Disclaimer : Yes, tab aku di vscode ada 8 space, deal with it

Arsikom:

1. a.

int a(int x, int y){

        while (y != 0) {

                uint32\_t carry = x & y;

                x = x ^ y;

                y = carry << 1;

        }

        return x;

}

Looping pada y untuk memastikan semua “carry” dapat ditambahkan ke digit berikutnya, seperti pertambahan biasa di base10

b.

uint32\_t adduint32(uint32\_t x, uint32\_t y){

        while (y != 0) {

                uint32\_t carry = x & y;

                x = x ^ y;

                y = carry << 1;

        }

        return x;

}

uint32\_t subuint32(uint32\_t x, uint32\_t y){

        return adduint32(adduint32(x, ~y), 1);

}

float b(float x, float y){

        // AKU UDAH BUAT YANG UBAH FLOAT JADI INTEGER DI PRAK ARSIKOM, PLEASE JUST LET ME USE POINTERS

        uint32\_t ux = \*(uint32\_t\*)&x;

        uint32\_t uy = \*(uint32\_t\*)&y;

        uint32\_t signx = ux >> 31;

        uint32\_t exponentx = (ux >> 23) & 0xFF;

        uint32\_t mantissax = (ux & 0x7FFFFF) | 0x800000;

        uint32\_t signy = uy >> 31;

        uint32\_t exponenty = (uy >> 23) & 0xFF;

        uint32\_t mantissay = (uy & 0x7FFFFF) | 0x800000;

        if((exponentx == 0xFF && mantissax != 0) || (exponenty == 0xFF && mantissay != 0)){

                uint32\_t nan = 0x7FC00000;

                return \*(float\*)&nan;

        }

        if(exponentx == 0xFF && mantissax == 0){

                if(exponenty == 0xFF && mantissay == 0 && signx != signy){

                        uint32\_t nan = 0x7FC00000;

                        return \*(float\*)&nan;

                }

                return x;

        }

        if(exponenty == 0xFF && mantissay == 0){

                return y;

        }

        if(exponentx == 0){

                mantissax = mantissax & 0x7FFFFF;

        }

        if(exponenty == 0){

                mantissay = mantissay & 0x7FFFFF;

        }

        if(exponentx > exponenty){

                uint32\_t exponent\_diff = subuint32(exponentx, exponenty);

                mantissay = mantissay >> exponent\_diff;

                exponenty = adduint32(exponenty, exponent\_diff);

        }

        else if(exponenty > exponentx){

                uint32\_t exponent\_diff = subuint32(exponenty, exponentx);

                mantissax = mantissax >> exponent\_diff;

                exponentx = adduint32(exponentx, exponent\_diff);

        }

        uint32\_t mantissa, exponent, sign;

        if(signx == signy){

                mantissa = adduint32(mantissax, mantissay);

                sign = signx;

        }

        else{

                if(mantissax > mantissay){

                        mantissa = subuint32(mantissax, mantissay);

                        sign = signx;

                }

                else{

                        mantissa = subuint32(mantissay, mantissax);

                        sign = signy;

                }

        }

        exponent = exponentx;

        while(mantissa >= (1 << 24)){

                mantissa = mantissa >> 1;

                exponent = adduint32(exponent, 1);

        }

        while((mantissa < (1 << 23)) && exponent > 0){

                mantissa = mantissa << 1;

                exponent = subuint32(exponent, 1);

        }

        mantissa = mantissa & 0x7FFFFF;

        if(exponent < 1){

                exponent = 0;

                mantissa = mantissa >> 1;

        }

        if(exponent >= 255){

                exponent = 255;

                mantissa = 0;

        }

        uint32\_t result = (sign << 31) | ((exponent & 0xFF) << 23) | (mantissa & 0x7FFFFF);

        if(result == 0x80000000){

                result = 0;

        }

        float result\_float = \*(float\*)&result;

        return result\_float;

}

Pada dasarnya hanya mengekestrak sign, exp, dan mantissa dari float. Kemudian di cek apakah angka nan atau inf, jika ya langsung di return. Lalu dilakukan operasi terhadap exponent dan mantissa sesuai dengan pertambahan serta dilakukan cek terhadap overflow dan underflow mantissa. Terakhir disusun kembali angka float nya dan di cek apakah dia -0 dan kemudian diubah menjadi 0 dan lalu result diubah kembali menjadi float dan selesai :D.

1. Karena arsitektur ARM memiliki SoC, SoC ini menggabungkan CPU, GPU, dan memori pada 1 chip. Desain ini mengurangi latency dan meningkatkan efisiensi througput data antar komponen. Apple juga mengoptimisasi software yang mereka buat agar dapat bekerja dengan baik dengan arsitektur ARM sehingga CPU seri M dapat terasa sangat cepat.
2. Instruction pipeline adalah cara untuk memproses beberapa instruksi disaat yang sama secara paralel sementara instruction cycle adalah urutan langkah yang diambil CPU untuk fetch, decode, read, dan execute sebuah instruksi.
3. a. Saat ketika system meminta data dari cache tetapi data tersebut tidak ada di cache.  
     
   b. Dengan cara menambahkan ukuran cache, mengoptimisasi program, menambahkan lifespan cache, atau mengurangi set instruksi.  
     
   c. Kecenderungan CPU untuk mengakses lokasi memori yang sama berulang kali dalam waktu singkat untuk mengoptimalkan efisiensi sistem  
     
   d. Menggunakan indexing dalam database agar index dapat disimpan dan data dapat dicari dengan lebih cepat
4. General Purpose Register:  
   - RAX, RBX, RCX, RDX : Untuk operasi umum seperti perhitungan aritmatika dan pemindahan data  
   - RSI, RDI : Pointer source dan destination pada operasi string  
   - RSP : Pointer pada puncak stack  
   - RBP : Pointer pada dasar stack  
   - R8 – R15 : Register general purpose tambahan  
     
   Pointer Register:  
   - RIP : Pointer pada instruction set berikutnya  
     
   Segment Register:  
   - CS (Code Segment) : Pointer pada segmen memori yang berisi kode execution  
   - DS (Data Segment) : Pointer pada segmen memori yang berisi data  
   - SS (Stack Segment) : Pointer pada segmen memori yang berisi stack  
   - ES : Pointer pada segmen memori extra untuk operasi string  
   - FS, GS : General purpose segment  
     
   RFLAGS Register:  
   Untuk menyimpan hasil operasi dan status control processor, berikut flag yang penting (yang suka aku ketemu saat melakukan pwn dan rev):  
   - CF (Carry Flag) : Menunjukkan carry atau borrow dalam operasi aritmatika  
   - ZF (Zero Flag) : Menunjukkan apakah hasil operasi = 0  
   - SF (Sign Flag) : Menunjukkan apakah hasil operasi negatif atau positif)  
   - OF (Overflow Flag) : Menunjukkan overflow dalam operasi aritmatika  
     
   Control Register:  
   Register untuk mengontrol operasi processor seperti memonry mangement, protection, atau mode OS  
     
   Debug Register:  
   Untuk debugging dan menentukkan breakpoint serta eksekusi program
5. a.

int a(int arr[], int size){

        if(size <= 0){

                return -1;

        }

        return arr[size-1] + a(arr, size - 1);

}

Penggunaan rekursif untuk menentukan jumlah elemen pada array

b.

int bmax(int arr[], int size){

        if(size <= 0){

                return -1;

        }

        if(size == 1){

                return arr[0];

        }

        else{

                int max = bmax(arr + 1, size - 1);

                return (arr[0] > max) ? arr[0] : max;

        }

}

int bmin(int arr[], int size){

        if(size <= 0){

                return -1;

        }

        if(size == 1){

                return arr[0];

        }

        else{

                int max = bmin(arr + 1, size - 1);

                return (arr[0] < max) ? arr[0] : max;

        }

}

Penggunaan rekursif juga untuk mencari nilai maksimum dan minimum

1. Keuntungannya diantara lain adalah konsumsi daya yang lebih sedikit karena banyak komponen pada 1 chip, ukurannya lebih kecil, dan latensi komunikasi antar komponen berkurang. Kerugiannya komponen SoC tidak dapat diupgrade secara terpisah dan biaya RnD yang cukup tinggi.
2. Karena format data little endian lebih mudah untuk melakukan operasi aritmatika dan secara historis x86 memang menggunakan little endian sehingga banyak yang menyesuaikan pada format tersebut.
3. Desain ARM apple dioptimalkan untuk perangkat apple sementara snapdragon lebih generik dan fleksible untuk perangkat lainnya, selain itu ARM apple hanya perlu fokus pada iOS sementara snapdragon harus bekerja pada berbagai OS lainnya.
4. Karena compiler melakukan optimisasi dan analisis pada program sehingga hasil dapat berbeda tergantung konteks yang diterima oleh compiler tersebut. Ketika GDB membaca binary file tersebut, ada kemungkinan tinggi beberapa bagian yang didisassemble telah berubah.
5. Programmer menulis kode program pada punch card yang mewakili suatu karakter atau instruksi dari bahasa pemrograman seperti Fortran atau COBOL yang kemudian akan dimasukkan ke mesin yang akan membaca lubang pada punch card tersebut. Lalu komputer akan mengeksekusi instruksi sesuai urutan kartu dan hasilnya biasanya akan dikeluarkan ke printer.

#include <stdio.h>

int main(){

        printf("What's up world\n");

        return 0;

}

Compiling:  
- Saat compiling, preprocessor meng “include” stdio.h  
- Kode diubah menjadi kode assembly oleh compiler  
- Assembly diubah menjadi kode mesin oleh assembler  
- Code object di link oleh linker dengan library yang diperlukan menjadi executable binary  
  
Running:  
- Loader me-load executable ke RAM dan menyiapkan stack, heap, dan segmen data  
- CPU meng-fetch instruksi dari memori  
- CPU meng-decode instruksi oleh control unit  
- CPU meng-execute instruksi oleh ALU  
- Program menampilkan “What’s up world” ke console  
Dibandingkan dengan arsitektur harvard, CPU tidak bisa membaca instruksi dan mengakses memori di saat yang sama karena arsitektur harvard memiliki memori terpisah untuk istruksi dan data. Hasilnya adalah arsitektur harvard lebih efisien karena instruksi dan data dapat di fetch secara bersamaan.

OS

1. a. BIOS:  
   - Pertama akan dilakukan POST (Power On Self Test) untuk mengecek komponen PC  
   - Lalu BIOS akan mencari bootstrap loader dari bootable device seperti CMOS, harddrive, USB, etc  
   - BIOS akan meng-load bootloader ke memori  
   - Terakhir, BIOS akan memberikan kontrol ke bootloader untuk memulai OS  
     
   b. UEFI:  
   - Pertama akan dilakukan POST seperti BIOS  
   - UEFI akan menginisialisasi hardware dan driver  
   - Lalu, UEFI boot manager akan membaca konfigurasi boot dan mengeksekusi OS boot loader atau kernel OS  
   - OS boot loader akan dideteksi secara otomatis oleh UEFI pada EFI System Partition  
   - Terakhir UEFI akan memberikan kontrol ke bootloader atau OS untuk memulai OS
2. Containerization mem-package kode software dengan library OS dan dependency, dan konfigurasi nya dalam satu paket yang disebut container. Sementara virtualization menjalankan OS lain termasuk kernel dan virtual hardware.  
     
   Perbandingannya containerization lebih ringan dan lebih cepat karena tidak ada OS lain yang berjalan, cocok untuk microservices. Sementara virtualization jauh lebih berat dan lebih lambat, tetapi cocok untuk menjalankan berbagai OS sekaligus atau environment yang butuh isolasi terhadap satu sama lain.
3. Write through:  
   Setiap kali cache diubah, perubahannya langsung ditulis ke memori. Digunakkan ketika sistem membutuhkan konsistensi data yang tinggi seperti database  
     
   Write back:  
   Data yang diubah di cache ditulis ke memori jika data tersebut diganti dari cache. Digunakkan ketika sistem membutuhkan kinerja yang tinggi dan dapat menangani beberapa ketidakkonsistennan  
     
   Read ahead:  
   Data yang dicari akan segera dibaca dari memori utama ke cache sebelum diperlukan. Digunakkan ketika data diproses secara sekuensial seperti pemrosesan video.  
     
   No read ahead:  
   Data akan dicari saat CPU benar-benar membutuhkannya. Digunakkan ketika data yang dicari tidak dapat diprediksi atau pengaksesannya secara acak  
     
   Adaptive read ahead:  
   Sistem menyesuaikan pengaksesan data secara dinamis berdasarkan pola akses data sebelumnya. Digunakkan ketika sistem memiliki pola akses data yang bervariasi seperti server atau database.
4. Perbedaan:  
   Kernel:  
   Windows memiliki kernel hybrid karena ada windows manager dan IPC manager.  
   Mac OS menggunakan kernel hybrid bernama XNU yang diciptakan dari 4.3BSD dan mach kernel.  
   Ubuntu menggunakan kernel monolitik linux  
     
   File System:  
   Windows menggunakan NTFS, FAT, dan exFAT  
   Mac OS menggunakan HFS+ dan Apple File System  
   Ubuntu menggunakan ext4  
     
   Shell:  
   Windows menggunakan command prompt dan powershell  
   Mac OS menggunakan Zsh  
   Ubuntu menggunakan Bash  
     
   Package Manager:  
   Windows menggunakan winget  
   Mac OS tidak mempunyai default package manager  
   Ubuntu menggunakan apt  
     
   Persamaan:  
   - Semua OS men-support multi user account  
   - Semua OS memiliki built-in security seperti firewall, user permision, encryption  
   - Semua OS memiliki GUI yang user-friendly berbasis window manager  
   - Semua OS men-support protokol networking seperti TCP/IP, Wi-Fi, ethernet, dan VPN
5. Karena android menggunakan API java sementara ubuntu menggunakan ibrary GNU libc dan API POSIX, selain itu android menggunakan framework GUI android yang dibuat menggunakan kotlin, sementara ubuntu menggunakan X11 sebagai graphical stack.
6. Kernel:  
   Ketika ada dua orang yang mencintai satu sama lain mempunyai seorang anak. Rumah tangga tersebut bisa dikatakan sebuah komputer dimana orang tua anak tersebut yang dapat mengatur semua kegiatan di rumah agar berjalan dengan baik sebagai kernel.  
     
   Driver Hardware:  
   Driver hardware seperti supir di rumah tangga tersebut yang dapat mengantar keluarga (komputer) itu ke tempat lain seperti toko (printer, keyboard, mouse) dengan baik.  
     
   Shell:  
   Shell itu seperti telepon, ketika kamu berbicara di telepon dan mengirim pesan ke teman, shell akan membantu berbicara dengan komputer untuk memberitahu apa yang harus dilakukan.  
     
   Multiprocessing:  
   Multiprocessing adalah seperti berbagai anak yang dapat bekerja sama untuk bermain/menyelesaikan tugas secara bersamaan.
7. RAM:  
   Ketika program dijalankan, OS akan mengalokasi memori pada RAM dan me-load instruksi program ke dalam RAM, jika RAM penuh, data yang tidak aktif akan kembali ke disk.  
     
   SSD/HDD:  
   Ketika program dijalankan, OS akan membaca program dari SSD/HDD agar bisa dipindahkan ke RAM.  
     
   Processor:  
   Saat program dijalankan, OS akan mengatur jadwal task, memastikan program mendapatkan waktu agar processor dapat melakukan kalkulasi dan logic operation yang diperlukan untuk menjalankan program, danmengatur multitasking dan prioritas proses.  
     
   Swap Memory:  
   OS akan mengelola swap space dan memutuskan data mana yang akan dipindahkan dari RAM ke swap memory dan memastikan data dapat dipindahkan kembali ke RAM saat diperlukan.
8. Istilah tersebut artinya unix meng-handle input/output dan resource dari harddrive, keyboard, printer, menggunakan stream melewati namespace file system. Contohnya seperti /dev/tty1 tempat terminal fisik, /proc/net/tcp tempat informasi tentang koneksi TCP, /etc/passwd tempat informasi user, etc.
9. Ext4:  
   Dikembangkan untuk linux, maximum file size 16TB, dan maximum volume size 1 EB. Fitur yang ada diantara lain journaling, extents, backward compatibility dengan ext3 dan ext2, delayed allocation, file-system checking yang lebih cepat, etc.  
     
   FAT32:  
   Dikembangkan untuk berbagai OS, maximum file size 4GB, maximum volume size 16TB. Tidak ada fitur khusus seperti Ext4 tetapi FAT32 simple dan mudah untuk di implementasi.
10. Untuk sistem yang CPU heavy, sebaiknya digunakan round robin karena round robin memecah proses untuk mendapat suatu jatah waktu dan jika proses tersebut tidak selesai dalam jatah waktu tersebut, proses akan dipindahkan ke belakang queue sehingga dapat memberikan respons yang adil dan menjaga keseimbangan workload CPU.  
      
    Untuk sistem real time, sebaiknya digunakan earliest deadline first scheduling karena EDF mengerjakan proses yang memiliki paling dekat dan dieksekusi terlebih dahulu sehingga bisa memberikan respons yang sesuai dengan kebutuhan realtime dengan utilisasi optimal.
11. Karena banyak software produktivitas seperti microsoft dan adobe yang lebih dioptimalkan di windows, dan juga game berjalan lebih baik di windows. Windows juga lebih user friendly dan tidak terlihat rumit. Windows juga sudah di pre-install di komputer yang dijual sehingga banyak user yang memang sudah terbiasa menggunakan windows sebagai OS utama mereka.   
      
    Linux unggul di pasar server karena linux stabil dan bisa berjalan bertahun-tahun tanpa reboot, struktur linux juga jauh lebih aman dibanding windows, lalu linux open source dan dapat dimodifikasi sesuai kebutuhan, kinerja linux juga jauh lebih efisien dibanding windows, dan terakhir package manager sepert apt juga memudahkan instalasi dan maintenance software.
12. – Privilege Escalation:  
    Exploit untuk mendapatkan akses ke resource tertentu yang biasanya tidak diberikan kepada user. Contohnya di beberapa kernel linux kita bisa menulis program yang mengatur current directory ke /etc/cron.d dan melakukan core dump di directory tersebut sehingga cron akan menganggap core dump tersebut sebagai text file biasa dan menjalankannya. Hasilnya adalah program yang bisa dijalankan tanpa root privilege.  
      
    - Session Hijacking:  
    Exploit untuk membajak sesi yang sudah diadakan untuk mem-bypass authentication. Contohnya dengan cara menangkap session ID seperti dengan sniffing atau cross site scripting dan menggunakan session ID tersebut untuk menyamar sebagai pengguna agar dapat menggunakan resource yang ada pada session ID itu. Dalam android penyerang dapat mencuri session token dari aplikasi mobile atau malware melalui serangan man in the middle sehingga penyerang dapat meng-hijack perangkat tersebut.  
      
    - Replay Attack:  
    Exploit untuk menangkap dan mengulang transmisi data yang valid dalam jaringan untuk mengecoh sistem penerima agar melakukan tindakan yang tidak sah tanpa melakukan authorization. Contohnya dengan menggunakan sniffer untuk mengambil login credential dan ditambahkan informasi dari penyerang seperti request untuk akses sehingga informasi tambahan tersebut dapat masuk ke sistem tanpa sistem tanpa dilakukan authorization. Dalam linux salah satu skenario ini dapat terjadi adalah saat authentication SSH, penyerang dapat menangkap sesi SSH dan mengulangi paket authentication sehingga penyerang dapat akses ke server.
13. Kernel level anticheat langsung di integrasi kan ke dalam kernel OS dan memungkinkan pemantauan yang lebih detail terhadap aktivitas sistem.  
      
    a. Dengan cara memantau proses, memory, dan file system secara real time dan mendeteksi manipulasi dari program cheat. Jika terdeteksi, game akan dihentikan dan pengguna akan di beri peringatan dari game. Client game juga akan memverifikasi integritas selama sesi game (alasan kenapa verifying file integrity di genshin lama bruh).  
      
    b. Karena kernel anticheat di kembangkan untuk windows dan tidak compatible untuk linux. Sistem keamanan linux juga berbeda dan banyak distro linux yang mengizinkan aplikasi untuk mengakses kernel.  
      
    c. Karena aplikasi yang masuk ke kernel dapat mengakses segala hal termasuk data pribadi. Dapat ada kekhawatiran tentang pengumpulan data pribadi tanpa persetujuan secara eksplisit. Sistem juga jadi lebih tidak stabil karena update pada OS dapat menyebabkan konlik dengan anticheat. Mengizinkan aplikasi untuk beroperasi dengan hak akses kernel juga membuka kemungkinan untuk adanya serangan dari luar jika sistem anticheat tersebut memiliki vulnerability.

Jarkom

1. – Saat menekan tombol kirim, email akan menghubungi SMTP yang diatur oleh configration email client  
   - Client akan membuat koneksi ke SMTP server dan meng-authenticate berdasar credential user  
   - Email client akan dikirim ke SMTP server  
   - SMTP server akan memeriksa DNS email penerima untuk menemukan server mail pengguna  
   - SMTP server akan melaukan query DNS untuk mendapatkan server mail  
   - SMTP server akan membuat koneksi ke SMTP server tujuan  
   - SMTP server tujuan akan menerima koneksi dari SMTP server pengirim dan menerima email  
   - SMTP server penerima akan mem-verifikasi DNS dan men-authenticate email  
   - Client penerima dapat membuka email dengan protokol POP3 atau IMAP
2. Error correcting akan mendeteksi dan memperbaiki kesalahan dalam data yang di transfer sementara error detection hanya mendeteksi adanya kesalahan dalam data yang di transfer.  
     
   Contoh error correcting code adalah hamming code:  
     
   function generateHammingCode(d4, d3, d2, d1):

p1 = parity(d1, d2, d4) // Calculate parity for positions 1, 2, 4

p2 = parity(d1, d3, d4) // Calculate parity for positions 1, 3, 4

p3 = parity(d2, d3, d4) // Calculate parity for positions 2, 3, 4

return p1, p2, d1, p3, d2, d3, d4

function decodeAndCorrectHammingCode(p1, p2, d1, p3, d2, d3, d4):

s1 = parity(p1, d1, d2, d4)

s2 = parity(p2, d1, d3, d4)

s3 = parity(p3, d2, d3, d4)

S = binary(s3, s2, s1) // Combine syndrome bits to find error position

if S ≠ 0:

flip the bit at position S in the code

return corrected d4, d3, d2, d1  
  
Hamming code digunakkan untuk memperbaiki kesalahan bit pada data yang disimpan seperti dalam server database.  
  
Contoh error detection code adalah checksum:  
  
function calculateChecksum(dataBytes):

sum = 0

for byte in dataBytes:

sum += byte

checksum = sum mod 256

return checksum

function verifyChecksum(dataBytes, originalChecksum):

sum = 0

for byte in dataBytes:

sum += byte

calculatedChecksum = sum mod 256

if calculatedChecksum == originalChecksum:

return True // Data is intact

else:

return False // Data is corrupted  
  
Checksum digunakkan pada pengiriman data seperti pada ethernet atau protokol lainnya untuk mengecek apabila terjadi kesalahan pada frame yang dikirim.

1. a. Cryptography adalah ilmu untuk membuat pesan yang dienkripsi sehingga hanya suatu pihak dengan kunci yang dapat membacanya. Cryptology adalah “superset” dari cryptography dan cryptanalysis yaitu studi tentang sistem berkomunikasi secara aman. Cryptanalysis adalah ilmu untuk memcahkan pesan yang sudah di encrypt tanpa mengetahui kunci atau algoritma encryption yang digunakkan.  
     
   b. Public key cryptography (Asymetric) adalah sistem encryption yang menggunakan 2 kunci yang berbeda tetapi saling terkait yaitu public key dan private key. Public key digunakkan untuk encryption sementara private key digunakkan untuk decryption, contohnya RSA dan ECC. Private key cryptography (Symmetric) adalah sistem encryption yang menggunakan key yang sama untuk encryption dan decryption, contohnya seperti AES. Digital signature adalah sistem cryptography yang digunakkan untuk mem-verifikasi keaslian dan integrity pesan atau dokumen digital dengan cara menggunakan private key untuk menandatangani data dan public key untuk memverifikasi tanda tangan, contohnya DSA. Hash adalah fungsi cryptography yang hasil panjangnya tetap dan hanya 1 arah yang berarti tidak bisa di decrypt, contohnya SHA-256 dan MD5.  
     
   c. IPSec adalah protocol yang mengamankan komunikasi IP dengan cara encryption paket IP. Beroperasi pada layer 3 (Network). Sementara SSL/TLS adalah protocol yang mengamankan data dengan cara encryption pada layer 4 (Transport).  
     
   d. CBC adalah block cipher mode dimana setiap block plaintext di xor dengan block ciphertext sebelumnya sebelum di encrypt dan block pertama di xor dengan IV (Initialization Vector). PCBC mirip dengan CBC, tetapi dengan tambahan propagation kesalahan di tial block. CFB adalah block cipher mode yang mnengubah block cipher menjadi stream cipherd an setiap block plaintext di xor dengan output encryption block sebelumnya. OFB mirip dengan CFB, tetapi setiap output dari encryption digunakkan sebagai input untuk encryption berikutnya tanpa menggunakan plaintext.
2. OSI memiliki 7 layer yaitu application, presentation, session, transport, network, data link, dan physical layer. Sementara TCP/IP hanya memiliki 5 layer yaitu application, transport, network, data link, dan physical layer. Perbedaannya berada di presentation dan session layer. Presentation layer bertanggung jawab untuk format dana dan enkripsi, session layer bertanggung jawab untuk mengatur komunikasi session. Di TCP/IP layer tersebut digabungkan di application layer.  
     
   Model OSI lebih sering digunakkan karena struktur nya lebih jelas dan detail, model tersebut juga dikembangkan oleh ISO sehingga lebih terstandarisasi dibanding model TCP/IP.
3. – Device seperti laptop mengirimkan sinyal radio ke access point  
   - AP menerima sinyal dari device dan meneruskannya ke router  
   - Router mengirimkan data ke internet melalui koneksi kabel dan menerima data dari internet untuk diteruskan ke device client.  
     
   Masalah yang dapat muncul:  
   - Banyak device yang terhubung atau menggunakan 1 saluran sehingga kecepatan dan performa menurun  
   - Jarak yang terlalu jauh dari AP sehingga sinyal lemah  
   - Pengaturan channel yang buruk sehingga banyak interferensi di channel dan performa menurun  
     
   Interferensi solusinya dengan menggunakan band 5 GHz yang lebih banyak salurannya, mengurangi beban dan kepadatan jaringan, menempatkan router di tempat yang lebih baik yang tidak terganggu dari device lain yang menghasilkan interferensi, dan menggunakan channel yang tidak tumpang tindih.
4. - 5350 MHz – 5470 MHz, karena sistem komunikasi satelit dan radar menggunakan rentang frekuensi tersebut  
   - 5600 MHz – 5650 MHz, karena rentang tersebut juga digunakan untuk radar cuaca dan komunikasi satelit  
     
   Dilarang untuk menghindari interferensi dengan layanan lain agar dapat beroperasi tanpa saling mengganggu.
5. - 802.11b direlease tahun 1999, maximum speednya 11 Mb/s dan frekuensinya 2.4GHz  
   - 802.11g direlease tahun 2003, maximum speednya 54 Mb/s dan frekuensinya 2.4 GHz  
   - 802.11n direlease tahun 2009, maximum speednya 600 Mb/s dan frekuensinya 2.4 dan 5 GHz  
   - 802.11ac direlease tahun 2013, maximum speednya 6933 Mb/s dan frekuensinya 5 GHz  
   - 802.11ax direlease tahun 2021, maximum speednya 9608 Mb/s dan frekuensinya 2.4, 5, dan 6 GHz  
   - 802.11be “supposedly” direlease tahun 2024, maximum speednya 23059 Mb/s dan frekuensi nya 2.4, 5, dan 6 GHz
6. – Application layer menyediakan layanan network langsung ke aplikasi pengguna, contoh protokol nya ada HTTP, FTP, SMTP, DNS  
   - Presentation layer mengubah data dari format aplikasi ke format network termasuk encryption, decryption, compression, dan decompression data, contoh protokol nya ada SSL/TLS, ASCII, JPEG  
   - Session layer mengatur session komunikasi antara 2 aplikasi, contoh protokolnya NetBIOS, PPTP  
   - Transport layer mentrasnsfer data end to end, contoh protokolnya TCP dan UDP  
   - Network layer menentukan rute dan mengirimkan paket data dari sumber ke tujuan, contoh protokol nya IP dan ICMP  
   - Data link layer mengatur pengiriman frame data yang terhubung, contoh protokolnya ethernet (MAC), wifi, switch  
   - Physical layer mengatur transmisi fisik melalui media seperti kabel, contoh protokolnya ethernet (kabel), fiber optic, coaxial
7. DHCP server adalah service yang secara otomatis mengelola konfigurasi jaringan device yang terhubung ke suatu network. Fungsinya agar mengurangi kerja manual dalam konfigurasi IP address, subnet mask, gateway, dan DNS pada setiap device yang terhubung ke network.  
     
   Tugas DHCP server:  
   - Alokasi IP address dan memastikan tiap device yang terhubung memiliki IP address yang unik  
   - Mengelola pool IP dan memastikan tidak ada 2 device yang mendapatkan IP address yang sama  
   - Memberikan informasi tambahan seperti subnet mask, default gateway, dan DNS server  
     
   Mekanisme umum DHCP  
   - Discovery, client DHCP mengirim broadcast untuk menemukan server DHCP  
   - Offer, server DHCP merespon dan menawarkan IP address dan informasi lainnya  
   - Request, client DHCP memilih salah satu IP address  
   - Acknowledgement, DHCP server mengkonfirmasi dan menyelesaikan proses dengan mengirim pesan ACK berisi informasi IP dan configuration nya  
     
   - DHCPDISCOVER berupa broadcast dengan IP tujuan 255.255.255.255 untuk mencapai semua server DHCP di local  
   - DHCPOFFER berupa broadcast walau bisa juga unicast jika server mengetahui MAC address client yang berisi tanggapan berupa tawaran IP address dan informasi lainnya atas DHCPDISCOVER  
   - DHCPREQUEST berupa broadcast yang dikirip oleh client DHCP untuk meminta IP address tertentu dari tawaran DHCPOFFER  
   - DHCPACK berupa unicast yang dikirim DHCP server untuk konfirmasi bahwa client dapat menggunakan IP address yang diminta
8. QUIC dibangun diatas UDP yang merupakan protokol yang lebih ringan dan lebih cepat, QUIC juga lebih reliable karena memeiliki mekanisme error detection dan mendukung multiplexed connection yang dapat membuat tiap endpoint independen antara satu sama lain sehingga tiap stream tidak akan mempengaruhi stream lainnya jika terjadi packet loss.
9. ISP di indonesia dapat memblokir DNS, URL/HTTP, dan IP situs ilegal tersebut sehingga ketika ada client yang mencoba mengakses situs tersebut mereka akan diarahkan ke halaman internet positif.  
     
   VPN dapat melewati pemblokiran dengan cara mengenkripsi data client sehingga ISP tidak bisa melihat konten data yang dikirim atau diterima, membuat tunnel agar semua network client diarahkan ke server VPN sebelum ke public, dan IP client akan ditutup oleh IP address server VPN.  
     
   Ketika DNS ISP diganti dengan DNS third party, request kedomain mereka tidak akan diarahkan melalui DNS ISP yang telah dikonfigurasi untuk memblokir situs tertentu karena blacklist yang ada di DNS ISP berbeda dengan yang ada di DNS third party.
10. – Man in the Middle attack:  
    Jenis serangan dimana penyerang menyelinap diantara 2 pihak yang sedang berkomunikasi dan memodifikasi pesan tanpa sepengetahuan pihak tersebut. Cara kerja nya dengan intersepsi seperti DNS spoofing atau menggunakan wifi yang tidak aman. Dapat di mitigasi dengan end to end encyption dan validasi sertifikat.  
      
    - Denial of Service:  
    Jenis serangan dimana penyerang mencoba membuat service tidak dapat diakses dengan cara membanjiri target dengan network yang berlebihian. Cara kerjanya dengan memberikan service dengan jutaan request sehingga resource server habis dan membuat server tersebut down.  
      
    - SQL Injection:  
    Jenis serangan dimana penyerang menyisipkan query SQL yang berbahaya dalam input yang kemudian di eksekusi di backend. Hal itu memungkinkan penyerang untuk mengakses, memodifikasi, atau menghapus data di database. Cara kerjanya dengan memasukkan query yang tidak di sanitize seperti UNION SELECT atau OR 1=1.
11. Torrent adalah cara berbagi file dengan protokol BitTorrent. Cara nya dengan user mendownload file .torrent yang berisi metadata file yangingin didownload, lalu server mengkoordinasikan komunikasi antara user yang mendownload (peers). Peers ada 2 jenis yaitu user yang mendownload semua file dan hanya menguploadnya (seeders) dan user yang masih mendownload file (leechers). File yang di download dibagi menjadi banyak bagian kecil dan peers mendownload berbagai potongan tersebut dari peers lain dan mengupload potongan yang sudah mereka miliki ke peers lain.  
      
    ISP Korsel dapat menginstall malware pada device yang menggunakan torrent dengan cara menganalisis user yang terlibat dari header dan payload packet, lalu akan disebarkan file .torrent yang telah dimodifikasi untuk mengarahkan peers agar mendownload file yang berisi malware.
12. – IP address adalah alamat unik yang diberikan ke setiap device yang terhubung, IPv4 menggunakan 32 bit sementara IPv6 menggunakan 128 bit.  
    - MAC address mirip seperti IP address, bedanya MAC address adalah alamat fisik yang diberikan pada tiap hardware device oleh parbik.  
    - OSPF (Open Shortest Path First) adalah protocol routing dinamis untuk menemukan jalur terpendek antar dua node network.  
    - BGP (Border Gateway Protocol) adalah protocol routing yang digunakan untuk membuat keputusan routing berdasar jalur, configuration, dan aturan di network.  
    - IS-IS (Intermediate System to Intermediate System) adalah protocol routing link-state untuk menemukan jalur terpendek dalam netowrk seperti OSPF.  
    - SDN (Software Defined Networking) adalah manajemen jaringan yang memisahkan kontrol secara software dari hardware.  
    - VLAN dan Trunking adalah teknologi untuk pemisahan network fisik dan network visual.  
    - Overlay Network adalah network virtual diatas network fisik untuk fitur tambahan.  
    - Spine Leaf Architecture adalah arsitektur network untuk data center yang meningkatkan performance dan scalability.  
    - FTP (File Transfer Protocol) adalah protocol untuk mentransfer file antara client di suatu network.  
    - gRPC adalah framework untuk remote procedure call.  
    - Websocket adalah protocol komunikasi untuk koneksi dua arah terus menerus antara client dan server.  
    - SSH (Secure Shell) adalah protocol network untuk koneksi remote ks sistem lain.  
    - SAMBA adalah software open source untuk integrasi file antara unix dan windows.  
    - PPTP (Point to Point Tunneling Protocol) adalah protocol tunneling untuk mengimplementasikan VPN.

Sisparter

1. Contoh

Miscellaneous

1. Free as in libre artinya merujuk pada kebebasan user terhadap suatu software entah untuk memodifikasinya, mempelajarinya, mendistribusikannya, etc. Contohnya GNU/Linux.  
     
   Free as in gratis artinya merujuk pada harga software. Software bisa didownload secara gratis tapi belum tentu semua fitur terbuka tanpa biaya tambahan. Contohnya seperti spotify, davinci resolve, etc.
2. – GNU General Public License (GPL):  
   User bisa menjalankan, mempelajari, mendistribusikan, atau memodifikasi software. License ini menggunakan copyleft yang artinya setiap karya turunan harus dilicense kan dibawah GPL yang sama. Contoh software yang menggunakan GPL adalah linux kernel, GCC (GNU Compiler Collection), dan Git.  
     
   - MIT License:  
   MIT license adalah license permissive yang artinya user bebas melakukan apa saja dengan software asalkan mereka menyertakan salinan license yang asli. Contoh software yang menggunakannya adalah X Window System, Ruby on Rails, dan Node.js.  
     
   - Apache License:  
   Apache license juga merupakan license permissive, tetapi ada terms of condition sendiri dari pembuatnya. Contoh software yang menggunakannya adalah Apache HTTP server, android (OS), dan Cython (goofy ahh language, i love it tho <3).
3. Karena filosofi mereka menekankan bahwa software harus sepenuh nya bebas (libre) dan bukan sekedar gratis (gratis). Mereka juga mendukung copyleft dan itu anggapannya terlalu ketat karena membatasi software bebas yang digunakan dalam proyek.  
     
   Menurutku mereka sebaiknya jangan terlalu memaksakan copyleft karena sangat membatasi software karena semua yang dipakai harus dibawah GPL, tidak bisa menggunakan apache atau MIT license. Selain itu pendapatku terhadap mereka biasa saja karena itu membantu menjaga intergritas software.
4. Menurut saya, open source project lebih aman karena kode nya transparan dan banyak user yang dapat memeriksa kode, mencari bug, dan memastikan kode aman. Open source project juga lebih fleksibel karena dapat disesuaikan kebutuhan user, tidak terkait pada fitur yang ditetapkan pada pembuat project. Selain itu, open source project biasanya tersedia secara gratis dan sering didukung komunitas developer, sehingga inovasi nya cepat karena developer dari seluruh dunia dapat berkolaborasi.