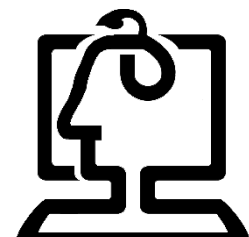




دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

فرم گزارش کار آزمایشگاه شبکه



دانشکده مهندسی کامپیوتر

نام و نام خانوادگی	فرهاد امان	شماره دانشجویی	۹۹۳۱۰۰۶	نام و شماره آزمایش	۷
				TCP تحلیل با استفاده از Wireshark	
هدف آزمایش	در این آزمایش، با ابزار Wireshark را بیشتر کار می‌کنیم و آمار و نمودارهای ارائه شده در آن را برای بسته‌های TCP را بررسی می‌کنیم.				
ابزارهای مورد نیاز	Wireshark				
شرح آزمایش	<p>سوال ۱:</p> <p>در پنجره‌ای که باز می‌شود، سه بخش "Hosts"، "Ports" و "Capture file comments" را مشاهده می‌کنید.</p> <p>در بخش "Hosts"، Mac address متناظر با هاست‌ها نمایش داده می‌شود Mac. address یک شناسه منحصر به فرد است که به رابط شبکه یک دستگاه اختصاص داده شده است و در لایه‌ی پیوند داده مدل OSI برای شناسایی دستگاه‌های شبکه محلی (local) استفاده می‌شود و در قالب هگزادسیمال نمایش داده می‌شود.</p> <p>در بخش "Ports"، نام سرویس‌ها همراه با port و نوع سرویس آن‌ها مشخص شده است.</p> <p>در بخش "Capture file comments" Comment هایی که در فایل‌ها ضبط شده‌اند، به نمایش در می‌آیند.</p> <p>سوال ۳:</p> <p>در این بخش، انواع پروتکل‌های به کار رفته در لایه‌های مختلف به صورت سلسله مراتبی با ترتیب لایه‌ها نمایش داده شده‌اند. برای هر پروتکل، درصد packet هایی که آن پروتکل را دارند، تعداد آن packet ها، درصد بایت و تعداد آن، سرعت بر حسب bits/s و غیره به صورت آمار نمایش داده شده است.</p>				

<p>سوال ۴: همانطور که در تصویر بالا نیز نمایش داده شده است، 95.3 درصد از ارتباط های IPv4 از TCP استفاده میکنند.</p> <p>سوال ۵: در این بخش، نشست های مختلف با دسته بندی پروتکل های مختلف نمایش داده می شوند. برای هر نشست، اطلاعاتی اعم از آدرس دو طرف conversation، تعداد packet ها و اندازه مجموع آن ها، تعداد packet های ارسال شده از هر host به دیگری و غیره نمایش داده شده است.</p> <p>سوال ۶: در پنجره ای که باز می شود، شما اطلاعات آماری هر نقطه پایانی (endpoint) را مشاهده می کنید. این اطلاعات شامل نمایش اطلاعات هر endpoint در دسته بندی های مختلف بر اساس پروتکل است و شامل مواردی مانند آدرس آن، تعداد و اندازه packet هایی که با آن در ارتباط بوده اند (ارسال یا دریافت) و نیز تعداد بسته های دریافت شده و ارسال شده و اندازه مجموع هر کدام می باشد.</p> <p>سوال ۷: ابتدا آدرس ip سیستم خود را با استفاده از دستور <code>ipconfig /all</code> مشاهده میکنیم. حال، در بخش TCP در پنجره endpoints، آدرس هایی که برابر با ip address ما نیستند را میتوان آدرس هایی دانست که با آن ها در ارتباط بوده ایم.</p> <p>سوال ۸: سیستم محلی ما بیشتر از سایر آدرس ها در ارتباط های ضبط شده شرکت کرده است. بنابراین، معمولاً تعداد بسته و یا حجم داده مبادله شده توسط آدرس ما، از سایر آدرس ها بیشتر است. در اینجا، دو Mac address وجود دارند که حجم داده بسیار زیادی انتقال داده اند. بیشترین داده مربوط به آدرس مشخص شده است و احتمال داده می شود مربوط به سیستم محلی ما باشد.</p> <p>حالا، با دستور "<code>ipconfig /all</code>" در cmd می توانیم آدرس Mac خود را مشاهده کنیم و با آدرس بالا مقایسه کنیم.</p>	
<p>بخش های مختلف آمار های ارائه شده توسط Wireshark مانند Resolved Addresses، Protocol Hierarchy، و نمودار هایی مانند I/O graph و نیز نمودار های مختلف TCP stream را مشاهده و اطلاعات موجود در هر یک را بررسی کردیم. همچنین آمار هایی اعم از conversation های موجود، endpoint ها و ... را نیز مشاهده کردیم و اطلاعات هر یک را مورد بررسی قرار دادیم.</p>	<p>نتیجه گیری</p>