BAB V PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian *penetration testing* yang telah dilakukan menggunakan metode PTES (*Penetration Testing Execution Standard*) yang dimulai dari tahap *pre-engagement* sampai *reporting* dengan menggunakan teknik *exploit, scanning service, nmap, sniffing, dan password guessing* terhadap kerentanan *server* Universitas VWX atau server SIM dengan melakukan pengujian dari kesalahan *user* maupun keamanan *server*, dapat disimpulkan bahwa:

1. Tingkat kerentanan pada *server* Universitas VWX cukup besar dan merupakan kerentanan yang berpotensi untuk dimanfaatkan dalam melakukan tindakan kejahatan dunia maya. Walaupun *firewall* pada *server* target aktif yang dapat mengganggu proses *remote* dari *server* ke *client* (*pentester*), namun dalam mendeteksi dan eksploitasi kerentanan masih dapat dilakukan tanpa memasang *backdoor*.
2. Kerentanan yang berpotensi diserang oleh *attacker* merupakan kerentanan pada layanan port 80 dan 53 yaitu *Password Guessing* tingkat kerentanan *critical*, *Cross-Site Tracing* (XST) dengan tingkat kerentanan *medium, Sensitive Data Exposure* tingkat kerentanan *medium, dan DDoS Attack* tingkat kerentanan *medium.*
3. Adapula tingkat kerentanan *high* yaitu *SSL Version 2 and 3 Protocol Detection*, dan *Sniffing*.
4. Kemudian pada *vulnerability SSL Certificate Expiry, SSL Self-Signed Certificate,* dan *SSL Certificate Cannot Be Trusted* dengan tingkat kerentanan *medium* membuktikan sertifikat SSL yang tidak *valid*.

Penemuan kerentanan tersebut membuktikan bahwa *server* Universitas VWX masih belum memenuhi komponen keamanan informasi yaitu *Confidentiality* (Kerahasiaan) dan *Integrity* (Keutuhan), serta kerentanan yang banyak muncul terdapat pada *port* 80 (HTTP). Solusi dalam melakukan pencegahan maupun perbaikan pada sistem *server* Universitas VWX dari serangan yang dapat terjadi di kemudian hari yaitu dengan melakukan *update* versi PHP yang *support*, menonaktifkan *method HTTP TRACE* karena apabila aktif maka penyerang akan mengkombinasikannya dengan serangan XSS dan membaca *cookie* otentikasi, membeli atau mengganti sertifikat SSL, menggunakan protokol yang aman yang dilengkapi enkripsi data, selalu memantau *traffic* jaringan, menutup direktori phpinfo, dan menggunakan *password* dan *username* yang sulit untuk ditebak khususnya yang mempunyai akses sebagai admin karena sekali tertebak maka seluruh data dapat dikuasai oleh penyerang

5.2 Saran

Dalam penelitian *penetration testing* yang telah dilakukan, diperlukan suatu pengujian dan pengembangan lebih lanjut mengenai uji penetrasi pada kerentanan *server*. Berikut adalah saran untuk penelitian ini:

1. Penambahan kegiatan *Sniffing* yaitu *Active Sniffing* melalui *ARP Poisoning* dan MITM (*Man In The Middle Attack*) yang bisa dilakukan untuk tahap *Post Exploitation* agar dapat mendemonstrasikan eksploitasi serangan dengan mengubah isi paket data dengan tujuan meyakinkan target terkait kerentanan yang ditemukan.
2. Melakukan eksploitasi dengan *tools* lain seperti *Veil-Evasion Framework*, *Social Engineering Toolkit*, atau antarmuka *Metasploit Framework* lainnya seperti *Armitage* dan *Msfcli* agar hasil eksploitasi lebih baik.