BAB 5
KESIMPULAN DAN SARAN

5.1. KESIMPULAN

Berdasarkan penelitian yang dilakukan, maka didapatkan kesimpulan yaitu:

1. Hasil pengujian *Scanning Port* pemantauan keamanan mengungkapkan beberapa *port* yang terbuka dan tertutup pada *server repository* IT Telkom Purwokerto, antara lain port 80 HTTP/WEB, *port* 445 HTTPS, dan *port* 9595 PDS. Disarankan menggunakan *firewall* untuk mengizinkan *port* tertentu sambil memblokir yang lain dalam upaya mempertahankan jaringan dari serangan *cyber*.
2. Hasil pengujian *vulnerability* di Zenmap didapatkan, pengujian protocol HTTP host target yang diperiksa mendukung protokol *POST, OPTIONS, GET,* dan *HEAD*. Disarankan menggunakan metode *POST* daripada metode *GET* karena lebih aman dan tidak pernah mengungkapkan data pengguna melalui URL web atau log server. Pengujian *HTTP proxy scanning* menunjukkan bahwa target ditemukan sebagai proxy yang difilter HTTP. Pengujian mendeteksi kerentanan *Cross-site scripting* menunjukkan tidak ada *cross-site scripting* yang terdeteksi. Hasil dari pengujian *SQL Injection* menunjukkan pada host target, injeksi SQL ditemukan.
3. Hasil pengujian pemantauan keamanan menggunakan *tools* Nessus diperoleh empat kategori kerentanan IP target untuk Repositori IT Telkom Purwokerto berupa 15 kerentanan untuk info, 3 untuk *medium*, 1 untuk *high,* dan 1 untuk *critical*. Disarankan untuk menggunakan Apache versi terbaru, membatasi akses ke *server DNS* dari jaringan publik atau konfigurasikan ulang untuk memblokir *request*, membatasi query ke host, mengembalikan *header HTTP X-Frame-Options* atau *Content-Security-Policy* (dengan arahan *'frame-ancestors'*) dengan respons halaman, dan memperbarui file konfigurasi Apache untuk menonaktifkan status mod atau membatasi akses ke host tertentu.

5.2. SARAN

Setelah melakukan penelitian Analisis Website Repository Security Institut Teknologi Telkom Purwokerto Menggunakan Metode *Vulnerability Assessment*, maka dapat diberikan, antara lain:

1. Pengujian yang dilakukan hanya sebatas rekomendasi perbaikan web untuk masalah keamanan web. Penelitian lebih lanjut dimaksudkan untuk membandingkan *Network Scanner* dengan pengujian serangan pada server, dan pengujian penetrasi,
2. Sangat penting untuk mengenkripsi data penting untuk membatasi bahaya kebocoran informasi penting,
3. Perlu adanya backup data secara berkala,
4. Atasi kerentanan pada server sehingga kerentanan pada jaringan server tidak dalam kategori *Critical*, *High* maupun *Medium* yang memungkin merusak sistem.