BAB II
TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

Tinjauan pustaka dalam penelitian ini akan membahas konsep-konsep utama yang menjadi dasar dalam pelaksanaan penetration testing pada aplikasi *mobile*, standar keamanan informasi ISO 27001, dan metode pengujian keamanan aplikasi.

2.1.1 ISO 27001 dan *Technical Vulnerability Management* (A.12.6.1)

ISO 27001 adalah standar internasional untuk Sistem Manajemen Keamanan Informasi (SMKI). Kontrol A.12.6.1 mengatur *Technical Vulnerability Management*, yakni identifikasi dan mitigasi kerentanan teknis secara berkelanjutan (Humphreys, 2016). Ini penting untuk menjaga keamanan informasi di organisasi.

2.1.2 *Penetration Testing*

Metodologi *penetration testing* umumnya mengikuti tahapan yang sistematis dan terstruktur. Beberapa metodologi yang populer digunakan diantaranya adalah:

a. Metodologi OWASP (Open Web Application Security Project): Khusus digunakan untuk pengujian aplikasi web, metodologi ini mencakup tahap persiapan, pengujian, dan pelaporan hasil.
b. Metodologi PTES (Penetration Testing Execution Standard): Merupakan standar yang mencakup seluruh siklus penetration testing, mulai dari fase pre-engagement hingga pelaporan dan pasca-uji.
c. NIST SP 800-115: Merupakan panduan resmi dari National Institute of Standards and Technology (NIST) yang menyediakan pedoman untuk perencanaan dan pelaksanaan penetration testing pada sistem informasi organisasi (Scarfone et al., 2008).

2.1.3 Metode *Penetration Testing*

Penetration testing dapat dikategorikan berdasarkan tujuan dan ruang lingkup pengujian:

a. Black Box Testing: Penguji tidak memiliki informasi awal tentang sistem yang diuji, sehingga simulasi serangan dilakukan seperti halnya seorang penyerang eksternal.
b. White Box Testing: Penguji memiliki akses penuh terhadap informasi sistem, termasuk kode sumber, diagram jaringan, dan konfigurasi. Hal ini memungkinkan pengujian yang lebih mendalam dan menyeluruh.

c. Gray Box Testing: Kombinasi antara black box dan white box, dimana penguji memiliki pengetahuan terbatas tentang sistem. Ini menggambarkan skenario di mana penyerang memiliki akses terbatas atau pengetahuan internal terbatas.

2.1.4 Keamanan Aplikasi *Mobile*

Aplikasi *mobile* menjadi target utama serangan siber, terutama yang mengelola data sensitif. Pengujian keamanan yang komprehensif diperlukan untuk melindungi data pengguna dan memastikan integritas sistem (Veracode, 2017).

2.1.5 Implementasi *Technical Vulnerability Management*

Implementasi *Technical Vulnerability Management* dalam organisasi harus terstruktur dan berkelanjutan. Ini mencakup pemantauan berkelanjutan, penilaian risiko, dan respon cepat terhadap ancaman (Jones & Ashenden, 2005). Pendekatan ini esensial untuk memenuhi persyaratan ISO 27001.

2.2 Dasar Teori

2.2.1 ISO 27001 dan *Technical Vulnerability Management*

ISO 27001 adalah standar internasional yang menyediakan kerangka kerja untuk Sistem Manajemen Keamanan Informasi (SMKI), yang bertujuan melindungi kerahasiaan, integritas, dan ketersediaan informasi dalam suatu organisasi. Standar ini membantu organisasi mengidentifikasi risiko keamanan informasi dan menerapkan kontrol yang tepat untuk mengelola dan mengurangi risiko tersebut. Salah satu kontrol penting dalam ISO 27001 adalah A.12.6.1, yang berfokus pada Technical Vulnerability Management. Kontrol ini mengharuskan organisasi untuk secara terus-menerus mengidentifikasi, mengevaluasi, dan mengatasi kerentanan teknis dalam sistem informasi. Proses ini meliputi pemantauan kerentanan, penerapan patch keamanan, dan tindakan mitigasi untuk mengurangi risiko eksploitasi. Technical Vulnerability Management penting dalam menjaga postur keamanan organisasi dengan memastikan bahwa sistem tetap terlindungi dari ancaman yang terus berkembang, sehingga mendukung keamanan informasi yang sesuai dengan standar ISO 27001 (Humphreys, 2016).

2.2.2 *Penetration Testing* dan *Greybox Testing*

Metode grey box dipilih dalam penetration testing karena memberikan keseimbangan antara pendekatan black box dan white box, sehingga dapat memberikan gambaran yang lebih realistis tentang keamanan sistem dari perspektif pengguna internal dengan akses terbatas. Dalam metode ini, penguji memiliki sebagian informasi tentang sistem,

seperti arsitektur jaringan atau kredensial login, yang memungkinkan pengujian dilakukan lebih efisien dibandingkan dengan black box testing, di mana penguji tidak memiliki informasi awal sama sekali. Metode grey box memungkinkan pengujian yang lebih mendalam pada area kritis tanpa harus melalui seluruh langkah eksplorasi seperti pada black box, namun tetap mensimulasikan serangan dari perspektif penyerang yang memiliki pengetahuan terbatas. Hal ini relevan karena dalam situasi nyata, ancaman sering kali datang dari pihak yang memiliki akses terbatas atau pengetahuan sebagian tentang sistem, seperti karyawan atau kontraktor. Oleh karena itu, penggunaan metode grey box dalam penetration testing dapat membantu mengidentifikasi kerentanan yang mungkin dilewatkan oleh metode lain, sekaligus memberikan hasil yang lebih akurat mengenai potensi ancaman yang dapat dieksploitasi oleh penyerang dengan pengetahuan parsial.

2.2.3 OWASP *Top* 10 dan OWASP API *Security Top* 10

Metodologi OWASP (*Open Web Application Security Project*) dipilih sebagai dasar teori dalam penetration testing karena metodologi ini secara khusus dirancang untuk mengidentifikasi dan mengatasi kerentanan dalam aplikasi web dan aplikasi, yang merupakan salah satu area paling rentan dalam keamanan siber. OWASP menyediakan panduan yang terstruktur dan praktis yang mencakup tahap persiapan, pengujian, dan pelaporan hasil, sehingga memudahkan penguji dalam menerapkan langkah-langkah yang relevan dan sesuai dengan best practice di industri. Selain itu, OWASP terus diperbarui untuk mengikuti perkembangan terbaru dalam ancaman keamanan web, menjadikannya metode yang adaptif dan relevan dengan tantangan keamanan saat ini. Dengan berfokus pada aplikasi web, OWASP membantu memastikan bahwa pengujian penetrasi dilakukan dengan pendekatan yang komprehensif dan sistematis, sehingga mampu mengidentifikasi dan menutup celah keamanan yang mungkin dieksploitasi oleh penyerang.

2.2.4 Keamanan Aplikasi *Mobile*

Aplikasi *mobile* menjadi target serangan siber, terutama yang mengelola data sensitif. Pengujian keamanan yang komprehensif diperlukan untuk memastikan keamanan aplikasi *mobile* (Veracode, 2017).