BAB I
PENDAHULUAN

1.1.Gambaran Umum

Penelitian ini bertujuan untuk meningkatkan keamanan sistem informasi di sektor perbankan, dengan fokus pada Bank Pembangunan Daerah (BPD) dan Bank Perkreditan Rakyat (BPR), melalui pendekatan *Vulnerability Assessment* dan *Penetration Testing* (VAPT). Ancaman siber yang semakin kompleks berpotensi menimbulkan kerentanan pada sistem, yang dapat menyebabkan kerugian finansial dan penurunan kepercayaan nasabah. Oleh karena itu, meningkatkan kesadaran akan pentingnya keamanan siber menjadi sangat krusial. Dengan penerapan VAPT, kondisi keamanan sistem dapat dievaluasi secara menyeluruh, sekaligus mendukung upaya strategis untuk memperkuat perlindungan terhadap berbagai ancaman.

Untuk mengatasi tantangan ini, penelitian ini dimulai dengan pengumpulan informasi untuk memetakan aset-aset yang rentan terhadap risiko ancaman. Selanjutnya, dilakukan pemindaian kerentanan menggunakan perangkat lunak keamanan yang sesuai dengan standar industri, yang diikuti oleh eksploitasi untuk menguji celah yang ditemukan. Hasil eksploitasi kemudian dianalisis dan disusun dalam laporan yang mencakup rekomendasi perbaikan yang dapat diterapkan secara praktis. Pendekatan ini bertujuan untuk mengidentifikasi ancaman yang mungkin tidak terdeteksi oleh sistem keamanan yang ada, serta memberikan solusi teknis untuk memperkuat sistem.

Penelitian ini menggabungkan pendekatan teknis dan manajerial untuk mengatasi masalah keamanan informasi. Dari segi teknis, penggunaan metode yang terstruktur memungkinkan identifikasi kerentanan secara efisien dan akurat. Di sisi lain, laporan yang dihasilkan memberikan panduan strategis bagi manajemen bank dalam meningkatkan kebijakan dan praktik keamanan informasi mereka. Lebih luas

lagi, penelitian ini berkontribusi pada penguatan aspek integritas, kerahasiaan, dan ketersediaan informasi, yang merupakan pilar utama dalam keamanan siber.

Sebagai langkah berikutnya, untuk mendapatkan pemahaman yang lebih mendalam mengenai kerentanannya, penelitian ini akan mengaplikasikan metode *black-box testing*. Metode ini melibatkan pengujian sistem dari perspektif eksternal, di mana evaluasi dilakukan dengan akses terbatas, seperti melalui daftar IP yang diberikan oleh pihak bank, tanpa pengetahuan mengenai struktur internal sistem. Tujuan utama dari pendekatan ini adalah untuk memberikan analisis objektif terhadap potensi kelemahan yang ada, dengan meniru serangan yang dapat dilakukan oleh pihak luar yang tidak memiliki informasi internal. Dengan demikian, metode ini memberikan gambaran yang lebih realistis mengenai potensi ancaman terhadap sistem dan membantu dalam identifikasi serta mitigasi kerentanannya secara lebih efektif.

Hasil dari penelitian ini diharapkan dapat memperkuat perlindungan sistem informasi pada Perusahaan termasuk BPD dan BPR terhadap ancaman siber, serta meningkatkan kepercayaan nasabah terhadap layanan perbankan. Selain itu, rekomendasi yang diberikan dapat menjadi dasar dalam membangun kerangka kerja keamanan informasi yang lebih komprehensif, yang tidak hanya relevan bagi sektor perbankan, tetapi juga bagi sektor keuangan lainnya.

1.2.Rumusan Masalah

Berikut rumusan masalah dari penelitian ini :

1. Bagaimana mengidentifikasi kerentanan yang ada pada sistem informasi di sektor perbankan menggunakan pendekatan *Vulnerability Assessment* dan *Penetration Testing* (VAPT)?
2. Bagaimana metode *black-box testing* dapat digunakan untuk menganalisis sistem informasi secara objektif tanpa akses ke informasi internal?
3. Apa langkah-langkah yang efektif untuk memetakan aset informasi yang rentan dan menguji potensi kelemahan sistem?

4. Bagaimana cara menyusun rekomendasi teknis dan strategis yang dapat diimplementasikan oleh manajemen bank untuk memperkuat keamanan sistem informasi?

1.3.Batasan Masalah

Berikut batasan masalah dari penelitian ini :

1. Penelitian ini hanya berfokus pada sektor perbankan, khususnya pada BPD dan BPR, dan tidak mencakup institusi keuangan lainnya di luar lingkup ini.
2. Pendekatan yang digunakan terbatas pada VAPT dengan metode *black-box testing*, tanpa melibatkan metode pengujian lain seperti *white-box testing* atau *grey-box testing*.
3. *Tools* yang digunakan untuk pemindaian dan eksploitasi kerentanan mengikuti standar industri yang berlaku, tetapi penelitian ini tidak mencakup perbandingan antara berbagai tools yang tersedia.
4. Penelitian hanya mencakup pengujian terhadap aset informasi yang terhubung dengan sistem teknologi informasi, seperti *server*, *network*, dan *web application*. Tidak termasuk pengujian perangkat keras fisik atau elemen non-digital lainnya.
5. Fokus penelitian hanya pada analisis, identifikasi dan eksploitasi kerentanan teknis dalam sistem informasi, tanpa membahas secara mendalam ancaman non-teknis, seperti serangan berbasis sosial (*social engineering*) atau *insider threat*.
6. Hasil penelitian dibatasi pada pemberian rekomendasi teknis dan strategis berdasarkan temuan dari VAPT, tanpa implementasi langsung terhadap sistem informasi yang diuji.
7. Penelitian ini lebih fokus pada pengujian kerentanan di level teknis misalnya, perangkat lunak, konfigurasi sistem, atau infrastruktur IT, dan tidak menguji secara mendalam aspek kebijakan atau tingkat kesadaran keamanan siber di kalangan staf bank atau pihak terkait lainnya.

8. Penelitian ini terbatas pada periode waktu tertentu dalam proses VAPT, yaitu pada tahap pengujian dan analisis yang dilakukan dalam jangka waktu penelitian ini, tanpa mempertimbangkan perubahan atau perbaikan yang mungkin dilakukan setelah penelitian selesai.
9. Penelitian difokuskan pada institusi perbankan yang beroperasi di wilayah Indonesia.

1.4.Tujuan

Berikut tujuan dari penelitian ini :

1. Melakukan identifikasi dan analisis terhadap potensi kerentanan pada sistem informasi milik BPD dan BPR menggunakan pendekatan VAPT sebagai langkah untuk meningkatkan keamanan siber di sektor perbankan.
2. Melaksanakan evaluasi terhadap kelemahan sistem informasi melalui metode *black-box testing*, yang memungkinkan penilaian dilakukan tanpa memanfaatkan informasi internal, sehingga memberikan gambaran objektif mengenai potensi ancaman yang mungkin terjadi.
3. Melakukan pemetaan aset informasi yang rentan sebagai bagian dari proses identifikasi dan pengujian kelemahan sistem, untuk mendapatkan gambaran menyeluruh tentang potensi risiko keamanan.
4. Menyusun rekomendasi perbaikan baik secara teknis maupun strategis berdasarkan hasil evaluasi, guna memperkuat kebijakan serta infrastruktur keamanan informasi di BPD dan BPR, serta meningkatkan pemahaman dan kesadaran manajemen perbankan terkait pentingnya pengelolaan risiko keamanan informasi untuk melindungi integritas, kerahasiaan, serta ketersediaan data dalam sistem perbankan.