دانشکده‌ی مهندسی کامپیوتر

شبکه‌های کامپیوتری مدرس: مهدی جعفری

تمرین تئوری لایه اول (لایه اپلیکیشن)

گردآورندگان: کسری امانی - کامیار درزی لاریجانی - امیرمهدی نامجو شنبه ۶ آبان ۱۴۰۲

توجه پاسخ سوالات حتما به صورت تایپ شده و جواب هر قسمت از سوالات توضیحی به صورت مختصر پاسخ داده شود.

سؤال ۱ یک برنامه کاربردی که از پروتوکل VoIP استفاده میکند (*Voice over IP*) به طور متوسط هر ۲۰ میلی ثانیه یک بسته ۱۶۰ بایتی ارسال می‌کند. اگر هر بسته یک هدر ۴۰ بایتی داشته باشد، پهنای باند لازم برای برقراری چهار تماس همزمان اگر *packet loss* ۱۰ درصد باشد چقدر است؟

سؤال ۲ تفاوت دو پروتوکل *IMAP* و *POP3* را شرح دهید و مزایا و معایب هردو را به طور مختصر بیان کنید.

سؤال ۳ افزونه ایمیل چند منظوره اینترنتی (*MIME*) را توضیح دهید. توضیح دهید که چگونه *MIME* باعث بهبود در عملکرد *SMTP* می‌شود.

سؤال ۴ ۱. میزان زمان تاخیر برای انتقال یک بسته به اندازه 1000 بایت در یک لینک با طول 2500 کیلومتر و سرعت انتشار $2.5 \times 10^8 m/s$ و نرخ انتقال $2Mbps$ چقدر است؟

۲. میزان زمان تاخیر برای انتقال یک بسته به اندازه L بایت در یک لینک با طول d و سرعت انتشار s و نرخ انتقال $Rbps$ چه قدر است؟

۳. آیا این تاخیر به طول بسته وابسته است؟ توضیح دهید.

۴. آیا این تاخیر به نرخ انتقال وابسته است؟ توضیح دهید.

سؤال ۵ فرض کنید در یک مروگر شما بر روی یک لینک کلیک می‌کنید که آی‌پی آن مشخص نیست. برای همین موضوع نیاز به *DNS Lookup* وجود دارد. فرض کنید برای بدست آوردن آی‌پی آن سایت نیاز به مراجعه به n سرور *DNS* وجود دارد که RTT آن‌ها به صورت $RTT_1, \cdots RTT_n$ است. در صفحه مد نظر، یک فایل HTML وجود دارد که درون خود به 8 فایل دیگر ارجاع دارد. با فرض این که RTT لازم برای برقراری ارتباط با این سرور RTT_0 باشد و همچنین با فرض صفر بودن زمان انتقال (*transmission time*) به سوالات زیر پاسخ دهید:

۱. کل زمان از شروع *DNS Lookup* ها تا بارگزاری کامل صفحه در صورت استفاده از *Non-persistent HTTP* بدون ارتباطات موازی TCP چقدر خواهد بود؟

۲. کل زمان از شروع *DNS Lookup* ها تا بارگزاری کامل صفحه در صورت استفاده از *Non-persistent HTTP* با 5 ارتباطات موازی TCP چقدر خواهد بود؟

۳. کل زمان از شروع *DNS Lookup* ها تا بارگزاری کامل صفحه در صورت استفاده از *Persistent HTTP* چقدر خواهد بود.

سؤال ۶

سوال عملی - دست گرمی. برای پاسخ به این سوال باید نرم‌افزار wireshark را از طریق راهنمایی که در پیوست قرار گرفته است نصب کنید. توجه کنید برای پاسخ به سوالات این بخش باید تصویر و اسکرین پنجره مورد نظر را نیز در wireshark در فایل پاسخ قرار دهید.

پوریا که دانشجویی کنجکاو در امنیت است یک نمونه حمله DDoS یا منع سرویس توزیع شده را پیاده سازی کرده است (در صورت علاقه می‌توانید نام آن را جستجو کنید!). این حمله هدفش این است که با ارسال درخواست‌هایی مانع از سرویس دهی یک سرور یا سرویس دهنده بشود. از آنجایی که قرار است در نقش مهندس شبکه این حمله را تشخیص دهید و آن را خنثی! کنید، فایل کپچر آن یا pcap در اختیار شما قرار گرفته است. این فایل شامل درخواست‌هایی از نوع GET است و اصطلاحا به حمله پیاده سازی شده get flood می‌گویند که تعداد زیادی درخواست GET به صورت یک سیل به سمت سرور ارسال می‌کند.

۱. ابتدا تمام آدرس‌هایی که درخواست GET به سمت آن‌ها ارسال شده است را استخراج کنید (راهنمایی: از پنجره statistics و امکانات آن استفاده کنید.)

۲. حال پورت‌ها را بر حسب حجم بسته‌های ارسالی آن‌ها مرتب کنید و پورتی که بیشترین درخواست را ارسال و یا دریافت کرده است را گزارش دهید. (راهنمایی: منو endpoint احتمالا به شما کمک می‌کند.)

۳. حال که پورت حمله کننده را تشخیص دادید، طول سرآمد یا header بسته‌های حمله را استخراج کنید.

موفق باشید