

53 → 53 Len=0      28      UDP 155.236.157.86      71.96.136.80      0.000000 53      -1

برای یافتن flag با به نگاه کلی متوجه شدم داخل UDP هست سپس با استفاده از فیلتر همه ایندکس ها را چک کردم (0 تا 56) در نتیجه پکت شماره 53 دارای flag بود.

-2

**پورت ها:** پورت ها در واقع درگاه هایی هستند که برای ارتباط با سرویس ها و برنامه ها در شبکه استفاده می شوند. هر پورت به یک شماره تعلق دارد و برای ارتباطات مختلف استفاده می شود. مثلاً، پورت 80 برای HTTP (پروتکل انتقال صفحات وب) و پورت 443 برای HTTPS (نسخه امن HTTP) استفاده می شود.

**پروتکل ها:** پروتکل ها قوانین و مقرراتی هستند که توسط دستگاه های شبکه برای ارتباط و تبادل اطلاعات پیروی می شوند. مثال هایی از پروتکل ها شامل TCP (کنترل انتقال پروتکل)، UDP (پروتکل دیتاگرام کوتاه)، ICMP (پروتکل کنترل پیام اینترنت) و IP (پروتکل اینترنت) هستند.

**آدرس های آی پی:** هر دستگاه در شبکه یک آدرس آی پی دارد که به عنوان شناسه آن دستگاه در شبکه عمل می کند. این آدرس ها برای ارسال و دریافت داده ها در شبکه استفاده می شوند. آدرس های IPv4 و IPv6 دو نوع اصلی آدرس آی پی هستند که در حال حاضر در اینترنت استفاده می شوند.

تحلیل محتوای خطوط شامل تفسیر اطلاعات محتوایی است که در بسته های شبکه قرار دارد. این محتوا می تواند اطلاعاتی مانند درخواست ها، پاسخ ها، دستورات، و داده های برنامه های کاربردی مختلفی که از پروتکل های مختلف استفاده می کنند، شامل باشد. به عنوان مثال، در تحلیل HTTP، محتوای بسته ها ممکن است شامل درخواست ها و پاسخ های HTTP باشد که شامل عنوان صفحات وب، داده های فرم، و سایر اطلاعات است.