KEAMANAN JARINGAN KOMPUTER

(HACKING)

NAMA: ERDA JULIAN LESI

NIM: 09011181419065

KELAS: SK6B

DOSEN PENGAMPUH: DERIS STIAWAN, M.T., PH.D.

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

HACKING

Hacking adalah kegiatan menerobos program komputer milik orang/pihak lain. Saat ini ***hacking*** memiliki arti menyerang suatu sistem, jaringan, dan aplikasi dengan cara mengkesploitasi kelemahan dari hal-hal tersebut dengan maksud untuk mendapatkan hak akses atas data dan sistem. Hacker adalah orang yang melakukan hacking.

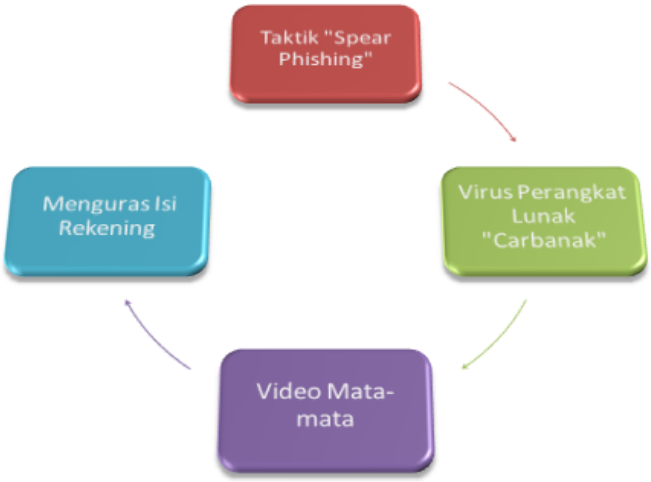
Fase-fase Hacking

1. Fase Persiapan
    - Mengumpulkan informasi sebanyak-banyaknya
2. Fase Eksekusi
    - Setelah mendapatkan informasi, biasanya akan didapatkan informasi mengenai OS yg digunakan, serta port yang terbuka dengan daemon yang sedang berjalan. Selanjutnya mencari informasi mengenai vulnerability holes (celah kelemahan suatu program) dan dimanfaatkan menggunakan exploit
    - Mengekspolitasi Vulnerability Holes
3. Fase Setelah Eksekusi
    - Menginstall backdoor, trojans, dan rootkit
    - Menghapus jejak dengan memodifikasi file log agar tidak dicurigai admin
    - Menyalin password

SKENARIO

Skenario hacker membobol seratus bank yang tersebar di 30 negara, kelompok ini menumpuk pundi-pundi uang yang mereka curi hingga US$ 1 miliar atau setara Rp 12,8 triliun.

1. Taktik "Spear Phishing"
   Kelompok menargetkan karyawan pada bank tertentu dan mengidentifikasi *e-mail* mereka. *E-mail* yang dikirim geng peretas untuk karyawan bank memiliki dokumen lampiran, yang ketika diunduh dan dibuka langsung dieksekusi virus perangkat lunak Carbanak dan memberikan peretas akses langsung pada sistem
2. Virus Perangkat Lunak "Carbanak"
   Carbanak memungkinkan geng kriminal untuk memonitor lalu lintas jaringan, mengambil potret layar komputer, serta merekam kata kunci pada mesin yang terinfeksi. Modal ini dipakai kelompok peretas untuk menemukan komputer induk yang akan dieksekusi oleh metode pengamatan video.



3. Video Mata-mata

   Data yang dikumpulkan virus perangkat lunak Carbanak lantas dieksekusi oleh video mata-mata ini. Dengan memantau layar ini, peretas dapat memperoleh pengetahuan yang mendalam tentang cara kerja sistem internal setiap bank. Dengan demikian, memungkinkan mereka untuk menyesuaikan setiap serangan.

4. Menguras Isi Rekening

   Kelompok menggunakan sistem perbankan *online* atau *e-payment* internasional untuk mentransfer uang dari rekening bank mereka sendiri. Mereka menggunakan akun bank yang diduga dari Cina dan Amerika Serikat. Metode kedua yang digunakan adalah menggunakan akses pada sistem akuntansi bank untuk menggelembungkan saldo rekening sebelum menguras habis-habisan uang korban. Misalnya, *hacker* bisa mengubah keseimbangan rekening korban dari US$ 1.000 menjadi US$ 10.000 sebelum menarik US$ 9.000. Dengan demikian, seolah-olah tak terjadi apa pun pada rekening korban.

Dampak

1) Merugikan orang lain, baik nasabah bank maupun bank itu sendiri, dan juga negara.
2) Merupakan tindak pencurian,
3) Pencurian data nasabah berupa PIN dsb.

Namun dengan adanya kejadian tersebut, pihak bank dapat menambah dan memperhatikan kekurangan dari security, keamanan pada sistem bank agar kejadian tersebut tidak terulang kembali.