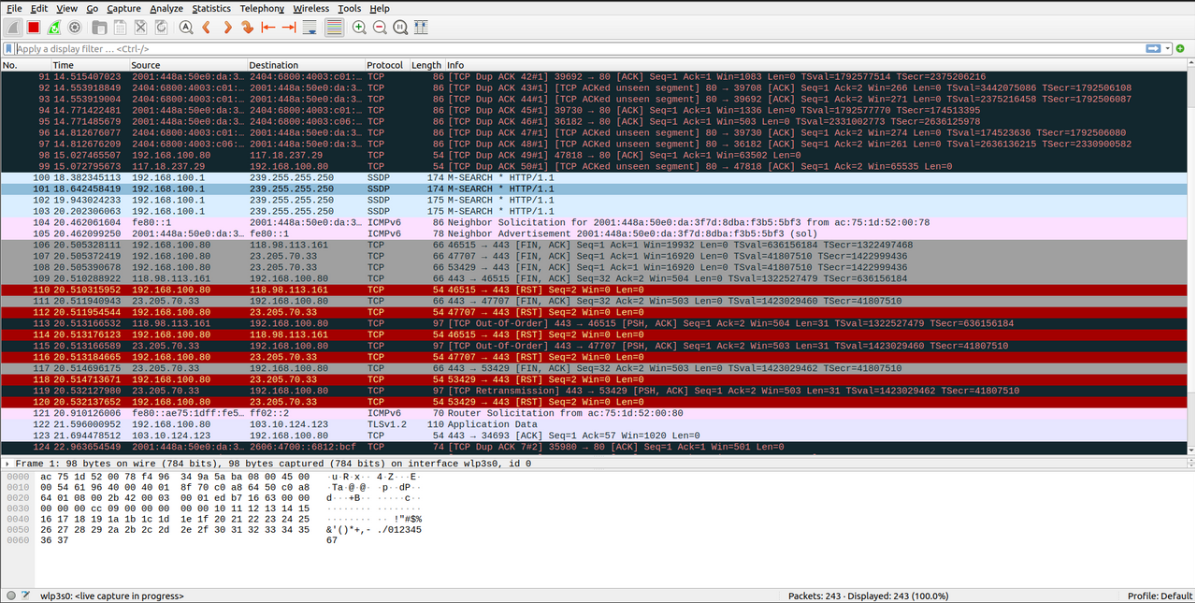
**Nama:Obed Christian s**

**D4ITA/3121600022**

**Praktikum 2**

1.Jelaskan Warna-Warna(color rules) Pada wireshark dibawah ini adalah contoh capture gambar dari wireshark



|  |  |
| --- | --- |
| Warna | Jenis |
| Hitam | (error)paket dengan kesalahan |
| Kuning muda | Lalu lintas khusus Windows,termasuk Server Message Block(SMB) dan NetBIOS |
| Ungu | TCP |
| Hijau muda | Trafic HTTP |
| Kuning gelap | Rute |
| Abu abu gelap | TCP SYN,FIN dan ACK lalu lintas |
| Biru muda | UDP |

APA ARTI DARI MASING-MASING WARNA DIATAS?

Bad TCP

TCP atau Transmission Control Protocol adalah merupakan bagian inti penting dari Internet Protocol sehingga sering disebut TCP/IP. TCP menyediakan komunikasi yang dapat diandalkan dan mempunyai urutan yang rapi. TCP berada pada transport layer.

HSRP State Change

Hot Standby Router Protocol (HSRP) adalah sebuah protokol standar CISCO yang menetapkan sebuah router yang secara otomatis mengambil alih jika router yang lain gagal. Dalam HSRP disetting dua status router yaitu aktif dan standby. Router standby baru digunakan jika router aktifnya gagal.

Spanning Tree Topology Change

protokol jaringan yang menjamin topologi jaringan bebas-perulangan bagi penghubung Ethernet LAN.

OSPF State Change

OSPF adalah protokol link state yang dianggap sebagai protokol paling terkenal di antara keluarga Interior Gateway Protocol (IGP), dikembangkan pada pertengahan 1980-an oleh kelompok kerja OSPF dari IETF.

ICMP errors

ICMP adalah kependekan dari Internet Control Message Protocol. ICMP merupakan bagian dari Internet Protocol. ICMP digunakan peralatan-peralatan yg terhubung melalui jaringan internet untuk keperluan analisa jaringan. Penggunaan ICMP yang terkenal adalah ping dan traceroute.

TCP RST

RST adalah reset.

TCP atau Transmission Control Protocol adalah merupakan bagian inti penting dari Internet Protocol sehingga sering disebut TCP/IP. TCP menyediakan komunikasi yang dapat diandalkan dan mempunyai urutan yang rapi. TCP berada pada transport layer.

SCTP ABORT

SCTP adalah protokol message- oriented yang handal. SCTP menyimpan batas- batas pesan dan pada saat yang sama mendeteksi kehilangan data, duplikasi data, dan out-of-order data. SCTP juga memiliki kontrol kongesti dan mekanisme kontrol aliran.

TTL low or unexpected

Time to Live (TTL) adalah mekanisme untuk membatasi umur data dalam komputer atau jaringan. TTL dapat di implementasikan sebagai counter atau timestamp terpasang atau tertanam dalam data.

Checksum Errors

Checksum Internet,[1][2] juga disebut checksum header IPv4 adalah checksum yang digunakan dalam versi 4 dari Internet Protocol (IPv4) untuk mendeteksi kerusakan pada header paket IPv4. Itu dibawa dalam header paket IP, dan mewakili hasil 16-bit dari penjumlahan kata-kata header.[3]

Protokol IPv6 tidak menggunakan checksum header. Perancangnya menganggap bahwa checksumming lapisan link seluruh paket yang disediakan dalam protokol, seperti PPP dan Ethernet, dikombinasikan dengan penggunaan checksum di protokol lapisan atas seperti TCP dan UDP, sudah cukup.[4] Dengan demikian, router IPv6 dibebaskan dari tugas menghitung ulang checksum setiap kali paket berubah, misalnya dengan menurunkan penghitung batas Hop pada setiap hop.

Checksum Internet wajib untuk mendeteksi kesalahan dalam paket UDP IPV6 (termasuk muatan data).

SMB

Blok pesan server (SMB) adalah jaringan file sharing dan protokol data Fabric. SMB digunakan oleh miliaran perangkat dalam sekumpulan sistem operasi yang beragam, termasuk Windows, MacOS, iOS, Linux, dan Android. Klien menggunakan SMB untuk mengakses data di server.

HTTP

HTTP atau Hypertext Transfer Protocol adalah protokol jaringan lapisan aplikasi (application layer) yang dikembangkan untuk membantu proses transfer antar komputer. Protokol ini berguna untuk mentransfer informasi seperti dokumen, file, gambar, dan video antar komputer.

DCERPC

DCE/RPC, kependekan dari "Lingkungan Komputasi Terdistribusi / Panggilan Prosedur Jarak Jauh", adalah sistem panggilan prosedur jarak jauh yang dikembangkan untuk Lingkungan Komputasi Terdistribusi (DCE). Sistem ini memungkinkan pemrogram untuk menulis perangkat lunak terdistribusi seolah-olah semuanya bekerja pada komputer yang sama, tanpa harus khawatir tentang kode jaringan yang mendasarinya.

Routing

Pengertian umum dari perutean atau routing adalah suatu proses pada paket yang meneruskan jaringan dari satu jaringan ke jaringan lainnya melalui internet. Fungsi routing adalah menghubungkan segmen jaringan lain untuk mengirimkan paket data. Routing penting untuk dipahami karena berguna untuk mengetahui dasar-dasar pada sebuah jaringan.

TCP SYN/FIN

TCP SYN-FIN Packets— Paket SYN dikirim untuk membuat koneksi TCP baru. Paket TCP FIN dikirim untuk menutup koneksi. Paket di mana flag SYN dan FIN diset seharusnya tidak pernah ada. Oleh karena itu paket-paket ini mungkin menandakan serangan pada perangkat dan harus diblokir.

TCP

TCP atau Transmission Control Protocol adalah merupakan bagian inti penting dari Internet Protocol sehingga sering disebut TCP/IP. TCP menyediakan komunikasi yang dapat diandalkan dan mempunyai urutan yang rapi. TCP berada pada transport layer.

UDP

UDP adalah singkatan dari User Data Protocol yang merupakan salah satu jenis protokol internet yang memungkinkan sebuah perangkat lunak pada komputer bisa mengirimkan pesan ke komputer lain melalui jaringan tanpa perlu ada komunikasi awal. Jadi saat Anda mengirimkan pesan melalui UDP, komputer pengirim dan penerima tidak perlu bernegosiasi saat akan melakukan pertukaran data.

Broadcast

Broadcast adalah sebuah metode dalam pengiriman data dimana data akan dikirim ke banyak titik sekaligus tanpa melakukan pengecekan apakah alamat yang dituju siap untuk menerima data atau tidak dan juga pengiriman paket juga tidak memperdulikan apakah data tersebut sampai pada alamat yang dituju atau tidak.

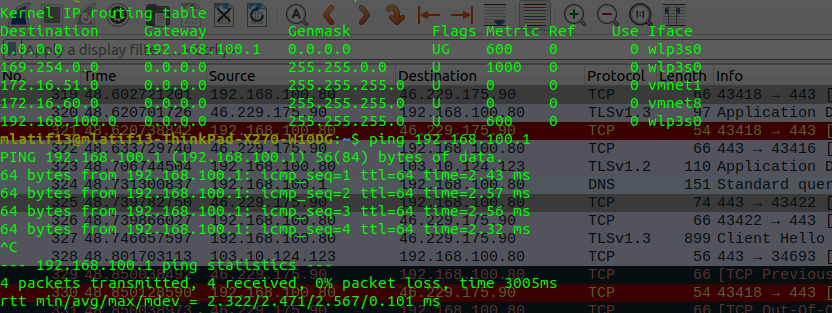
System Event

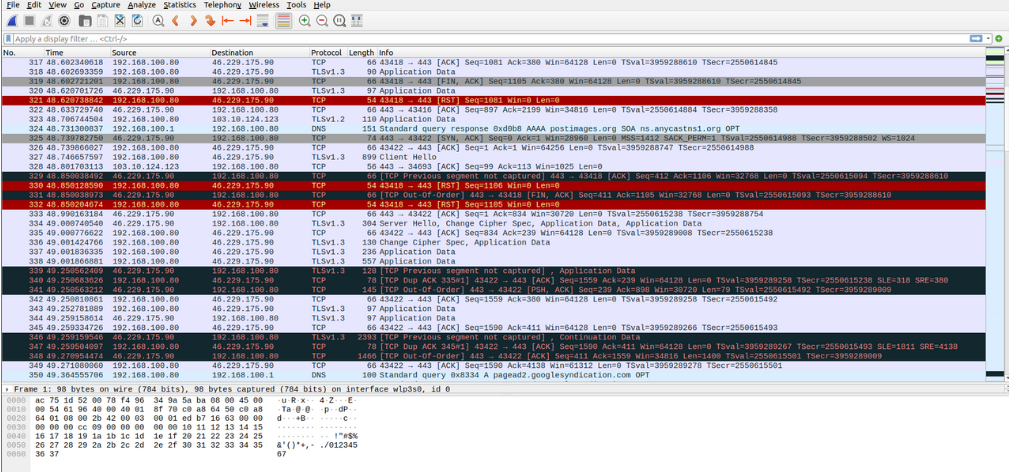
adalah titik dalam pelaksanaan program di mana tugas komputasi yang dapat diidentifikasi berlangsung. Contoh kejadian sistem meliputi: menulis ke file, memasukkan data ke dalam tabel database, memanggil subrutin, dan membuat instance thread program.

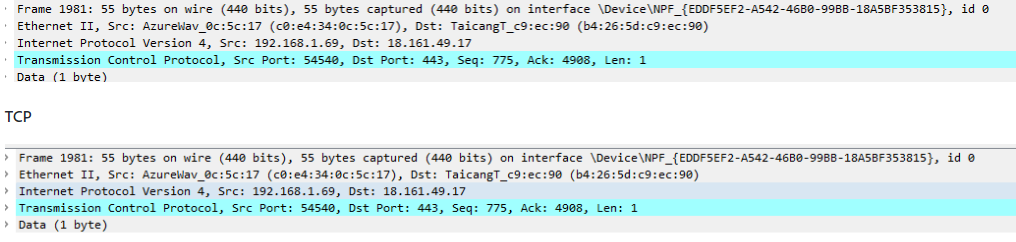
SOAL Jelaskan apa itu IP HEADER PADA WIRESHARK

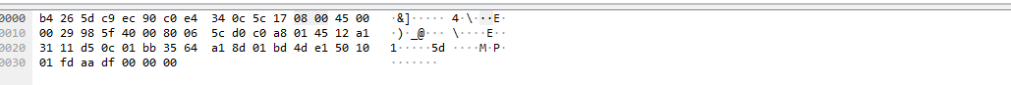
1.Kita jalankan wireshark dan pilih wifi, ping dengan cmd dengan alamat gateway default pada ipconfig

2.Pilih dan buka note yang ping

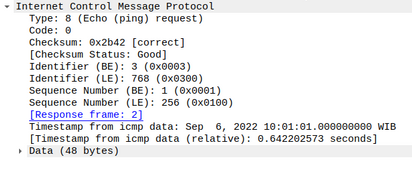








|  |  |  |
| --- | --- | --- |
| Nama field | Ukuran | Keterangan |
| Source Port | 2 byte(16bit) | Mengindikasikan sumber protokol lapisan aplikasi yang mengirimkan segmen TCP yang bersangkutan. Gabungan antara \_field\_ \*\*Source IP Address\*\* dalam \_header IP\_ dan \_field\_ \*\*Source Port\*\* dalam \_field\_ \_header TCP\_ disebut juga sebagai \*\*\_socket\_ sumber\*\*, yang berarti sebuah alamat global dari mana segmen dikirimkan. Lihat juga port TCP. |
| Destination Port | 2 byte (16bit) | Mengindikasikan tujuan protokol lapisan aplikasi yang menerima segmen TCP yang bersangkutan. Gabungan antara field Destination IP Address dalam header IP dan field Destination Port dalam field header TCP disebut juga sebagai \*\*\_socket\_ tujuan\*\*, yang berarti sebuah alamat global ke mana segmen akan dikirimkan. |
| Sequence Number | 4 byte(32 bit) | Mengindikasikan nomor urut dari oktet pertama dari data di dalam sebuah segmen TCP yang hendak dikirimkan. Field ini harus selalu diset, meskipun tidak ada data (payload) dalam segmen. Ketika memulai sebuah sesi koneksi TCP, segmen dengan flag SYN (Synchronization) diset ke nilai 1, field ini akan berisi nilai Initial Sequence Number (ISN). Hal ini berarti, oktet pertama dalam aliran byte (byte stream) dalam koneksi adalah ISN+1. |
| Acknowledgment Number | 4 byte(32 bit) | Mengindikasikan nomor urut dari oktet selanjutnya dalam aliran byte yang diharapkan oleh untuk diterima oleh pengirim dari si penerima pada pengiriman selanjutnya. Acknowledgment number sangat dipentingkan bagi segmen-segmen TCP dengan flag ACK diset ke nilai 1 |
| Data Offset | 4 bit | Mengindikasikan di mana data dalam segmen TCP dimulai. Field ini juga dapat berarti ukuran dari header TCP. Seperti halnya field \*\*Header Length\*\* dalam header IP, field ini merupakan angka dari word 32-bit dalam header TCP. Untuk sebuah segmen TCP terkecil (di mana tidak ada opsi TCP tambahan), field ini diatur ke nilai 0x5, yang berarti data dalam segmen TCP dimulai dari oktet ke 20 dilihat dari permulaan segmen TCP. Jika field Data Offset diset ke nilai maksimumnya (24=16) yakni 15, header TCP dengan ukuran terbesar dapat memiliki panjang hingga 60 byte. |
| Reserved | 6 bt | Direservasikan untuk digunakan pada masa depan. Pengirim segmen TCP akan mengeset bit-bit ini ke dalam nilai 0. |
| Flags | 6 bit | Mengindikasikan flag-flag TCP yang memang ada enam jumlahnya, yang terdiri atas: URG (Urgent), ACK (Acknowledgment), PSH (Push), RST (Reset), SYN (Synchronize), dan FIN (Finish). |
| Window | 2 byte(16bit) | Mengindikasikan jumlah byte yang tersedia yang dimiliki oleh buffer host penerima segmen yang bersangkutan. Buffer ini disebut sebagai Receive Buffer, digunakan untuk menyimpan byte stream yang datang. Dengan mengimbuhkan ukuran window ke setiap segmen, penerima segmen TCP memberitahukan kepada pengirim segmen berapa banyak data yang dapat dikirimkan dan disangga dengan sukses. Hal ini dilakukan agar si pengirim segmen tidak mengirimkan data lebih banyak dibandingkan ukuran Receive Buffer. Jika tidak ada tempat lagi di dalam Receive buffer, nilai dari field ini adalah 0. Dengan nilai 0, maka si pengirim tidak akan dapat mengirimkan segmen lagi ke penerima hingga nilai field ini berubah (bukan 0). Tujuan hal ini adalah untuk mengatur lalu lintas data atau \_flow control\_. |
| Checksum | 2 byte(16bit) | Mampu melakukan pengecekan integritas segmen TCP (\_header\_-nya dan \_payload\_-nya). Nilai field Checksum akan diatur ke nilai 0 selama proses kalkulasi checksum. |
| Urgent Pointer | 2 byte(16bit) | Menandakan lokasi data yang dianggap “urgent” dalam segmen. |
| Options | 4 byte(32bit) | Berfungsi sebagai penampung beberapa opsi tambahan TCP. Setiap opsi TCP akan memakan ruangan 32 bit, sehingga ukuran header TCP dapat diindikasikan dengan menggunakan field Data offset. |
| ICMP |  |  |



1.Version (4 bit). Menunjukkan format dari internet header. Versi saat ini sebagaimana dijelaskan pada RFC 791 adalah versi 4.

2.Internet header length (IHL: 4 bit). Menjelaskan panjang dari header menggunakan 32-bit word. Ukuran minimum header yang diijinkan adalah 5 word.

3.Type of service / jenis servis (8 bit). Data pada field ini menunjukkan kualitas layanan yang diinginkan.

4.Total Length/panjang keseluruhan (16 bit). Panjang keseluruhan ICMP dalam oktet, termasuk header dan data IP. Field ini memungkinkan datagram berisi sampai 66535 oktet. Standar yang ada menganjurkan tiap host bersiap siap untuk menerima datagram dengan panjang paling tidak 576 oktet.

5.Identification (16 bit). Field identifikasi digunakan untuk membantu proses penggabungan kembali pecahan-pecahan dari sebuah datagram.

6.Flag (3 bit). Field ini berisi tiga control flag.

7.Bit 0. Dicadangkan , harus 0.

8.Bit 1 (DF). 0 = bisa dipecah menjadi fragmen; 1 = tidak boleh dipecah

9.Bit 2 (MF). 0 = fragmen terakhir; 1 = masih ada fragmen lagi.

10.Bila sebuah datagram dipecah, MF bit untuk tiap fragmen kecuali yang terakhir bernilai 1.

11.Fragment Offset / posisi fragmen (13 bit). Untuk datagram yang dipecah, menunjukkan posisi fragmen ini dalam datagram.

12.Time To Live / waktu hidup (8 bit). Menunjukkan waktu maksimum bagi sebuah datagram untuk berada dalam suatu jaringan. Bila field ini memberi nilai 0, datagram akan dibuang. Field ini di modifikasi selama tahap pemrosesan header IP dan umum nya dihitung dalam detik. Namun tiap modul IP yang menangani datagram harus mengurangi Time To Live ini dengan 1. mekanisme ini memastikan bahwa datagram yang tak terkirim suatu saat akan dibuang.

13.Protokol (8 bit). Protokol lapisan atas yang berhubungan dengan bagian data dari datagram.

14.Header checksum (16 bit) Sebuah nilai checksum untuk header saja. Nilai ini harus dihitung ulang tiap kali header dimodifikasi.

15.Source Address (32 bit). Alamat IP dari host yang mengirimkan datagram.

16.Destination Address (32 bit). Alamat IP dari host yang merupakan tujuan akhir datagram.

17.Option (0 sampai 11 32-bit word). Dapat berisi 0 atau lebih pilihan.

**Ethernet 2**

****

1. Prembule – Bingkai Ethernet dimulai dengan Pembukaan 7-Bytes. Ini adalah pola alternatif 0 dan 1 yang menunjukkan awal dari frame dan memungkinkan pengirim dan penerima untuk membuat sinkronisasi bit. Awalnya, PRE (Pembukaan) diperkenalkan untuk memungkinkan hilangnya beberapa bit karena penundaan sinyal. Tetapi Ethernet berkecepatan tinggi saat ini tidak memerlukan Pembukaan untuk melindungi bit frame. PRE (Pembukaan) menunjukkan penerima bahwa frame akan datang dan memungkinkan penerima untuk mengunci ke aliran data sebelum frame yang sebenarnya dimulai.
2. Start of frame delimiter (SFD) – Ini adalah bidang 1-Byte yang selalu disetel ke 10101011. SFD menunjukkan bahwa bit yang akan datang memulai dari frame, yang merupakan alamat tujuan. Terkadang SFD dianggap sebagai bagian dari PRE, inilah alasan Pembukaan digambarkan sebagai 8 Bytes di banyak tempat. SFD memperingatkan stasiun atau stasiun bahwa ini adalah kesempatan terakhir untuk sinkronisasi.
3. Destination Address – Ini adalah bidang 6-Byte yang berisi alamat MAC mesin tempat data ditujukan.
4. Source Address – Ini adalah bidang 6-Byte yang berisi alamat MAC mesin sumber. Karena Alamat Sumber selalu merupakan alamat individu (Unicast), bit paling tidak signifikan dari byte pertama selalu 0. Panjang – Panjang adalah bidang 2-Byte, yang menunjukkan panjang seluruh bingkai Ethernet. Bidang 16-bit ini dapat menampung nilai panjang antara 0 hingga 65534, tetapi panjangnya tidak boleh lebih besar dari 1500 karena beberapa keterbatasan Ethernet sendiri.
5. Data – Ini adalah tempat di mana data aktual dimasukkan, juga dikenal sebagai Payload . Baik header IP dan data akan disisipkan di sini jika Internet Protocol digunakan melalui Ethernet. Data maksimum yang ada mungkin selama 1500 Bytes. Jika panjang data kurang dari panjang minimum yaitu 46 byte, maka padding 0 ditambahkan untuk memenuhi panjang minimum yang mungkin.
6. Cyclic Redundancy Check (CRC) – CRC adalah bidang 4 Byte. Bidang ini berisi kode hash data 32-bit, yang dihasilkan melalui bidang Alamat Tujuan, Alamat Sumber, Panjang, dan Data. Jika checksum yang dihitung oleh tujuan tidak sama dengan nilai checksum yang dikirim, data yang diterima rusak.

REFRENSI

https://en.wikipedia.org/wiki/DCE/RPC

https://accurate.id/teknologi/routing-adalah/

https://www.cisco.com/assets/sol/sb/Switches\_Emulators\_v2\_3\_5\_xx/help/250/index.html#page/tesla\_250\_olh/types\_of\_attacks.html

https://heriyansah007.wordpress.com/2013/10/21/what-is-time-to-live-ttl/#:~:text=Time%20to%20Live%20(TTL)%20adalah,terpasang%20atau%20tertanam%20dalam%20data.