Selesksi Bagian A Lab Sister 2022

13520163 Frederik Imanuel Louis

A. Organisasi dan Arsitektur Komputer

1.

2. Micro operation adalah operasi dasar yang dilakukan pada level register, misalnya shift, and, or, xor dll. Semua instruksi mesin kompleks diimplementasikan menggunakan rangkaian micro ops. Micro ops dilakukan secara fisik menggunakan implementasi microarsitektur CPU. Operasi yang sama dapat memiliki desain mikroarsitektur yang berbeda pada CPU yang berbeda.

3.

4. Untuk mengatasi no exec bit, kita dapat memanggil shell dari fungsi libc (ret2libc), dengan memanggil system() dari libc. Tetapi karena terdapat randomization address space, kita perlu memanggil system@PLT dari procedure linkage table, yang posisinya tidak pernah dirandomize. Passing parameter "/bin/sh" juga dapat menggunakan strcpy@PLT. Tentu saja, semua pemanggilan fungsi tersebut menggunakan eksploitasi buffer overflow dari scan buf[256]. Dengan itu, kita cukup memasukkan payload pada program yang berisi: (1) 256 byte junk, (2) pengcopyan "/bin/sh" dengan beberapa kali pemanggilan strcpy@PLT, (3) pemanggilan "system@PLT", (4) noop sled secukupnya.

5. Memory dengan hierarchy yang lebih tinggi memiliki access time yang lebih rendah. Hal tersebut dapat dimanfaatkan untuk melakukan timing attack, misalnya dengan membuat page fault atau cache miss menggunakan input yang sesuai. Terlebih lagi, jika paging atau caching ini dipengaruhi oleh branching, maka value yang dibandingkan pada conditional jump dapat diketahui dari execution time yang bertambah cepat/lambat (akibat access time yang berbeda dari kedua branch).

6.

B. Sistem Operasi

1. Zombie process adalah process yang sudah selesai melakukan seluruh instruksinya (sudah exit), tetapi masih tercatat di process table. Hal tersebut berarti proses tersebut masih PID (process ID) oleh operating system. Zombie process biasanya muncul akibat child process sudah exit, tapi tidak di-wait oleh parent processnya. Saat parent process tersebut masih berjalan dan child process sudah exit dan tidak di-wait, terciptalah zombie process. Jika parent process kemudian exit tanpa melakukan wait, child process biasanya akan "dibersihkan" secara otomatis oleh operating system, misalnya dengan mengassign parent dari process tersebut ke init (PID 1), dan initlah yang akan melakukan wait sehingga zombie process akan hilang. Reassign parent dari child process tersebut merupakan proses yang dilakukan fungsi *find_new_reaper*. Zombie process yang masih ada setelah parentnya sudah exit menandakan adanya bug dalam operating system.

2. Scheduler adalah proses yang mengalokasikan resource CPU kepada task yang berjalan pada suatu komputer. O(1) scheduler dan Completely Fair Scheduler menggunakan algoritma yang berbeda saat mengalokasikan resource tersebut. O(1) scheduler memprioritaskan kecepatan pengambilan keputusan saat mengalokasikan resource tersebut (dengan waktu konstan) sehingga menghasilkan overhead yang lebih kecil. CFS memprioritaskan utilisasi CPU maksimal yang dibagi se-adil mungkin antar task yang

sedang berjalan. Proses I/O bound adalah proses yang membutuhkan lebih banyak waktu melakukan I/O dibandingkan utilisasi CPU, dan sebaliknya, proses CPU bound membutuhkan lebih banyak utilisasi CPU dibandingkan I/O.

3. Virtual memory juga memiliki peran dalam memory protection. Page table yang diimplementasikan dalam virtual memory dapat mengassign tiap page dengan akses tertentu, misalnya read only, no execute, dsb. Memory protection dilakukan pada level hardware dan software. Dari segi software, operating system dapat memberikan proteksi misalnya dengan memberikan base dan limit register pada suatu proses. Dari segi hardware, MMU (dan dengan itu MPU), dapat memastikan bahwa memori yang diakses dilakukan menggunakan hak akses yang sesuai.

4. Jika command cd berhasil dieksekusi oleh shell, maka current working directory dari shell dan semua thread yang berjalan berubah menjadi directory yang ditunjuk parameter cd. Command cd yang digunakan merupakan fungsi built-in shell agar fungsi dari cd, yaitu merubah current working directory, dapat terlaksana dengan baik. Jika cd dieksekusi sebagai binary, maka current working directory yang akan diubah adalah current working directory dari lingkungan eksekusi cd, yaitu “subshell” yang dibuat oleh exec(). Kemudian, setelah subshell tersebut exit, cwd dari shell utama tidak akan berubah. Perlu dicatat bahwa /bin/cd tetap ada dan jika dijalankan, memiliki behaviour yang disebutkan diatas.

5. Copy on Write membuat copy dari suatu data pada memory hanya jika data tersebut ingin dimodifikasi (write). Hal tersebut mempercepat fork/clone karena proses child dan parent dapat merujuk ke datayang sama dalam memory tanpa perlu pengcopyan seluruh page yang digunakan program tersebut jika tidak ada data yang berubah. Hanya segmen data yang perlu diubah yang akan dicopy pada memory.

6. Sebuah komputer secara garis besar terbagi menjadi dua bagian, yaitu hardware dan software. Hardware adalah perangkat keras yang dapat dilihat secara fisik pada komputer, misalnya CPU, monitor, dan mouse. Software adalah perangkat lunak yang bekerja di dalam komputer, yang dapat dilihat sebagai “otak” dari komputer. Fungsi-fungsi komputer yang sering digunakan, seperti bermain game, menonton youtube, menulis dokumen, dilakukan dengan software yang sesuai. Operating system adalah software dasar yang menjembatani komunikasi antara hardware dan seluruh software lainnya. Seluruh instruksi yang dikirimkan software tingkat tinggi, misalnya menonton video, akan “diterjemahkan” oleh operating system menjadi instruksi yang dapat dijalankan oleh hardware. Komunikasi dari hardware ke software, misalnya gerakan dan klik mouse, juga dilakukan melalui operating system.

Operating system melakukan hal tersebut dengan menggunakan Basic Input Output System (BIOS) yang disediakan oleh hardware untuk melakukan operasi yang diperlukan software lainnya. Operasi tersebut disediakan melalui kernel dan dapat diakses secara langsung melalui shell. Selain itu, saat komputer dinyalakan, operating system adalah software pertama yang akan diload kedalam memory menggunakan bootloader yang terdapat pada Read Only Memory (ROM).

C. Jaringan Komputer

1. Dynamic IP adalah IP address yang diassign pada user yang dapat berubah dari waktu ke waktu, sedangkan Static IP adalah IP address yang tidak pernah berubah. Static IP diberikan oleh Internet Service Provider (ISP) sedangkan Dynamic IP diberikan oleh Dynamic Host Configuration Protocol (DHCP). Static IP digunakan jika ada third party yang perlu mengingat IP address user, seperti untuk whitelist IP. Dynamic

IP lebih umum digunakan karena sifatnya lebih aman. Dynamic IP lebih sulit dilacak ke pengguna, sedangkan Static IP dapat langsung dilacak ke pengguna.

2. ARP Poisoning adalah teknik mengalihkan semua traffic dari dan menuju suatu IP Adresss ke attacker. Hal tersebut dilakukan dengan memberi ARP yang spoofed ke suatu network agar MAC (physical) address dari device attacker diasosiasikan dengan IP dari user yang ingin diserang. Koneksi tersebut dapat kemudian digunakan dalam man in the middle attack.

3. TCP merupakan protokol koneksi yang memungkinkan komunikasi dua arah antara client dan server setelah three-way handshake. Pertama-tama, client mengirimkan segmen dengan SYN (Synchronize Sequence Number) kepada server yang menandakan client ingin memulai komunikasi dengan server. Kemudian, server membalas client dengan signal SYN-ACK, dan terakhir , client mengirimkan kembali signal ACK kepada server dan transfer data akan dimulai.