پیش گزارش ۲

کیان پورآذر. ۴۰۱۳۱۴۰۱

سوال اول:

برنامه Wireshark تحلیل‌کننده پروتکل و شنود کننده ارتباط متن‌باز بر روي سیستم‌عامل‌هاي خانواده ویندوز و لینوکس است که به شما اجازه می‌دهید ترافیک شبکه خود را تحلیل کنید . پروژهي Wireshark در سال 1998 با نام Etherealتوسط Gerald Combs آغاز شد. این پروژه در سال 2006به Wiresharkتغییر نام داد. این نرمافزار توسط چهارچوب Qt و با زبان C/C++ نوشته شده است. این برنامه قادر به تحلیل برخط بیش از 1000پروتکل در نسخه 1.10.6 است. همچنین قادر به خواندن اطلاعات خروجی انواع برنامه‌هاي شنود و تحلیل دیگر مانند Microsoft Network Monitor ، TCPdumpاست. خروجی این برنامه می‌تواند به‌صورت PostScript،CSV،XML یا Plaintext باشد.

سوال دوم:

در سیستم‌عامل خانواده ویندوز، برنامهWireshark شنود بسته‌ها با استفاده از کتابخانهWinpcap انجام می‌دهد. معماري نرمافزار Winpcap به این گونه است که، از دو بافر یکی در سطح کرنل و دیگري در سطح کاربر، یک

ماشین فیلتر کننده که فیلترهایی را به بسته‌ها اعمال می‌کند و همچنین دو فایل wpcap.dllو packet.dll که اینتفریس‌های این برنامه را ارائه می‌کنند تشکیل شده است. در ابتدا کاربر می‌تواند فیلترهایی را مشخص کند که این فیلترها توسط Netgroup Packet Filter (NPF)به دستوراتی ترجمه می‌شوند که توسط فیلترها بر روي بسته‌ها اعمال می‌شوند . به « دریافت شوند UDP پروتکل یک فیلتر را به صورت »صرفا بسته‌هاي عنوان مثال کاربر می‌تواند تعریف کند. بسته‌ها پس از اینکه توسط گرداننده شبکه، از واسط شبکه خوانده شدند جمع‌آوري می‌شوند ؛ بنابراین کارایی Winpcap وابسته به گرداننده شبکه است. همچنین مشخص است که صرفا یک کپی از بسته‌ها توسط Winpcapدریافت می‌شود و بسته‌ها همزمان می‌توانند پشته پروتکلی سیستم‌عامل که در شکل با نام Other protocol stack مشخص شده است را طی کنند.

سوال سوم:

برنامه Wireshark دو نوع فیلتر کننده بسته دارد. یک نوع Capture Filter است و نوع دیگر Display Filter. Capture Filter قبل از شروع به شنود بسته مقداردهی می‌شود و در حقیقت همان فیلتري است که توسط NPF بر روي بسته‌هاي دریافت شده از گرداننده شبکه اعمال می‌گردد؛ بنابراین این فیلتر بر جمع‌آوري بسته‌ها تاثیر می‌گذارد. در مقابل Display Filter صرفا مربوط به فیلتر کردن بسته‌هاي جمع‌آوري شده است. با استفاده از Display Filter می‌توان تعدادي از بسته‌هاي جمع‌آوري شده را مشخص کرد که در پنجره Wiresharkنمایش داده شوند.