Subject:
Date ۱۴۰۳/۰۲/۱۲

پروژه شماره چهار شبکه های کامپیوتری - سینا سرای

۱- ابتدا با استفاده از فیلترها ترافیک را دسته بندی کردم. ← ۱. TCP ۲. HTTP (که البته ترافیکی از این دسته وجود نداشت.) ۳. UDP ۴. ICMP

پکت های TCP بدون فلگ بودند و پکتی از نوع HTTP وجود نداشت. در پکت های UDP یک پکت با Info متفاوت وجود داشت که با مشاهده اطلاعات آن متوجه Flag شدم.

=> flag{4QA05V4}

۲. پکت های موجود از انواع ۱. TCP ۲. UDP ۳. ICMP بودند که اطلاعاتی از قبیل DNS بر روی آن ها سوار شده بود. پکت های TCP همگی خالی از محتوا (Payload) بودند و Stream Index آن ها از ۰ تا ۱۹ بود همگی Source Port اشان ۲۰، DST Port اشان ۸۰ بود و SYN ← Flag اشان فعال بود.

پکت های UDP همگی به جز یکی دارای طول ۰ بودند و Src Port و DST Port اشان ۵۳ بود.

۲ تا از پکت های ICMP از نوع Multicast بودند و همگی درخواست Ping بود. به جز ۲ پکت بقیه پکت های ICMP از نوع Ping بدون پاسخ ماندند.

دسته ای دیگر از پکت بود که به عنوان IPV4 نمایش داده شده بود و در توضیحات آن نوشته شده:

IPv6 Hop-by-Hop Options

یک درخواست UDP ← DNS هم وجود داشت که Flag مورد نظر ما در آن قرار گرفته بود.