BAB 5 PENUTUP

5.1 Kesimpulan

Dari penelitian yang telah dilakukan, didapatkan beberapa kesimpulan sebagai berikut

1. Hasil pengujian untuk mengidentifikasi evaluasi risiko celah keamanan sistem pada *web* terbaru Fakultas Ilmu Komputer UPN Veteran Jakarta dilakukan menggunakan metode OSSTMM yaitu sebagai berikut.
    - Menentukan Aset yang akan diproteksi berupa *web* terbaru Fakultas Ilmu Komputer UPN Veteran Jakarta dengan alamat http://new-fik.upnvj.ac.id/
    - Menentukan *Zone Engagement* berupa dua poin yaitu:
        - Mekanisme proteksi menggunakan protokol HTTP, TLS versi 1.0 dan TLS versi 1.1 dan CMS Wordpress *login*.
        - Proses/layanan berupa perkenalan profil Fakultas Ilmu Komputer UPN Veteran Jakarta
    - Mendefinisikan *Scope* yaitu berupa energi listrik untuk menjalankan *server*, kebijakan regulasi menggunakan UU ITE dan menggunakan *Hosting*.
    - Menentukan *Vector* yaitu pengetesan satu arah melalui internet dan menuju sistem target.
    - Menentukan *Channel* dengan menggunakan *Channel Data Network Security*
    - Menentukan tipe tes dengan menggunakan *greybox testing*
    - Menentukan *Rules of Engagement* dengan merujuk Lampiran 1 pada Pakta Integritas Penelitian
    - Melakukan Implementasi dengan poin sebagai berikut
        - *Operations* berjumlah 21
        - *Controls Class-A Interactive* berjumlah 8
        - *Controls Class-B Interactive* berjumlah 4
        - *Limitations* berjumlah 31

- Melakukan perhitungan RAV dengan menghitung *Porosity*, OPSEC *Base*, *Total Loss Controls*, *Total Missing Controls*, *True Controls*, *Full Controls*, *Total True Coverage, Limitations*, *Actual Security Delta*, *True Protection* dan hasil akhir berupa *Actual Security.*
- Perhitungan poin tersebut akan ditaruh pada format STAR sebagai *report* merujuk pada Gambar 4.92.
- Terakhir melakukan rekomendasi yang merujuk pada Tabel 4.4, sehingga celah keamanan tersebut agar dilakukan perbaikan lebih lanjut.

2. Hasil pengujian menggunakan metode OSSTMM menunjukkan luaran nilai berupa *Actual Security* sebesar 74,0088 sehingga dapat disimpulkan nilai tersebut kurang dari 100 sehingga *security* pada *web* terbaru Fakultas Ilmu Komputer UPN Veteran Jakarta masih kurang baik. Kemudian ditemukan poin *Limitations* yaitu berupa,
    a. *Vulnerability* berupa *Cross-origin resource sharing:arbitrary origin Trusted* pada 4 subURL
    b. *Vulnerability* berupa *Cross Site Scripting (Reflected)* yang ditemukan pada 25 subURL.
    c. *Weakness* berupa mendapatkan *username* dan *password* untuk *login* CMS Wordpress.
    d. *Concerns* berupa Versi TLS yang sudah usang dan harus segera dilakukan *update/patch*.

5.2 Saran

Berdasarkan penelitian yang dilakukan, peneliti menyarankan agar kerentanan yang ditemukan pada *web* tersebut agar diperbaiki secepatnya agar tidak dieksploitasi dan disalahgunakan, perbaikan tersebut berfokus pada *Limitations* dengan poin *Vulnerability*, *Weakness* serta *Concerns* yang ditemukan pada Tabel 4.3 Rangkuman Keamanan OSSTMM: Data Network *Security* Channel serta Tabel 4.4 sebagai rekomendasi perbaikan. Dengan adanya perbaikan pada aspek *Limitations*, terjadi pengurangan

temuan sehingga didapatkan nilai yang mendekati 100 (*Security* Sempurna) dalam penilaian *Actual Security*.