Nama Kelompok : 1. Ahmat Cholid (L200160113)
2. Reyhannisa Erico Dwi R (L200160122)
3. Muhammad Afwaz Nafis (L200160089)
4. Hamzah Miftakhuddin (L200160137)

Kelas : B

HACKING DAN CRACKING

1. Konsep dan Definisi

a. Hacking

1) *Hacking* merupakan tindakan yang dilakukan untuk mencari kelemahan yang ada pada suatu sistem komputer. Pelaku yang melakukan *hacking* disebut dengan *Hacker*. Hasil dari *hacking* biasanya berupa penemuan *bug* atau celah dari sistem yang bisa dimanfaatkan untuk tujuan tertentu oleh orang lain yang tidak seharusnya diizinkan.
2) Jenis-Jenis Hacker
   - **White Hat Hacker**
     Hacker ini menunjukkan suatu kelemahan dalam sebuah sistem, dan juga melindungi sebuah sistem. White Hat cenderung akan melaporkan *bug* atau kelemahan keamanan sistem kepada pemilik sistem supaya diperbaiki.
   - **Black Hat Hacker**
     Kebalikan dari White Hat yang akan melaporkan kelemahan keamanan kepada pemilik sistem, Black Hat justu akan memanfaatkan kelemahan tersebut untuk tujuan tertentu.
3) Konsep
   Memberikan atau mencari informasi tentang kelemahan suatu sistem serta memberikan ide untuk bisa memperbaiki kelemahan sistem yang telah ditemukan.

b. Cracking

1) Cracking merupakan tindakan yang di lakukan untuk menjebol komputer milik orang lain dengan tujuan yang jahat.
2) Cracker merupakan sebutan bagi orang-orang yang melakukan cracking dimana orang-orang ini mencari kelemahan dan memasuki sistem orang lain

untuk kepentingan peribadi seperti pencurian data, penghapusan data dan lain-lain.

3) Tingkatan-tingkatan Cracker:
   - **Elite** orang-orang yang paham betul akan suatu sistem operasi, mampu mengkonfigurasi dan menyambungkan jaringan secara global, dan yang pasti selalu melakukan pemrograman setiap hari.
   - **Semi Elite** merupakan adik dari kaum Elite, dimana mereka juga memiliki kemampuan seperti kaum Elite, biasanya mereka dibekali dengan beberapa program yang cukup untuk mengubah program eksploit .
   - **Developed Kiddie** sebutan ini disematkan pada hacker yang masih menduduki bangku sekolah atau masih muda. Pada tingkatan ini mereka masih dalam tahanpan pembelajaran, dimana mereka mencoba berbagai sistem, namun masih belum mampu untuk menemukan titik lemah pada suatu sistem.
   - **Script Kiddie** aktivitas yang dilakukan hampir sama dengan Developed Kiddie, para Script Kiddie hanya mempunyai pengetahuan teknik jaringan yang sangat minim, biasanya mereka menggunakan trojan untuk menakuti dan menyusahkan hidup sebagian pengguna internet.
   - **Lamer** merupakan sekumpulan orang-orang yang tidak memiliki pengalaman maupun pengetahuan tentang teknik jaringan dan komputer. Biasanya mereka melakukan hacking dengan menggunakan trojan, nuke dan DoS.

4) Konsep

   Para cracker menggunakan celah-celah keamanan yang belum di perbaiki oleh pembuat sistem untuk menyusup dan merusak suatu sistem.

2. Perangkat atau Alat

Ada beberapa alat yang digunakan dalam kegiatan *hacking* dan *cracking*, diantaranya:

a. **Metasploit** : membantu untuk menemukan kerapuhan pada platform berbeda.
b. **Acunetix WVS** : mampu menjelajahi situs website dan menemukan kerentanan berbahaya dari cross-site Scripting, injeksi SQL da kerentenan lainnya.
c. **Nmap** : menemukan jaringan yang efisiensi dan mengaudit keamanan.

d. **Wireshark** : Menganalisis jaringan, menangkap pocket secara langsung dan pemindaian secara mendalam ratusan protokol.

e. **Nessus Vulnerability Scanner :** Dapat memindai berbagai kelemahan seperti kelemahan akses jarak jauh, kesalahan konfigurasi pada peringatan, penilakan layanan TCP/IP stack, persiapan audit PCI DSS, deteksi malware, pencarian data sensitif, dan lainnya.

3. **Kontrol Audit**

Untuk melakukan pengendalian terhadap sistem terdapat dua jenis, yaitu pengendalian secara umum dan pengendalian pada aplikasi.

a. Pengendalian Secara Umum

Merupakan pengendalian sistem informasi yang paling luar dan yang pertama harus dihadapi oleh pemakai sistem informasi, pengendalian umum terdiri dari:

1) Pengendalian Organisasi

Adanya pemisahan tugas dan tanggungjawab yang tegas sehingga kesempatan untuk melakukan gangguan sulit diperoleh.

2) Pengendalian Dokumentasi

Pengendalian dokumentasi penting untuk keperluan seperti mempelajari cara pengoperasian sistem, sebagai bahan penelitian, dasar pengembangan sistem lebih lanjut, dasar dalam melakukan modofikasi dan perbaikan sistem dimasa yang akan datang, dan materi acuan bagi auditor dalam melakukan pemeriksaan.

3) Pengendalian keamanan data

Beberapa cara pengendalian untuk keamanan data yang dapat diaplikasikan adalah dipergunakan data log, proteksi file, pembatasan pengaksesan, data back-up atau recovery.

b. Pengendalian Aplikasi

Pengendalian ini dipasang dalam program aplikasinya yaitu pengendalian pada tahap masukan, pengendalian pada tahap pengolahan atau proses dan pengendalian pada tahap keluaran.

1) Pengendalian pada tahap masukan mempunyai tujuan untuk meyakinkan bahwa data transaksi yang valid telah lengkap, terkumpul

secara keseluruhan dan terbebas dari kesalahan sebelum masuk ke proses pengolahan.

2) Pengendalian pengolahan terdapat tujuan yang ingin dicapai yaitu untuk mencegah kesalahan-kesalahan yang terjadi selama proses pengolahan data yang dilakukan setelah data dimasukkan ke komputer.
3) Pengendalian keluaran dimaksudkan untuk kedua macam bentuk keluaran yaitu keluaran dalam bentuk *hard copy* dan pengeluaran dalam bentuk *soft copy*.

Referensi

1. http://sinta89.wordpress.com/category/my-articles/hacking-dan-cracking/
2. http://www.kompasiana.com/faisalazharagala/58ce95384ef9fdc7418b5f8b/hacker-dan-cracker?page=all#
3. https://www.codepolitan.com/10-tool-terbaik-untuk-hacking-di-awal-2017
4. http://dueeg.blogspot.com/2010/11/normal-0-false-false-false-en-us-x-none.html
5. Hari Murti. 2005. Cybercrime. *Jurnal Teknologi Informasi DINAMIK*. 10(1): 2.