Nama : Ferian Andhika Toasi

Kelas : 1D

NIM : 17090095

BAB IX

1. **Jelaskan apa yang dinamakan *Bug, Chameleons, Logic Bomb, Trojan Horse, Virus, Worm dan spy.***
   a. **BUG**
      Bug merupakan kesalahan-kesalahan yang terdapat pada suatu program aplikasi yang terjadi secara tidak disengaja. Hal ini umumnya dikarenakan kecerobohan dari pihak programer pada waktu menulis program tersebut. Bug ini mempunyai dampak yang bermacam-macam seperti komputer menjadi hang atau bahkan bisa merusak media penyimpanan pada sistem komputer kita.
   b. **Chameleons**
      Chameleons sesuai dengan namanya merupakan program yang diselundupkan atau disisipkan ke dalam suatu sistem komputer dan berfungsi untuk mencuri data dari sistem komputer yang bersangkutan. Program ini tidak merusak peralatan pada sistem komputer yang dijangkitnya, targetnya ialah mendapatkan data dan kadang kala berusaha untuk melakukan pengubahan pada data tersebut.
   c. **Logic Bomb**
      Bomb akan ditempatkan atau dikirimkan secara diam-diam pada suatu sistem komputer yang menjadi target dan akan meledak bila pemicunya diaktifkan. Berdasarkan pemicu yang digunakan, logic bomb dapat digolongkan menjadi tiga, yaltu software bomb, logic bomb, dan time bomb. Software bomb akan meledak jika dipicu oleh suatu software tertentu, logic bomb akan meledak jika memenuhi suatu kondisi tertentu, sedangkan time bomb akan meledak pada waktu yang telah ditentukan.
   d. **Trojan Horse**
      Prinsip kerja dari trojan horse mirip seperti chameleons, bedanya trojan home akan melakukan sabotase dan perusakan terhadap sistem komputer yang dijangkitinya
   e. **Virus**
      Pada awalnya virus komputer merupakan suatu program yang dibuat hanya untuk menampilkan Hama samaran serta beberapa baris kata dan pembuatnya, dan sama sekali tidak membahayakan komputer. Tetapi pada perkembangan selanjutnya, pembuat virus komputer mulai menggabungkan beberapa karakteristik dan beberapa program pengganggu dan perusak lainnya dan mulailah bermunculan banyak virus yang dibuat dengan tujuan merusak suatu sistem komputer.
   f. **Worm**
      Worm merupakan suatu program pengganggu yang dapat memperbanyak diri dan akan selalu berusaha menyebarkan diri dari satu komputer ke komputer yang lain dalam suatu jaringan. Worm menjadikan ukuran suatu file menjadi membengkak dan bahkan dapat menguras kapasitas media penyimpanan.

g. Spy

Spyware adalah sejenis komputer program yang dibuat untuk 'mencuri' informasi-informasi penting/Pribadi dari komputer yang terinfeksi dan mengirimnya ke lokasi tertentu di internet untuk kemudian diambil oleh pembuatnya. Informasi yang menjadi target utama contohnya: nomor kartu kredit, User ID dan PIN/password, nomor rekening, alamat email, dan lain-lain. Spyware dapat ter-install melalui email attachment, program yang di-install dari sumber-sumber yang tidak jelas, ataupun oleh website yang 'jahat'. Namun, berbeda dengan virus yang sifatnya lebih merusak, spyware bekerja secara diam-diam agar tidak terlacak sehingga lebih mudah mengumpulkan informasi yang diinginkan sang pembuat/penyebar spyware.

2. Jelaskan tentang Firewall utk keamanan komputer

firewall sangat penting digunakan dalam suatu jaringan yang terkoneksi langsung ke internet atau yang lebih dikenal dengan jaringan publik yang dapat diakses oleh siapapun dan dimanapun. Sehingga peran firewall disana sangat berguna karena sebagai pembatas yang mengatur dan mengendalikan akses yang dilakukan untuk mengurangi dan mencegah ancaman-ancaman dari internet yang masuk ke jaringan lokal.

3. Jelaskan macam-macam kriptografi

Teknik dalam kriptografi ada berbagai cara, diantaranya yaitu :

a. Substitusi

Ini adalah algoritma kriptografi yang mula-mula digunakan oleh kaisar Romawi, Julius Caesar (sehingga dinamakan juga caesar cipher), untuk menyandikan pesan yang ia kirim kepada para gubernurnya.

Caranya adalah dengan mengganti setiap karakter dengan karaktewr lain dalam susunan abjad (alfabet). Misalnya, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan abjad. dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu k=3).

b. Transposisi

Pada cipher transposisi, plainteks tetap sama, tetapi urutannya diubah. dengan kata lain, algoritma ini melakukan transpose terhadap rangkaian karakter didalam teks. Nama lain untuk metode ini adalah permutasi (pemindahan).

c. Blocking

Sistem enkripsi ini terkadang membagi plaintext menjadi beberapa blok yang terdiri dari beberapa karakter, kemudian di enkripsikan secara independen.

d. Permutasi

Salah satu teknik enkripsi yang terpenting adalah permutasi atau sering juga disebut transposisi. Teknik ini memindahkan atau merotasikan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi. Dalam teknik substitusi, karakter berada pada posisi yang tetap tapi identitasnya yang diacak. Pada teknik permutasi, identitas karakternya tetap, namun posisinya yang diacak.

e. **Ekspansi**
   Suatu metode sederhana untuk mengacak pesan adalah dengan memelarkan pesan itu dengan aturan tertentu. Salah satu contoh penggunaan teknik ini adalah dengan meletakkan huruf konsonan atau bilangan ganjil yang menjadi awal dari suatu kata di akhhiran "an". Jika suatu kata dimulai dengan huruf vokal atau bilangan genap, ditambahkan akhiran "i".
f. **Pemampatan**
   Mengurangi panjang pesan atau jumlah bloknya dengan cara lain untuk menyembunyikan isi pesan.

4. **Jelaskan Langkah-langkah logis Proses hacking seperti : Footprinting, Scanning, Enumeration, Gaining Access, EscalatingPrivilege, Pilfering, coveringTracks, Creating Backdoors, Denial of Service.**
   a. **Footprinting**
      Mencari rincian informasi terhadap sistemsistem untuk dijadikan sasaran, mencakup pencarian informasi dengan search engine, whois, dan DNS zone transfer.
      Pada tahap footprinting, hacker baru mencari-cari sistem mana yang dapat disusupi.
      Footprinting merupakan kegiatan pencarian data berupa:
      - Menentukan ruang lingkup (scope) aktivitas atau serangan
      - Network enumeration
      - Interogasi DNS
      - Mengintai jaringan

   b. **Scanning**
      Terhadap sasaran tertentu dicari pintu masuk yang paling mungkin. Digunakan ping sweep dan port scan.
      Tahap scanning lebih bersifat aktif terhadap sistem-sistem sasaran. Di sini diibaratkan hacker sudah mulai mengetuk-ngetuk dinding sistem sasaran untuk mencari apakah ada kelemahannya. Kegiatan scanning dengan demikian dari segi jaringan sangat 'berisik' dan mudah dikenali oleh sistem yang dijadikan sasaran, kecuali menggunakan stealth scanning. Scanning tool yang paling legendaris adalah nmap (yang kini sudah tersedia pula untuk Windows 9x/ME maupun DOS), selain SuperScan dan UltraScan yang juga banyak digunakan pada sistem Windows. Untuk melindungi diri anda dari kegiatan scanning adalah memasang firewall seperti misalnya Zone Alarm, atau bila pada keseluruhan network, dengan menggunakan IDS (Intrusion Detection System) seperti misalnya Snort.

c. Enumeration

Telaah intensif terhadap sasaran, yang mencari user account absah, network resource and share, dan aplikasi untuk mendapatkan mana yang proteksinya lemah.

Tahap enumerasi sudah bersifat sangat intrusif terhadap suatu sistem. Di sini penyusup mencari account name yang absah, password, serta share resources yang ada. Pada tahap ini, khusus untuk sistem-sistem Windows, terdapat port 139 (NetBIOS session service) yang terbuka untuk resource sharing antar-pemakai dalam jaringan. Anda mungkin berpikir bahwa hard disk yang di-share itu hanya dapat dilihat oleh pemakai dalam LAN saja. Kenyataannya tidak demikian. NetBIOS session service dapat dilihat oleh siapa pun yang terhubung ke Internet di seluruh dunia! Tools seperti Legion, SMBScanner , atau SharesFinder membuat akses ke komputer orang menjadi begitu mudah (karena pemiliknya lengah membuka resource share tanpa password).

d. Gaining Acces

Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran. Meliputi mengintip dan merampas password, menebak password, serta melakukan buffer overflow.

Tahap gaining access adalah mencoba mendapatkan akses ke dalam suatu sistem sebagai user biasa. Ini adalah kelanjutan dari kegiatan enumerasi, sehingga biasanyadi sini penyerang sudah mempunyai paling tidak user account yang absah, dan tinggal mencari passwordnya saja. Bila resource share-nya diproteksi dengan password, maka password ini dapat saja ditebak (karena banyak yang menggunakan password sederhana dalam melindungi komputernya). Menebaknya dapat secara otomatis melalui dictionary attack (mencobakan kata-kata dari kamus sebagai password) atau brute-force attack (mencobakan kombinasi semua karakter sebagai password). Dari sini penyerang mungkin akan berhasil memperoleh logon sebagai user yang absah.

e. Escalating Prifilege

Bila baru mendapatkan user password di tahap sebelumnya, di tahap ini diusahakan mendapat privilese admin jaringan dengan password cracking atau exploit sejenis getadmin, sechole, atau lc_messages.

Tahap Escalating Privilege mengasumsikan bahwa penyerang sudah mendapatkan logon access pada sistem sebagai user biasa. Penyerang kini berusaha naik kelas menjadi admin(padasistem Windows) atau menjadi root (pada sistem Unix/Linux). Teknik yang digunakan sudah tidak lagi dictionary attack atau brute-force attack yang memakan waktu itu, melainkan mencuri password file yang tersimpan dalam sistem dan memanfaatkan kelemahan sistem. Pada sistem Windows 9x/ME password disimpan dalam file .PWL sedangkan pada Windows NT/2000 dalam file .SAM. Bahaya pada tahap ini bukan hanya dari penyerang di luar sistem, melainkan lebih besar lagi bahayanya adalah 'orang dalam' yaitu user absah dalam jaringan itu sendiri yang berusaha 'naik kelas' menjadi admin atau root.

f. Pilfering

Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke trusted system. Mencakup evaluasi trust dan pencarian cleartext password di regiatry, config file, dan user data

g. Convering Tricks

Begitu kontrol penuh terhadap system diperoleh, maka menutup jejak menjadi prioritas.Meliputi membersihkan network log dan penggunaan hide toolseperti macam-macam rootkit dan file streaming.

h. Creating Backsdoors

Pintu belakang diciptakan pada berbagai bagian dari sistem untuk memudahkan masuk kembali ke sistem ini dengan cara membentuk user account palsu,menjadwalkan batch job, mengubah startup file, menanamkan service pengendali jarak jauh serta monitoring tool, dan menggantikan aplikasi dengan trojan

i. Danial of Service

Bila semua usaha di atas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir. Meliputi SYN flood, teknik-teknik ICMP, Supernuke, land/latierra, teardrop, bonk, newtear, trincoo, dan lain-lain. Terakhir, denial of service, bukanlah tahapan terakhir,melainkan kalau penyerang sudah frustrasi tidak dapat masuk ke dalam sistem yang kuat pertahanannya, maka yang dapat dilakukannya adalah melumpuhkan saja sistem itu dengan menyerangnya menggunakan paket-paket data yang bertubi-tubi sampai sistem itu crash. Denial of service attack sangat sulit dicegah, sebab memakan habis bandwidth yang digunakan untuk suatu situs. Pencegahannya harus melibatkan ISP yang bersangkutan. Para script kiddies yang pengetahuan hacking-nya terbatas justru paling gemar melakukan kegiatan yang sudah digolongkan tindakan kriminal di beberapa negara ini.

5. Jelaskan apa itu sql injection

SQL Injection adalah teknik hacking untuk memanipulasi query (perintah database). injeksi sering di lakukan melalui inputan inputan yang tidak di lakukan pengecekan kebenaran data yang di input. untuk lebih jelasnya saya berikan contoh program dan query yang di injeksi

6. Jelaskan kejahatan komputer berupa : carding, hacking, cracking, defacing, phising, spamming dan malware

a. Carding

Carding adalah jenis kejahatan memalsukan nama identitas seseorang, contoh berbelanja menggunakan nomor dan kartu identitas milik orang lain, yang diperoleh secara ilegal, biasanya dengan mencuri data melalui internet. Sebutan pelakunya adalah Carder. Sebutan lain untuk kejahatan jenis ini adalah cyberfroud alias penipuan di social media atau dunia maya.

b. Hacking

Hacking adalah kegiatan menerobos program komputer milik orang lain. Hacker adalah orang yang gemar menerobos komputer, memiliki keahlian membuat dan membaca program tertentu, dan terobsesi mengamati keamanan security. Hacker memberi tahu kepada programer yang komputernya diterobos, akan adanya kelemahan-kelemahan pada program yang dibuat, sehingga bisa "bocor", agar segera diperbaiki. Sedangkan, hacker pencoleng, menerobos program orang lain untuk merusak dan mencuri datanya.

c. Cracking

Cracking adalah hacking untuk tujuan jahat. Sebutan untuk cracker adalah hacker bertopi hitam (black hat hacker). Berbeda dengan carder yang hanya mengintip kartu kredit, cracker mengintip simpanan para nasabah di berbagai bank atau pusat data sensitif lainnya untuk keuntungan diri sendiri. Meski sama-sama menerobos keamanan komputer orang lain, hacker lebih fokus pada prosesnya. Sedangkan cracker lebih fokus untuk menikmati hasilnya

d. Defacing

Defacing adalah kegiatan mengubah halaman situs/website pihak lain,tindakan ini semata mata hanya iseng , unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang jahat, untuk mencuri data dan dijual kepada pihak lain untuk menghasilkan uang.

e. Pishing

Phising adalah kegiatan memancing pemakai komputer di internet (user) agar mau memberikan informasi data diri pemakai (username) dan kata sandinya (password) pada suatu website yang sudah di-deface. Phising biasanya diarahkan kepada pengguna online banking. Isian data pemakai dan password yang vital yang telah dikirim akhirnya akan menjadi milik penjahat tersebut dan digunakan untuk belanja dengan kartu kredit atau uang rekening milik korbannya.

f. Spamming

Spamming adalah pengiriman berita atau iklan lewat surat elektronik (e-mail) yang tak dikehendaki. Spam sering disebut juga sebagai bulk email atau junk e-mail alias "sampah". Meski demikian, banyak yang terkena dan menjadi korbannya. Yang paling banyak adalah pengiriman e-mail dapat hadiah, lotere, atau orang yang mengaku punya rekening di bank di Afrika atau Timur Tengah, minta bantuan "netters" untuk mencairkan, dengan janji bagi hasil. Kemudian korban diminta nomor rekeningnya, dan mengirim uang/dana sebagai pemancing, tentunya dalam mata uang dolar AS, dan belakangan tak ada kabarnya lagi. Seorang rector universitas swasta di Indonesia pernah diberitakan tertipu hingga Rp1 miliar dalam karena spaming seperti ini.

g. Malware

Malware adalah program komputer yang mencari kelemahan dari suatu software. Umumnya malware diciptakan untuk membobol atau merusak suatu software atau operating system. Malware terdiri dari berbagai macam, yaitu: virus, worm, trojan horse, adware, browser hijacker, dll. Di pasaran alat-alat komputer dan toko perangkat lunak (software) memang telah tersedia antispam dan anti virus, dan anti malware. Meski demikian, bagi yang tak waspadai selalu ada yang kena. Karena pembuat virus dan malware umumnya terus kreatif dan produktif dalam membuat program untuk mengerjai korban-korbannya.