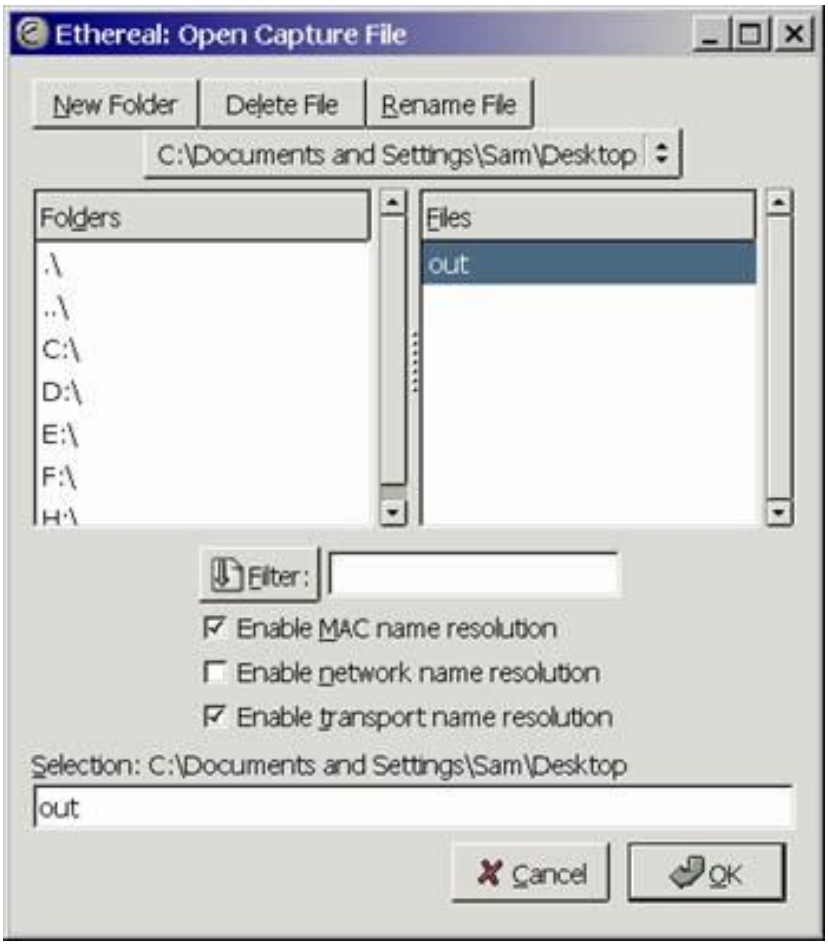
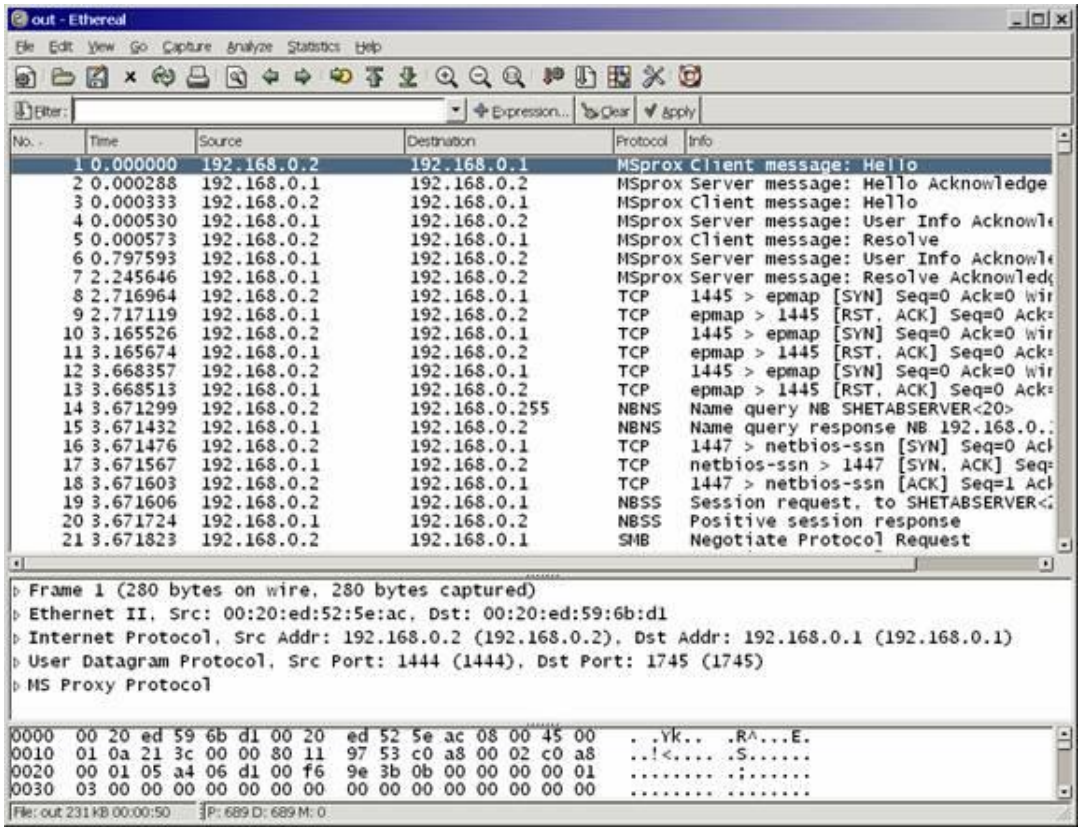
برای استفاده از فیلترهای نمایشی، می‌توان از خروجی‌های پیشین و عملیات Capture قبلی استفاده کرد. به این منظور یکی از پرونده‌های قبلی را باز می‌کنیم:

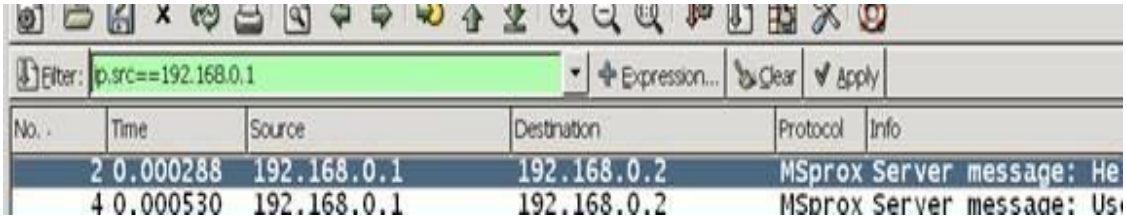


این پرونده به‌عنوان نمونه‌یی از عمل دریافت بسته‌ها تهیه شده است. پس از باز کردن این پرونده، بسته‌های موجود در آخرین عمل دریافت، در پنجره‌ی اصلی ظاهر خواهند شد:



طبیعی‌ست که برای دسته‌بندی بسته‌ها بر اساس یکی از پارامترهای زمان دریافت، آدرس مبدأ یا مقصد و نوع پروتکل می‌توان به کلیک کردن بر روی برچسب هریک از ستون‌ها، اطلاعات را بر حسب آن ستون مرتب‌کرد. عمل تعریف فیلتر و اعمال آن بر روی اطلاعات، متفاوت از این مرتب‌سازی است. به بیان دیگر، با استفاده از فیلتر می‌توان شروط پیچیده‌تری برای مشاهده‌ی بسته‌ها تعریف کرد.

اکنون می‌خواهیم با استفاده از تعریف فیلترها نمایش در این نرم‌افزار، بسته‌های مورد نظر خود را جدا کنیم. برای این‌کار می‌توان فیلتر را مستقیماً در قسمت Filter، پایین Toolbar اصلی، در پنجره‌ی اصلی تعریف کرد:

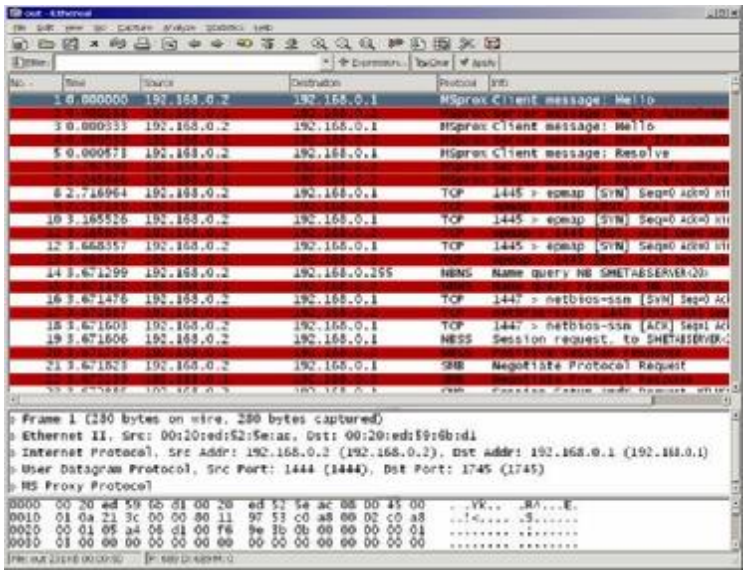


همان‌گونه که مشاهده می‌کنید، در این محل، برای تعریف فیلتری که تنها بسته‌هایی با مبدأ 192.168.0.1 را نمایش دهد از نوع دیگری از تعریف فیلتر استفاده می‌کنیم. به بیان دیگر، زبان تعریف فیلتر برای دو نوع Capture و نمایش (Analyze) با یکدیگر متفاوت است. با مراجعه به سایت این نرم‌افزار، می‌توانید با هر دو زبان آشنا شوید.

روش دیگر استفاده از فیلترهای نمایش استفاده از منوی Analyze و انتخاب Display Filters در این منو است. با این انتخاب پنجره‌ای مشابه پنجره‌ی Capture Filters نمایش داده می‌شود:

در مثال بالا، مجدداً فیلتری، از نوع نمایشی، با نام Simple تعریف کرده‌ایم که زبان تعریف آن همان زبان فیلترهای نمایش است. با فشار دکمه‌ی Apply، فیلتر مورد نظر اعمال می‌شود و شکل پنجره‌ی اصلی تنها بسته‌های با آدرس مبدأ 192.168.0.1 را نمایش می‌دهد. باید توجه داشت که بقیه‌ی بسته‌ها در این مرحله از میان نمی‌روند و استفاده از فیلترها تنها نمایش را به بازه‌ی مورد درخواست کاربر محدود می‌کند.

از دیگر قابلیت‌های مفید این نرم‌افزار، فیلترهای رنگی آن است. این فیلترها را می‌توان در منوی View با انتخاب Coloring Rules تعریف کرد. زبان و روش تعریف این فیلترها مشابه فیلترهای نمایش است. شکل زیر پنجره‌ی اصلی را پس از تعیین فیلتر رنگی ip.src=192.168.0.1 و تغییر رنگ بسته‌هایی که آدرس مبدأ آنها 192.168.0.1 است، نشان می‌دهد :



طبیعی است که می‌توان از چند فیلتر رنگی به‌طور هم‌زمان استفاده کرد.

با توجه به سه قسمت ارایه شده در باب معرفی این نرم‌افزار که حاکی از قابلیت‌ها متنوع آن است، Ethereal را می‌توان به جرأت قدرت‌مندترین نرم‌افزار از سری ابزارهای Sniffer به حساب آورد. لازم به ذکر است که این ابزار امکانات دیگری نیز دارد که با مراجعه به منوهای Analyze و Statistics می‌توانـــید از آن‌ها استفاده کنید.

Tools security

SuperScan

قسمت اول

یکی از اولین قدم ها برای تعیین میزان آسیب‌پذیری یک سیستم رایانه‌یی، استفاده از ابزارها و روش‌هایی است که به ما امکان می دهد خود به بررسی وضعیت امنیتی سیستم، از دید یک کاربر بیرونی، و در برخی شرایط از دید یک نفوذگر به شبکه و سیستم‌های رایانه‌یی، بپردازیم. به عبارت دیگر، چنانچه امکان بررسی وضعیت امنیتی سیستم مان، با چنین روش‌هایی وجود داشته باشد، چاره‌اندیشی برای مقابله با شرایط خطیر و برطرف نمودن ضعف‌های سیستم، آسان می‌شود.

در معرفی ابزارهای گوناگون در این بخش، جدا از معرفی ابزارهایی که به‌محافظت در برابر حملات احتمالی به سیستم‌مان به ما یاری می‌رسانند، تاکنون نرم‌افزارهایی را نیز معرفی کرده‌ایم که امکان بررسی وضعیت امنیتی سیستم مورد نظر را فراهم می‌کنند. در این دسته از نرم‌افزارها، پویش‌گرهای امنیتی، به عنوان راه‌کارهای جامعی که به کلیه‌ی ابعاد امنیتی یک سیستم می‌پردازند جای‌گاهی ویژه دارند. همان‌گونه که در مرورهای پیشین مشاهده کرده‌اید، هدف از استفاده از این پویش‌گرها، مجتمع‌سازی امکان بررسی امنیتی یک سیستم، بدون نیاز به استفاده از چند ابزار هم‌زمان است. در پویش‌گرهای امنیتی، وضعیت امنیتی سیستم از ابعاد مختلفی همچون پویش سیستم‌های موجود بر روی شبکه، تعیین سیستم‌های‌عامل موجود، وضعیت اصلاحیه‌های امنیتی، وضعیت درگاه‌های باز و غیره بررسی می‌گردد.

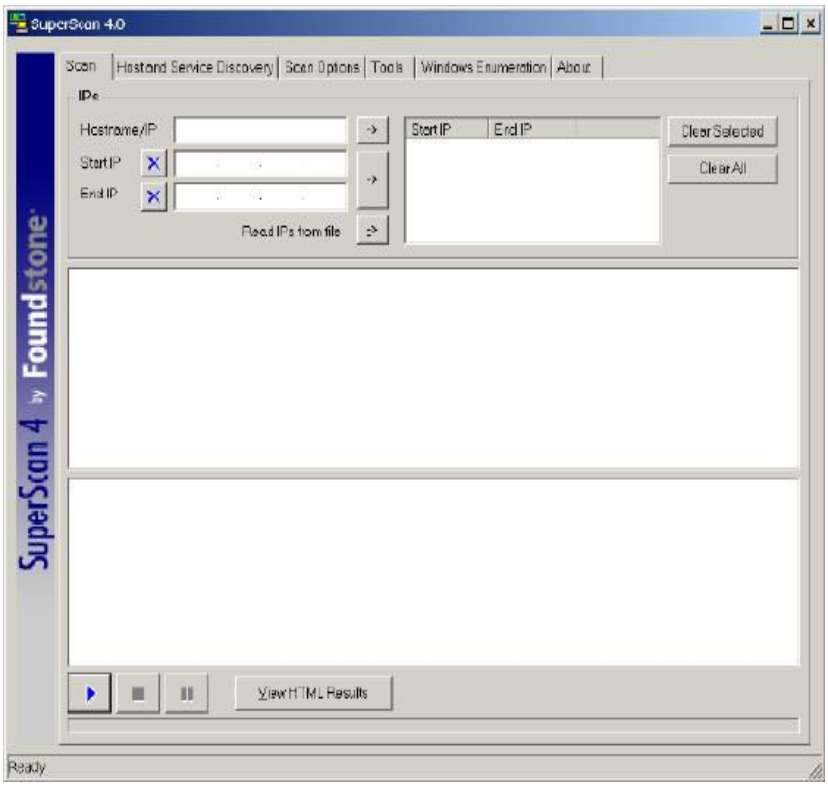
با وجود امکان استفاده از این دسته از پویش‌گرها امنیتی، در مواردی که تنها به پویش وضعیت امنیتی یک سیستم، از جنبه‌یی خاص، داریم، می‌توانیم تنها از دسته‌یی از نرم‌افزارها استفاده کنیم که بررسی امنیتی را به ابعادی خاص محدود می‌کنند. برای مثال یک پویش‌گر درگاه (که در این متن قصد معرفی یکی از متداول‌ترین نرم‌افزارهای این دسته ابزارها را داریم)، تنها به بررسی بازبودن درگاه‌های یک سیستم می‌پردازد.

پویش‌گرهای درگاه، به‌همراه پویش‌گرهای آدرس، دو دسته ابزاری هستند که اغلب توسط نفوذگران، برای بررسی اولیه‌ی وضعیت سیستم مورد نظر استفاده می‌گردند. از آن‌جایی که ارتباطات مبتنی بر پروتکل TCP/IP بر اساس شماره‌ی درگاه TCP/UDP مورد نظر انجام می‌گیرد، لذا هر درگاه عملاً نماینده‌ی نرم‌افزار خاصی است. برای مثال درگاه استاندارد Web Serverها درگاه شماره‌ی 80 است، لذا در صورتی که نفوذگر از باز بودن این درگاه مطلع شود، می‌تواند نوع Web Server را نیز مشخص کرده و با اطلاعاتی که در مورد ضعف‌های امنیتی آن دارد به حمله از طریق این درگاه مبادرت نماید. روند کار در مورد دیگر درگاه‌ها نیز مشابه است.

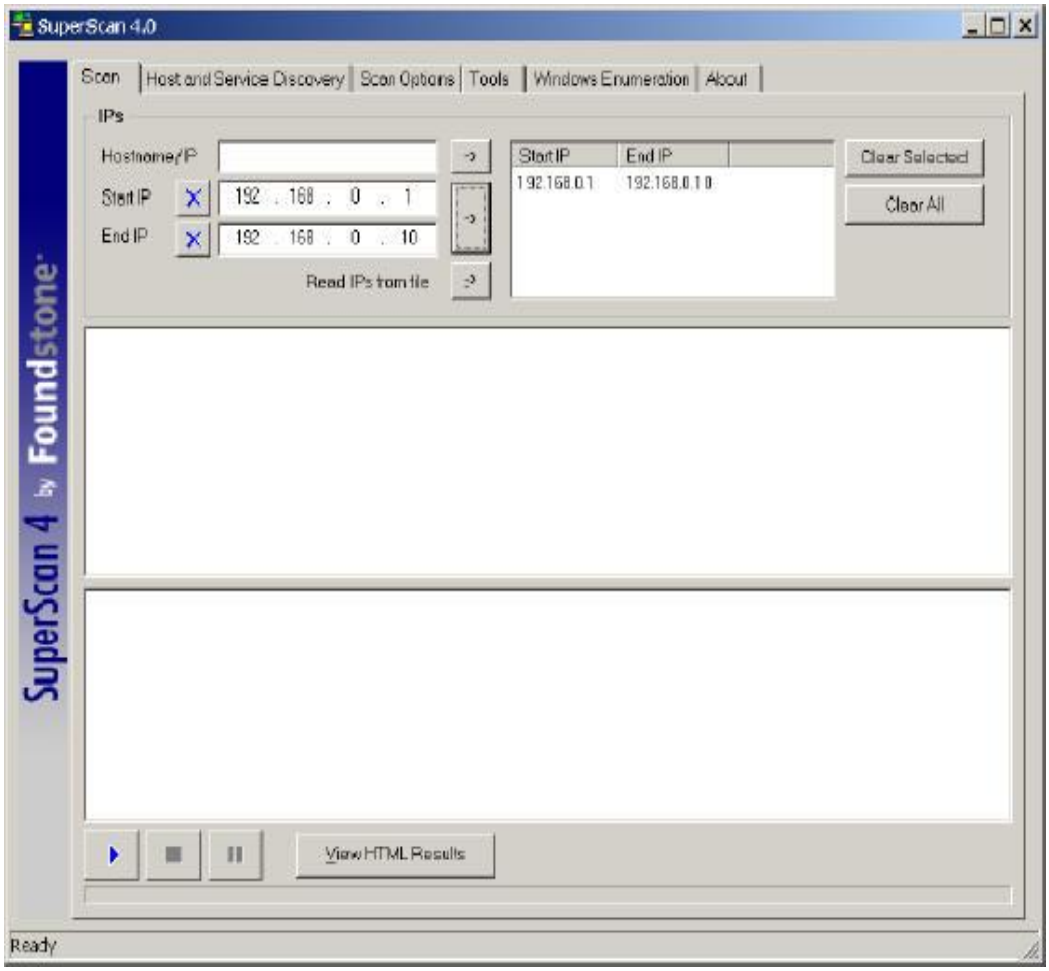
با توجه به اهمیتی که درگاه‌های باز روی سیستم در بالا رفتن خطر حملات دارند، یکی از قدم‌های اولیه برای تعیین میزان امنیت کنونی سیستم، اطلاع یافتن از درگاه‌های باز است. همان‌گونه که گفته شد، این نوع پویش قسمتی از وظایف پویش‌گرهای امنیت است و در صورت استفاده از آنها می‌توان برای اطلاع یافتن از وضعیت درگاه‌های باز، به گزارش‌های حاصل از پویش جزئی‌ی این نرم‌افزارهای رجوع کرد.

برای پویش درگاه‌های یک سیستم نرم‌افزارهای متعددی وجود دارند که نرم‌افزار SuperScan یکی از متداول‌ترین این ابزارهاست. این نرم‌افزار که محصول شرکت Foundstone است و امکان پویش آدرس‌های IP را نیز دارد،

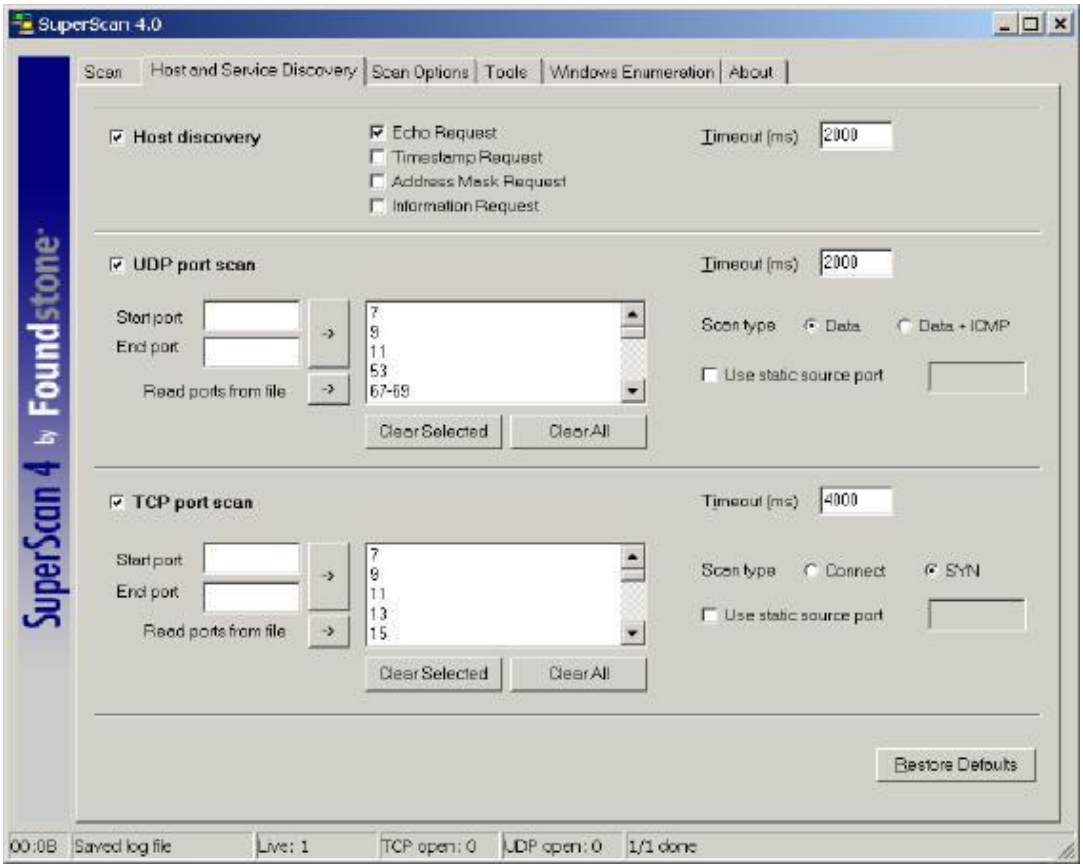
این نرم‌افزار که دارای حجم بسیار کمی است، تنها شامل یک فایل است و گزارش‌های خود را نیز در قالب HTML تولید می کند. شکل زیر صفحه‌ی اصلی این نرم‌افزار در ابتدای اجرا را نشان می‌دهد :



در قسمت اول، امکان ورود اسم یا آدرس IP یا بازه‌یی از آدرس‌های IP وجود دارد. در شکل زیر بازه‌یی از IPها برای عمل پویش تعیین شده‌اند:



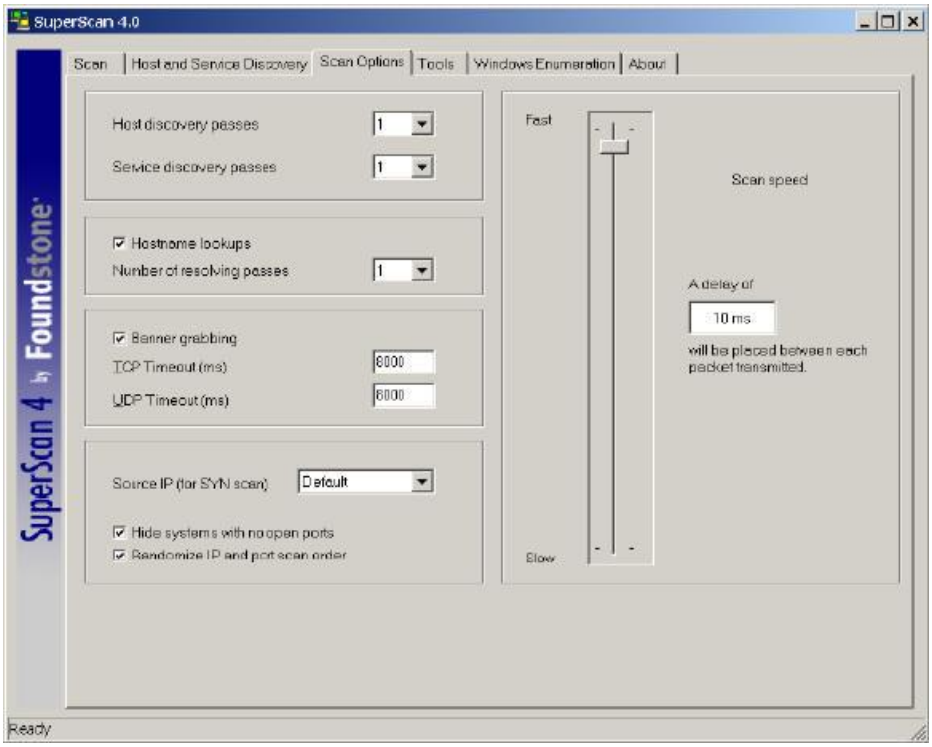
در قسمت دوم، امکان تعیین پارامتر برای تعیین نوع پویش وجود دارد. مقادیر پیش فرض در شکل زیر نمایش داده شده‌اند:



برای تعیین پارامترها، سه بخش مجزا وجود دارد که به عنوان سه وظیفه‌ی اصلی این ابزار است. در قسمت اول، امکان استفاده از این ابزار به عنوان یک پویش‌گر آدرس IP وجود دارد. در دو قسمت دیگر، پویش یا عدم پویش درگاه‌های پروتکل‌های TCP یا UDP و همچنین بازه‌ی درگاه‌های مورد نظر تعیین می‌گردد. بازه‌های تعیین شده به‌صورت پیش‌فرض، اختصاص به درگاه‌های متداول و مورد استفاده دارد. در صورت نیاز می‌توان به این بازه از درگاه‌ها، شماره‌های دیگری را نیز اضافه کرد. در قسمت درگاه‌های TCP/UDP، امکان تعیین درگاهی به عنوان درگاه مبدأ، به صورت ثابت، نیز وجود دارد.

در هریک از این سه بخش، زمانی که ابزار منتظر پاسخ از سوی سیستم مورد نظر می‌ماند، بر حسب میلی ثانیه، تعیین می‌شود. البته باید به‌خاطر داشت که این اعداد به‌معنای فاصله میان بسته‌های ارسالی نیست. این عدد در بخش دیگری قابل تنظیم است.

شکل زیر پنجره‌ی بعدی، یعنی Scan Options، برای تعیین پارامترهای دیگر این ابزار را نشان می‌دهد:



در این بخش امکان تعیین تعداد دفعاتی که پویش، چه برای آدرس و چه برای درگاه، انجام می‌گردد، وجود دارد. با تکرار پویش، نتایج دقت بیشتری می‌یابند، خصوصاً اگر در حال پویش بر روی شبکه‌یی با سرعت پایین هستیم.

پارامتر مهم دیگر در این میان امکان Banner Grabbing است که برای سرویس‌هایی که اصطلاحاً Banner نشان می‌دهند، همچون Web Serverها و FTP Server، کاربرد دارد. معمولاً با استفاده از Banner، می‌توان از نوع و سازنده‌ی Server مورد نظر آگاه شد.

در قسمت سمت راست، سرعت پویش تعیین می‌گردد. این سرعت که با تعیین فاصله‌ی میان بسته‌های تولیدی قابل تنظیم است، در صورتی که در حال پویش تعداد زیادی سیستم، بر روی شبکه‌یی گسترده با سرعتی قابل قبول هستیم، در کوتاه کردن زمان اجرای ابزار نقش به‌سزایی دارد.

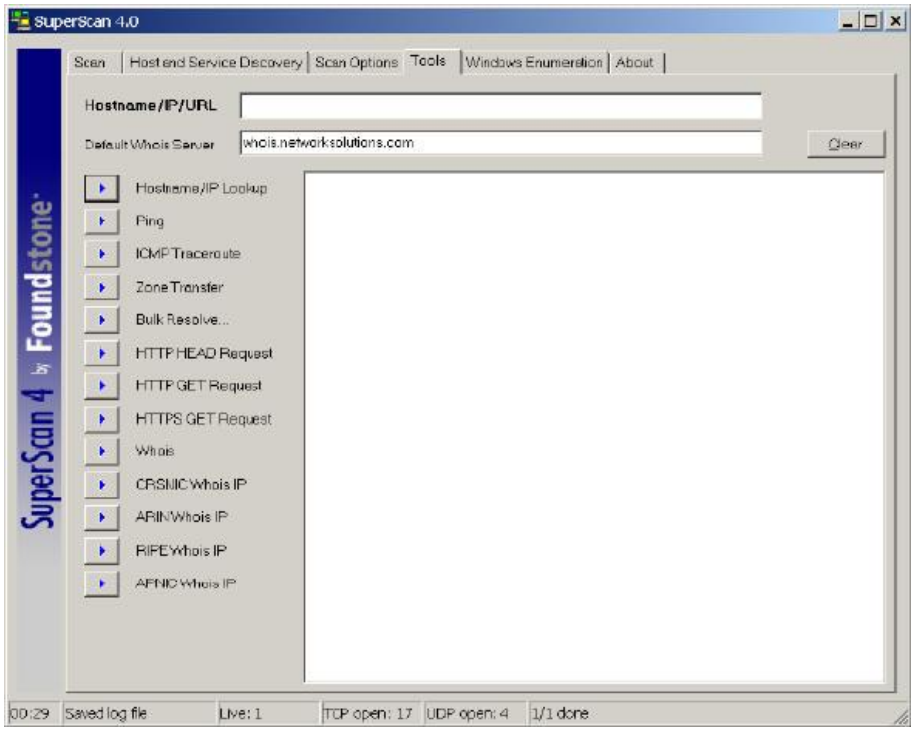
در قسمت بعدی از مرور این نرم‌افزار به امکانات دیگر آن خواهیم پرداخت.

SuperScan

قسمت دوم

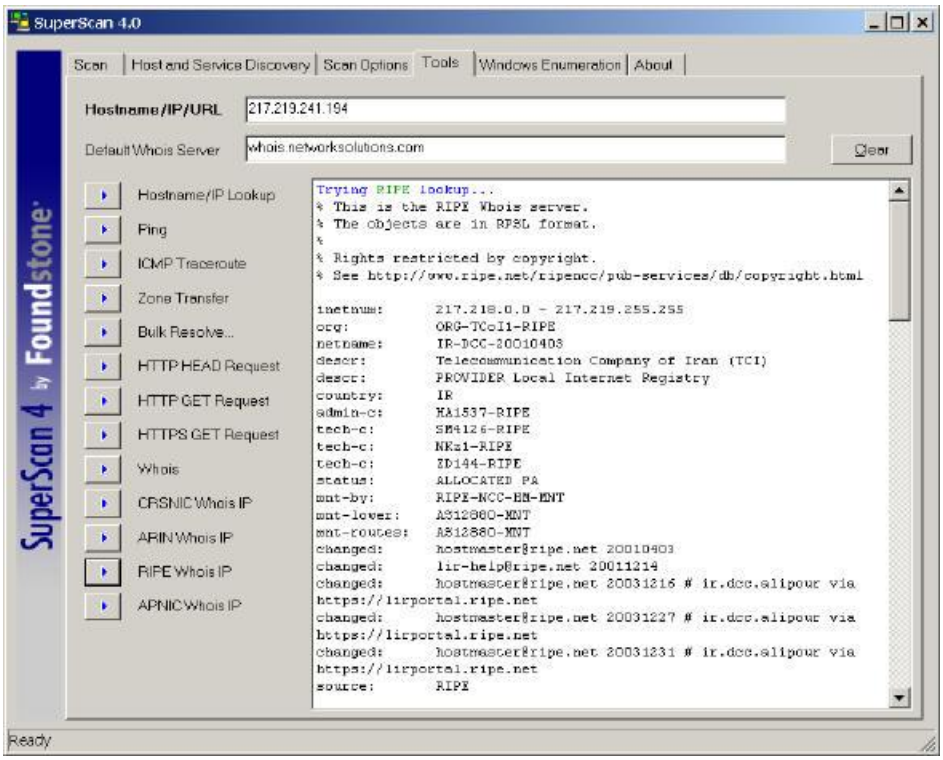
در ادامه‌ی قسمت پیشین، که در آن به معرفی متداول‌ترین دسته از نرم‌افزارهای بررسی امنیتی سیستم های رایانه‌یی، یعنی پویش‌گرهای آدرس و درگاه، پرداختیم، در این قسمت به ادامه‌ی معرفی امکانات ویژه‌ی این نرم‌افزار می‌پردازیم.

در پنجره‌ی زیر، بخش ابزارهای همراه با این نرم‌افزار را مشاهده می‌کنید:



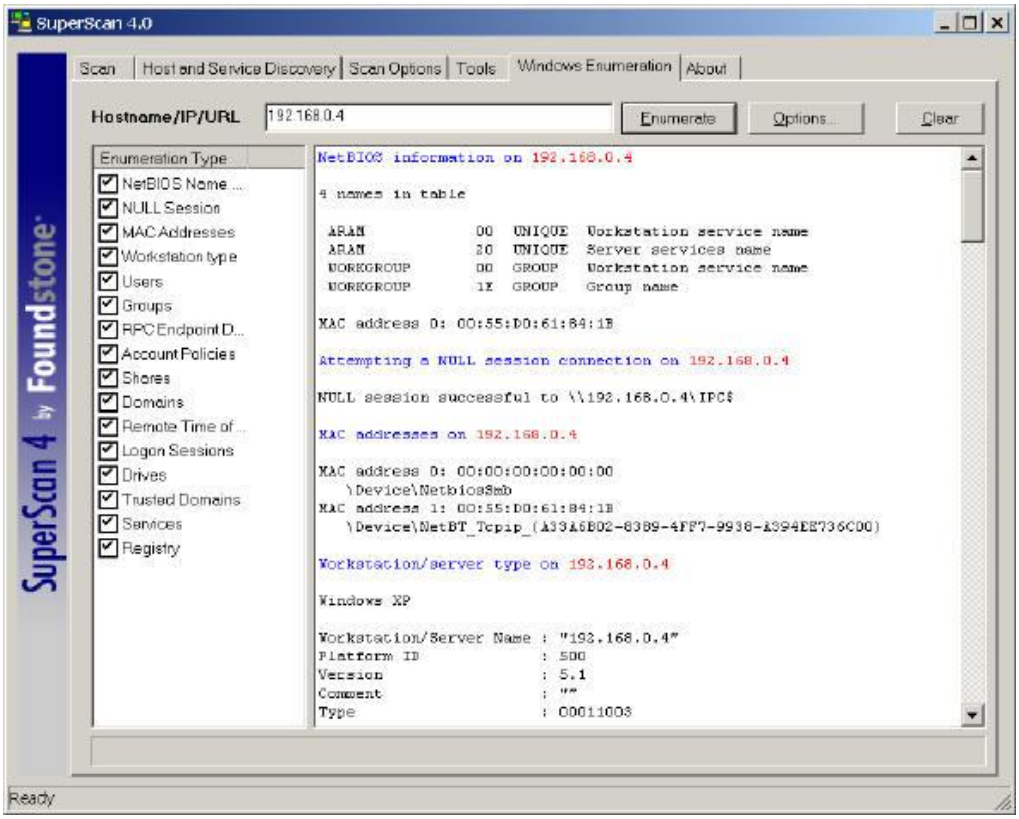
این نرم‌افزار، با در اختیار قراردادن ابزارهای کوچک و متداول، که در بررسی وضعیت شبکه‌ها استفاده می‌شود، عملاً امکانی مجتمع برای استفاده‌های متداول محسوب می‌گردد.

در این بخش امکان به دست آوردن آدرس IP از نام، Ping کردن یک ایستگاه، استفاده از امکانات HTTP، بررسی مالکیت یک دامنه‌ی اینترنتی و حتی بررسی مالکیت یک آدرس IP نیز وجود دارد. شکل زیر مثالی از اجرای RIPE Whois IP برای یکی از آدرس‌های متعلق به شرکت مخابرات ایران را نشان می دهد. خروجی این ابزار، اطلاعات جامعی در مورد آدرس IPی مورد نظر و مالک آن است:



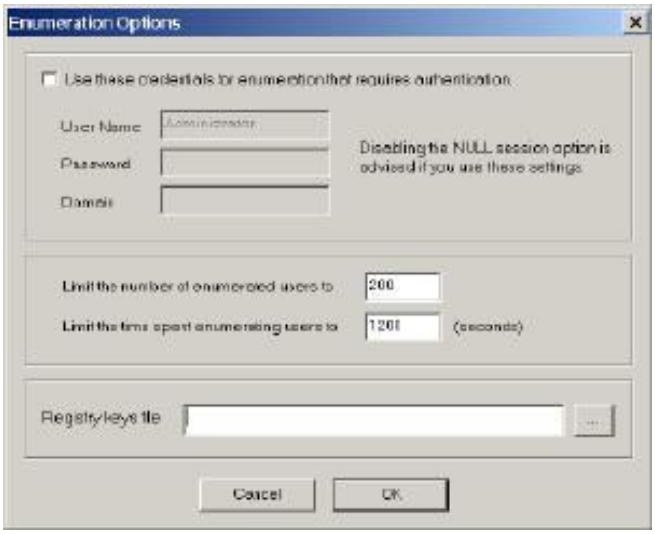
از دیگر امکانات ویژه‌ی این نرم‌افزار، امکان بررسی سیستم‌های مبتنی بر Windows است. بررسی‌هایی که در این راستا انجام می‌گیرد تمامی ابعاد معمول یک سیستم را در بر می‌گیرد، از جمله نام NetBIOS، گروه‌ها و کاربران آن سیستم، دامنه‌های محلی‌یی که سیستم به آن متصل است، منابع به اشتراک گذارده شده و دیگر ابعاد.

شکل زیر صفحه‌یی نمونه از اجرای آزمایشی این بررسی بر روی یک سیستم نمونه با آدرس IP محلی 192.168.0.4 را نشان می‌دهد:



در سمت چپ این پنجره، امکان تعیین بررسی‌های ویژه‌یی که مد نظر است نیز امکان‌پذیر است. برای مثال می توان تنها به بررسی نام NetBIOS و یا تنها گروه‌ها و کاربران پرداخت.

در همین قسمت، امکان تعیین پارامترهایی، مجزا از نوع عمل‌کرد ابزار وجود دارد. با انتخاب گزینه‌ی Options، می‌توان آن‌ها را تعیین کرد:



مهم‌ترین پارامتر قابل تعیین در این میان، تعیین نام کاربری است که برای بررسی یک سیستم مبتنی بر سیستم عامل خانواده‌ی Windows به‌کار می‌رود. به‌عبارت دیگر با تعیین کاربری که اختیارات کاملی دارد، مانند Administrator، می‌توان تمامی اطلاعات مورد نظر درباره‌ی سیستم راه دور را به‌دست آورد. نکته‌یی که در این میان اهمیت دارد این است که در اغلب موارد، بررسی انجام شده توسط کاربر Administrator یا کاربران دیگری که اختیار تام در سیستم مورد نظر دارند، هدف نیست. به‌بیان دیگر هدف اصلی از استفاده از این امکان ویژه، بررسی امکان دسترسی به اطلاعات سیستم توسط یک **کاربر نوعی بدون داشتن دسترسی‌های ویژه** است. در واقع وجود امکان دسترسی به اطلاعات حیاتی در مورد سیستم، برای کاربران متفرقه است که امکان وجود خطر حملات به سیستم را بالا می‌برد و نه امکان دسترسی برای کابران در سطوح مدیریتی.

امکان فوق را، با توجه به سبکی این نرم‌افزار از نظر حجمی، و ساده‌گی آن از نظر استفاده، می‌توان به‌نوعی یک امکان پویش امنیتی به‌حساب آورد. استفاده‌ی اغلب کاربران

خانه‌گی از سیستم‌های عامل سری Windows نیز به اهمیت این امکان ویژه افزوده و آن را بیش‌تر به عنوان یک پویش‌گر امنیتی ساده مطرح می‌کند.

WinDump

قسمت اول : Snifferها

این ابزارWinDump که نسخه‌ی تحت Windows نرم‌افزار قدیمی و مشهور tcpdump تحت سیستم‌های عامل خانواده‌ی Unix می‌باشد، عملاً یک تحلیل‌گر ترافیک شبکه است. از آن‌جاکه اغلب استفاده کننده‌گان سیستم‌های کامپیوتری خانه‌گی در کشورمان را کاربران سیستم‌های عامل خانواده‌یWindows تشکیل می‌دهند، معرفی WinDump را به بررسی tcpdump ترجیح داده‌ایم.

یک تحلیل‌گر ترافیک شبکه، که عموماً با نام Sniffer از آن یاد می‌گردد، وظیفه‌ی بررسی بسته‌های رد و بدل شده بر روی شبکه را برعهده دارد که نرم‌افزار Ethereal نمونه‌ی متداول و پرطرفداری از یک Sniffer است. از آن‌جاکه در معرفی نرم‌افزار پیشین بصورت اجمالی به این دسته از ابزارها پرداخته بودیم، در معرفی WinDump نیاز به ذکر مقدمات بیش‌تری از Snifferها داریم.

با استفاده از یک Sniffer، با تعیین یک رابط شبکه‌ی خاص، می‌توان به پایش و تحلیل بسته‌های اطلاعاتی رد و بدل شده بر روی شبکه‌یی که رابط شبکه‌ی مورد نظر به آن متصل است پرداخت. به عبارت دیگر یک Sniffer را می‌توان به یک سیستم پایش تشبیه کرد که تمامی اطلاعات منتقل شده بر روی بستر فیزیکی را بررسی و ذخیره می‌کند. در نهایت با به دست آوردن این اطلاعات دو عمل می‌توان بر روی محتوای بسته‌های بررسی شده انجام داد:

- **تحلیل کلی ترافیک شبکه**

این عمل توسط تحلیل‌گر انجام می‌گردد و از آن‌جاکه حجم اطلاعات رد و بدل شده بر روی شبکه بسیار زیاد است، تحلیل‌گر باید توانایی تمیز دادن اطلاعات مربوط به پروتکل‌های مختلف با مبدأ و مقصدهای مختلف را داشته باشد.

- فیلتر کردن بسته‌هایی با محتوایی خاص

با فیلترکردن بسته‌هایی خاص و نمایش اختصاصی آن‌ها توسط Sniffer، می‌توان تمیزدادن بسته‌های مربوط به یک پروتکل خاص، از/به مبدأ/مقصد خاص، با محتوایی از رشته‌یی تعیین شده و دیگر ویژه‌گی‌ها را به نرم‌افزار Sniffer سپرد. پس از به دست آوردن خروجی دل‌خواه تحلیل آن بسیار آسان‌تر است.

قابلیت پایش بسته‌های رد و بدل شده بر روی شبکه، قابلیتی مختص سخت‌افزار است. به عبارت دیگر رابط شبکه در حالتی خاص قرار می‌گیرد که تمامی بسته‌هایی که مقصد آدرس فیزیکی آن‌ها رابط مورد نظر نیست نیز مانند بسته‌های مربوط دریافت شده و محتوای آنها را می‌توان ذخیره کرد. در حالت عادی، سخت‌افزار و لایه‌ی Datalink بسته‌هایی که به رابط مورد نظر با آدرس فیزیکی خاص، ارتباطی ندارند را از روی شبکه بر نمی‌دارد.

با این وجود، از آن‌جاکه هدف از استفاده از Snifferها بررسی تمامی ترافیک شبکه، با استفاده از پایش تمامی بسته‌هایی که از مبدآهای مختلف به مقاصد دیگر ارسال می‌شوند می‌باشد، لذا پیش‌نیاز استفاده از این دسته از ابزارها اساساً وجود نسخه‌یی از تمامی ترافیک شبکه بر روی بستر متصل به رابط شبکه‌ی مورد نظر است.

این پیش‌نیاز، پیش‌نیازی سخت‌افزاری را به استفاده کننده از Sniffer تحمیل می‌کند، زیرا با استفاده از سوییچ‌ها، که در حال حاضر تقریباً در تمامی موارد جای Hubها را گرفته‌اند، ترافیکی که بر روی هریک از درگاه‌های سوییچ به سمت سیستم مورد نظر فرستاده می‌شود، تنها مختص آن سیستم است و ترافیک دیگر گره‌های شبکه بر روی آن قرار ندارد. لذا در شبکه‌یی که بر اساس سوییچ عمل می‌کند، عملاً امکان استفاده از Sniffer در شرایط معمول وجود ندارد.

با این‌وجود بسیاری از سوپیچ‌ها با هدف در اختیار گذاردن درگاهی خاص، امکان قرار دادن تمامی ترافیک شبکه بر روی یک کانال را فراهم می‌کنند و سیستمی که به این درگاه متصل باشد می‌تواند به پایش ترافیک شبکه بپردازد. امکان استفاده از این قبیل درگاه‌ها بر روی سوییچ‌ها، در صورت وجود، محدود بوده و تنها مختص مدیران شبکه می‌باشد. این امکان تنها برای جامه‌ی عمل پوشانیدن به یکی از اهدف استفاده از Snifferها، یعنی استفاده توسط مدیران شبکه برای تحلیل ترافیک فعال، در برخی از سوییچ‌ها وجود دارد.

در استفاده از این دسته از Snifferها دو کاربرد خاص مد نظر بوده است:

- استفاده توسط مدیران و تحلیل‌گران شبکه برای عیب‌یابی و رفع کاستی‌های شبکه
- استفاده توسط نفوذگران به شبکه‌ها و سیستم‌ها
- شناسایی تلاش‌ها برای نفوذ

هدف اول، عمل‌کردی است که در مورد آن صحبت شد. کاربرد بعدی، استفاده از قابلیت این دسته از نرم‌افزارها توسط نفوذگران به شبکه‌ها است. نفوذگران با پایش داده‌ها، به تلاش برای تحلیل داده‌های شبکه و به‌دست‌آوردن اطلاعاتی هرچه بیشتر در مورد شبکه