
-

Flag{OII3L5N} -1

از آنجایی که در فایل کپچر شده فقط ٤ پروتکل وجود داشت و در پروتکل های udp, tcp, icmp پیدا نشد، با فیلتر کردن این سه پروتکل، فقط پروتکل ipv4 باقی ماند و از بین آنها در خط ١٦٢، flag مورد نظر رو پیدا کردم:

ip && not udp && not tcp && not icmp

-2

پورتها:پورتها در واقع درگاههایی هستند که برای ارتباط با سرویسها و برنامه ها در شبکه استفاده میشوند. هر پورت به یک شماره تعلق دارد و برای ارتباطات مختلف استفاده میشود. مثالً، پورت 80برایHTTP(پروتکل انتقال صفحات وب) و پورت443برایHTTPS(نسخه امن HTTP)استفاده میشود.
2.پروتکل ها:پروتکلها قوانین و مقرراتی هستند که توسط دستگاه های شبکه برای ارتباط و تبادل اطلاعات پیروی میشوند. مثالهایی از پروتکل ها شاملTCP(کنترل انتقال پروتکل)،UDP (پروتکل دیتاگرام کوتاه)،ICMP(پروتکل کنترل پیام اینترنت) وIP(پروتکل اینترنت) هستند.

3.آدرسهای آیپی:هر دستگاه در شبکه یک آدرس آیپی دارد که به عنوان شناسه آن دستگاه در شبکه عمل میکند. این آدرسها برای ارسال و دریافت دادهها در شبکه استفاده میشوند. آدرسهایIPv4وIPv6دو نوع اصلی آدرس آیپی هستند که در حال حاضر در اینترنت استفاده میشوند. تحلیل محتوای خطوط شامل تفسیر اطلاعات محتوایی است که در بسته های شبکه قرار دارد. این محتوا میتواند اطلاعاتی مانند درخواست ها، پاسخ ها، دستورات، و داده های برنامه های کاربردی مختلفی که از پروتکل های مختلف استفاده میکنند، شامل باشد. به عنوان مثال، درتحلیلHTTP، محتوای بسته ها ممکن است شامل درخواست ها و پاسخ هایHTTPباشد که شامل عنوان صفحات وب، داده های فرم، و سایر اطلاعات است.