جواب سوال ۱:

فلگ ذکر شده در صورت سوال در پکت با شماره ۵۰ یافت شد.

روند پیدا کردن فلگ به این صورت بود که پس از بررسی پروتکل های موجود در فایل حاوی ترافیک مربوطه با استفاده از اعمال فیلتر به بررسی پکت ها با پروتکل های مربوط به آنها به صورت جداگانه پرداخته شد که پس از اعمال فیلتر tcp بر روی ستون protocol و پس از بررسی پکت ها و چک کردن بخش بیت های مربوط به پکت ها پکت شماره ۵۰ که حاوی فلگ زیر بود پیدا شد:

Flag{TKRY7DI}

که در تی سی پی استریم شماره ۱۵ ام قرار گرفته بود.

جواب سوال ۲ :

پس از بررسی پکت های موجود در فایل ترافیکی داده شده. اطلاعاتی جمع بندی شده بدست آمد

به عنوان مثال پس از بررسی پکت های بر پایه پروتکل TCP و UDP اطلاعاتی از پورت های مبدا و مقصد این پکت ها به دست آمد به این گونه که پکت های بر پایه پروتکل TCP حاوی پورت منبع ۲۰ و پورت مقصد ۸۰ میباشند به همین شکل پکت های بر پایه پروتکل UDP دارای پورت منبع و پورت مقصد ۵۳ میباشند

پس از آن به پکت های بر پایه پروتکل ICMP برخوردیم که با بررسی آن ها ، به جز پکت شماره ۴۷ که توانست جوابی در پاسخ به درخواست خود از طرف سرور دریافت کند که نوع کانال ارتباطی آن بر پایه multicast مشخص شد ، مابقی پکت ها جوابی از سمت سرور دریافت نکردند و با پیغام no response found برخوردند که علت آن میتواند یکی از دلایل ذکر شده باشد:

تایم اوت پینگ:

هنگامی که یک دستگاه یا هاست را ping می‌کنید، دستگاه شما یک درخواست echo ICMP ارسال می‌کند و انتظار دارد که یک پاسخ echo ICMP دریافت کند. اگر دستگاه مقصد در دسترس نباشد یا مشکلات شبکه باعث تأخیر شود، دستگاه شما به دلیل تایم‌اوت در انتظار دریافت پاسخ ICMP خواهد بود و پیام "no response found" نمایش داده می‌شود.

مسدودسازی توسط فایروال:

فایروال‌ها می‌توانند به گونه‌ای تنظیم شوند که ترافیک ICMP را مسدود کنند، از جمله درخواست‌های echo/reply ICMP. اگر فایروال دستگاه مقصد یا فایروال‌های میانی در مسیر شبکه ترافیک ICMP را مسدود کنند، شما پاسخ‌های مورد انتظار را دریافت نخواهید کرد که منجر به نمایش پیام "no response found" می‌شود.

اختلالات در شبکه:

اختلالات شبکه یا مشکلات در تجهیزات شبکه می‌تواند باعث تأخیر یا از دست دادن بسته‌ها شود که منجر به گمشدن بسته‌های ICMP در حال انتقال شود. بدون پاسخ ICMP متناظر، دستگاه شما اعلام می‌کند که پاسخی دریافت نشده است.

مقصد قابل دسترسی نیست:

در برخی موارد، ممکن است دستگاه مقصد تنظیم شده باشد که به درخواست‌های echo ICMP پاسخ ندهد. این ممکن است عمدی (به دلایل امنیتی) یا به دلیل اشتباه در تنظیمات باشد.

مشکلات در دستگاه‌های میانی:

اگر مشکلاتی با روترها، سوئیچ‌ها یا سایر تجهیزات شبکه در مسیر بین دستگاه شما و دستگاه مقصد وجود داشته باشد، بسته‌های ICMP ممکن است به مقصد نرسند یا پاسخ دریافت نکنند.

در آخر هم به بررسی پکت های مبنی بر IPV4 پرداختیم که در تمامی آن ها ارور Malformed Packet رخ داده است که یکی از علل ذکر شده میتواند باعث رخ دادن آن شده باشد:

ساختار نادرست:

این بسته ممکن است دارای هدر نادرست، فیلدهای گمشده یا داده‌های اضافی باشد که باعث می‌شود از قالب استاندارد پروتکل خارج شود.

داده‌های نامعتبر:

داده‌های داخل بسته ممکن است نامعتبر یا به طور نادرست قالب‌بندی شده باشند که باعث مشکلات در پردازش توسط سیستم دریافت‌کننده می‌شود.

فساد بسته:

در حین انتقال، اگر بخشی از بسته فاسد یا گم شود، می‌تواند باعث بروز Malformed Packet در سرانجام مقابله‌کننده شود.

ناسازگاری پروتکل:

گاهی اوقات، یک بسته ممکن است بر اساس یک پروتکل یا نسخه متفاوت از آن باشد که سیستم دریافت‌کننده انتظار دارد، که منجر به بروز Malformed Packet می‌شود.

حملات امنیتی:

افراد بدخواه ممکن است عمداً بسته‌هایی با ساختارهای متشکل بسازند تا از آسیب‌پذیری‌ها در تجهیزات یا نرم‌افزارهای شبکه بهره‌برداری کنند.

پس از بررسی یکی از پکت ها میتوان احتمال داد که علت رخ دادن این موضوع ساختار نادرست باشد به دلیل که پس از بررسی بخش IPV6 hop-by-hop option پیغام زیر مشاهده شد:

(Error/Protocol): IPv6 Hop-by-Hop extension header must appear immediately after IPv6 header