جرم یابی شبکه به چه مفهومی اطلاق می شود ؟

جرم یابی شبکه در واقع ثبت، ضبط و تحلیل رویدادهای شبکه است.

کاربرد جرم یابی شبکه در چیست ؟

جرم یابی شبکه از دو جنبه کاربرد دارد. اولین بعد در رابطه با امنیت است که شبکه را نظارت میکند و برای تشخیص ترافیک غیرعادی شبکه و تشخیص نفوذ به شبکه است. دومین بعد، بررسی های قانونی است که در این حالت تحلیلگر تمامی رفت و آمدهای کاربر در شبکه، کلیدواژه های استفاده شده و تمام ارتباطات، ایمیل ها و گفتگوهایش را بازیابی می کند.

جمع آوری اطلاعات شبکه

برای جمع آوری اطلاعات شبکه برای جرم یابی از دو روش استفاده میشود:

• روش Catch-it-as-you-can

در این روش، تمامی بسته هایی که از شبکه عبور میکنند، روی حافظه ضبط و ذخیره میشوند و تحلیل مورد نظر، روی حجمی از داده ها انجام می شود. این روش نیازمند حجم حافظه ی بسیار زیاد است.

• روش Stop, look and listen:

در این روش، بسته ها در حافظه بررسی می شوند و تنها اطلاعات مهم آن برای تحلیل های آینده ذخیره می گردند. برای این که همزمان با ترافیک شبکه پردازش و تحلیل صورت پذیرد، این روش نیاز به پردازنده ی سریع دارد.

در ادامه به معرفی مهمترین ابزارهای تحلیل شبکه میپردازم

ابزار Microsoft Network Monitor

این ابزاربه عنوان تحلیل کننده ی بسته به شما اجازه می دهد که ترافیک شبکه را ثبت، تحلیل یا حتی فقط نگاه کنید. توسط این ابزار می توانیم شبکه و یا برنامه های کاربردی داخل شبکه را عیب یابی کنیم. ویژگی اصلی آن شامل پشتیبانی از ۳۰۰ پروتکل عمومی و اختصاصی مایکروسافت، ثبت همزمان نشست ها، حالت نظارت بر شبکه های بی سیم و شنود ترافیک شبکه به صورت بی قاعده میباشد.

ابزار Capsa Free

ابزاری برای تحلیل ترافیک شبکه است که به شما اجازه ی نظارت بر ترافیک شبکه، عیب یابی آن و تحلیل بسته ها را می دهد. از ویژگی های آن میتوان به پشتیبانی از ۳۰۰ پروتکل شبکه (توانایی ایجاد و سفارشی سازی پروتکل ها را نیز دارد)

ابزار NetworkMiner

ابزار NetworkMiner بسته های شبکه را ثبت کرده و داده های آن را به صورت فایل و عکس تجزیه میکند و به بازسازی رویدادی که توسط کاربر در شبکه رخ داده است، کمک میکند. این ابزار امکان این عمل را روی فایل های از پیش ثبت شده (PCAP) نیز می دهد. NetworkMiner در دسته ای از ابزارهای جرم یابی شبکه قرار دارد که می تواند اطلاعاتی مانند نام میزبان، نام سیستم عامل و پورت های بازی که میزبان با آنها ارتباط دارد را نمایش دهد.

ابزار Angry IP Scanner

ابزار Angry IP Scanner یک برنامه ی مستقل برای ساده سازی اسکن آدرس های IP و پورت ها می باشد. این برنامه محدوده ای از آدرسهای IP را به دنبال یک میزبان فعال اسکن می کند و اطلاعاتی از آن شامل آدرس MAC، پورت ها، نام میزبان، زمان Ping و اطلاعات NetBios را برمی گرداند.

ابزار ntopng

درNtopng آخرین نسخه از تحلیلگر محبوب شبکه به نام ntop است ntopng در پس زمینه کار می کند و تمام اطلاعات ترافیک شبکه را جمع آوری و سپس، این اطلاعات را به همراه آمارهای به دست آمده از فعالیت شبکه را در یک رابط کاربری تحت وب نمایش می دهد.

ابزار WirelessNetView

WirelessNetView بزار بسیار کوچکی است که به صورت یک بسته ی اجرایی مستقل موجود است. این ابزار، شبکه های بی سیم قابل دسترس را شناسایی کرده و اطلاعاتی از آنها مانند SSID، کیفیت سیگنال، آدرس MAC، شماره ی کانال، الگوریتم رمزنگاری مورد استفاده و غیره را در اختیار می گذارد.

ابزار WireShark

ابزار WireShark رایج ترین ابزار مورد استفاده برای ثبت و تحلیل پروتکل های شبکه است که قابلیت بررسی صدها پروتکل شبکه را دارا بوده و بر روی انواع سیستم های عامل قابل اجرا است.