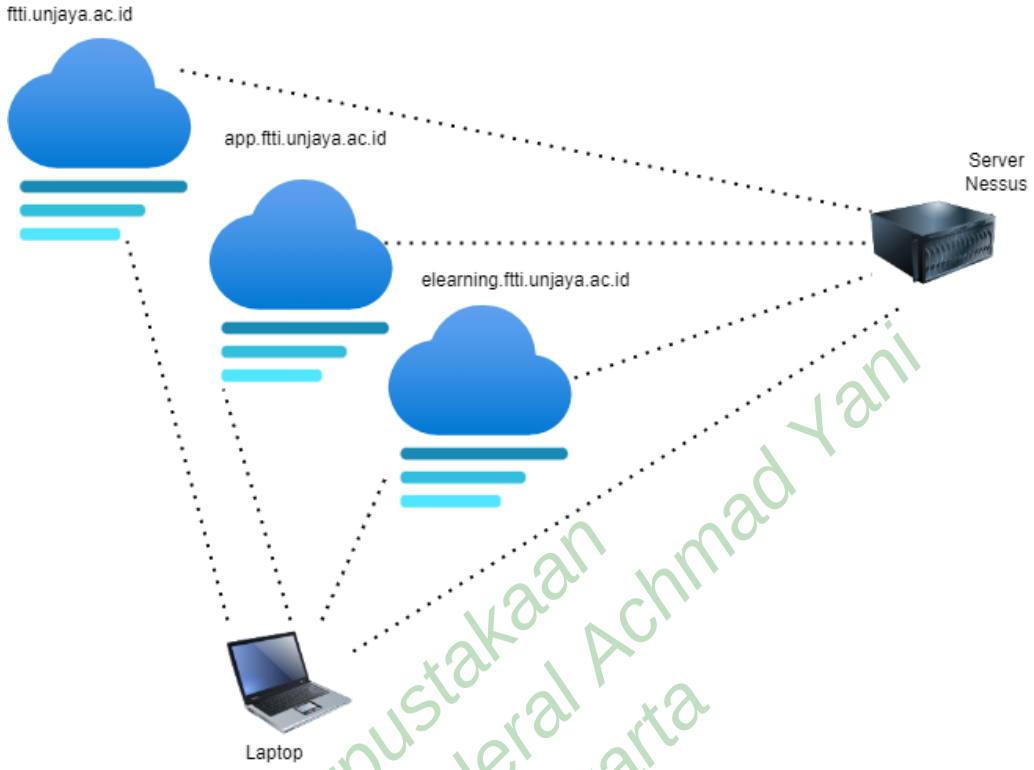
# BAB 4
# HASIL PENELITIAN

## 4.1 RINGKASAN HASIL PENELITIAN

Penelitian ini dilakukan untuk melakukan penilaian kerentanan yang ada pada situs web FTTI yaitu ftti.unjaya.ac.id, elearning.ftti.unjaya.ac.id, dan app.ftti.unjaya.ac.id. Dengan izin yang telah didapatkan peneliti untuk melakukan analisis terhadap situs web tersebut.. Hasil didapatkan dari tiga alat seperti Nmap, Nessus, dan WPScan. Dengan menggunakan Nmap terdapat beberapa port yang terbuka pada masing-masing IP seperti pada seperti pada situs web ftti.unjaya.ac.id dengan IP 45.127.135.131 memiliki 12 port yang terbuka, pada elearning.ftti.unjaya.ac.id dengan IP 103.247.15.114 memiliki 5 port yang terbuka, sedangkan pada app.ftti.unjaya.ac.id dengan IP 103.247.15.115 memiliki 13 port yang terbuka. Kemudian dilakukan pemindaian pada ketiga IP tersebut menggunakan Nessus. Ada beberapa tingkatan risiko yang dinilai oleh CVSS yang ada pada Nessus dari *informational* sampai tingkat kerentanan *critical*. Dari hasil pemindaian, situs web ftti.unjaya.ac.id terdeteksi paling aman sedangkan app.ftti.unjaya.ac.id memiliki kerentanan pada tingkat kerentanan *critical*. Dikarenakan situs web ftti.unjaya menggunakan WordPress, maka peneliti melakukan pemindaian menggunakan WPScan dengan hasil juga tidak ada kerentanan yang parah pada situs web tersebut.

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

## 4.2 ARSITEKTUR SISTEM




**Gambar 4.1** Topologi jaringan

Penelitian ini menggunakan Nmap dan WPScan yang berupa aplikasi dengan penginstalan pada laptop, namun Nessus menggunakan *web server* untuk pemindaian tetapi juga harus menyiapkan paket Nessus yang telah dipasang pada laptop. Gambar 4.1 menunjukan topologi jaringan yang digunakan oleh peneliti.

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

## 4.3 TESTING

Pada tahap ini, peneliti melakukan pemindaian pada ketiga situs web untuk mendapatkan hasil. Adapun hasil pemindaian yang diperoleh sebagai berikut.

### 4.3.1 Identifikasi *Headers* menggunakan DNSdumpster

Sebelum melakukan pemindaian menggunakan WPScan, peneliti memeriksa DNS pada ketiga situs web menggunakan alat DNSDumpster untuk memastikan situs web mana yang menggunakan WordPress agar bisa dilakukan

pemindaian menggunakan WPScan, terdapat beberapa informasi yang dimuat pada GET HTTP Headers sebagai berikut.

```
HTTP/1.1 301 Moved Permanently
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
content-type: text/html; charset=UTF-8
x-redirect-by: WordPress
location: https://ftti.unjaya.ac.id/
vary: Accept-Encoding
content-length: 20
content-encoding: gzip
date: Sat, 27 Aug 2022 07:57:54 GMT
server: LiteSpeed

HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
content-type: text/html; charset=UTF-8
link: ; rel="https://api.w.org/", ; rel="alternate"; type="application/json", ; rel=shortlink
vary: Accept-Encoding
transfer-encoding: chunked
content-encoding: gzip
date: Sat, 27 Aug 2022 07:57:56 GMT
server: LiteSpeed
alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-
Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"
```

**Gambar 4.2** Informasi HTTP Headers pada ftti.unjaya.ac.id menggunakan DNSDumpster

Pada tampilan informasi HTTP Headers yang ditunjukan pada gambar 4.2 menunjukan bahwa ftti.unjaya.ac.id menggunakan WordPress. Dengan demikian situs web tersebut bisa dilakukan pemindaian menggunakan DNSDumpster.

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

```
HTTP/1.1 200 OK
Date: Sat, 27 Aug 2022 09:51:27 GMT
Server: Apache/2.4.53 (Unix) OpenSSL/1.0.2k-fips
Last-Modified: Thu, 12 May 2022 09:09:34 GMT
ETag: "9c-5deccea9e1168-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 122
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

**Gambar 4.3** Informasi HTTP Headers pada app.ftti.unjaya.ac.id menggunakan DNSDumpster.

Pada tampilan informasi HTTP Headers yang ditunjukan pada gambar 4.3 menunjukan bahwa app.ftti.unjaya.ac.id menunjukan bahwa situs web tersebut tidak menggunakan WordPress. Dengan demikian situs web tersebut tidak cocok untuk dilakukan pemindaian menggunakan WPScan.

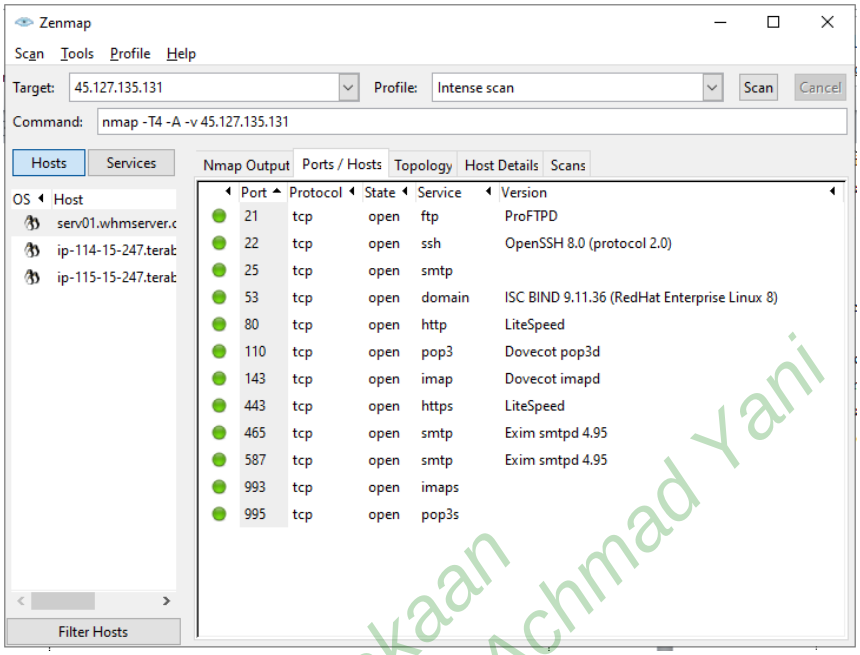
```
HTTP/1.1 301 Moved Permanently
Date: Sat, 27 Aug 2022 09:54:35 GMT
Server: Apache
Location: https://elearning.ftti.unjaya.ac.id/
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 200
Connection: close
Content-Type: text/html; charset=iso-8859-1

HTTP/1.1 200 OK
Date: Sat, 27 Aug 2022 09:54:36 GMT
Server: Apache
Set-Cookie: MoodleSession=hgcake9ru4gih8ff2bmqad7co1; path=/
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0, no-transform
Pragma: no-cache
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-UA-Compatible: IE=edge
Last-Modified: Sat, 27 Aug 2022 09:54:36 GMT
Accept-Ranges: none
X-Frame-Options: sameorigin
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
```

**Gambar 4.4** Informasi HTTP Headers pada elearning.ftti.unjaya.ac.id menggunakan DNSDumpster.

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

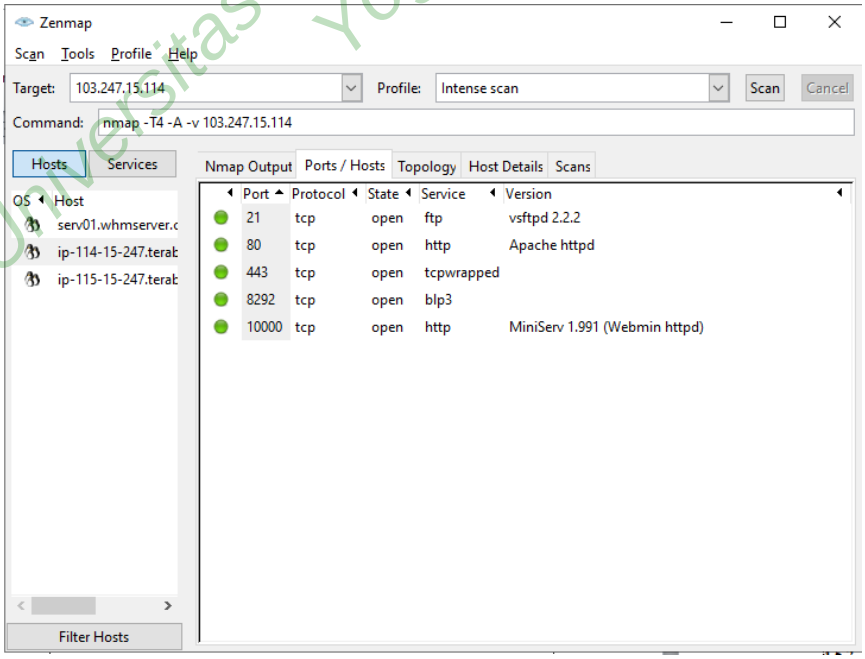
Pada tampilan informasi HTTP Headers yang ditunjukan pada gambar 4.4 menunjukan bahwa elearning.ftti.unjaya.ac.id menunjukan bahwa situs web tersebut tidak menggunakan WordPress. Dengan demikian situs web tersebut tidak cocok untuk dilakukan pemindaian menggunakan WPScan.

### 4.3.2 Pemindaian pada IP target menggunakan Nmap




**Gambar 4.5** Pemindaian Nmap pada ftti.unjaya.ac.id

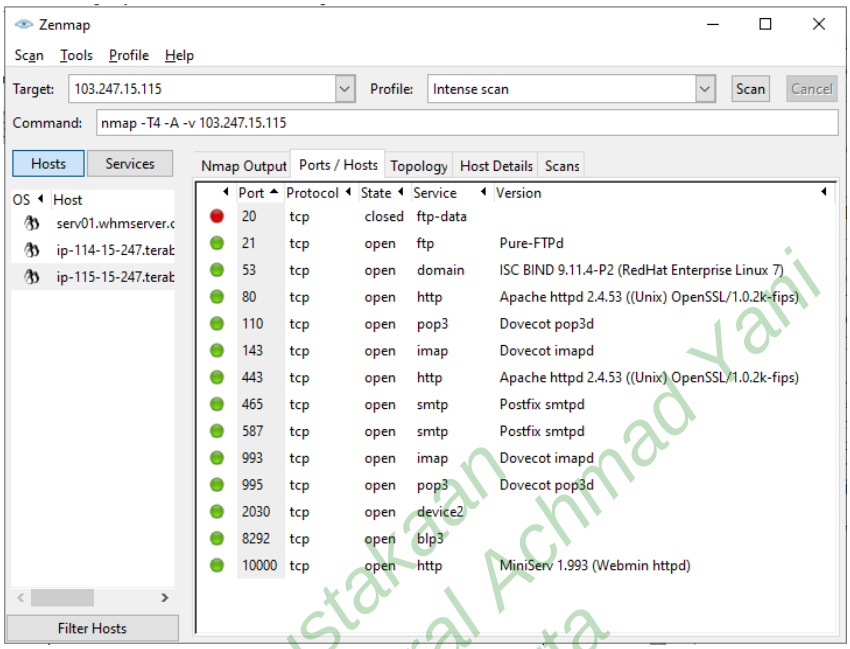
Pemindaian situs web ftti.unjaya.ac.id menggunakan Nmap terdapat hasil seperti Gambar 4.5. Pada pemindaian ini terdapat 12 port yang terbuka yaitu 21, 22, 25, 53, 80, 110, 143, 443, 465, 597, 993, dan 995 dengan informasi yang ditampilkan seperti *protocol*, *service*, dan *version*.




**Gambar 4.6** Pemindaian Nmap pada elearning.ftti.unjaya.ac.id

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

Pada situs web elearning.ftti.unjaya hanya terdapat 5 port yang terbuka yaitu 21, 80, 443, 8292, dan 10000 dengan informasi seperti yang ditampilkan Gambar 4.6.




**Gambar 4.7** Pemindaian Nmap pada app.ftti.unjaya.ac.id

Sedangkan pada situs web app.ftti.unjaya.ac.id terdapat 14 output port dengan 1 port yang tertutup. Ditunjukan pada Gambar 4.7 terdapat yang tertutup yaitu 20 sebagai *file transfer protocol* tipe data, dan 13 port yang terbuka yaitu 21, 53, 80, 110, 143, 443, 465, 587, 993, 2030, 8292, dan 10000 dengan informasi yang ditampilkan.

### 4.3.3 Pemindaian kerentanan menggunakan WPScan

Pada penelitian ini, WPScan digunakan pada situs web ftti.unjaya.ac.id. Karena hanya situs web tersebut yang menggunakan WordPress. Pemindaian ini mendapatkan hasil yang menjelaskan bahwa ftti.unjaya.ac.id masih dalam kategori yang cukup aman. Berikut hasil scan pada WPScan. Pemindaian ini menggunakan *API TOKEN* agar bisa menampilkan semua hasil pemindaian oleh WPScan. Dalam pemindaian, peneliti menambahkan perintah setelah *url* untuk menampilkan proses *enumeration* pada situs web tersebut seperti `-e vp` untuk memproses *enumeration* pada *vulnerability plugins* dan `-e vt` untuk memproses *enumeration* pada *vulnerability themes*.

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

**Gambar 4.8** Tampilan pertama pemindaian WPScan

Pada tampilan pertama menunjukan beberapa informasi tentang headers, robots.txt, dan *output* lainnya. Hasil yang ditunjukan pada Gambar 4.8 menunjukan bahwa situs web ftti.unjaya.ac.id tidak memiliki kerentanan yang parah. Hal tersebut dijelaskan dengan *icon* yang berwarna hijau.

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

```
C:\Program Files\WindowsApps\Microsoft.PowerShell_7.2.5.0_x64__8wekyb3d8bbwe\pwsh.exe
[+] jetpack
 | Location: https://ftti.unjaya.ac.id/wp-content/plugins/jetpack/
 | Last Updated: 2022-08-02T14:06:00.000Z
 | [!] The version is out of date, the latest version is 11.2
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 11.1.2 (100% confidence)
 | Found By: Query Parameter (Passive Detection)
 |  - https://ftti.unjaya.ac.id/wp-content/plugins/jetpack/css/jetpack.css?ver=11.1.2
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - https://ftti.unjaya.ac.id/wp-content/plugins/jetpack/readme.txt
 |  Change Log (Aggressive Detection)
 |   - https://ftti.unjaya.ac.id/wp-content/plugins/jetpack/CHANGELOG.md, Match: '## 11.1.2 -'

[+] onepress-plus
 | Location: https://ftti.unjaya.ac.id/wp-content/plugins/onepress-plus/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 2.2.8 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - https://ftti.unjaya.ac.id/wp-content/plugins/onepress-plus/readme.txt

[+] whatsapp-for-wordpress
 | Location: https://ftti.unjaya.ac.id/wp-content/plugins/whatsapp-for-wordpress/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | The version could not be determined.

[+] wordpress-seo
 | Location: https://ftti.unjaya.ac.id/wp-content/plugins/wordpress-seo/
 | Last Updated: 2022-08-09T09:29:00.000Z
 | [!] The version is out of date, the latest version is 19.5.1
 |
 | Found By: Comment (Passive Detection)
 |
 | Version: 19.3 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - https://ftti.unjaya.ac.id/, Match: 'optimized with the Yoast SEO plugin v19.3 -'
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - https://ftti.unjaya.ac.id/wp-content/plugins/wordpress-seo/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - https://ftti.unjaya.ac.id/wp-content/plugins/wordpress-seo/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:01:00 <=> (137 / 137) 100.00% Time: 00:01:00

[i] No Config Backups Found.

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 6
 | Requests Remaining: 57

[+] Finished: Thu Aug 11 00:08:58 2022
[+] Requests Done: 197
[+] Cached Requests: 0
[+] Data Sent: 64.094 KB
[+] Data Received: 1.217 MB
[+] Memory used: 275.344 MB
[+] Elapsed time: 00:01:36
PS C:\Windows\System32>
```

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

**Gambar 4.9** Tampilan kedua pemindaian WPScan

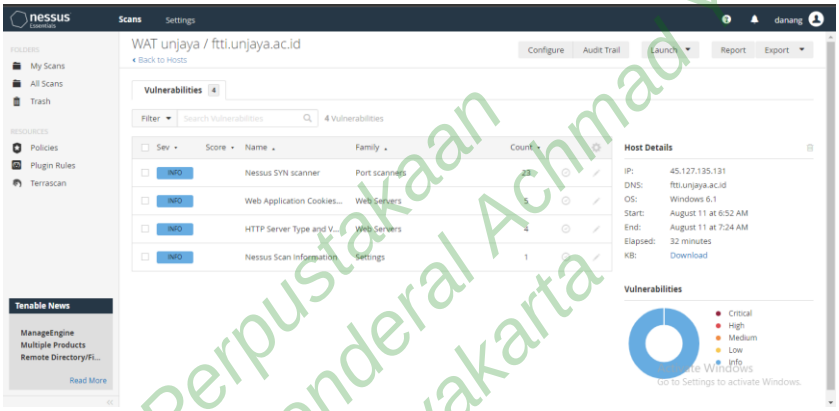
Pada tampilan kedua terdapat peringatan tentang versi WordPress yang masih menggunakan 19.3, sedangkan versi terbaru yaitu 19.5.1. Pada Gambar 4.9 juga ditunjukan bahwa situs web ftti.unjaya.ac.id tidak ditemukan *Config Backups*. Namun, hal ini tidak terlalu berisiko pada keentanan situs web

### 4.3.4 Pemindaian kerentanan menggunakan Nessus

Dari hasil yang ditemukan dari ketiga pemindaian IP dari Nessus, terdapat beberapa kerentanan. Pada Nessus terdapat beberapa tingkatan kategori

kerentanan yang ditandai dengan *icon* warna yang berbeda. *Icon* warna biru menunjukan *Info*, warna kuning menunjukan *Low*, warna *orange* menunjukan *Medium*,warna merah menunjukan *High*, warna merah tua menunjukan *Critical* dan warna ungu menunjukan *Mixed* yaitu terdapat beberapa kategori risiko yang berada dalam satu kelompok. Tingkatan risiko tersebut juga terdapat tabel yang berupa informasi data yang telah diolah oleh Nessus untuk mempermudah dalam analisis pengolahan data. Berikut hasil pemindaian kerentanan dari ketiga IP berdasarkan kategori tingkat risiko.

1. Pemindaian situs web ftti.unjaya.ac.id

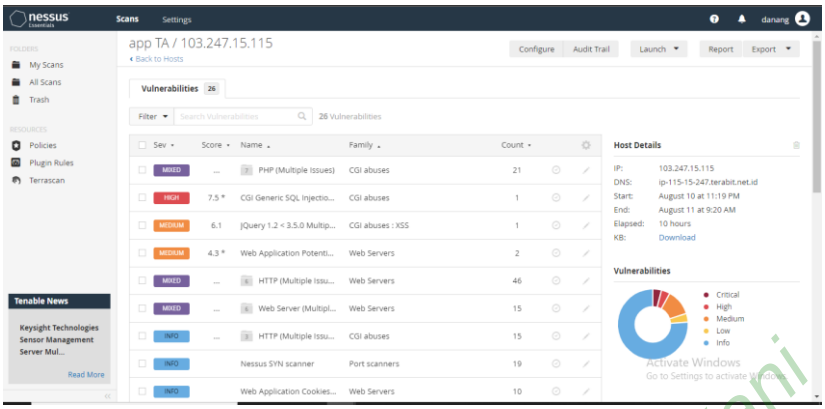



**Gambar 4.10** Pemindaian ftti.unjaya.ac.id pada Nessus

Hasil pemindaian pada Gambar 4.10 menunjukan bahwa pada situs web tersebut memiliki 4 kelompok dengan total 33 hasil pemindaian dari 100.00 % kategori *Info* . Pada hasil penilaian *(Vulnerability Priority Rating ) VPR Top Threats* menunjukan bahwa tidak ada kerentanan yang terdeteksi pada situs web ini.

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

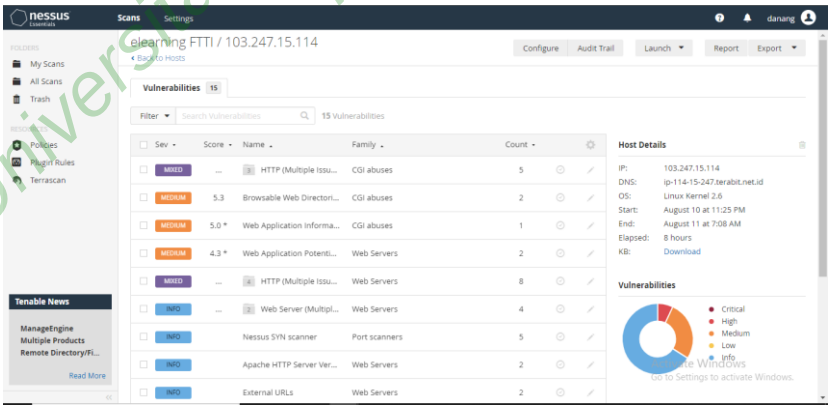
2. Pemindaian situs web app.ftti.unjaya.ac.id




**Gambar 4.11** Pemindaian app.ftti.unjaya.ac.id pada Nessus.

Hasil pemindaian pada Gambar 4.11 menunjukan bahwa pada situs web app.ftti.unjaya.ac.id terdapat 26 kelompok dengan total 174 hasil pemindaian dari semua kategori yang ada. Pada tabel hasil terdapat beberapa kategori seperti *Info* ada 82.18 %, *Low* ada 4.02 %, *Medium* ada 8.05 %, *High ada* 4.02 % , dan *Critical* ada 1.72 %. Namun pada tabel hasil terdapat juga *Mixed* yang berarti didalamnya ada kategori yang campuran pada satu kelompok. Pada hasil penilaian pada *VPR Top Threats* menunjukan bahwa tingkat ancaman pada *level Medium* .

3. Pemindaian situs web elearning.ftti.ac.id



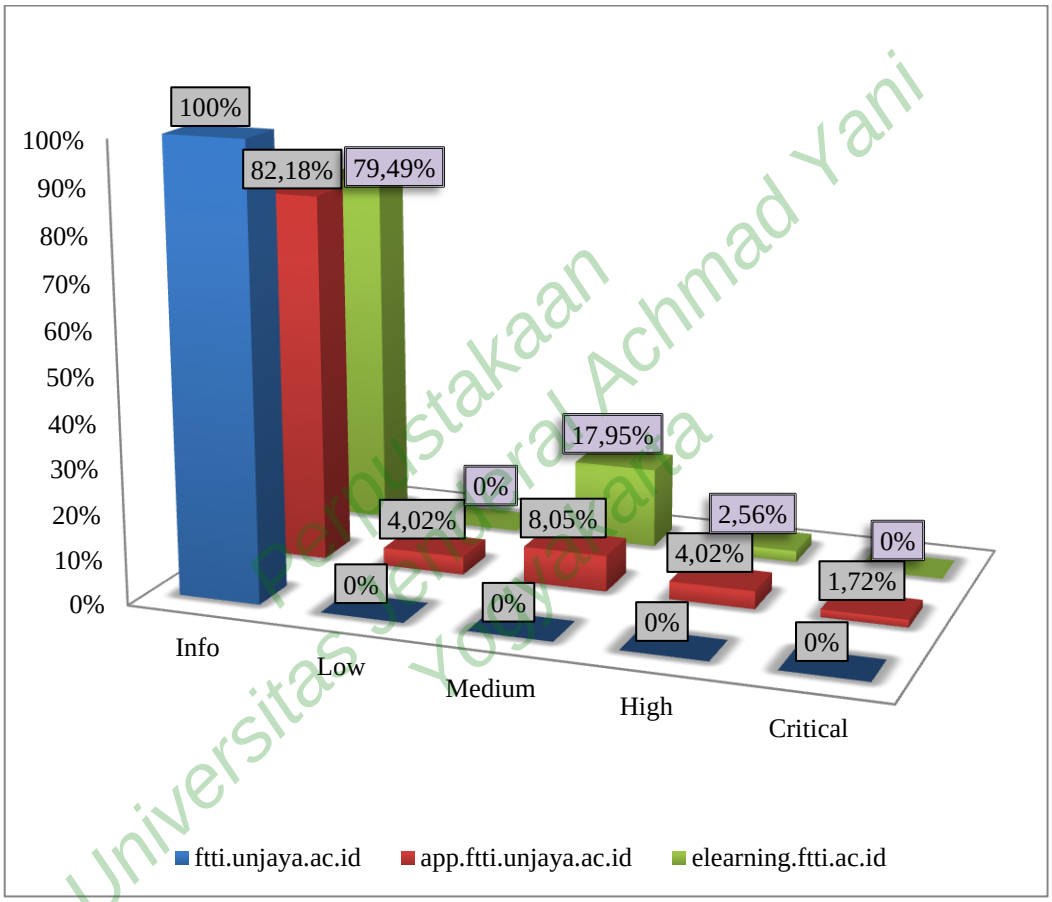

**Gambar 4.12** Pemindaian elearning.ftti.unjaya.ac.id pada Nessus

Sedangkan hasil pemindaian yang ditampilkan pada Gambar 4.12 menunjukan bahwa situs web elearning.ftti.unjaya.ac.id terdapat 15 kelompok dengan total 39 hasil pemindaian dari beberapa kategori tingkat risiko seperti Info

Universitas Jenderal Achmad Yani Yogyakarta Perpustakaan

ada 79.49 %, Medium ada 17.95 %, dan High ada 2.56 %. Pada tabel hasil juga terdapat kelompok Mixed. Hasil penilaian yang terdapat pada *VPR Top Threats* menunjukan bahwa elearning.ftti.unjaya.ac.id memiliki tingkat ancaman pada *level Medium.*

4. Grafik perbandingan kerentanan




Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

**Gambar 4.13** Grafik perbandingan kerentanan

Perbandingan pada pemindaian ketiga situs web tang ditampilkan pada gambar 4.13 menunjukan bahwa tingkat kerentanan pada *level Info* terdapat persentase yang tinggi seperti ftti.unjaya.ac.id dengan 100%, app.ftti.unjaya.ac.id dengan 82,18% dan elearning.ftti.unjaya.ac.id dengan 79,49%. Sedangkan tingkat kerentanan yang memiliki persentase tertendah hanya pada situs web app.ftti.unjaya.ac.id dengan 1,72% yaitu pada *level Critical*.

## 4.4 ANALISIS

Analisis dilakukan dengan mengumpulkan informasi mengenai kerentanan yang telah dipindai. Dengan menganalisis data yang didapat ini penting untuk meningkatkan keamanan situs web dari serangan orang yang tidak bertanggung jawab.

### 4.4.1 Analisis hasil pemindaian menggunakan Nmap

Pada hasil pemindaian menggunakan Nmap, peneliti menemukan beberapa port yang terbuka dari ketiga situs web dan dirangkum dalam tabel dibawah ini yang menjelaskan fungsi *service* pada *port* yang terbuka.

**Tabel 4.1** Daftar fungsi port yang terbuka menggunakan Nmap

| No | Port Terbuka | Fungsi |
|---|---|---|
| 1 | 21/tcp | Port untuk *FTP(File Transfer Protocol)* |
| 2 | 22/tcp | Port standar sebagai *SSH (Secure Shell)*. Berfungsi untuk mengirimkan data dalam bentuk terenkripsi melalui jaringan |
| 3 | 25/tcp | Berfungsi untuk *SMTP ( Simple mail Transfer Protocol)*, memastikan pengiriman email aman melalui jaringan. |
| 4 | 53/tcp | Sebagai domain yang menjadi penerjemah *IP Address* pada setiap host. |
| 5 | 80/tcp | Sebagai *HTTP (Hypertext Transfer Protocol)* yang memungkinkan browser terkoneksi ke halaman web. |
| 6 | 110/tcp | Sebagai *POP3 (Post Office Protocol 3)* yaitu port tanpa dienkripsi |
| 7 | 143/tcp | Sebagai *IMAP (Internet Message Access Protocol)* untuk mengambil email dari server yang jauh tidak harus mengunduh email |
| 8 | 443/tcp | Sebagai HTTP yang digunakan oleh perangkat sebagai protokol virtual untuk mengalihkan lalu lintas pada jaringan. |
| 9 | 465/tcp | Sebagai SMTP, untuk mengamankan email dengan enkripsi pesan menggunakan SSL, namun harus menggunakan port yang terpisah |

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

| No | Port Terbuka | Fungsi |
|---|---|---|
| 10 | 587/tcp | Sebagai *MSA(Mail Submission Agent)* yaitu sebuah protokol yang menangani surat baru. |
| 11 | 993/tcp | Sebagai IMAP yang melalui SSL. |
| 12 | 995/tcp | Sebagai *POP3* melalui SSL. |
| 13 | 2030/tcp | Sebagai *device* 2 yaitu layanan Oracle yang digunakan untuk transaksi Microsoft |
| 14 | 8292/tcp | Sebagai BLP3(Bloomberg Professional) untuk mengatur komunikasi ujung ke ujung. |
| 15 | 10000/tcp | Sebagai HTTP dengan port yang digunakan Webmin untuk layanan pengelolaan yang berbasis web |

Pemindaian menggunakan Nmap yang telah diringkas pada tabel 4.1 menunjukan bahwa setiap port yang terbuka pada masing-masing situs web memiliki fungsi yang berbeda. Namun, dari *output scanning* yang ditampilkan pada gambar 4.6 tentang pemindaian Nmap pada elearning.ftti.injaya.ac.id terdapat hanya 5 (lima) port yang terbuka. Hal ini mengakibatkan port yang tertutup tidak dapat menjalankan tugasnya

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

### 4.4.2 Analisis hasil pemindaian menggunakan WPScan

**Tabel 4.2** Analisis hasil pemindaian ftti.unjaya.ac.id menggunakan WPScan

| No | Hasil Pemindaian | Keterangan | Kerentanan |
|---|---|---|---|
| 1 | Header | Menggunakan server Litespeed | - |
| 2 | Versi WordPress | Versi 5.9.3 | - |
| 3 | WordPress theme | Menggunakan Onepress dengan versi terbaru | - |
| 4 | Plugin Jetpack | Versi 11.1.2 | Versinya sudah kadaluwarsa dan versi terbarunya adalah 11.2 |
| 5 | WordPress-seo | Versi 19.3 | Versinya sudah kadaluwarsa dan versi terbarunya adalah 19.5.1 |

Berdasarka hasil pemindaian menggunakan WPScan, situs web ftti.unjaya.ac.id tidak memiliki kerentanan yang cukup parah. Namun terdapat peringatan tentang versi yang sudah kadaluwarsa pada plugin Jetpack dan Wordpress-seo.

### 4.4.3 Analisis hasil pemindaian menggunakan Nesus

**Tabel 4.3** Tabel ringkasan pengujian menggunakan Nessus

| No | Level | Situs web | Kerentanan |
|---|---|---|---|
| 1 | Critical | ftti.unjaya.ac.id | - |
| | | app.ftti.unjaya.ac.id | PHP *unsupported version detection* |
| | | elearning.ftti.unjaya.ac.id | - |
| 2 | High | ftti.unjaya.ac.id | - |
| | | app.ftti.unjaya.ac.id | Versi PHP yang berjalan pada *web server* jarak jauh adalah sebelum 7.3.24. |
| | | | Versi PHP yang berjalan pada *remote web server* adalah 7.2.x atau 7.3.x sebelum 7.3.21. |
| | | | *CGI generic SQL injection (blind)* |
| | | elearning.ftti.unjaya.ac.id | *Remote web server* menghosting satu atau lebih skrip CGI yang gagal membersihkan *request strings* secara memadai dan tampaknya rentan terhadap serangan 'injeksi SSI'. |
| 3 | Medium | ftti.unjaya.ac.id | - |
| | | app.ftti.unjaya.ac.id | Versi JQuery yang di hosting pada *remote web server* sebelum 3.5.0. |
| | | | *Web application* berpotensi rentan terhadap *Clickjacking* |
| | | | Metode *HTTP TRACE / TRACK* diizinkan. |
| | | elearning.ftti.unjaya.ac.id | Direktori pada *web server* yang dapat dijelajahi. |

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

| No | Level | Situs web | Kerentanan |
|---|---|---|---|
| | | | Setidaknya ada satu *web application* untuk di hosting pada *remote web server* yang mengungkapkan jalur fisik ke direktorinya ketika permintaan salah dikirim ke *remote web server*. |
| | | | *Web application* berpotensi rentan terhadap *clickjacking*. |
| | | | *HTTP TRACE / TRACK methods allowed.* |
| 4 | Low | ftti.unjaya.ac.id | - |
| | | app.ftti.unjaya.ac.id | *Web server* mentransmisikan *cleartext credentials*. |
| | | | *Web server* mengizinkan *password auto-completion* |
| | | elearning.ftti.unjaya.ac.id | - |
| 5 | Info | ftti.unjaya.ac.id | Cookie *web application* sudah kedaluwarsa |
| | | | Plugin pada ftti.unjaya.ac.id menampilkan untuk setiap host yang diuji. |
| | | | Plugin ftti.unjaya.ac.id mencoba untuk menentukan jenis dan versi *remote web server* |
| | | app.ftti.unjaya.ac.id | Transportasi properti HTTP *cookie 'secure'* tidak cocok |
| | | | *Header respons HTTP X-Frame-Options* tidak ada atau permisif |
| | | elearning.ftti.unjaya.ac.id | HSTS hilang dari server HTTPS |
| | | | Pengungkapan Informasi robots.txt *web server*. |
| | | | *Header respons HTTP X-Frame-Options* tidak ada atau permisif |
| | | | Versi server HTTP Apache |

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

Pemindaian menggunakan Nessus yang diringkas pada tabel 4.3 dengan penilaian yang diproses oleh CVSS versi 3.0, penilaian dengan 5 (lima) tingkatan kerentanan tidak sepenuhnya terdapat pada setiap situs web. Ada 2 (dua) situs web yang hanya memiliki sebagian kerentanan seperti ftti.unjaya.ac.id memiliki 1 (satu) tingkat kerentanan yaitu *Info,* dan elearning.ftti.unjaya memiliki 3 (tiga) tingkat kerentanan yaitu *Info, Medium,* dan *High.* Sedangkan pada app.ftti.unjaya.ac.id memiliki semua tingkatan kerentanan yang ada.

## 4.5 PEMBAHASAN

Penelitian yang telah dilakukan mendapatkan hasil dari pemindaian ketiga situs web yang masing-masing memiliki tingkat risiko. Dari ketiga alat pemindain terdapat fungsi pada penelitian ini seperti Nmap untuk mengetahui port yeng terbuka pada situs web target, Nessus sebagai pemindaian celah kerentanan dan mengetahui skor dari risiko yang ditemukan dengan masing-masing risiko terdapat keterangan dan solusi. Dengan solusi yang disarankan oleh Nessus, peneliti merangkum guna menjadikan rekomendasi bagi pihak PUSI agar lebih meningkatkan tingkat keamanan pada situs web FTTI dari serangan orang yang tidak bertanggung jawab. Sedangkan WPScan digunakan untuk memindai kerentanan pada situs web ftti.unjaya.ac.id yang menggunakan WordPress

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

### 4.5.1 Rekomendasi

Rekomendasi perbaikan celah yang diperoleh dari pemindaian situs web dirangkum dalam bentuk tabel. Dengan menggunakan Nessus terdapat nilai kerentanan dan juga tingkatan kerentanan yang dinilai menggunakan CVSS yang ada pada aplikasi tersebut. Pada Tabel 4.4 dibawah ini menunjukan bahwa pemberian skor dari masing-masing tingkat kerentanan hanya terdapat pada tingkatan *Low* sampai *Critical.*

**Tabel 4.4** Tabel Rekomendasi perbaikan celah

| No | Kerentanan | Skor /level | Rekomendasi perbaikan celah |
|---|---|---|---|
| 1 | PHP *unsupported version* | 10.0 | Disarankan untuk meningkatkan ke versi |

| No | Kerentanan | Skor /level | Rekomendasi perbaikan celah |
|---|---|---|---|
| | *detection* | /*Critical* | PHP yang terbaru |
| 2 | Versi PHP yang berjalan pada *remote web server* adalah sebelum 7.3.24. | 7.5 /*High* | Disarankan untuk meningkatkan PHP versi 7.3.24 atau ke versi yang lebih baru |
| 3 | Versi PHP yang berjalan pada *remote web server* adalah 7.2.x atau 7.3.x sebelum 7.3.21. | 7.5 /*High* | Disarankan untuk meningkatkan PHP versi 7.3.22 atau ke versi yang lebih baru |
| 4 | *CGI generic SQL injection (blind)* | 7.5 /*High* | Disarankan untuk mengubah skrip CGI yang terpengaruh, sehingga skrip tersebut lolos dari argumen dengan benar. |
| 5 | *Remote web server* menghosting satu atau lebih skrip CGI yang gagal membersihkan *request strings* secara memadai dan tampaknya rentan terhadap serangan 'injeksi SSI'. | 7.5 /*High* | *Disable server side* walaupun tidak dijalankan, atau batasi akses ke aplikasi yang rentan. |
| 6 | Versi JQuery yang di hosting pada *remote web server* sebelum 3.5.0. | 6.1 /*Medium* | Disarankan untuk meningkatkan JQuery versi 3.5.0 atau yang terbaru. |
| 7 | *HTTP TRACE / TRACK methods allowed* | 5.3 /*Medium* | Disarankan untuk menonaktifkan metode HTTP ini. |
| 8 | Direktori pada *web server* yang dapat dijelajahi. | 5.3 /*Medium* | Disarankan untuk memastikan direktori yang dapat dijelajah tidak membocorkan informasi rahasia atau memberikan akses ke sumber daya sensitif dan gunakan pembatasan akses atau nonaktifkan pengindeksan direktori untuk semua yang melakukannya. |

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

| No | Kerentanan | Skor /level | Rekomendasi perbaikan celah |
|---|---|---|---|
| 9 | Setidaknya ada satu *web application* yang dihosting pada *remote web server* yang mengungkapkan jalur fisik ke direktorinya ketika permintaan salah dikirim ke sana. | 5.0 /*Medium* | Sortir pesan kesalahan yang berisi informasi jalur |
| 10 | *Web application* berpotensi rentan terhadap *clickjacking*. | 4.3 /*Medium* | Kembalikan header HTTP *X-Frame-Options* arau *Content-Security-policy ('frame-ancestors')* dengan respons halaman. Hal ini mencegah konten halaman dirender oleh situs lain saat menggunakan *iframe*. |
| 12 | *Web server* mentransmisikan *cleartext credentials*. | 2.6/*Low* | Pastikan bahwa setiap formulir sensitif mengirimkan konten melalui HTTPS. |
| 13 | *Web server* mengizinkan *password auto-completion* | 2.6/*Low* | Tambahkan atribut '*autocomplete=off*' ke bidang ini untuk mencegah browser melakukan caching kredensial. |
| 14 | Cookie *web application* sudah kedaluwarsa | *Info* | Setiap cookie harus ditinjau dengan cermat untuk menentukan apakah cookie tersebut berisi data sensitif atau duandalkan guna keputusan keamanan. |
| 14 | Transportasi properti HTTP *cookie 'secure'* tidak cocok | *Info* | Tetap waspada untuk memastikan properti aman dan tidak disetek dengan sengaja |
| 15 | *Header respons HTTP X-Frame-Options* tidak ada atau permisif | *Info* | Konfigurasikan *web server* untuk menyertakan '*X-Frame-* |

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

| No | Kerentanan | Skor /level | Rekomendasi perbaikan celah |
|---|---|---|---|
| | | | *Options*' |
| 16 | HSTS hilang dari server HTTPS | *Info* | Konfigurasikan *remote web server* untuk menggunakan HSTS |
| 17 | Pengungkapan Informasi robots.txt *web server* | *Info* | Tinjau file robots.txt, gunakan tag META Robots sebagai ganti entri dalam file robots.txt dan sesuaikan kontrol akses *web server* untuk membatasi akses ke materi sensitif. |
| 18 | Versi server HTTP Apache | *Info* | *Remote host* menjalankan Aphace HTTP server, *web server* terbuka. |

Pada tabel 4.4 menjelaskan bahwa setiap kerentanan dengan masing-masing tingkatan risiko memiliki rekomendasi untuk diperbaiki. Dengan adanya skor dan tingkatan pada setiap kerentanan, maka rekomendasi tersebut bertujuan untuk menunjukan kerentanan apa saja yang paling krusial. Sedangkan tingkatan *Info* tidak diberi skor penilaian kerentanan. Hal ini dikarenakan tingkatan *Info* tidak terdapat kerentanan, namun sekedar memberikan informasi dari pemindaian yang dilakukan.

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta