سوال اول

Flag ==in packet TCP stream 12

Flag =={FS5LTPP}

برای پیدا کردن فلگ مورد نظر در شبکه ابتدا باید وارد وایر شارک شده و به فایلی که از قبل تعیین شده برای پیدا کردن فلگ مورد نظر دسترسی پیدا می کنیم. سپس پروتکل های موجود را که مشاهده کرده بررسی می کنیم.بعد از آن همه ی پروتکل ها را بررسی کرده و در هر پروتکل که الگوی خاصی را مشاهده کردیم و آن ها را به ترتیب بررسی میکنیم و اما این نکته حائز اهمییت است که فلگ ممکن است در هر پروتکلی باشد

مثلا پروتکل هایی که مشاهده میکنیم مثل UDP,TCP,... را با پسوند استریم چک میکنیم از مقادیر 0 به بالا سپس به هر مقداری که رسیدیم و معلوم شد در آن فلگ مورد نظر وجود دارد پس آن گزینه درست است و به جواب نهایی می رسیم.

سوال دوم

روش های کارآمد برای تحلیل فیلترهای مختلف در یک فایل شبکه، استفاده از ابزارهای مانیتورینگ ترافیک شبکه مانند Wireshark یا tcpdump است.

اعمال فیلترها: پس از بارگیری فایل شبکه در ابزار تحلیل، باید فیلترهای مورد نظر را اعمال کنیم این فیلترها می‌توانند بر اساس مشخصه‌های مختلفی مانند آدرس IP، پورت، پروتکل، و ... اعمال شوند.

تحلیل کردن جزئیات پکت ها برای پیدا کرد ن

• برای تحلیل جزئیات هر پکت، کافی است روی آن کلیک راست کرده و گزینه Follow و سپس نوع پروتکل

مورد نظر مثال Stream TCP یا HTTPرا انتخاب کنیم وبه جواب مورد نظر دسترسی پیدا میکنیم.

تحلیل ترافیک: با اعمال فیلترها، می‌توانیم ترافیک شبکه را مورد بررسی قرار دهید. این شامل بررسی پکت‌های منتخب، آمارهای ترافیکی، و تحلیل بر روی الگوهای مشاهده شده در ترافیک است.

ارزیابی تأثیرات: پس از تحلیل ترافیک با فیلترهای مختلف، باید تأثیرات این فیلترها بر رفتار و عملکرد شبکه را ارزیابی کنیم. این ارزیابی می‌تواند شامل افزایش یا کاهش کارایی، افزایش یا کاهش امنیت، تغییرات در میزان ترافیک، و ... باشد.

نتیجه گیری درمورد شبکه باید نتایج تحلیل خود را گزارش دهیم و این گزارش می‌تواند شامل توضیحات درباره فیلترهای مورد استفاده، تأثیرات آن‌ها بر شبکه، پیشنهادات برای بهبود عملکرد یا امنیت شبکه و ... باشد.