پارسا حائری ۴۰۱۱۳۰۲۵۳

سوال ۱

پروتکل یک مجموعه قواعد تکنیک ها و قوانین است که به ما اجازه میدهد تا بین دوتا موجودیت داخل اینترنت ارتباط برقرار کنیم

Http: hypertext transfer protocol

یکی از پایه ای ترین پروتکل ها است که برای برقراری ارتباط مورد اسفتاده قرار میگیرد

به مرورگر های ما اجازه میده تا انواع عکس، متن، ویدیو و... را بفرستد و جواب را بگیرد و به ما نشان دهد

Dns: domain name system

مثل یک دفترچه تلفن میماند که به ما اجازه میدهد به جای ای پی، ادرس و دامنه داشته باشیم

ما برای برقراری ارتباط چیزی به اسم دامنه نداریم و باید مستقیم به ای پی متصل شویم

در واقع برای ترجمه نام های دامنه به ادرس های ای پی استفاده میشه

Dhcp: dynamic host configuration protocol

برای توزیع و تقسیم ای پی به کار میره

به ما اجازه میدهد به صورت اتوماتیک ای پی ها را به دستگاه های داخل شبکمان assign کنیم

برای تخصیص خودکار اددرس ای پی و سایر تنظیمات شبکه به دستگاه ها استفاده میشود

سوال ۲

کپچر ترافیک سایت alandtour.com

از قسمت اینترفیس ها وای فای را انتخاب و سایت را باز و سپس ترافیک را کپچر میکنیم. در مجموع ۱۴۴۵ پکت از ثانیه ۰ تا ثانیه ۱۶.۲۳۳۸۵۴ کپچر شد.سورس ها و دستینیشن های مختلفی شناسایی شد اما در مجموع بیشترین سورس و دستینیشن مربوط به ای پی سیستم خودم است. غالب سورس ها و دستینیشن ها IPV4 هستند اما تعدادی IPV6

انواع پروتکل های dns و arp و quic و ... موجود است اما بیشترین پروتکل مربوط به tcp است. طول QUIC برابر ۱۲۹۲ بایت و طول ARP برابر ۴۲ بایت است.

TCP و DNS طول های متفاوتی دارند.

TCP یا پروتکل کنترل انتقال نحوه برقراری و حفظ یک مکالمه شبکه‌ای که برنامه‌ها از طریق آن بتوانند داده‌ها را مبادله کنند، تعریف می‌کند و به این دلیل بیشترین تعداد را دارد و دارای رنگ های مختلف است.

حداقل طول ۴۲ بایت و حداکثر طول ۴۲۰۵۴ بایت است که مربوط به پروتکل TLSv1.2 است که یک پروتکل رمزنگاری است که امنیت داده های ارسال شده رو بررسی میکنه و غالبا عملیات application data را انجام میدهد.

قسمت info برای dns شامل ترجمه ادرس های ای پی به معادل نام دامنه در شبکه است و عملیات standard query. چیزی به اسم ادرس نداریم و دیتا داره توسط DNS ها مدیریت میشه.

یک پکت رو انتخاب میکنیم از پروتکل TCP و به تحلیل دقیق تر ان میپردازیم

پکت شماره ۲۰۷ با زمان ۷.۸۰۳۳۶۶ و سورس و دستینیشن هر دو از جنش IPV4. سورس از کامپیوتر من و دستینیشن به ای پی مربوط به سایت است. دارای ۵۴ بایت طول است که در قسمت ماشین کد قابل مشاهه اند. به سراغ دیتای موجود در پکت میرویم. در ۴ لایه شامل:

Frame 207:

سکشن نامبر ۱

انکپسیولیشن تایپ: ethernet (1)

Ethernet 2: مک ادرس دستینیشن برابر :Destination: b6:5b:3f:22:e1:e2

مک ادرس سورس

تایپ IPV4

IPV4: ای پی ما ورژن ۴ با طول هدر ۲۰ بایت و طول نهایی ۴۰ بایت و سرویس فیلد و در time to live برابر ۱۲۸ و سورس ادرس و دستینیشن ادرس برابر ۱۸۵.۴۴.۳۶.۱۲۹

Transmission control protocol:

سورس پورت ۵۷۹۹۸

دستینیشن پورت ۴۴۳

استریم ایندکس ۱۱

استریم پکت نامبر ۷۳