جرم‌یابی شبکه

نیلوفر محبی
nlf_mhb@yahoo.com

شهاب‌الدین نمازی‌خواه
namazikhah@cert.um.ac.ir

آزمایشگاه تخصصی آپا در زمینه امنیت فن‌آوری اطلاعات و ارتباطات

http://cert.um.ac.ir
cert@um.ac.ir

ویرایش اول – تیرماه ۱۳۹۳

شماره سند: APA_FUM_W_FNSC_0119

چکیده

در این مقاله، مفهوم جرم‌یابی شبکه مورد بررسی قرار می‌گیرد و اصول جرم‌یابی و ابزارهایی که در این راه به کارشناسان فن‌آوری اطلاعات کمک می‌کنند معرفی می‌شود.

واژه‌های کلیدی

جرم‌یابی شبکه، جرم‌یابی دیجیتال، تحلیل ترافیک شبکه، شنود، WireShark، Network Forensic

۱- مقدمه

ساختار سازمان‌ها بیش از گذشته به شبکه‌های کامپیوتری وابسته شده‌اند. بنابراین، نظارت بر عملکرد و مدیریت این شبکه‌ها بسیار حائز اهمیت است. گذشت زمان، مدیریت و نظارت بر شبکه‌ها را پیچیده‌تر می‌کند. از علل پیچیده‌تر شدن مدیریت بر شبکه‌های امروزی می‌توان به موارد ذیل اشاره کرد:

- **شبکه‌ها سریع‌تر و حجم داده‌ها بیشتر می‌شوند:** با افزایش سرعت شبکه‌ها، سازمان‌های فن‌آوری اطلاعات به دنبال ابزاری برای نظارت بر شبکه‌ها هستند که با سرعت شبکه همگام باشد. طبق بررسی‌های اخیر انجام شده توسط محققان TRAC، ۵۹٪ از تحلیل‌گران[1] فن‌آوری اطلاعات در مورد ابزارهای نظارت بر شبکه‌ی موجود ابراز نگرانی کردند. زیرا به دلیل افزایش سرعت شبکه، میزان بسته‌های از دست رفته نسبت به بسته‌های ثبت شده در شبکه بیشتر شده است و ۵۱٪ از محققان به صحت داده‌های ثبت شده اطمینان ندارند.
- **اطلاعات مانند VOIP یا Video over IP غنی‌تر و سنگین‌تر می‌شوند:** امروزه VOIP به عنوان استانداردی برای مکالمات تلفنی در سازمان‌ها و Video Over IP به عنوان کانالی برای انتقال محتوا در تجارت مورد استفاده هستند. سازمان‌ها برای تحلیل و بهینه‌سازی این سرویس‌های ارتباطی مهم، صرف‌نظر از این که این سرویس روی شبکه‌های محلی قدیمی پیاده شده باشند یا در شبکه‌های G40، نیاز به ابزارهای دقیقی دارند. ثابت شده است که ابزارهای تحلیل شبکه‌ای که بر اساس نمونه‌برداری کار می‌کنند، برای حل مشکل کارایی در برنامه‌های کاربردی با زمان تاخیر بسیار کم مانند VOIP مناسب نیستند.
- **تهدیدهای امنیتی مخرب‌تر و هوشمندانه‌تر می‌شوند:** رایج‌ترین تهدیدهای امنیتی تا یک دهه‌ی گذشته، سیل گسترده‌ای از نامه‌های مزاحم، کرم‌ها یا سایر بدافزارهایی بودند که یا شبکه را مسدود و یا عملیاتی را متوقف می‌کردند. امروزه تهدیدهای امنیتی بسیار هوشمندانه‌تر، پیچیده‌تر و خطرناک‌تر شده‌اند.
- **داده‌های نمونه‌برداری شده مورد تحلیل قرار می‌گیرند:** همزمان با افزایش ترافیک شبکه‌ها از نظر حجم و پیچیدگی، ابزارهای تحلیل شبکه نیز به سمت سادگی میل می‌کنند. محصولات جدیدتر مانند NetFlow و SFlow به جای تحلیل کل ترافیک شبکه، نمونه‌ای از آن را مورد بررسی قرار می‌دهند. سیستم‌های تحلیل مبتنی

[1] Analysts

بر جریان در بین سازمان‌های فن‌آوری اطلاعات جایگاه خود را پیدا کرده‌اند. آن‌ها راه‌حلی مقرون‌به‌صرفه برای اعمال نفوذ از طریق زیرساخت‌های شبکه مانند مسیریاب‌ها و سوییچ‌ها پیدا کرده‌اند، اما زمانی که برای عیب‌یابی مشکلات پیچیده استفاده شوند و یا برای تعیین این که پیام (شامل داده‌های اصلی یا مخرب)، داده‌های نمونه یا آماری باشد، به اندازه‌ی کافی دقیق نیستند.

تمام این تغییرات و کشمکش‌ها وظیفه‌ی کارشناسان فن‌آوری اطلاعات را برای پاسخ دادن به سوالاتی در مورد کارایی و بهره‌وری شبکه‌ها سخت‌تر می‌کند. برای پاسخ به این‌گونه سوالات، باید متخصصین فن‌آوری اطلاعات به ترافیک شبکه دسترسی پیدا کنند، اما امروزه ترافیک شبکه در مقایسه با گذشته بسیار سنگین‌تر و پیچیده‌تر است. برای بررسی اطلاعات ترافیک شبکه راهی جز ثبت آن‌ها بر روی دیسک نیست، زیرا زمان حضورشان بر روی شبکه کوتاه‌تر از آنی است که بشود آن‌ها را مورد بررسی قرار داد. ضبط شبکه – یا *جرم‌یابی شبکه*[1] که ابزارهای قدرتمند جستجو و تحلیل داده‌ها را دارند – سازمان‌های فن‌آوری اطلاعات را برای پاسخ‌گویی به این سوالات تواناتر می‌سازد.

با توجه به این که متخصصین فن‌آوری اطلاعات به دنبال مدرکی برای حمله‌های امنیتی می‌گردند، چنانچه ضبط شبکه به درستی پیاده‌سازی شود، جرم‌یابی شبکه باعث می‌شود که متخصصین فن‌آوری اطلاعات بتوانند سوزن را در انبار کاه پیدا کنند. دلایل زیادی مانند حل مشکلات کارایی، امنیت و مشکلات سیاست‌گذاری در شبکه‌های سریع امروزی وجود دارند که سازمان‌های فن‌آوری اطلاعات را وادار به پیاده‌سازی جرم‌یابی شبکه کنند.

۲- تعاریف پایه

جرم‌یابی شبکه از زیرشاخه‌های جرم‌یابی دیجیتال است. برای درک بهتر موضوع، ابتدا علم جرم‌یابی را تعریف می‌کنیم.

۲-۱- جرم‌یابی

علم جرم‌یابی[2] علمی است که برای اهداف قانونی استفاده می‌شود. جرم‌یابی، روش علمی برای جمع‌آوری و ارزیابی اطلاعات در مورد گذشته است.

[1] Network forensic
[2] Forensic science

۲-۲- جرم‌یابی دیجیتال

جرم‌یابی دیجیتال[1] به جرایم کامپیوتری مربوط شده و مترادف با جرم‌یابی کامپیوتری است، اما قابل گسترش برای تمام دستگاه‌های دیجیتالی می‌باشد که قابلیت ذخیره‌ی داده‌های دیجیتالی را دارند.

۲-۳- جرم‌یابی شبکه

جرم‌یابی شبکه از زیرشاخه‌های جرم‌یابی دیجیتال است. جرم‌یابی شبکه در واقع ثبت، ضبط و تحلیل رویدادهای شبکه است که با نام‌های بسته‌کاوی، جرم‌یابی بسته یا جرم‌یابی دیجیتال هم شناخته می‌شود. صرف‌نظر از نام‌گذاری انجام شده، هدف همه یکی است: ثبت تمام بسته‌های ترافیک شبکه از جمله ایمیل‌ها، گزارش‌های بانک اطلاعات و وبگردی‌ها در یک فضای قابل جستجو که تمام اطلاعات با تمام جزئیات قابل دریافت باشند. بر خلاف سایر مباحث جرم‌یابی کامپیوتری، جرم‌یابی شبکه با داده‌های پویا سر و کار دارد. موسسه‌ی SANS در این زمینه گفته است: "جرم‌یابی شبکه مشخص می‌کند که چه کسی با چه کسی در چه زمانی و به چه مدت و چگونه ارتباط داشته است."

۲-۴- کاربرد جرم‌یابی شبکه

جرم‌یابی 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، بررسی‌های قانونی است که در این حالت تحلیل‌گر تمامی رفت و آمدهای کاربر در شبکه، کلیدواژه‌های استفاده شده و تمام ارتباطات، ایمیل‌ها و گفتگوهایش را بازیابی می‌کند.

۲-۵- سطوح مختلف جرم‌یابی شبکه

سطوح مختلف جرم‌یابی شبکه عبارتند از:

- **اترنت:** استفاده از جرم‌یابی در اترنت توسط جریانی از بیت‌های استراق سمع و با ابزار شنود انجام می‌شود. رایج‌ترین ابزار در این لایه WireShark است که به عنوان Ethereal هم شناخته می‌شود. این ابزار تمام

[1] Digital forensic

داده‌های این لایه را جمع‌آوری کرده و اجازه می‌دهد که کاربر داده‌ها را بر اساس رویدادهای مختلف فیلتر کند. برای جمع‌آوری داده‌ها در اترنت، *کارت واسط شبکه*[1] میزبان در حالت بی‌قاعده قرار می‌گیرد، به این ترتیب می‌تواند تمام اطلاعات ترافیک شبکه (نه فقط اطلاعات مربوط به همان میزبان را) را جمع‌آوری کند. اگر مهاجم به شنود ارتباطش آگاه باشد، اطلاعات را به گونه‌ای رمز می‌کند که معمولا قابل شکستن نیستند. در صورتی که ارتباط مشکوک با میزبان که تماما رمزگذاری شده باشد ادامه پیدا کند، می‌تواند به این معنا باشد که میزبان نیز همدست مهاجم است.

- **TCP/IP:** در لایه‌ی شبکه، *پروتکل اینترنت*[2] مسؤول ارسال بسته‌های تولید شده توسط TCP به همراه اطلاعات منبع و مقصدی که توسط مسیریاب‌ها به دست می‌آیند، در شبکه هستند. بسته‌های دیجیتالی شبکه هم مثل GPRS از پروتکلی مشابه IP استفاده می‌کنند. جدول مسیرهای موجود در مسیریاب‌های میانی، در زمان شناسایی تهدید و مسیریابی آن، از بهترین منابع اطلاعاتی هستند. برای انجام این کار لازم است که بسته‌های مهاجم را تا پیدا کردن فرستنده‌ی بسته دنبال کنیم. یکی دیگر از منابع شواهد ما در این لایه *فایل‌های ثبت رخداد عملیات احراز هویت*[3] هستند. این فایل‌ها می‌توانند حساب کاربری را که با این تهاجم همکاری داشته به ما نشان دهد.
- **اینترنت:** اینترنت منبع بسیار قوی از مدارک شامل مرورگرها، ایمیل‌ها، اخبارهای گروهی و گفتگوها است. به عنوان مثال، تاریخچه‌ی یک سرویس‌دهنده‌ی وب می‌تواند برای نشان دادن زمان یک دسترسی مشکوک مورد استفاده قرار گیرد. حساب‌های کاربری ایمیل هم می‌توانند مدارک محکمی باشند، اما باید توجه داشت که سرآیند[4] ایمیل می‌تواند به راحتی ساخته شود. بنابراین، از جرم‌یابی شبکه برای تشخیص منبع دقیق تهاجم استفاده می‌شود. همچنین، با جرم‌یابی شبکه می‌توان معین کرد که چه کسی می‌تواند از یک کامپیوتر مشخص استفاده کند.
- **جرم‌یابی در شبکه‌های بی‌سیم:** هدف اصلی پیدا کردن روش‌ها و ابزارهایی برای جمع‌آوری و تحلیل ترافیک شبکه‌ی بی‌سیم است که می‌توانند شواهد معتبری باشند. شواهد جمع‌آوری شده می‌توانند شبیه داده‌های ساده بوده و یا با استفاده‌ی گسترده از فن‌آوری VOIP به دست آمده باشند.

[1] Network Interface Card (NIC)
[2] Internet Protocol (IP)
[3] Authentication logs
[4] Header

۲-۶- دلایل استفاده از جرم‌یابی شبکه

از جمله دلایل استفاده از جرم‌یابی شبکه می‌توان به موارد ذیل اشاره کرد:

- **پیدا کردن مدرکی در مورد یک حمله‌ی امنیتی:** راه‌حل‌های نظارت امنیتی مانند *سیستم‌های تشخیص نفوذ*[1] هشدارهای لازم در مورد فعالیت مشکوک در شبکه را با جزئیات کافی می‌دهند و با بررسی این رکوردهای جامع که شامل اطلاعات ترافیک شبکه است، کارشناس فن‌آوری اطلاعات می‌تواند حمله را در صورت وجود اثبات کرده و خرابی‌ها را بازسازی کند.
- **عیب‌یابی متناوب مشکلات شبکه:** اگر مشکلی در ساعات خاصی اتفاق بی‌افتد، کارشناس فن‌آوری اطلاعات داده‌های آن ساعت و آن روز را برای شناسایی رفتار شبکه بررسی می‌کند.
- **نظارت بر فعالیت‌های کاربر برای سازگاری با سیاست‌های واحد فن‌آوری اطلاعات و منابع انسانی:** از آن‌جایی که جرم‌یابی شبکه کلیه‌ی اطلاعات ترافیک شبکه را مثل نامه‌ها، پیوست‌های نامه‌ها، تماس‌ها و کلیه‌ی ارتباطات را ثبت و ضبط می‌کند، مدیر فن‌آوری اطلاعات و دپارتمان منابع انسانی می‌توانند متوجه شوند که هر یک از کاربران قوانین استفاده از منابع و شبکه را رعایت کرده‌اند یا خیر.
- **تشخیص منشاء نشتی اطلاعات و نظارت بر تراکنش‌های تجاری و عیب‌یابی سیستم‌ها**

۲-۷- قابلیت‌های مورد نیاز در راه حل‌های جرم‌یابی شبکه

برای سادگی تحقیقات دیجیتالی، یک راه حل جرم‌یابی شبکه باید دارای سه ویژگی زیر باشد:

- **توانایی ثبت داده‌ها:** به طوری که حجم عظیمی از داده‌ها را که با سرعت زیاد در شبکه در حال انتقال است، بدون از دست دادن حتی یک بسته ثبت کند.
- **توانایی کشف داده‌ها:** به طوری که همزمان با ثبت داده‌ها، باید بر اساس نیاز داده‌ها را فیلتر کند. فیلتر کردن داده‌ها می‌تواند بر اساس آدرس IP، محتوا، برنامه‌ی کاربردی مورد استفاده و یا غیره باشد. کارشناسان فن‌آوری اطلاعات توسط این ابزارها از بین حجم بسیار زیاد داده‌ها، یک بسته‌ی خاص را به موقع استخراج می‌کنند.

[1] Intrusion Detection System (IDS)

- **توانایی تحلیل داده‌ها:** برای سرعت بخشیدن به کشف و تحلیل، کارشناسان فن‌آوری اطلاعات از راه‌حل‌های جرم‌یابی برای بررسی الگوها و ناهنجاری‌های پیدا شده در طول پردازش بهره می‌برند. تحلیل خودکار که شامل تحلیل خبره می‌شود، رویدادهای شبکه را توضیح می‌دهد و به کارشناسان فن‌آوری اطلاعات کمک می‌کند تا به سرعت رفتارهای شبکه و هویت فرد ناشناس را شناسایی کنند.

غیر از این سه ویژگی کلیدی، سایر ویژگی‌های جرم‌یابی شبکه عبارتند از:

- **دقت:** یعنی در ثبت اطلاعات در شبکه‌ای با سرعت بسیار بالا، خطا نداشته باشد و بسته‌ای را از دست ندهد.
- **مقیاس‌پذیری:** برای این که جرم‌یابی شبکه توانایی پشتیبانی از ثبت اطلاعات در شبکه‌های با سرعت بالا مانند G10 و G40 را داشته باشد، باید قادر به ضبط، جستجو و تجزیه و تحلیل ده‌ها یا صدها ترابایت حجم داده‌ها به صورت مقرون به صرفه و قابل کنترل باشد.
- **انعطاف‌پذیری:** یعنی باید قادر به کار در شبکه‌های ناهمگن باشد تا سازمان‌ها مجبور به خرید ابزارهای مجزا برای سرعت‌های مختلف شبکه نباشند.
- **دسترس‌پذیری:** به این معنا که در حالی که به طور دایم در حال ثبت اطلاعات است، قادر به تحلیل داده‌ها در لحظه هم باشد. به این ترتیب، کارشناسان فن‌آوری اطلاعات می‌توانند فعالیت شبکه را در زمان‌های مختلف مقایسه کنند و نیازی به پیاده‌سازی، نگهداری و آموزش دو ابزار برای تحلیل جرم‌یابی و تحلیل در لحظه ندارند.

۲-۸- آن‌چه جرم‌یاب شبکه باید بداند

جرم‌یاب شبکه باید در مورد مفاهیمی خاص، اطلاعات لازم را داشته باشد. به عنوان نمونه، جرم‌یاب شبکه ممکن است با بدافزارها مواجه شود. پس باید دانش لازم درباره‌ی نحوه‌ی عملکرد بدافزارها و این که چه اثری روی سیستم عامل و سیستم فایل می‌گذارند، داشته باشد. جرم‌یاب شبکه باید شبکه و پروتکل‌های آن را بشناسد و توانایی بررسی ترافیک شبکه را داشته باشد. جرم‌یاب باید بتواند بسته‌ها را ببیند و آن‌ها را تحلیل کند. در واقع کسی که این توانایی‌ها را دارد، ممکن است مدیر، معمار و مهندس شبکه باشد.

جرم‌یاب شبکه باید به نوعی مدیر ارشد سیستم باشد، اطلاعات کاملی در مورد سیستم‌های عامل داشته باشد، دانش

کافی برای بررسی اطلاعات فایل‌های ثبت رخداد داشته باشد، توانایی کشف فایل‌های مخفی شده در پارتیشن‌های مخفی را داشته باشد، درک و شناختی از ابزارهای مدیریتی سیستم و نحوه‌ی استفاده از آن‌ها در ویندوز داشته باشد، توانایی کار با ابزارهای خط فرمان و همچنین درک درستی در مورد نحوه‌ی کار کردن ویندوز با دیسک‌ها و ذخیره‌ی داده‌ها داشته باشد.

جرم‌یاب شبکه باید در مورد سیستم‌های عامل مبتنی بر UNIX مانند Mac OS، Linux، FreeBSD و OpenBSD شناخت داشته باشد. دستورات خط فرمان متناسب با این سیستم‌های عامل از جمله fsck، dd، file و غیره را بشناسد و نحوه‌ی اجرای آن‌ها را بداند. در ساده‌ترین حالت، باید دستورات جستجوی فایل‌ها، تغییر دایرکتوری‌ها، نمایش فایل‌ها و دایرکتوری‌ها، به دست آوردن ویژگی‌ها و مجوزهای فایل‌ها و دایرکتوری‌ها را بداند.

جرم‌یاب شبکه باید انواع سیستم فایل را بشناسد و تفاوت آن‌ها را بداند. وی باید سیستم فایل‌های FAT16، FAT32 و NTFS که مبتنی بر ویندوز هستند و یا سیستم فایل‌های utfs، ext2، ext3، ext4، jfs و غیره را که مبتنی بر UNIX هستند را بشناسد و بداند چه هستند و چگونه اجرا می‌شوند.

جرم‌یاب شبکه باید در مورد پارتیشن‌بندی دیسک دانش کافی داشته باشد. در مورد این که Master Boot Record چیست، چه چیزهایی در آن ذخیره می‌شود و تفاوت پارتیشن‌های فیزیکی و منطقی در چیست. وی باید بداند وقتی یک پارتیشن منطقی اضافه می‌شود، چه اتفاقی برای دیسک و نقشه‌ی پارتیشن‌ها می‌افتد.

اطلاعات حداقلی که باید جرم‌یاب در مورد شبکه داشته باشد، این است که TCP/IP را بشناسد، شناخت اولیه‌ای از Socketها داشته باشد و این که Socketها برای برقراری ارتباط بین سیستم‌ها چگونه کار می‌کنند.

علاوه بر موارد فوق، جرم‌یاب باید اطلاعات اولیه‌ای در مورد مدیریت حافظه داشته باشد، مکانیزم‌های تخصیص حافظه توسط سیستم عامل را بشناسد، بداند که پشته چیست یا هیپ چگونه حافظه تخصیص می‌دهد و در زمان اجرای برنامه چه اتفاقی می‌افتد. در ضمن باید در مورد حافظه‌های مجازی نیز دانش کافی داشته باشد، این که حافظه‌ی مجازی چیست، فایل‌ها را کجا ذخیره می‌کند و این که چرا باید از حافظه‌ی مجازی استفاده کرد.

به طور کل، یک جرم‌یاب شبکه باید اطلاعات پایه‌ای راجع به سیستم‌های عامل و سیستم فایل آن‌ها، پارتیشن‌بندی دیسک‌ها و جدول پارتیشن‌ها، شبکه و به خصوص پروتکل TCP/IP و همچنین درک اولیه از مدیریت حافظه داشته باشد.

۳- جمع‌آوری اطلاعات شبکه

برای جمع‌آوری اطلاعات شبکه برای جرم‌یابی از دو روش استفاده می‌شود:

- **روش Catch-it-as-you-can :** در این روش، تمامی بسته‌هایی که از شبکه عبور می‌کنند، روی حافظه ضبط و ذخیره می‌شوند و تحلیل مورد نظر، روی حجمی از داده‌ها انجام می‌شود. این رهیافت نیازمند حجم حافظه‌ی بسیار زیاد است.
- **روش Stop, look and listen :** در این روش، بسته‌ها در حافظه بررسی می‌شوند و تنها اطلاعات مهم آن برای تحلیل‌های آینده ذخیره می‌گردند. برای این که همزمان با ترافیک شبکه پردازش و تحلیل صورت پذیرد، این روش نیاز به پردازنده‌ی سریع دارد.

۳-۱- روش‌های بررسی جرم‌یابی شبکه

مانند تمام روش‌های دیگر جرم‌یابی، پوشش دادن و تحلیل شواهد از منابع شبکه باید به گونه‌ای انجام شود که نتایج قابل تولید مجدد و دقیق باشند. برای تضمین مفید بودن خروجی، محققان جرم‌یابی باید کارها را در یک چارچوب قانون‌مند و تعریف شده اجرا کنند. برای این منظور، روند گام به گام زیر پیشنهاد می‌شود که به روش OSCAR معروف است.

- ***جمع‌آوری اطلاعات***[1]**:** در اولین مرحله‌ی تحقیق باید دو کار انجام شود. جمع‌آوری اطلاعات در مورد واقعه، مانند توضیحی در مورد اتفاقی که افتاده، زمان و تاریخ و روش کشف واقعه، افراد مرتبط، سیستم و داده‌های درگیر شده و همچنین، جمع‌آوری اطلاعات در مورد پیرامون واقعه مانند مدل تجاری، مسائل حقوقی، توپولوژی شبکه، منابع در دسترس شواهد شبکه، ساختار سازمانی، سیستم‌های ارتباطی و منابع موجود.
- **استراتژی**[2]**:** در این گام، منابع و شواهد الویت‌بندی شده و با طرح همگام می‌شوند.
- ***جمع‌آوری شواهد***[3]**:** در این گام توسط طرح به دست آمده از گام قبل، از تمام منابع، شواهد جمع‌آوری می‌شوند.

بهترین شیوه‌های جمع‌آوری شواهد عبارتند از:

[1] Obtain information
[2] Strategize
[3] Collect evidence

- شواهد را به صورت قانونی و در سریع‌ترین زمان ممکن به دست آوریم.
- یک نسخه‌ی رمزنگاری شده‌ی معتبر از آن ایجاد کنیم.
- دسترسی به نسخه‌ی اصلی را محدود کنیم.
- تحلیل‌ها را بر روی نسخه‌ی کپی انجام دهیم.
- از ابزارهای قابل برگشت و مطمئن استفاده کنیم.
- کلیه‌ی اقدامات انجام شده را مستند کنیم.

- **تحلیل :** اگرچه روند تحلیل اطلاعات عموما عملی غیرخطی است، اما عناصر اصلی دارد که باید به آن‌ها توجه شود، مانند ارتباط بین منابع، زمان، رخدادهای مورد علاقه و غیره.
- **گزارش**[1] **:** اکثر ابزارهای جرم‌یابی این قابلیت را دارند، اما چندان در این زمینه قدرتمند نیستند. یک گزارش باید سه ویژگی اساسی داشته باشد: اول این که توسط فرد غیرحرفه‌ای قابل درک باشد، دوم این که کاملا قابل دفاع باشد و سوم این که واقعی باشد.

۴- ابزارها و راه‌حل‌های جرم‌یابی شبکه

۴-۱- WildPacketها، یکی از راه‌حل‌های جرم‌یابی شبکه

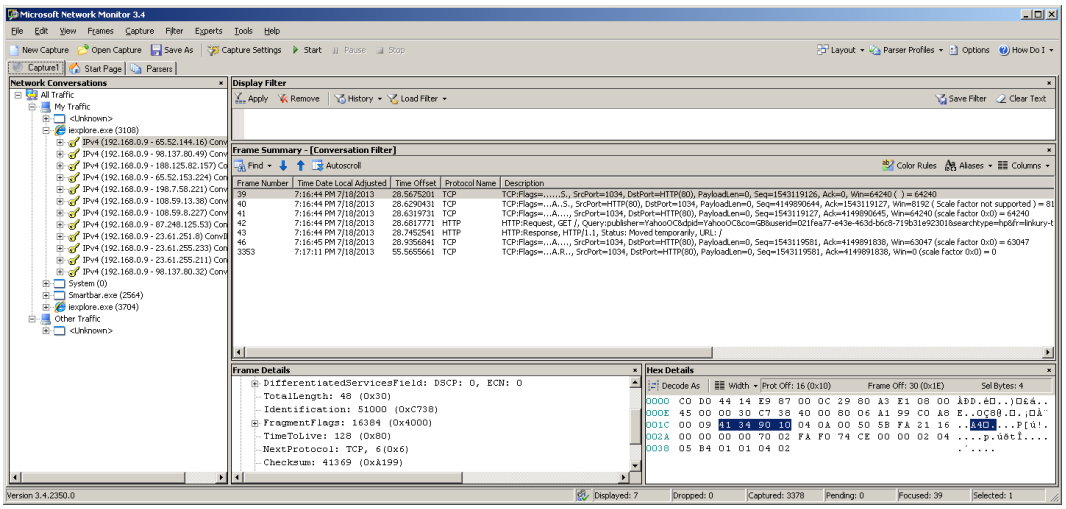
شرکت WildPacket در سال ۱۹۹۰ میلادی توسط مهبد ضابطیان و تیم مک کرری تاسیس شد. اولین محصول تولید شده توسط این شرکت برای سیستم عامل Mac نوشته شد. این محصول Etherpeek نام داشت که برای تجزیه و تحلیل در پروتکل شبکه‌های اترنت استفاده می‌شد. در سال ۱۹۹۷ میلادی نسخه‌ی سازگار با سیستم عامل ویندوز این محصول تولید شد. در نسخه‌ی بعدی این محصول به نام AiroPeek پشتیبانی از شبکه‌های بی‌سیم با پروتکل IEEE 802.11 نیز در نظر گرفته شد.

[1] Report

۴-۲- ابزارهای تحلیل شبکه

۴-۲-۱- ابزار Microsoft Network Monitor

Microsoft Network Monitor به عنوان تحلیل‌کننده‌ی بسته به شما اجازه می‌دهد که ترافیک شبکه را ثبت، تحلیل یا حتی فقط نگاه کنید. توسط این ابزار می‌توانیم شبکه و یا برنامه‌های کاربردی داخل شبکه را عیب‌یابی کنیم. ویژگی اصلی آن شامل پشتیبانی از ۳۰۰ پروتکل عمومی و اختصاصی مایکروسافت، ثبت همزمان نشست‌ها، حالت نظارت بر شبکه‌های بی‌سیم و شنود ترافیک شبکه به صورت بی‌قاعده می‌باشد.

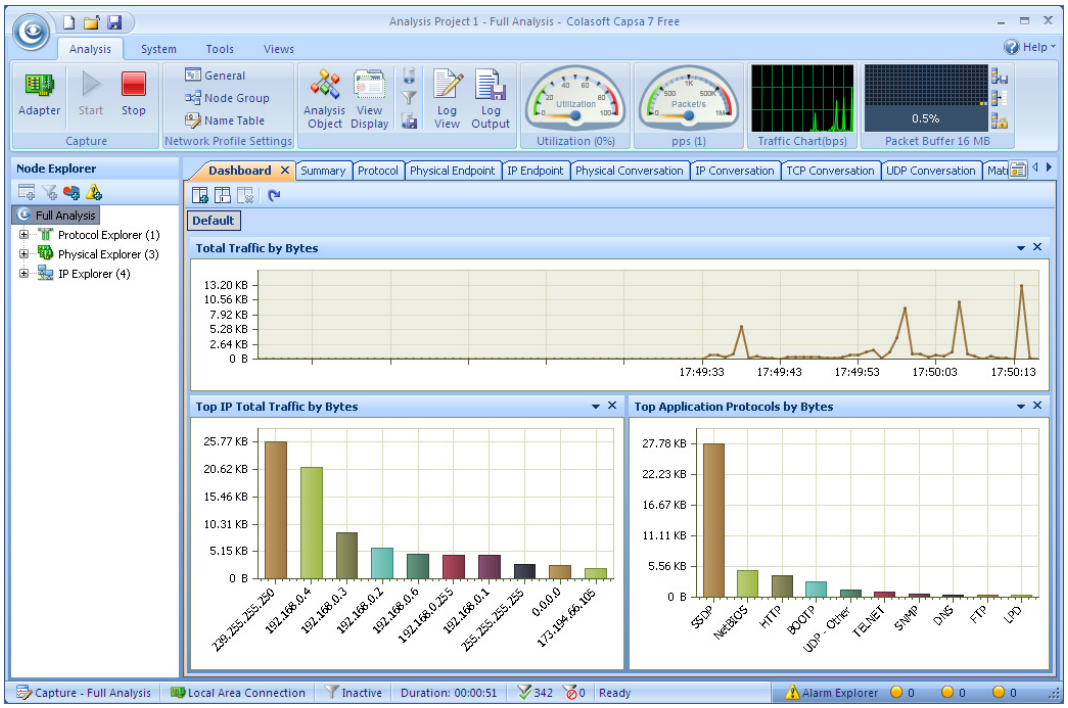


پس از اجرای این نرم‌افزار، کارت شبکه‌ی مورد نظر برای اتصال را از پنجره‌ی اصلی انتخاب و گزینه‌ی New Capture را برای ایجاد یک زبانه‌ی جدید کلیک می‌کنیم. در زبانه‌ی باز شده، گزینه‌ی Capture Setting را برای تنظیم فیلتر یا تنظیمات کارت شبکه و سایر تنظیمات عمومی کلیک کرده و سپس، گزینه‌ی Start را برای شروع ضبط بسته‌ها انتخاب می‌کنیم.

۴-۲-۲- ابزار Capsa Free

Capsa Free ابزاری برای تحلیل ترافیک شبکه است که به شما اجازه‌ی نظارت بر ترافیک شبکه، عیب‌یابی آن و تحلیل بسته‌ها را می‌دهد. از ویژگی‌های آن می‌توان به پشتیبانی از ۳۰۰ پروتکل شبکه (توانایی ایجاد و سفارشی‌سازی

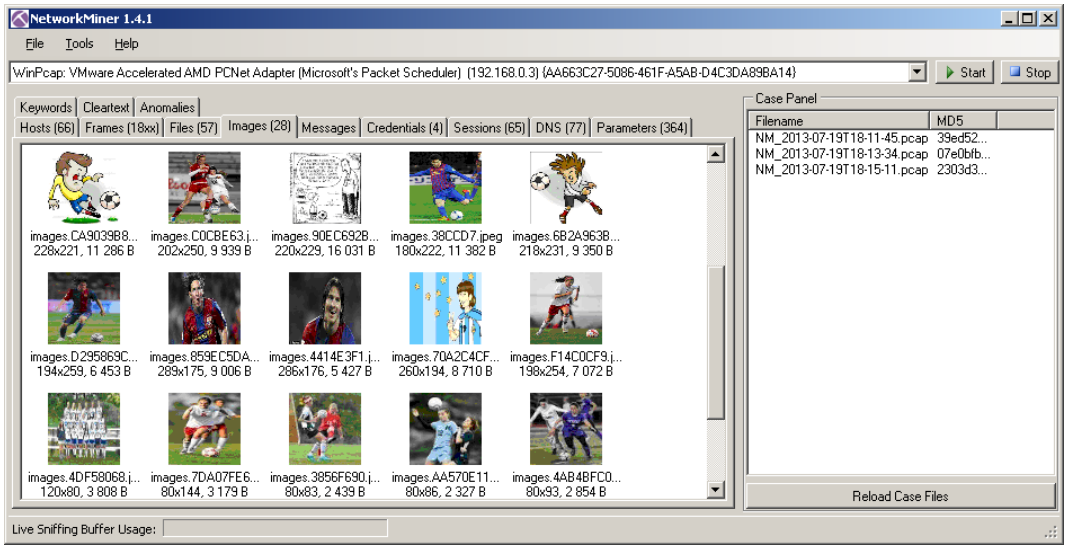
پروتکل‌ها را نیز دارد)، فیلترهایی برای MSN و Yahoo Messenger، نظارت و ذخیره‌سازی ایمیل‌ها و سفارشی‌سازی گزارش‌ها نام برد.



با اجرای Capsa، کارت شبکه‌ی مورد نظر که قصد اتصال به آن را دارید، انتخاب و گزینه‌ی Start را برای شروع عمل ضبط کلیک نمایید. از سربرگ‌های موجود در صفحه‌ی اصلی برای دیدن داشبورد، نمایش خلاصه‌ای از آمار ترافیک شبکه و ارتباطات TCP/IP استفاده کنید.

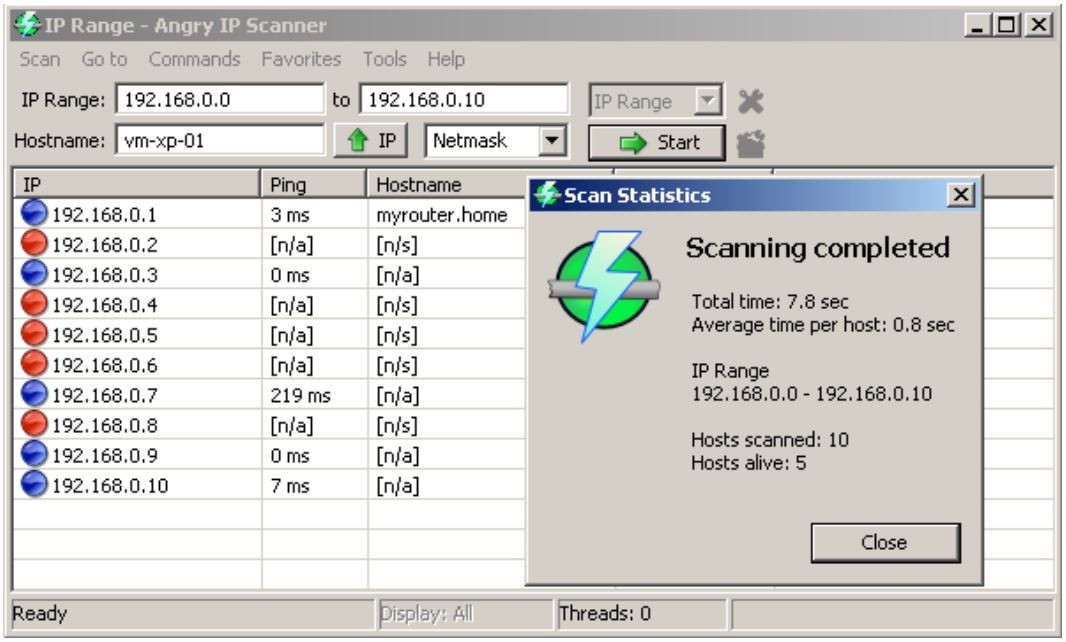
۴-۲-۳- ابزار NetworkMiner

NetworkMiner بسته‌های شبکه را ثبت کرده و داده‌های 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 فایل‌های از پیش ثبت شده (PCAP) نیز می‌دهد. NetworkMiner در دسته‌ای از ابزارهای جرم‌یابی شبکه قرار دارد که می‌تواند اطلاعاتی مانند نام میزبان، نام سیستم عامل و پورت‌های بازی که میزبان با آن‌ها ارتباط دارد را نمایش دهد.



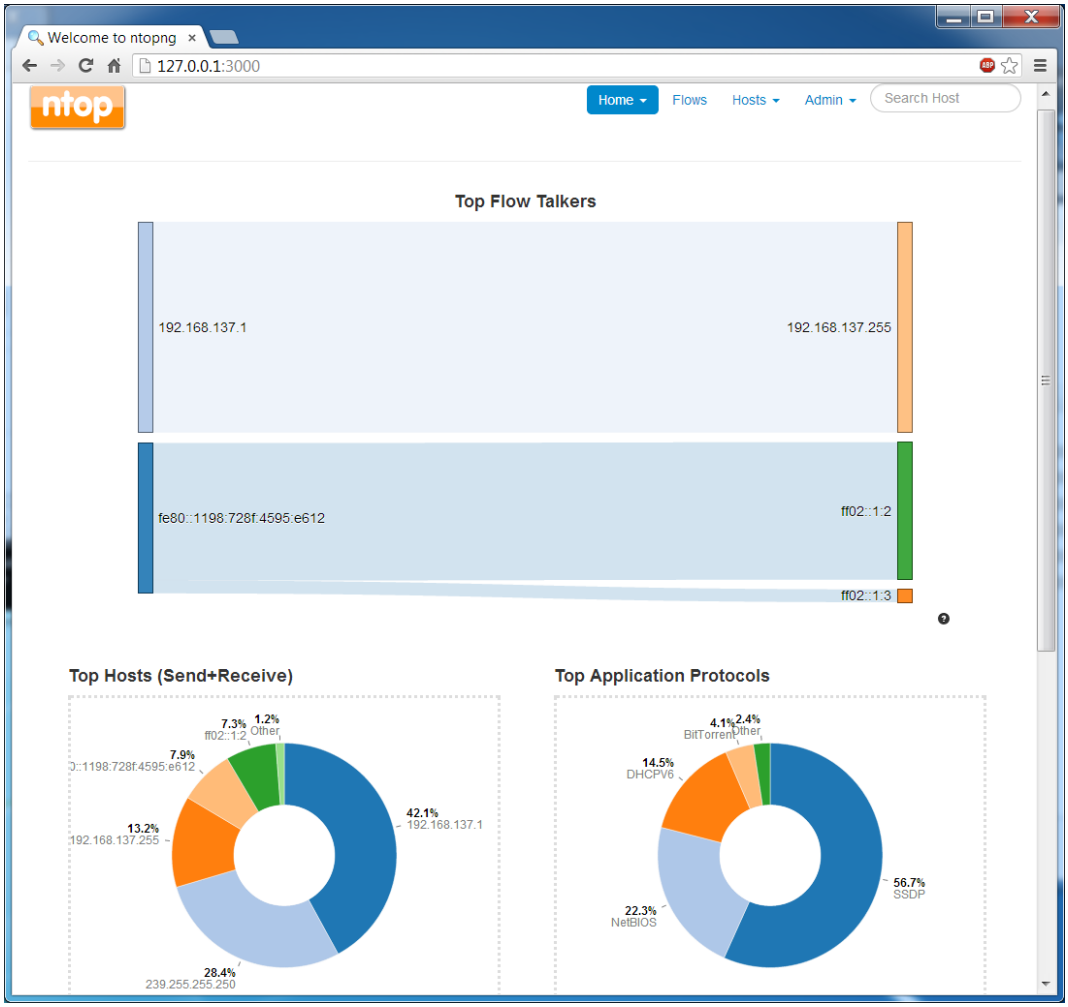
۴-۲-۴- ابزار Angry IP Scanner

Angry IP Scanner یک برنامه‌ی مستقل برای ساده‌سازی اسکن آدرس‌های IP و پورت‌ها می‌باشد. این برنامه محدوده‌ای از آدرس‌های IP را به دنبال یک میزبان فعال اسکن می‌کند و اطلاعاتی از آن شامل آدرس MAC، پورت‌ها، نام میزبان، زمان Ping و اطلاعات NetBios را بر می‌گرداند.



۴-۲-۵- ابزار ntopng

ntopng[1] آخرین نسخه از تحلیل‌گر محبوب شبکه به نام ntop است. ntopng در پس‌زمینه کار می‌کند و تمام اطلاعات ترافیک شبکه را جمع‌آوری و سپس، این اطلاعات را به همراه آمارهای به دست آمده از فعالیت شبکه را در یک رابط کاربری تحت وب نمایش می‌دهد. اگرچه نسخه‌ی اصلی آن برای سیستم‌های مبتنی بر Unix طراحی شد، اما هم‌اکنون نسخه‌ی تحت سیستم عامل ویندز آن نیز وجود دارد. این نسخه با قیمت اندک و نسخه‌ی پیش‌نمایش[2] آن که تنها توانایی جمع‌آوری ۲۰۰۰ بسته را دارد، در دسترس عموم قرار دارد. چنانچه از Unix استفاده می‌کنید، می‌توانید از نسخه‌ی کامل آن به صورت رایگان استفاده نمایید.

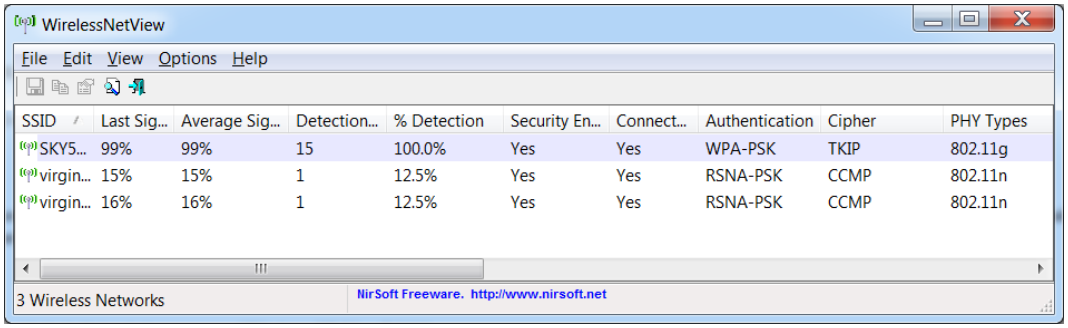


[1] در نام این ابزار، ng مخفف next generation است.

[2] Demo

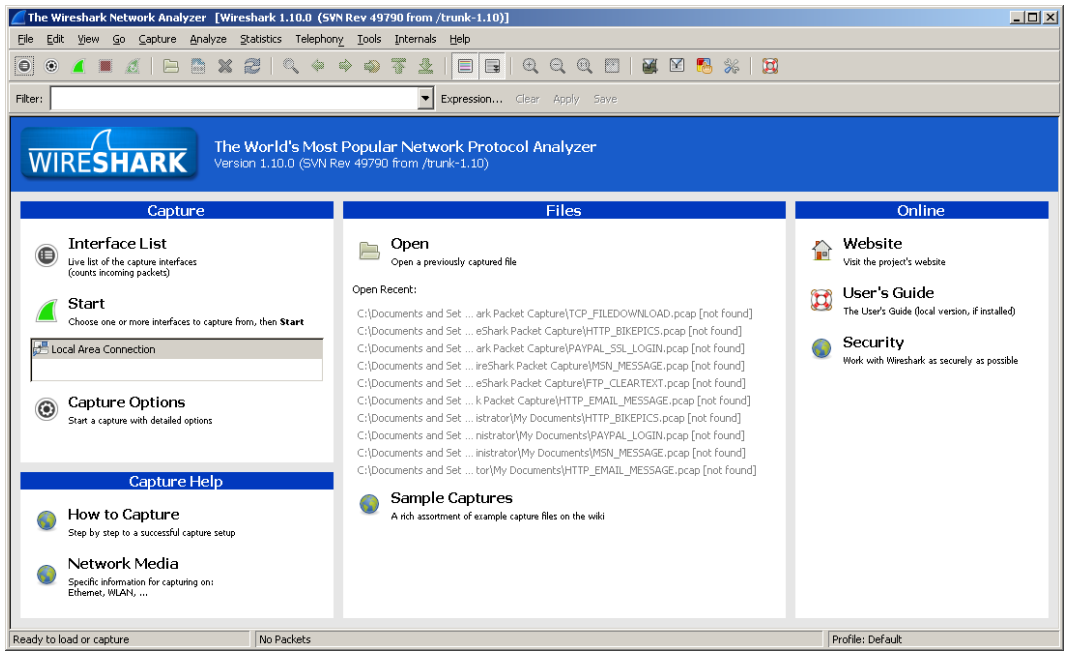
۴-۲-۶- ابزار WirelessNetView

WirelessNetView ابزار بسیار کوچکی است که به صورت یک بسته‌ی اجرایی مستقل موجود است. این ابزار، شبکه‌های بی‌سیم قابل دسترس را شناسایی کرده و اطلاعاتی از آن‌ها مانند SSID، کیفیت سیگنال، آدرس MAC، شماره‌ی کانال، الگوریتم رمزنگاری مورد استفاده و غیره را در اختیار می‌گذارد.



۴-۲-۷- ابزار WireShark

WireShark رایج‌ترین ابزار مورد استفاده برای ثبت و تحلیل پروتکل‌های شبکه است که قابلیت بررسی صدها پروتکل شبکه را دارا بوده و بر روی انواع سیستم‌های عامل قابل اجرا است.



اطلاعات جمع‌آوری شده توسط WireShark را می‌توانید برای بررسی‌های بعد به صورت فایل ذخیره کنید و یا از فیلترهای موجود در این ابزار برای به دست آوردن اطلاعات دسته‌بندی شده استفاده نمایید.

مراجع

[1] Frankel, David S., *Model Driven Architecture: Applying MDA to Enterprise Computing*, OMG Press, Wiley Publishing, 2003.

[2] Sannella, M. J., *Constraint Satisfaction and Debugging for Interactive User Interfaces*, Ph.D. Thesis, University of Washington, Seattle, WA, 1994.

[3] Zachman, John A., *"A Framework for Information Systems Architecture"*, IBM Systems Journal, Vol. 26, No. 3, 1987.

[4] Plamondon, R., Lorette, G., *"Automatic Signature Verification and Writer Identification - The State of the Art"*, Pattern Recognition, Vol. 22, pp. 107-131, 1989.

[5] Object Management Group. *Unified Modeling Language: Superstructure*, Version 2.0, ptc/03-07-06, July 2003, http://www.omg.org/cgi-bin/doc?ptc/2003-08-02.