

## **BAB 5**

### **PENUTUP**

#### **5.1 Kesimpulan**

Dari penelitian yang telah dilakukan, didapatkan beberapa kesimpulan sebagai berikut.

1. Penelitian ini dilakukan dengan menguji dua dari lima channel keamanan yang ada pada metode OSSTMM yaitu Data Network Security Channel, dan Physical Security Channel Security Channel, di mana objek penelitian yang dipilih adalah situs Pembelajaran Daring Universitas PQR.
2. Jenis vulnerability yang diujikan pada metode OSSTMM diantaranya adalah Brute Force Login, DoS, injeksi SQL dan XSS (Cross-Site Scripting).
3. Hasil perhitungan nilai actual security pada Data Network Security Channel adalah sebesar 83,3464 sedangkan pada Physical Security Channel, nilai actual security yang didapatkan adalah 85,1582.
4. Kontrol keamanan pada Data Network Security Channel sudah cukup baik. Dari percobaan serangan yang dilakukan oleh Penulis, didapatkan hasil bahwa sistem sudah dapat mengantisipasi serangan Brute Force Login, DoS, injeksi sql dan Cross-Site Scripting (XSS) dengan baik sehingga tidak terjadi kebocoran data sistem pada penelitian ini, perbaikan pada channel ini dapat dilakukan dengan Membeli sertifikat SSL dari organisasi terpercaya untuk menghindari Man-In-The-Middle attack dan menonaktifkan protokol TLS versi 1.0 dan versi 1.1, serta mengaktifkan protokol TLS versi 1.2 dan 1.3.
5. Kontrol keamanan aset pada Physical Security Channel juga sudah cukup baik, lingkungan aset terjaga dan terpelihara dari berbagai ancaman dan gangguan yang berpotensi merusak aset. Perbaikan pada channel ini dapat dilakukan dengan mengoreksi vulnerability, weakness dan concern yang ditemukan.

## 5.2 Saran

Dari penelitian yang telah dilakukan, dapat disimpulkan bahwa metode OSSTMM memiliki panduan lengkap yang dapat membantu peneliti untuk menguji keamanan suatu aset secara menyeluruh. Namun demikian, lingkup serangan yang diujikan pada Data Network Security Channel tidak cukup banyak dan cenderung sedikit sehingga metode ini kurang tepat untuk digunakan sebagai acuan keamanan suatu aplikasi Web. Metode ini akan lebih tepat untuk diterapkan sebagai metode untuk pengujian infrastruktur keamanan suatu organisasi secara menyeluruh dengan menganalisis semua channel yang tersedia untuk mendapatkan hasil yang lebih maksimal. Untuk penelitian selanjutnya, peneliti lain dapat menembangkannya dengan memilih channel lain untuk dapat melengkapi keseluruhan pengujian keamanan terhadap aset terkait.