Nama : Arifur Rahman

Nim : 1310651107

Kelas : E

Keamanan Informasi

1.

No	Peneliti	Judul	Tools	Hasil
1	Zaid Amin	ANALISIS VULNERABILITAS HOST PADA KEAMANAN JARINGAN KOMPUTER DI PT. SUMEKS TIVI PALEMBANG (PALTV) MENGGUNAKAN ROUTER BERBASIS UNIX	Unix	Penggunaan Operating System Yang Ilegal Yang dapat memungkinkan sistem operasi menjadi Crash (rusak)
2	Yulius Kurnia Susanto Dan Ratih Handayani	INTENSITAS ANCAMAN KEAMANAN SISTEM INFO RMASI AKUNTANSI KOMPUTERISASIAN	computerized accounting	secara keseluruhan tidak ada perbedaan antara organisasi yang menggunakan SIAK yang terintegrasi secara on-line dan terintegrasi secara manual
3	Siti Syaroh, Ellensyah Kurniawan	AUDIT SISTEM INFORMASI CALL CENTER PADA PT ARGA BANGUN BANGSA (ESQ LEAERSHIP CENTER) DENGAN MENGGUNAKAN FRAMEWORK COBIT	Cobit	Penerapan tekonologi informasi dengan menggunakan COBIT Framework dapat memberikan manfaat dalam arsitektur bisnis, arsitektur informasi, arsitektur teknologi dan arsitektur solusi sebagai pedoman untuk pengembangan sistem call center pada ESQ LC.

2. Chipertext merupakan text informasi yang telah diubah penulisannya menjadi kode rahasia, sehingga tidak ada orang yang mampu menggunakannya kecuali dia mempunyai kata kunci untuk membukanya. Metoda yang digunakan ntuk mengolah suatu text agar menjadi ciphertext ini adalah dengan menggunakan algoritma Cipher.
   Berikut ini adalah beberapa teknik dasar dalam membuat chipertext.

   a.Substitusi
   Caesar cipher adalah cipher substitusi sederhana yang mencakup pergeseran alfabet 3 posisi ke kanan. Caesar cipher merupakan subset dari cipher polialfabetik Vigenere. Pada Caesar cipher karakter-karakter pesan dan pengulangan kunci dijumlahkan bersama, modulo 26. Dalam penjumlahan modulo 26, huruf-huruf A-Z dari alfabet masing-masing memberikan nilai 0 sampai 25. Tipe cipher ini dapat diserang menggunakan analisis frekuensi. Dalam frekuensi analisis, digunakan karakteristik frekuensi yang tampak dalam penggunaan huruf-huruf alfabet pada bahasa tertentu.
   b.Transposisi (Permutasi)
   Pada cipher ini, huruf-huruf plaintext dipermutasi. Sebagai contoh, hurufhuruf plaintext A T T A C K A T D A W N dapat dipermutasi menjadi D C K A A W N A T A T T. Cipher transposisi kolumnar adalah cipher dimana plaintext ditulis secara horisontal pada kertas dan dibaca secara vertikal. Cipher transposisi dapat diserang melalui analisis frekuensi, namun cipher menyembunyikan properti statistik dari pasangan huruf-huruf, seperti IS dan TOO.
   c. Vernam Cipher (One Time Pad)
   Cipher ini diimplementasikan melalui sebuah kunci yang terdiri dari sekumpulan random karakter-karakter yang tidak berulang. Setiap huruf kunci dijumlahkan modulo 26 dengan huruf pada plaintext. Pada One Time Pad, tiap huruf kunci digunakan satu kali untuk satu pesan dan tidak digunakan kembali. Panjang stream karakter kunci sama dengan panjang pesan.
   d. Book Key Cipher / Running Key Cipher
   Cipher ini menggunakan teks dari sebuah sumber (misalnya buku) untuk mengenkripsi plaintext. Kunci, diketahui oleh pengirim dan penerima yang dimaksud, dapat berupa halaman dan jumlah baris dari teks pada buku. Teks ini adalah karakter yang sesuai untuk karakter dengan plaintext, dan penjumlahan modulo 26 dijalankan untuk memperngaruhi enkripsi. Running key cipher mengeliminasi periodisitas, namun masih dapat diserang dengan memanfaatkan redundansi pada kunci.