BAB 4
HASIL PENELITIAN

4.1 RINGKASAN HASIL PENELITIAN

Penelitian ini bertujuan untuk mengevaluasi kerentanan dan keamanan yang terdapat pada situs web *e-learning* FKES dengan alamat eling-fkes.unjaya.ac.id. Penelitian ini telah diberikan izin untuk melakukan analisis pada situs web tersebut. Hasil penelitian diperoleh melalui tiga alat berikut yaitu NsLookup, Nmap, dan Nessus.

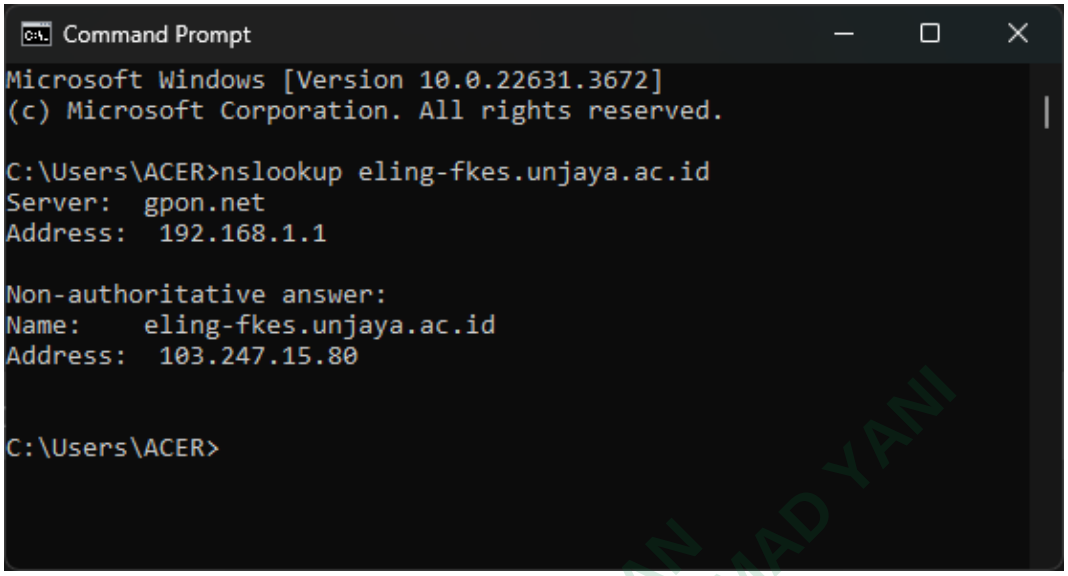
Dari hasil penggunaan NsLookup, berhasil mendapatkan alamat IP dari *website e-learning* FKES dengan domain eling-fkes.unjaya.ac.id, yaitu 103.247.15.80. Setelah memperoleh alamat IP tersebut, dilakukan pemindaian menggunakan Nmap, dan ditemukan beberapa port yang terbuka pada IP 103.247.15.80, dengan total 3 port yang terbuka dan 1 port yang tertutup. Selanjutnya, alamat IP tersebut juga dianalisis menggunakan Nessus. Berdasarkan hasil pemindaian dengan Nessus, terdapat beberapa tingkatan risiko yang dinilai, yaitu *Info, Low, Medium, High,* dan *Critical*. Namun, berdasarkan hasil pemindaian tersebut, *website e-learning* FKES cenderung aman.

4.2 TESTING

Dalam tahap ini, melakukan pemindaian (*scanning*) pada situs web *e-learning* FKES UNJAYA yaitu eling-fkes.unjaya.ac.id. Periode pemindaian dalam pengambilan data dilakukan dari 10 Juni 2024 sampai 27 Juni 2024. Pemindaian ini bertujuan untuk memperoleh informasi yang akan digunakan dalam penulisan laporan tugas akhir. Berikut ini adalah hasil yang diperoleh.

4.2.1 Identifikasi alamat IP menggunakan NsLookup

Sebelum melakukan *scanning* dengan Nmap dan Nessus, melakukan pemindaian menggunakan NsLookup untuk mendapatkan alamat IP pada *website e-learning* FKES UNJAYA.



Gambar 4.1 Hasil Pemindaian Alamat Web

Berdasarkan hasil pemindaian menggunakan NsLookup pada Gambar 4.1, didapatkan bahwa alamat IP pada *website e-learning* FKES UNJAYA yaitu 103.247.15.80.

Hasil pemindaian sebagai berikut:

1. Server
   Nama : gpon.net
   Alamat IP : 192.168.1.1
2. *Non-authoritative answer*
   Nama Domain : eling-fkes.unjaya.ac.id
   Alamat IP : 103.247.15.80

4.2.2 Pemindaian alamat IP menggunakan Nmap

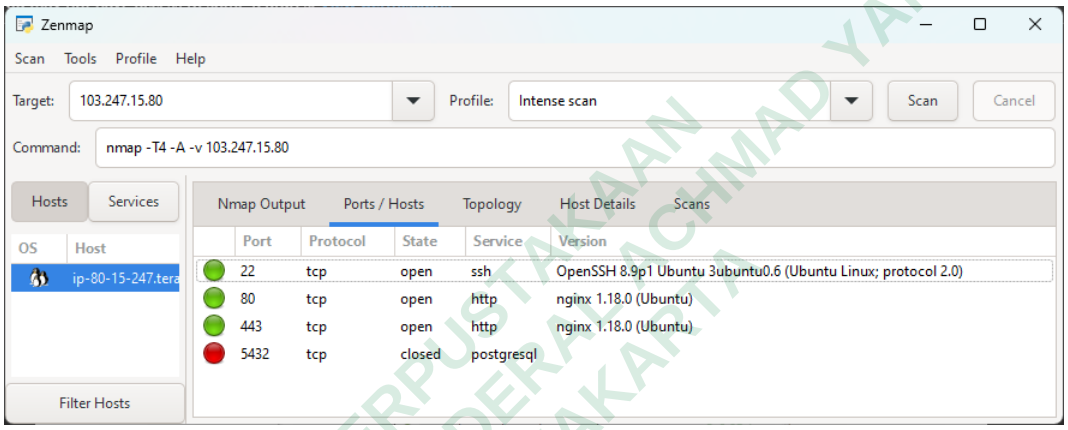
Dari hasil pemindaian menggunakan Nmap terdapat beberapa port yang terbuka. Di Nmap sendiri *output* untuk port yang terbuka akan berwarna hijau, sedangkan port yang tertutup akan berwarna merah. berikut topologi Nmap dari pemindaian alamat IP *website e-learning* target yang ditunjukan pada Gambar 4.2 berikut.

Gambar 4.2 Topologi Nmap

Berikut topologi Nmap dari pemindaian alamat IP *website e-learning* target yang ditunjukan pada Gambar 4.2 di atas. Berikut adalah penjelasan dari topologi tersebut:

1. *localhost*: Titik awal pemindaian yang merupakan komputer atau perangkat yang menjalankan Nmap.
2. *Hop* atau Lompatan: Setiap lingkaran dan titik di sepanjang garis menuju target akhir menunjukkan "*hop*" atau lompatan jaringan. Ini mewakili perangkat atau router yang dilewati oleh paket data saat bergerak dari sumber (*localhost*) ke tujuan akhir (ip-80-15-247.terabit.net.id).
3. Alamat IP: Setiap titik di sepanjang garis diidentifikasi dengan alamat IP atau nama *host* mereka, yang menunjukkan perangkat atau *router* dalam jalur jaringan:
    a. 125.163.176.1
    b. 125.160.1.197
    c. 36.93.250.173
    d. ip-24.135.101.terabit.net.id
    e. ip-214.135.101.terabit.net.id
    f. ip-80-15-247.terabit.net.id (103.247.15.80)

4. Target Akhir: Titik yang ditandai dengan ikon komputer berwarna kuning adalah target akhir dari pemindaian Nmap, yaitu ip-80-15-247.terabit.net.id (103.247.15.80).
5. Visualisasi Rute: Diagram ini menunjukkan rute yang diambil oleh paket data dari sumber (*localhost*) ke tujuan akhir, melewati beberapa *hop* atau lompatan jaringan. Ini memberikan gambaran visual tentang jalur jaringan yang dilalui.

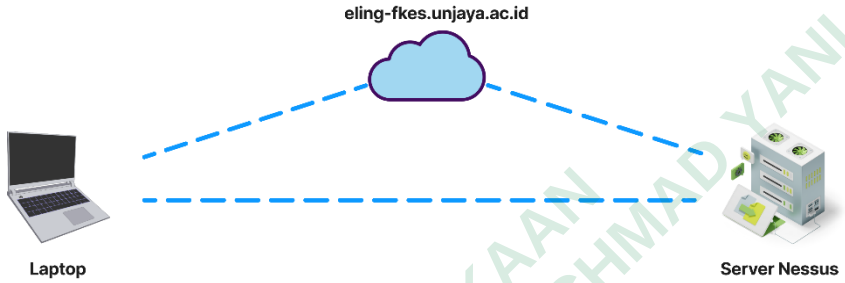


Gambar 4.3 Hasil pemindaian IP menggunakan Nmap

Pada hasil pemindaian alamat IP *website e-learning* yaitu eling-fkes.unjaya.ac.id (103.247.15.80) menggunakan Nmap yang ditunjukan pada Gambar 4.3 di atas, terdapat 3 port yang terbuka, yaitu 22, 80, dan 443. Sedangkan terdapat 1 port yang tertutup yaitu 5432. Dengan informasi kategori *protocol*, *state*, *service*, dan *version*.

4.2.3 Pemindaian alamat IP menggunakan Nessus

Pada tahap ini, penelitian ini juga menggunakan Nessus untuk melakukan pemindaian dan menganalisa *website* target. Nessus menggunakan web server untuk berinteraksi dengan pengguna, tetapi juga memerlukan paket Nessus yang telah diinstal pada laptop untuk melakukan pemindaian dengan efektif. Topologi Nessus dapat dilihat pada Gambar 4.4 berikut.



Gambar 4.4 Topologi Nessus

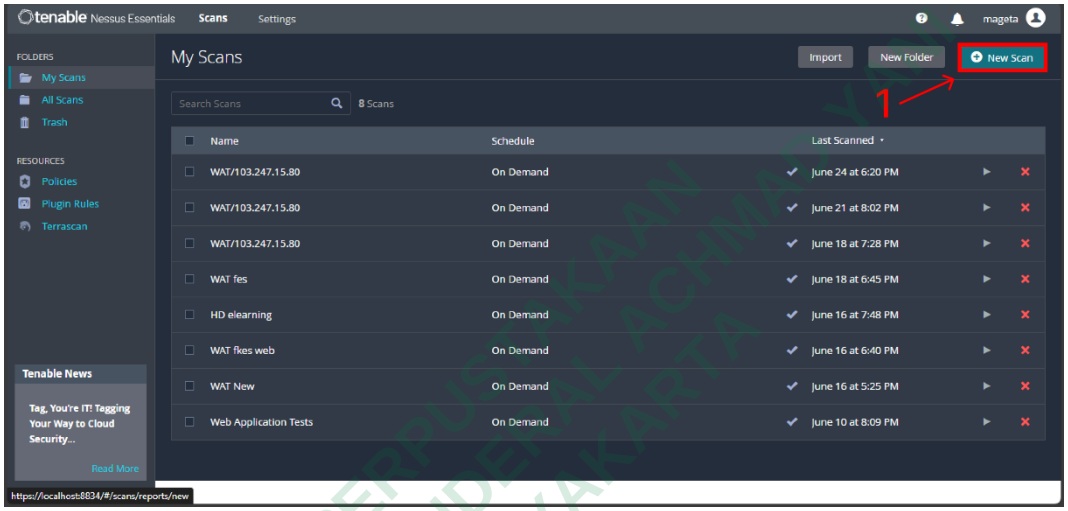
Berdasarkan pemindaian *website e-learning* menggunakan Nessus, terdapat beberapa hasil. Pada Nessus terdapat beberapa kategori kerentanan yang ditunjukan dengan beberapa warna yang berbeda, seperti pada Tabel 4.1 berikut.

Tabel 4.1 Keterangan Kategori Kerentanan Pada Nessus

No	Warna	Nama	Keterangan
1	Merah Gelap	*Critical*	Kerentanan dengan dampak kritis. Skor CVSS v3 tertinggi untuk kerentanan adalah antara 9,0 dan 10,0.
2	Merah	*High*	Kerentanan dengan dampak tinggi. Skor CVSS v3 tertinggi untuk kerentanan adalah antara 7,0 dan 8,9.
3	Jingga	*Medium*	Kerentanan dengan dampak sedang. Skor CVSS v3 tertinggi untuk kerentanan adalah antara 4,0 dan 6,9.
4	Kuning	*Low*	Kerentanan dengan dampak rendah. Skor CVSS v3 tertinggi untuk kerentanan adalah antara 0,1 dan 3,9.
5	Biru	*Information* (*Info*)	Adanya resiko dengan dampak minimal dan sekedar memberikan informasi dari pemindaian yang dilakukan. Skor CVSS v3 tertinggi untuk

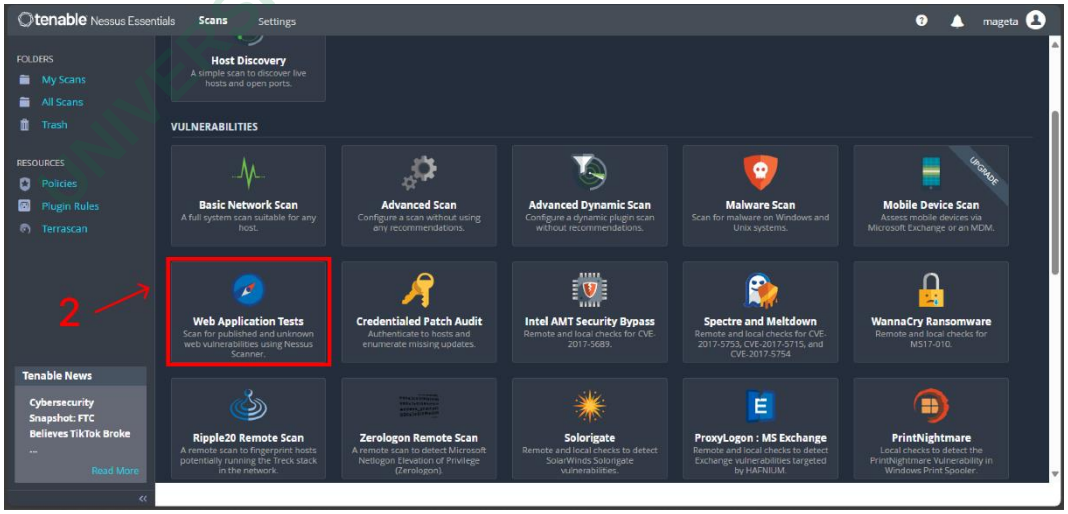
No	Warna	Nama	Keterangan
			kerentanan adalah 0, atau tidak menemukan kerentanan.

Pemindaian yang dilakukan pada penelitian ini dilakukan secara menyeluruh atau *complex*. Berikut pengaturan yang dipakai pada Nessus sebelum melakukan pemindaian pada *website* target:



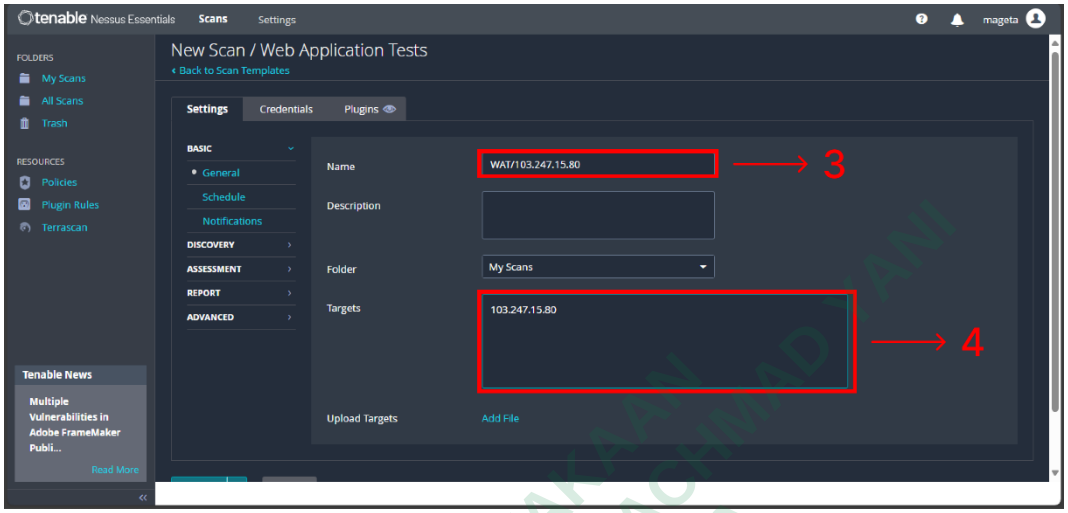
Gambar 4.5 Tahapan Pertama

Pada tahap ini klik "*New Scan*", seperti yang ditunjukkan pada Gambar 4.5, tahapan ini dilakukan untuk awalan proses *scanning* yang akan dilakukan.



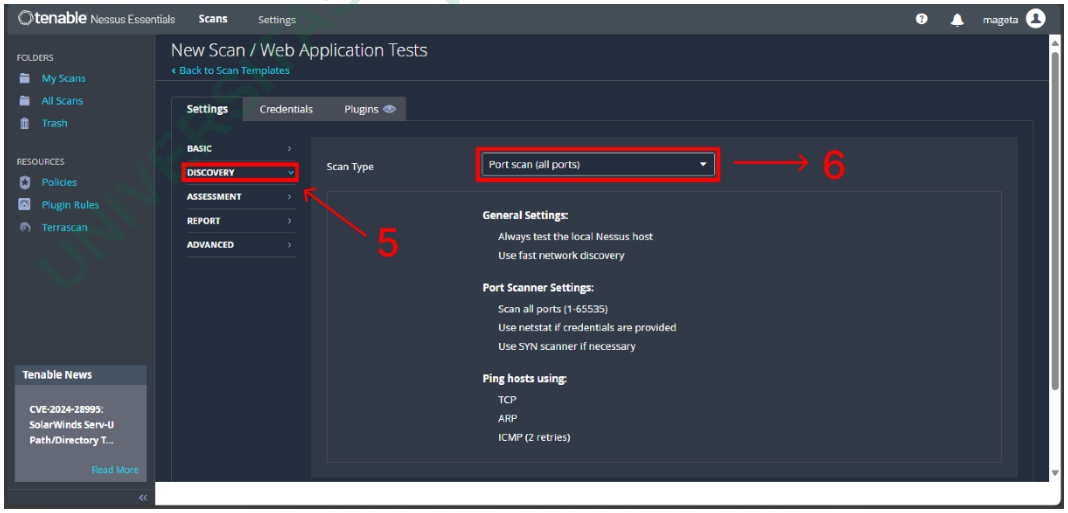
Gambar 4.6 Tahapan Kedua

Karena ingin melakukan pemindaian terhadap kerentanan sebuah *website*, maka pada tahap ini pilih "*Web Application Tests*" seperti yang ditunjukkan pada Gambar 4.6 di atas.



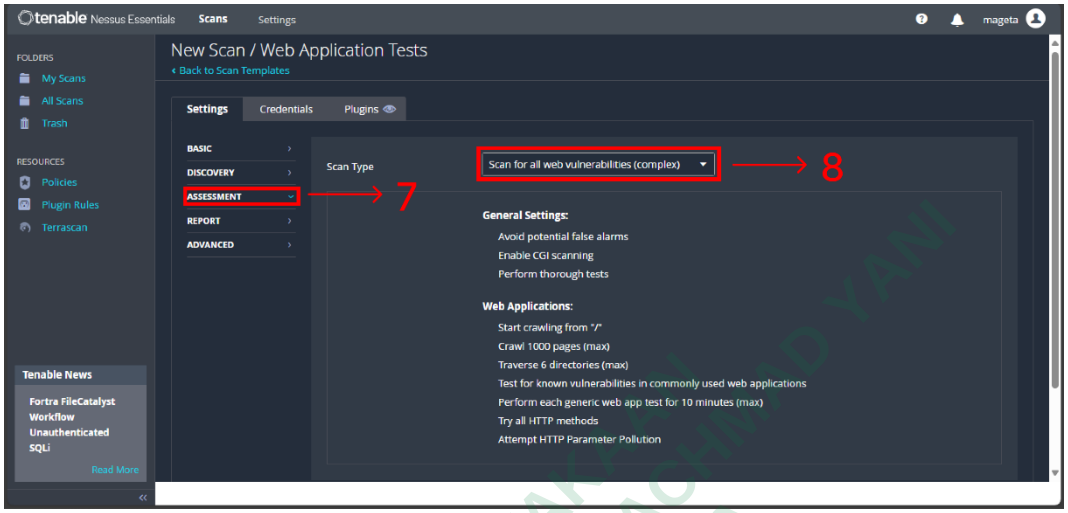
Gambar 4.7 Tahapan Ketiga

Setelah itu pada langkah ke-3, pada kolom *Name* berikan nama pada tugas agar mempermudah dalam pencarian tugas tersebut nantinya. Pada kolom *Targets* pada langkah ke-4 bisa menggunakan *domain* atau alamat IP dari *website* target, seperti pada Gambar 4.7 di atas.



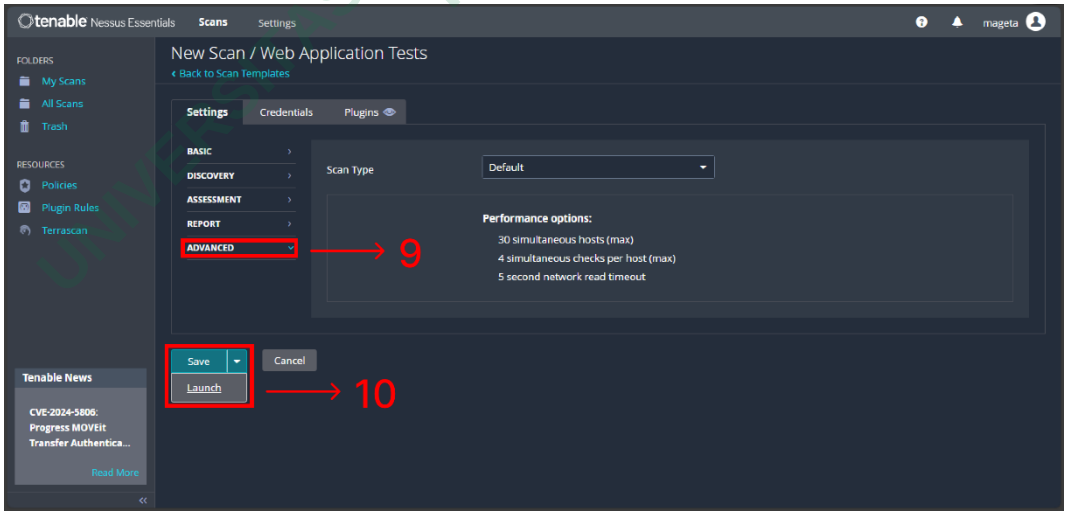
Gambar 4.8 Tahapan Keempat

Pada langkah ke-5, pilih menu *DISCOVERY* seperti yang ditunjukkan pada Gambar 4.8 dan pada *scan type* langkah ke-6 pilih "*Port scan (all ports)"*, bertujuan untuk pemindaian port secara menyeluruh.



Gambar 4.9 Tahapan Kelima

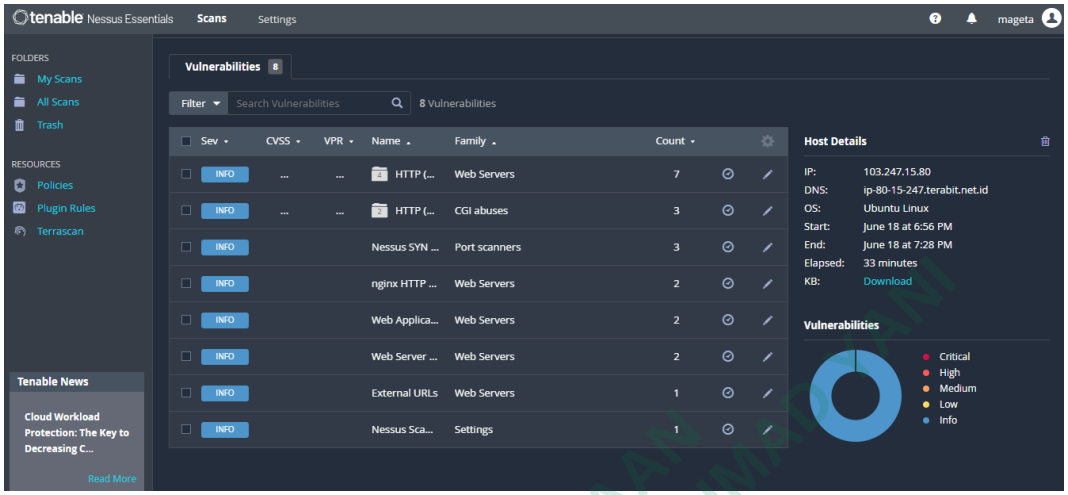
Seperti pada Gambar 4.9 di atas, lalu langkah ke-7 pilih menu *ASSESSMENT* dan pada *scan type* langkah ke-8 pilih "*Scan for all web vulnerabilities (complex)".* Bertujuan agar pemindaian kerentanan yang dilakukan pada Nessus secara menyeluruh.



Gambar 4.10 Tahapan Keenam

Langkah terakhir seperti yang ditunjukkan pada Gambar 4.10 di atas, pada langkah ke-9 pilih menu *ADVANCED* dan langkah ke-10 pada menu *Save*, klik *icon* panah

ke bawah. Setelah itu klik "*Launch"*, Maka Nessus akan melakukan pemindaian, lalu tunggu sampai pemindaian selesai.



Gambar 4. 11 Hasil Pemindaian IP Menggunakan Nessus

Dari hasil pemindaian yang terlihat pada Gambar 4.11 di atas, hasil tersebut terbagi menjadi 8 kelompok dengan total 21 hasil pemindaian. Semua hasil pemindaian termasuk dalam kategori *Info* dengan *score* 100%, yang berarti adanya resiko dengan dampak minimal dan sekedar memberikan informasi dari pemindaian yang dilakukan.

4.3 ANALISA

Dengan mengumpulkan data dari hasil pemindaian kerentanan dengan menggunakan Nmap dan Nessus yang telah dilakukan sebelumnya, maka kemudian akan menganalisis informasi data tersebut. Analisis ini diharapkan dapat mempermudah dalam memahami data hasil pemindaian yang telah dilakukan dan membantu meningkatkan keamanan serta menjaga *website* target dari kemungkinan serangan yang tidak bertanggung jawab.

4.3.1 Analisis hasil pemindaian menggunakan Nmap

Dari hasil pemindaian menggunakan Nmap, ditemukan bahwa terdapat 3 port yang terbuka pada *website e-learning*. Informasi ini kemudian dirangkum dalam Tabel 4.2 di bawah ini, yang menjelaskan fungsi dari setiap layanan yang terbuka pada port tersebut.

Tabel 4.2 Daftar port yang terbuka pada Nmap

No	Port Terbuka	Fungsi
1	22/tcp	digunakan oleh protokol *Secure Shell* (SSH) untuk menyediakan akses masuk yang aman ke komputer atau server dari jarak jauh.
2	80/tcp	digunakan untuk protokol HTTP, yang merupakan protokol utama yang digunakan untuk mentransfer halaman web dan data lainnya di internet.
3	443/tcp	merupakan versi aman dari HTTP. HTTPS menggunakan enkripsi SSL/TLS untuk mengamankan komunikasi antara browser dan server web.

Pemindaian menggunakan Nmap yang telah diringkas pada Tabel 4.2 di atas menunjukkan bahwa setiap port memiliki fungsi yang berbeda. Dan berdasarkan hasil pemindaian pada Gambar 4.2 terdapat 3 yang terbuka dengan 1 port yang tertutup. Port tertutup adalah port yang tidak memiliki layanan yang aktif. Meskipun port ini merespons permintaan dari Nmap, tidak ada aplikasi yang siap menerima koneksi pada port tersebut.

4.3.2 Analisis hasil pemindaian menggunakan Nessus

Dari hasil pemindaian menggunakan Nessus, berikut adalah informasi yang telah dirangkum berdasarkan hasil pemindaian *website e-learning* tersebut dalam Tabel 4.3 di bawah ini.

Tabel 4.3 Daftar hasil kerentanan pada Nessus

No	Level	Skor CVSS	Nama *Output*	Jumlah	Keterangan
1	*Info*	-	HTTP (Web *Servers*) (*Multiple Issues*)	7	-
2	*Info*	-	HTTP (CGI *abuses*) (*Multiple Issues*)	3	-

No	Level	Skor CVSS	Nama *Output*	Jumlah	Keterangan
3	*Info*	-	Adanya port yang terbuka (Nessus SYN *Scanner*)	3	Beberapa port terbuka yang dapat dieksploitasi.
4	*Info*	-	nginx HTTP (Web *Servers*)	2	Informasi mengenai server web nginx yang sedang berjalan. Ini mencakup versi nginx yang digunakan dan bisa digunakan untuk mengidentifikasi potensi kerentanan pada versi tersebut.
5	*Info*	-	Web *Application* (Web *Servers*)	2	Mencakup konfigurasi atau aplikasi tertentu yang dapat dieksploitasi jika tidak dikonfigurasi dengan benar.
6	*Info*	-	Web Server (Web *Servers*)	2	Informasi umum mengenai server web yang berjalan. Ini bisa mencakup berbagai jenis server web yang diidentifikasi selama pemindaian.
7	*Info*	-	*External* URLs (Web *Servers*)	1	Menunjukkan URL eksternal yang dapat diakses dari server web. Ini bisa menjadi titik akses yang dapat dieksploitasi oleh penyerang.
8	*Info*	-	Nessus *Scan Information* (*Settings*)	1	Memberikan informasi tentang pengaturan pemindaian Nessus. Informasi ini bisa sangat berguna untuk memahami konfigurasi pemindaian dan mengidentifikasi area yang memerlukan perbaikan.

Dalam hasil pemindaian kerentanan yang telah dirangkum dalam Tabel 4.3 di atas, pada Nessus penilaian kerentanan berdasarkan CVSS v3.0 (*Common Vulnerability Scoring System*). Nessus menggunakan CVSS untuk memberikan skor pada kerentanan yang ditemukan. CVSS adalah standar yang digunakan untuk menilai tingkat keparahan kerentanan. Nessus juga memberikan faktor risiko seperti *Critical, High, Medium, Low,* dan *Info* berdasarkan tingkat keparahan dan dampak kerentanan.

Hasil pemindaian pada *website e-learning* menunjukkan hanya ada satu kategori tingkat kerentanan, yaitu *Info*. Kategori ini mengindikasikan risiko minimal dengan tidak ada kerentanan yang memiliki dampak signifikan pada *website* tersebut dan sekedar memberikan informasi dari pemindaian yang dilakukan. Meskipun kategori *Info* cukup aman dan tidak dianggap berbahaya secara langsung, namun tetap penting untuk diperhatikan.

Dari 8 kelompok hasil pemindaian yang ditemukan berdasarkan hasil pemindaian yang ditunjukkan pada Tabel 4.3 di atas, terdapat 2 jenis kelompok dengan beberapa masalah (*multiple issues*) yaitu HTTP (Web *Servers*) dan HTTP (CGI *abuses*).

Berikut daftar dari informasi data yang diperoleh telah dirangkum dalam Tabel 4.4 dibawah ini:

Tabel 4.4 Daftar HTTP (*Web Servers*) dan HTTP (*CGI abuses*).

No	Nama *Output*	Daftar *Output*	Jumlah	Keterangan
1	HTTP (Web *Servers*) (*Multiple Issues*)	HTTP *Methods Allowed* (*per directory*)	2	Menunjukkan bahwa beberapa metode HTTP yang diizinkan oleh server mungkin tidak aman. Metode-metode ini perlu diperiksa dan, jika mungkin, dibatasi untuk meminimalkan risiko eksploitasi.
		HTTP *Server Type and Version*	2	Menunjukkan tipe dan versi server HTTP yang digunakan. Informasi ini dapat membantu penyerang

No	Nama *Output*	Daftar *Output*	Jumlah	Keterangan
				dalam mengidentifikasi kerentanan spesifik pada versi server tersebut. Penting untuk memastikan bahwa server dijalankan dalam versi terbaru dan teraman.
		HyperText Transfer Protocol (HTTP) *Information*	2	Menunjukkan bahwa metode TRACE dan TRACK diizinkan pada server. Metode ini dapat digunakan untuk meluncurkan serangan *cross-site tracing* (XST) dan sebaiknya dinonaktifkan jika tidak diperlukan.
		HSTS *Missing from* HTTPS *Server*	1	Menunjukkan bahwa HTTP *Strict Transport Security* (HSTS) tidak diimplementasikan pada server HTTPS.
2	HTTP (CGI *abuses*) (*Multiple Issues*)	*Missing or Permissive Content-Security-Policy frame-ancestors* HTTP *Response Header*	2	Menunjukkan bahwa ada implementasi HTTP *Strict Transport Security* (HSTS) yang hilang atau buruk. Kurangnya HSTS atau implementasi yang buruk dapat membuka peluang bagi serangan *downgrade* atau *man-in-the-middle* (MITM).
		Missing or Permissive X-Frame-Options HTTP *Response Header*	1	Menunjukkan bahwa ada kebijakan keamanan konten (*Content Security Policy*) yang hilang atau buruk. Kurangnya CSP atau implementasi yang buruk dapat meningkatkan risiko serangan pada aplikasi web.

4.4 PEMBAHASAN

Penelitian ini dilakukan dengan mengumpulkan data hasil pemindaian kerentanan dari *website e-learning* menggunakan dua alat, yaitu Nmap dan Nessus. Nmap digunakan untuk memindai port yang terbuka pada *website* target, sedangkan Nessus digunakan untuk mengidentifikasi risiko celah kerentanan keamanan pada *website* target, disertai dengan skor dan solusi untuk setiap risiko yang ditemukan. Hasil pemindaian ini memungkinkan pemberian rekomendasi solusi untuk setiap celah kerentanan yang teridentifikasi, guna menjaga keamanan *website e-learning* FKES UNJAYA dari kemungkinan serangan yang tidak bertanggung jawab.

4.4.1 Rekomendasi

Berikut adalah rekomendasi solusi yang diperoleh dari hasil pemindaian *website* yang telah dirangkum dalam bentuk tabel. Hasil pemindaian menunjukkan bahwa *website* target memiliki tingkat kategori *Info*. Kategori ini mengindikasikan risiko minimal, dengan tidak ada kerentanan yang memiliki dampak signifikan pada *website* tersebut. Secara umum, kategori *Info* hanya memberikan informasi dari pemindaian yang dilakukan.

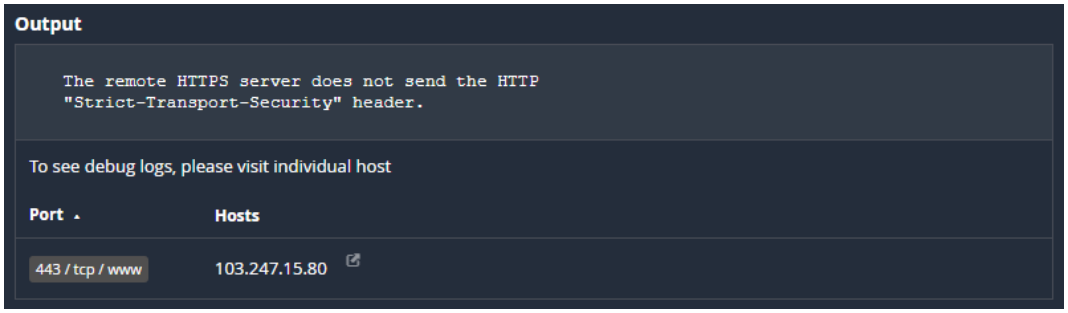
Namun, dari semua hasil pemindaian hanya 4 *output* dalam kategori *Info* yang memperoleh rekomendasi solusi dari Nessus yang ditunjukkan pada Tabel 4.5, Tabel 4.6, Tabel 4.7, dan Tabel 4.8 berikut.

1. HSTS *Missing from* HTTPS Server

Tabel 4.5 HSTS *Missing from* HTTPS Server

No	Nama *Output*	Skor CVSS	Solusi
1	HSTS *Missing from* HTTPS Server	-	Untuk konfigurasikan server web jarak jauh sebaiknya menggunakan HSTS.

Dan dengan *output* dari Nessus seperti pada Gambar 4.12 berikut.



Gambar 4.12 *Output* HSTS *Missing from* HTTPS Server

Berdasarkan Tabel 4.5 dan Gambar 4.12 di atas, berikut data yang diperoleh berdasarkan *output* HSTS *Missing from* HTTPS Server.

a. Nessus *Output*:

   Server HTTPS jarak jauh tidak mengirimkan *header* "*Strict-Transport-Security*".

b. *Hosts* Terdampak:

   Port: 443 / tcp /www

   IP *Address*: 103.247.15.80

Nessus telah mendeteksi bahwa server HTTPS jarak jauh tidak menerapkan HTTP *Strict Transport Security* (HSTS). HSTS adalah *header respons* opsional yang dapat dikonfigurasi pada server untuk menginstruksikan *browser* agar hanya berkomunikasi melalui HTTPS. Kurangnya HSTS memungkinkan terjadinya serangan *downgrade*, serangan SSL-*stripping man-in-the-middle*, dan melemahkan perlindungan terhadap *hijacking cookie*.

Sebagaimana solusi pada Tabel 4.5 di atas, server web dengan alamat IP 103.247.15.80 yang berada di lokasi jarak jauh tidak mengirimkan *header* HSTS yang diperlukan. Kondisi ini dapat membuat server menjadi rentan terhadap beberapa jenis serangan keamanan. Oleh karena itu, langkah-langkah harus diambil untuk mengkonfigurasi server agar menggunakan HSTS, sehingga memastikan bahwa komunikasi selalu aman dan terenkripsi.

2. *Missing or Permissive Content-Security-Policy frame-ancestors* HTTP *Response Header*

Tabel 4.6 *Missing or Permissive Content-Security-Policy frame-ancestors* HTTP *Response Header*

No	Nama *Output*	Skor CVSS	Solusi
2	*Missing or Permissive Content-Security-Policy frame-ancestors* HTTP *Response Header*	-	Atur *header Content-Security-Policy frame-ancestors* agar tidak permisif untuk semua sumber daya yang diminta.

Dan dengan *output* dari Nessus seperti pada Gambar 4.13 dibawah berikut.

Gambar 4.13 *Output Missing or Permissive Content-Security-Policy frame-ancestors* HTTP *Response Header*

Berdasarkan Tabel 4.6 dan Gambar 4.13 di atas, berikut data yang diperoleh berdasarkan *output Missing or Permissive Content-Security-Policy frame-ancestors* HTTP *Response Header*.

a. Nessus *Output*:

Halaman berikut tidak mengatur *header Content-Security-Policy frame-ancestors* atau mengatur kebijakan yang permisif:

http://ip-80-15-247.terabit.net.id/

b. *Hosts* Terdampak:

Port : 80 / tcp /www

IP *Address* : 103.247.15.80

c. Nessus *Output*:

Halaman berikut tidak mengatur *header Content-Security-Policy frame-ancestors* atau mengatur kebijakan yang permisif:

https://ip-80-15-247.terabit.net.id/auth/

https://ip-80-15-247.terabit.net.id/lib/

d. *Hosts* Terdampak:

Port : 443 / tcp /www

IP Address : 103.247.15.80

Server web yang berada di lokasi jarak jauh dalam beberapa responnya mengatur *header Content-Security-Policy* (CSP) *frame-ancestors* dengan kebijakan yang permisif atau bahkan tidak mengaturnya sama sekali. *Header* CSP *frame-ancestors* ini diusulkan oleh W3C (*World Wide Web Consortium*) *Web Application Security Working Group* sebagai cara untuk mengurangi risiko serangan *cross-site scripting* (XSS) dan *clickjacking*.

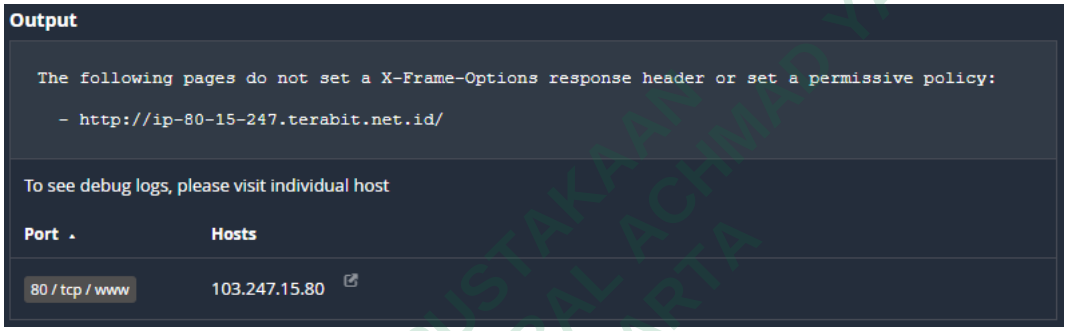
Server web dengan alamat IP 103.247.15.80 yang berada di lokasi jarak jauh tidak mengatur *header Content-Security-Policy* (CSP) *frame-ancestors* dengan benar, sehingga membuatnya rentan terhadap serangan *cross-site scripting* (XSS) dan *clickjacking*. Tindakan harus diambil untuk mengkonfigurasi server agar menggunakan *header* CSP *frame-ancestors* yang tidak memperbolehkan, sehingga memastikan bahwa halaman web tidak dapat dimuat dalam *frame* atau *iframe* di domain yang tidak diizinkan.

3. *Missing or Permissive X-Frame-Options* HTTP *Response Header*

Tabel 4.7 *Missing or Permissive X-Frame-Options* HTTP *Response Header*

No	Nama *Output*	Skor CVSS	Solusi
3	*Missing or Permissive X-Frame-Options* HTTP *Response Header*	-	Atur *header X-Frame-Options* yang dikonfigurasi dengan benar untuk semua sumber daya yang diminta.

Dan dengan *output* dari Nessus seperti pada Gambar 4.14 dibawah berikut.



Gambar 4.14 *Output Missing or Permissive X-Frame-Options* HTTP *Response Header*

Berdasarkan Tabel 4.7 dan Gambar 4.14 di atas, berikut data yang diperoleh berdasarkan *output Missing or Permissive X-Frame-Options* HTTP *Response Header*.

a. Nessus *Output:*

   Halaman berikut tidak mengatur *header X-Frame-Options* atau mengatur kebijakan yang permisif:

   http://ip-80-15-247.terabit.net.id/

b. *Hosts* Terdampak:

   Port : 80 / tcp /www

   IP Address : 103.247.15.80

Server web yang berada di lokasi jarak jauh dalam beberapa responnya mengatur *header X-Frame-Options* dengan kebijakan yang permisif atau bahkan tidak mengaturnya sama sekali. *Header X-Frame-Options* diusulkan oleh Microsoft sebagai cara untuk mengurangi resiko serangan *clickjacking* dan saat ini didukung oleh semua vendor *browser* utama.

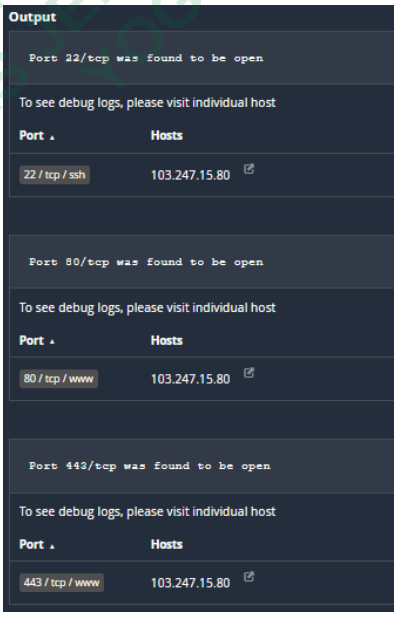
Server web dengan alamat IP 103.247.15.80 yang berada di lokasi jarak jauh tidak mengatur *header X-Frame-Options* dengan benar, sehingga membuatnya rentan terhadap serangan *clickjacking*. Sebaiknya mengkonfigurasi server agar menggunakan *header X-Frame-Options* yang sesuai, sehingga memastikan bahwa halaman web tidak dapat dimuat dalam *frame* atau *iframe* di domain yang tidak diizinkan.

4. Nessus SYN *scanner*

Tabel 4.8 Nessus SYN *scanner*

No	Nama *Output*	Skor CVSS	Solusi
4	Adanya port yang terbuka (Nessus SYN *scanner)*	-	Lindungi dengan filter IP. Filter IP mengatur aturan *firewall* atau filter IP untuk membatasi akses ke port yang terbuka, hanya mengizinkan koneksi dari sumber yang terpercaya.

Dan dengan *output* dari Nessus seperti pada Gambar 4.15 dibawah berikut.



Gambar 4.15 *Output* Nessus SYN *scanner*

Berdasarkan Tabel 4.8 dan Gambar 4.15 di atas, berikut data yang diperoleh berdasarkan *output* Nessus SYN *scanner*.

a. Nessus *Output*:

   Port 22/tcp : Ditemukan terbuka

   Port 80/tcp : Ditemukan terbuka

   Port 443/tcp : Ditemukan terbuka

b. *Hosts* Terdampak:

   Port : 22 / tcp / ssh

   IP Address : 103.247.15.80

   Port : 80 / tcp /www

   IP Address : 103.247.15.80

   Port : 443 / tcp /www

   IP Address : 103.247.15.80

Plugin ini merupakan pemindai port dengan metode *'half-open'* SYN. *Plugin* ini dirancang untuk beroperasi dengan cepat bahkan terhadap target yang dilindungi oleh *firewall.*

Port 22 (SSH), port 80 (HTTP), dan port 443 (HTTPS) pada server dengan alamat IP 103.247.15.80 ditemukan dalam keadaan terbuka. Hal ini menunjukkan bahwa server tersebut sedang terkoneksi pada ketiga port ini. Untuk melindungi server dari potensi serangan, disarankan untuk mengkonfigurasi filter IP atau aturan *firewall* yang membatasi akses ke port-port ini hanya dari alamat IP yang dapat dipercayai.