می‌پردازند. دسته‌ی مهمی از این اطلاعات کدهای کاربری و کلمات عبور نرم‌افزارهای مختلفی است که به‌صورت رمزنشده بر روی شبکه در حال انتقال هستند. یک نفوذگر، با تحلیل ترافیک، ابتدا به نوع نرم‌افزارهای فعال بر روی شبکه پی‌برده و سپس در پی شناخت بیش‌تر یک نرم‌افزار نمونه و تشخیص حفره‌های امنیتی موجود در آن، به فیلترکردن بسته‌های مختص آن نرم‌افزار پرداخته و سعی در گردآوری اطلاعات بیش‌تر در مورد آن می‌کند. با به دست آوردن اطلاعات مورد نظر، اقدامات بعدی برای حمله، توسط اطلاعات حیاتی به دست آمده، انجام می‌گیرد.

استفاده از سوییچ‌ها، علاوه بر بالابردن کارایی استفاده از سخت‌افزار و بستر شبکه، به بالابردن امنیت موجود نیز کمک شایانی کرده و احتمال پایش ترافیک توسط نفوذگران، بر روی سیستم‌های متفرقه‌ی موجود بر روی شبکه را پایین می‌آورد. **هرچند که باید به خاطر داشت که روش‌هایی نیز وجود دارد که می‌توان این امکان سوییچ‌ها را غیرفعال کرد و یا سوییچ را مجبور ساخت که کلیه‌ی ترافیک را به یک درگاه خاص بفرستد.** لذا استفاده از سوییچ تضمین قطعی جلوگیری از پایش ناخواسته‌ی ترافیک نیست.

هدف دیگری که می‌توان برای استفاده از Snifferها متصور بود امکان تشخیص تلاش‌های در حال انجام برای نفوذ است. تلاش‌هایی از قبیل حمله به آدرس یا درگاه خاص بر روی یک پروتکل خاص، و یا حمله به یک نرم‌افزار خاص، توسط یک تحلیل‌گر شبکه‌ی ماهر و با استفاده از یک Sniffer، قابل تشخیص است. با در نظر گرفتن این هدف، از Snifferها می‌توان بر روی یک سیستم منفرد، به منظور پایش ارتباطات انجام گرفته با سیستم، و تشخیص حملات احتمالی در حال انجام، استفاده کرد، هرچند که در این قبیل موارد استفاده از دیوارهای آتش، حتی انواع شخصی آن، کمک شایانی به کاربر می‌کنند.

با توجه به آن‌چه به‌صورت پراکنده درخلال متن گفته شد، راه‌های مقابله با Snifferها را می‌توان به سه دسته تقسیم نمود :

- استفاده از ابزارهای رمزنگاری داده‌ها
- استفاده از سوییچ در شبکه به جای Hub
- استفاده از ابزارهای ضد Sniff که امکان تشخیص رابط‌های شبکه‌یی که در حال Sniff قرار دارند را به وجود می‌آورد.

WinDump

قسمت دوم

در قسمت پیش، مقدمه‌یی درباره‌ی Snifferها، که ابزارهایی برای تحلیل ترافیک شبکه هستند، بیان شد. در آن بخش، پس از تعریف این دسته از نرم‌افزارها، فواید استفاده از این ابزارها، برای تحلیل ترافیک شبکه مورد بررسی قرار گرفت. در ادامه، همچنین به روش‌هایی که با استفاده از آن‌ها نفوذگران دست به حمله به سیستم‌ها و شبکه‌های رایانه‌یی می‌زنند پرداخته شد و در انتها برخی از روش‌های مقابله با این قبیل نفوذها را ذکر کردیم.

در قسمت دوم و پایانی از این بررسی، به نرم‌افزار WinDump، که نمونه‌یی مرسوم از این ابزارها است می‌پردازیم. این نرم‌افزار عملاً نسخه‌ی تحت سیستم‌های‌عامل سری Windows ابزار tcpdump است. tcpdump که نرم‌افزاری قدیمی و متداول تحت سیستم‌عامل خانواده‌ی Unix می‌باشد، جزو اولین و ساده‌ترین Snifferها است.

دریافت و نصب نرم‌افزار

برای دسترسی به این نرم‌افزار و دریافت آن می‌توانید به آدرس http://windump.polito.it مراجعه کنید. این نرم‌افزار از کتابخانه‌یی سازگار با libpcab استفاده می‌کند که نگارش تحت Windows آن به WinPcap موسوم است. این نرم‌افزار را می‌توانید از همان سایت دریافت کنید. پس از نصب آخرین نگارش WinPcap، نرم افزار WinDump عملیاتی می شود. نکته‌یی که باید به‌خاطر داشته باشید این است که برای آنکه این نرم‌افزار تمامی و یا اغلب بسته‌های در حال انتقال بر روی شبکه را شناسایی و دریافت کند، باید از آخرین نگارش آن استفاده کنید، هرچند که

این نرم‌افزار مدت‌هاست که به روز نشده، با این وجود اگر به‌طریقی نگارشی دیگر و قدیمی از این نرم‌افزار را به دست آوردید، برای کارایی بهتر، نسخه‌ی جدیدتر را دریافت کنید.

قابلیت‌های WinDump

محیط استفاده از این نرم‌افزار، محیطی ساده و متنی است. در واقع وجود این محیط به‌منظور سادگی بیشتر و تشابه هرچه بیش‌تر آن با نرم افزار tcpdump است. با وجود این سادگی، WinDump دارای قابلیت‌های متنوعی است.

پس از اجرای این نرم‌افزار، با تعیین رابط شبکه‌یی که WinDump می‌باید به‌دریافت بسته‌های رد و بدل شده بر روی شبکه‌ی مرتبط با رابط مورد نظر بپردازد، این نرم‌افزار، Header تمامی بسته‌های دریافت شده را بر روی صفحه‌ی نمایش داده و زمان و تاریخ هریک را نیز نشان می‌دهد.

شناسایی و تعیین پروتکل‌ها

WinDump، بسیاری از پروتکل‌ها را شناسایی می‌کند و در این صورت نام پروتکل مورد نظر را بر روی صفحه نشان می‌دهد. با این وجود این امکان وجود دارد که تنها پروتکلی خاص برای تحلیل و شناسایی مورد نظر قرار گیرد و WinDump تنها بسته‌های پروتکل تعیین شده را در گزارش نشان دهد.

از سوی دیگر، این نرم‌افزار امکان شناسایی بسته‌هایی با انواع خاص، مانند بسته‌هایی متعلق به VLANهای تعریف شده بر روی شبکه، یا بسته‌های متعلق به ارتباطات VPN را دارد. در مورد بسته‌های متعلق به VPN، امکان رمزگشایی آنها با تعیین الگوریتم رمزنگاری و تعیین کلید مربوطه نیز وجود دارد.

- تعیین مبدأ و مقصد خاص

در صورت نیاز، با استفاده از کلیدهایی، می‌توان بسته‌هایی را مشاهده کرد که از مبدأ(هایی) به مقصد(هایی) خاص در حال گذر هستند.

خروجی‌های مختلف

این نرم‌افزار، بر اساس پروتکل‌های مختلف خروجی‌های مختلفی را نشان می‌دهد. به‌عبارت دیگر، برای هر بسته، بر اساس اینکه متعلق به چه نوع پروتکلی است، نوع خروجی، یا خط گزارش مورد نظر، مستقل از زمان و تاریخ دریافت بسته، متفاوت است. هرچند که برای اکثر آنها، نام یا آدرس و شماره‌ی پورت مورد نظر بسته، نمایش داده می‌شود.

در صورت نیاز و به منظور بالاتر رفتن سرعت پردازش WinDump، می‌توان قابلیت استخراج اسامی سیستم‌ها در قالب مبدأ و مقصد را، حذف نمود و تنها به مشاهده‌ی آدرس اکتفا کرد. در این صورت، تأخیری که صرف به دست آوردن نام سیستم مبدأ یا مقصد می‌شود از بین می‌رود.

فیلترهای متنوع خروجی

یکی از قابلیت‌های خاص این نرم‌افزار، امکان استفاده از فیلترهای مختلف برای تعیین خروجی و بررسی بسته‌های ویژه است. برای تعیین نوع گزارش، می‌توان پارامترهای مختلفی را تعیین نمود که بر اساس آنها، WinDump گزارش بسته‌های خاصی را نمایش می‌دهد و بسته‌های دیگر را نادیده می گیرد.

نمونه‌یی از این فیلترها، فیلتر اندازه‌ی بسته و یا نوع بسته در قالب یک پروتکل واحد است. به عبارت دیگر، توسط این فیلترها، می‌توان بسته‌هایی با اندازه‌هایی خاص را مورد نظر قرار داد و یا برای مثال می‌توان بسته‌های خاصی از پروتکل TCP را بررسی کرد و دیگر بسته‌ها را نادیده گرفت.

برای تعیین فیلترها، علاوه بر عباراتی که به‌صورت پیش‌فرض در این نرم‌افزار قابل دسترسی هستند، عباراتی جدید را نیز با ترکیب عبارات ساده می‌توان به‌دست آورد. عبارات پایه، برای تعیین پارامترهای ابتدایی مانند مبدأ، مقصد، پورت، پروتکل و دیگر پارامترها هستند.

ذخیره‌ی گزارش

این نرم‌افزار قابلیت ذخیره‌ی گزارش مورد نظر به صورت یک پرونده را نیز دارد. پرونده به‌صورت خام و پردازش نشده ذخیره می‌شود و برای پردازش بر روی آن، می‌توان از همین نرم‌افزار، با تعیین از پارامتری خاص، استفاده نمود که در آن صورت عملاً گزارش اولیه تولید می‌شود.

با توجه به قابلیت‌هایی که در مورد این نرم‌افزار، به‌اختصار، مورد اشاره قرار گرفت، این ابزار را می‌توان ابزاری قوی برای کاربرانی که به ابزار متداول و قدیمی tcpdump عادت داشته‌اند دانست. با این وجود از آنجاکه روش کار با آن برای کاربران عادی، به دلیل نبود رابط کاربری گرافیکی مناسب، کمی خسته کننده است، می‌توان از Snifferهای دیگری همچون نرم‌افزار Ethereal استفاده کرد، که با استفاده از رابط کاربری آنها، تحلیل و تعیین روش کار به‌راحتی صورت گرفته، و خروجی تولید شده خوانایی بیش‌تری دارد.

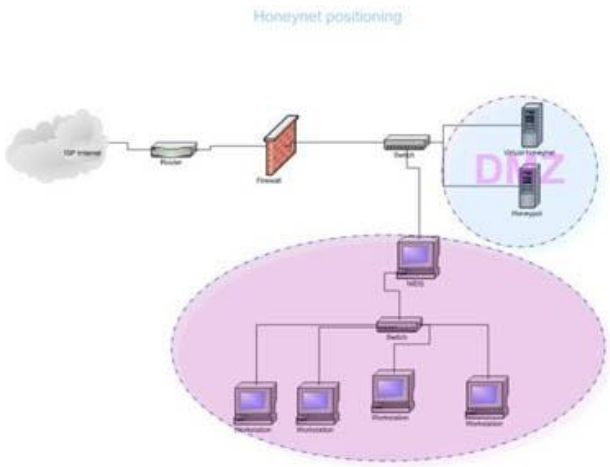
نکته‌یی که علاوه بر ذکر در بخش اول در این‌جا نیز مجدداً بر روی آن تأکید می‌کنیم این است که تقریباً در **تمامی موارد، Snifferها تنها در شرایطی کاربرد دارند که در شبکه‌ی مورد نظر از سوییچ استفاده نشده باشد یا در صورت استفاده از سوییچ، درگاهی خاص برای تحلیل تمامی ترافیک در حال پردازش توسط سوییچ بر روی درگاه‌های دیگر، قابل تعریف باشد.**

Honeypot قسمت اول

Honeypot ها یک تکنولوژی جدید می باشند که قابلیتهای فراوانی برای جامعه امنیتی دارند. البته مفهوم آن در ابتدا به صورتهای مختلفی تعریف شده بود به خصوص توسط Cliff Stoll در کتاب « The Cuckoos Egg » . از آنجا به بعد بود که Honeypot ها شروع به رشد کردند و به وسیله ابزارهای امنیتی قوی توسعه یافتند و رشد آنها تا به امروز ادامه داشته است. هدف این مقاله تعریف و شرح واقعی Honeypot می باشد و بیان منفعت ها و مضرات آنها و اینکه آنها در امنیت چه ارزشی برای ما دارند.

تعریف

قدم اول در فهم اینکه Honeypot چه می باشند بیان تعریفی جامع از آن است. تعریف Honeypot می تواند سخت تر از آنچه که به نظر می رسد باشد. Honeypot ها از این جهت که هیچ مشکلی را برای ما حل نمی کنند شبیه دیواره های آتش و یا سیستمهای تشخیص دخول سرزده نمی باشند. در عوض آنها یک ابزار قابل انعطافی می باشند که به شکلهای مختلفی قابل استفاده هستند.آنها هر کاری را می توانند انجام دهند از کشف حملات پنهانی در شبکه های IPv6 تا ضبط آخرین کارت اعتباری جعل شده! و همین انعطاف پذیریها باعث شده است که Honeypot ها ابزارهایی قوی به نظر برسند و از جهتی نیز غیر قابل تعریف و غیر قابل فهم!!



Honeypot ۱

یک Honeypot یک منبع سیستم اطلاعاتی می باشد که با استفاده از ارزش کاذب خود اطلاعاتی از فعالیتهای بی مجوز و نا مشروع جمع آوری می کند.

البته این یک تعریف کلی می باشد که تمامی گونه های مختلف Honeypot ها را در نظر گرفته است. ما در ادامه مثالهای مختلفی برای Honeypot ها و ارزش امنیتی آنها خواهیم آورد. همه آنها در تعریفی که ما در بالا آورده ایم می گنجند ، ارزش دروغین آنها برای اشخاص بدی که با آنها در تماسند. به صورت کلی تمامی Honeypot ها به همین صورت کار می کنند. آنها یک منبعی از فعالیتها بدون مجوز می باشند. به صورت تئوری یک Honeypot نباید هیچ ترافیکی از شبکه ما را اشغال کند زیرا آنها هیچ فعالیت قانونی ندارند. این بدان معنی است که تراکنش های با یک Honeypot تقریبا تراکنش های بی مجوز و یا فعالیتهای بد اندیشانه می باشد. یعنی هر ارتباط با یک Honeypot می تواند یک دزدی ، حمله و یا یک تصفیه حساب می باشد. حال آنکه مفهوم آن ساده به نظر می رسد (و همین طور هم است) و همین سادگی باعث این هم موارد استفاده شگفت انگیز از Honeypot ها شده است

فواید Honeypot ها

Honeypot مفهوم بسیار ساده ای دارد ولی دارای توانایی های قدرتمندی می باشد.

۱. داده های کوچک دارای ارزش فراوان: Honeypot ها یک حجم کوچکی ار داده ها را جمع آوری می کنند. به جای اینکه ما در یک روز چندین گیگابایت اطلاعات را در فایلهای ثبت رویدادها ذخیره کنیم توسط Honeypot فقط در حد چندین مگابایت باید ذخیره کنیم. به جای تولید ۱۰۰۰۰ زنگ خطر در یک روز آنها فقط ۱ زنگ خطر را تولید می کنند. یادتان باشد که Honeypot ها فقط فعالیتهای ناجور را ثبت می کنند و هر ارتباطی با Honeypot می تواند یک فعالیت بدون مجوز و یا بداندیشانه باشد. و به همین دلیل می باشد که اطلاعات هر چند کوچک Honeypot ها دارای ارزش زیادی می باشد زیرا که آنها توسط افراد بد ذات تولید شده و توسط Honeypot ضبط شده است. این بدان معنا می باشد که تجزیه و تحلیل اطلاعات یک Honeypot آسانتر (و ارزانتر) از اطلاعات ثبت شده به صورت کلی می باشد.

۲. ابزار و تاکتیکی جدید : Honeypot برای این طراحی شده اند که هر چیزی که به سمت آنها جذب می شود را ذخیره کنند. با ابزارها و تاکتیکهای جدیدی که قبلا دیده نشده اند.

۳. کمترین احتیاجات: Honeypot ها به کمترین احتیاجات نیاز دارند زیرا که آنها فقط فعالیتهای ناجور را به ثبت می رسانند. بنابراین با یک پنتیوم قدیمی و با ۱۲۸ مگابایت RAM و یک شبکه با رنج B به راحتی می توان آن را پیاده سازی کرد.

٤. رمز کردن یا IPv6 : بر خلاف برخی تکنولوژیهای امنیتی (مانند IDS ها) Honeypot خیلی خوب با محیطهای رمز شده و یا IPv6 کار می کنند. این مساله

مهم نیست که یک فرد ناجور چگونه در یک Honeypot گرفتار می شود زیرا Honeypot ها خود می توانند آنها را شناخته و فعالیتهای آنان را ثبت کنند.

مضرات Honeypot ها

شبیه تمامی تکنولوژیها ، Honeypot ها نیز دارای نقاط ضعفی می باشند. این بدان علت می باشد که Honeypot ها جایگزین تکنولوژی دیگری نمی شوند بلکه در کنار تکنولوژیهای دیگر کار می کنند.

۱- محدودیت دید : Honeypot ها فقط فعایتهایی را می توانند پیگیری و ثبت کنند که به صورت مستقیم با آنها در ارتباط باشند. Honeypot حملاتی که بر علیه سیستمهای دیگر در حال انجام است را نمی توانند ثبت کنند به جز اینکه نفوذگر و یا آن تهدید فعل و انفعالی را با Honeypot داشته باشد.

۲- ریسک : همه تکنولوژیهای امنیتی دارای ریسک می باشند. دیوارهای آتش ریسک نفوذ و یا رخنه کردن در آن را دارند. رمزنگاری ریسک شکستن رمز را دارد، IDS ها ممکن است نتوانند یک حمله را تشخیص دهند. Honeypot ها مجزای از اینها نیستند. آنها نیز دارای ریسک می باشند. به خصوص اینکه Honeypot ها ممکن است که ریسک به دست گرفتن کنترل سیستم توسط یک فرد هکر و صدمه زدن به سیستمهای دیگر را داشته باشند. البته این ریسکها برای انواع مختلف Honeypot ها فرق می کند و بسته به اینکه چه نوعی از Honeypot را استفاده می کنید نوع و اندازه ریسک شما نیز متفاوت می باشد.ممکن است استفاده از یک نوع آن، ریسکی کمتر از IDS ها داشته باشد و استفاده از نوعی دیگر ریسک بسیار زیادی را در پی داشته باشد.ما در ادامه مشخص خواهیم کرد که چه نوعی از Honeypot ها دارای چه سطحی از ریسک می باشند. چگونگی و شیوه به کار بردن Honeypot ها می باشد که ارزش و فواید و مضرات آنها را مشخص می کند. در ادامه بیشتر روی آن بحث خواهد شد.

Honeypot قسمت دوم

در قسمت اول، تعریفی از Honeypot ها ارائه دادیم و فواید و مضرات آنها را بیان کردیم. در این قسمت درباره انواع آنها بحث خواهیم کرد

انوع Honeypot ها

Honeypot ها در اندازه و شکلهای مختلفی هستند و همین امر باعث شده است که فهم آنها کمی مشکل شود. برای اینکه بتوان بهتر آنها را فهمید همه انواع مختلف آنها را در دو زیر مجموعه آورده ایم:

۱- Honeypot های کم واکنش

۲- Honeypot های پرواکنش

این تقسیم بندی به ما کمک می کند که چگونگی رفتار آنها را بهتر درک کنیم. و بتوانیم به راحتی نقاط ضعف و قدرت آنها و توانایی ها یشان را روشن تر کنیم. واکنش در اصل نوع ارتباطی که یک نفوذگر با Honeypot دارد را مشخص می کند.

Honeypot های کم واکنش دارای ارتباط و فعالیتی محدود می باشند.آنها معمولا با سرویسها و سیستم های عامل را شبیه سازی شده کار می کنند. سطح فعالیت یک نفوذگر با سطحی از برنامه های شبیه سازی شده محدود شده است. به عنوان مثال یک سرویس FTP شبیه سازی شده که به پورت ۲۱ گوش می کند ممکن است فقط یک صفحه login و یا حداکثر تعدادی از دستورات FTP را شبیه سازی کرده باشد . یکی از فواید این دسته از Honeypot های کم واکنش سادگی آنها می باشد.

نگهداری Honeypot های کم واکنش بسیار راحت و آسان است و خیلی راحت می توان آنها را گسترش داد و ریسک بسیار کمی دارند. آنها بیشتر درگیر این هستند که

چه نرم افزارهایی باید روی چه سیستم عاملی نصب شود و همچنین می خواهید چه سرویسهایی را برای آن شبیه سازی و دیده بانی (Monitor) کنید.

همین رهیافت خودکار و ساده آنها است که توسعه آن را برای بسیاری از شرکت ها راحت می کند. البته لازم به ذکر است که همین سرویسهای شبـــیه سازی شده باعث می شود که فعالیت های فرد نفوذگر محدود شود و همـــین امر باعث کاهش ریسک می گردد. به این معنی که نفوذگر نمی تواند هیچگاه به سیستم عامل دسترسی پیدا کند و به وسیله آن به سیستم های دیگر آسیب برساند.

یکی از اصلی ترین مضرات Honeypot های کم واکنش این است که آنها فقط اطلاعات محدودی را می توانند ثبت کنند و آنها طراحی می شوند که فقط اطلاعاتی راجع به حملات شناخته شده را به ثبت برسانند.همچنین شناختن یک Honeypot کم واکنش برای یک نفوذگر بسیار راحت می باشد. نگران این نباشید که شبیه سازی شما چه اندازه خوب بوده است زیرا که نفوذگران حرفه ای به سرعت یک Honeypot کم واکنش را از یک سیستم واقعی تشخیص می دهند. از Honeypot های کم واکنش می توان Spector , Honeyd و KFSensor را نام برد.

Honeypot های پر واکنش متفاتند. آنها معمولا از راه حل های پیچیده تری استفاده می کنند زیرا که آنها از سیستم عاملها و سرویسهای واقعی استفاده می کنند. هیچ چیزی شبیه سازی شده نیست و ما یک سیستم واقعی را در اختیار نفوذگر می گذاریم.

اگر شما می خواهید که یک Honeypot لینوکس سرور FTP داشته باشید شما باید یک لینوکس واقعی به همراه یک سرویس FTP نصب کنید. فایده این نوع Honeypot دو چیز است. شما می توانید یک حجم زیادی از اطلاعات را به دست آورید. با دادن یک سیستم واقعی به فرد نفوذگر شما می توانید تمامی رفتار او از rootkit های جدید گرفته تا یک نشست IRC را زیر نظر بگیرید.

دومین فایده Honeypot های پرواکنش این است که دیگر جای هیچ فرضیه ای روی رفتار نفوذگر باقی نمی گذارد و یک محیط باز به او می دهد و تمامی فعالیتهای او را زیر نظر می گیرد. همین امر باعث می شود که Honeypot های پرواکنش رفتارهایی از فرد نفوذگر را به ما نشان دهند که ما انتظار نداشته ایم و یا نمی توانسته ایم حدس بزنیم!!

بهترین جا برای استفاده از این نوع Honeypot ها زمانی است که قصد داریم دستورات رمز شده یک در پشتی را روی یک شبکه غیر استاندارد IP به دست بیاریم. به هر حال همین امور است که ریسک اینگونه Honeypot ها را افزایش می دهد زیرا که نفوذگر یک سیستم عامل واقعی را در اختیار دارد و ممکن است به سیستم های اصلی شبکه صدمه بزند. به طور کلی یک Honeypot پرواکنش می تواند علاوه بر کارهای یک Honeypot کم واکنش کارهای خیلی بیشتری را انجام دهد.

برای فهم بهتر اینکه Honeypot کم واکنش و پرواکنش چگونه کار می کنند بهتر است دو مثال واقعی در این زمینه بیاوریم. با Honeypot های کم واکنش شروع می کنیم.

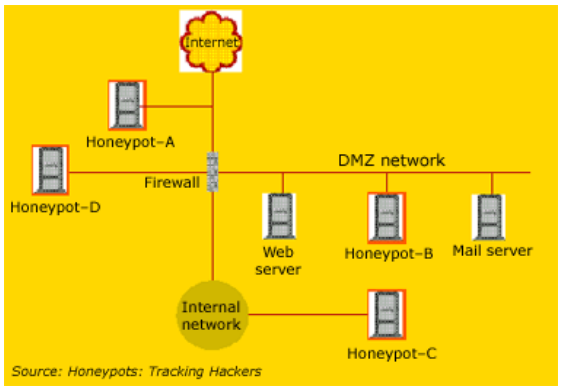


Figure 1. Honeypots can be deployed from a variety of locations. This diagram shows four different possible locations. The optimum location for deployment depends on an array of factors, such as the type of information the organization is interested in gathering, and the level of risk that organization can tolerate to obtain the maximum amount of data.

Honeyd : یک Honeypot کم واکنش

Honeyd یک Honeypot کم واکنش است که توسط Provos Niels ساخته شده است. Honeyd به صورت کد باز می باشد و برای مجموعه سیستم عاملهای یونیکس ساخته شده است.(فکر کنم روی ویندوز هم برده شده است). Honeyd بر اساس زیر نظر گرفتن IP های غیر قابل استفاده بنا شده است. هر چیزی که قصد داشته باشد با یک IP غیر قابل استفاده با شبکه ارتباط برقرار کند ارتباطش را با شبکه اصلی قطع کرده و با نفوذگر ارتباط برقرار می کند و خودش را جای قربانی جا می زند.

به صورت پیش فرض Honeyd تمامی پورتها TCP و یا UDP را زیر نظر گرفته و تمامی درخواستهای آنها را ثبت می کند. همچنین برای زیر نظر گرفتن یک پورت خاص شما می توانید سرویس شبیه سازی شده مورد نظر را پیکربندی کنید مانند شبیه سازی یک سرور FTP که روی پروتکل TCP پورت ۲۱ کار می کند.وقتی که نفوذگر با یک سرویس شبیه سازی شده ارتباط برقرار می کند تمامی فعالیتهای او را با سرویسهای شبیه سازی شده دیگر ثبت کرده و زیر نظر می گیرد. مثلا در سرویس FTP شبیه سازی شده ما می توانیم نام کاربری و کلمه های رمزی که نفوذگر برای شکستن FTP سرور استفاده می کند و یا دستوراتی که صادر می کند را به دست آوریم و شاید حتی پی ببریم که او به دنبال چه چیزی می گردد و هویت او چیست!

همه اینها به سطحی از شبیه سازی بر می گردد که Honeypot در اختیار ما گذاشته است. بیشتر سرویسهای شبیه سازی شده به یک صورت کار می کنند. آنها منتظر نوع خاصی از رفتارهای هستند و طبق راههایی که قبلا تعیین کرده اند به این رفتارهای واکنش نشان می دهند.

اگر حمله A این را انجام داد از این طریق واکنش نشان بده و اگر حمله B این کار را کرد از این راه واکنش نشان بده!

محدودیت این برنامه ها در این است که اگر نفوذگر دستوراتی را وارد کند که هیچ پاسخی برای آنها شبیه سازی نشده باشد. بنابراین آنها نمی دانند که چه پاسخی را باید برای نفوذگر ارسال کنند. بیشتر Honeypot های کم واکنش - مانند Honeyd - یک پیغام خطا نشان می دهند. شما می توانید از کد برنامه Honeyd کل دستوراتی که برای FTP شبیه سازی کرده است را مشاهده کنید.

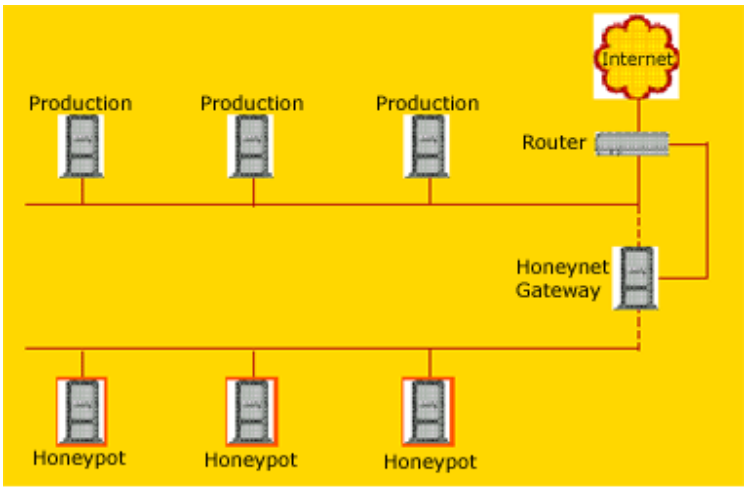


Figure 2. In this Honeynet (a research honeypot used to gather information), the Honeynet Gateway is a Layer 2 bridge that isolates the Honeynet from the rest of the production network. The bridge controls inbound and outbound traffic. Systems are placed in the Honeynet as intended targets for attackers to break into and interact with.

Honeynet ها : یک Honeypot پر واکنش

Honeynet یک مثال بدیهی برای Honeypot های پرواکنش می باشد. Honeynet ها یک محصول نمی باشند. آنها یک راه حل نرم افزاری که بتوان روی یک کامپیوتر نصب شوند نمی باشد. Honeynet ها یک معماری می باشند. یک شبکه بی عیب از کامپیوترهایی که طراحی شده اند برای حملاتی که روی آنها انجام می گیرد. طبق این نظریه ما باید یک معماری داشته باشیم که یک کنترل بالایی را روی شبکه ایجاد کند تا تمامی ارتباطات با شبکه را بتوان کنترل کرد و زیر نظر گرفت.

درون این شبکه ما چندین قربانی خیالی در نظر می گیریم البته با کامپیوترهایی که برنامه های واقعی را اجرا می کنند. فرد هکر این سیستم ها را پیدا کرده و به آنها حمله می کند و در آنها نفوذ می کند اما طبق ابتکار و راهکارهای ما ! یعنی همه چیز در کنترل ما می باشد. البته وقتی آنها این کارها را انجام می دهند نمی دانند که در یک Honeynet گرفتار شده اند. تمامی فعالیت های فرد نفوذگر از نشست های رمز شده SSH گرفته تا ایمیل ها و فایلهایی که در سیستم ها قرار می دهند همه و همه بدون آنکه آنها متوجه شوند زیر نظر گرفته و ثبت می شود. در همان زمان نیز Honeynet تمامی کارهای نفوذگر را کنترل می کند. Honeynet ها این کارها را توسط دروازه ای به نام Honeywall انجام می دهند. این دروازه به تمامی ترافیک ورودی اجازه می دهد که به سمت سیستم های قربانی ما هدایت شوند ولی ترافیک خروجی باید از سیستم های مجهز به IDS عبور کند. این کار به نفوذگر این امکان را می دهد که بتواند ارتباط قابل انعطاف تری با سیستم های قربانی داشته باشد اما در کنار آن اجازه داده نمی شود که نفوذگر با استفاده از این سیستم ها به سیستم های اصلی صدمه وارد کند.

Keylogger ابزاری برای جاسوسی

Keylogger ابزاری است که دنباله کلیدهایی که کاربر بر روی صفحه‌کلید کامپیوتر می‌فشارد، را ثبت می‌کند. این ابزار که به صورت‌های سخت‌افزاری و نرم‌افزاری تولید شده و در دسترس است در موارد متنوع و با کاربردهای مختلف به کار می‌رود. نمونه‌های مختلف Keylogger مقدار کمی از منابع سیستم شامل حافظه و پردازنده را مورد استفاده قرار می‌دهند. علاوه بر این در Task manager و لیست فرایندهای سیستم هم ظاهر نمی‌شوند، بنابراین تشخیص آنها بر روی دستگاه به سادگی امکان‌پذیر نیست.

علی رغم اهمیت زیادی که این ابزار در از بین رفتن حریم شخصی افراد و سرقت اطلاعات آنها دارد، توجه زیادی به این ابزار و تهدیدات ناشی از آن نمی‌شود. شاید دلیل این امرشهرت بیشتر ویروس‌ها، اسب‌های تروا و کرم‌ها و شناخت بیشتر نسبت به آنهاست. با توجه به سادگی انتشار این ابزار و تهدیدات ناشی از آن در این مقاله به معرفی keylogger و روش‌های مقابله با آن پرداخته است.

قابلیت‌های Keylogger ها

قابلیت Keylogger ها در این است که هر کلیدی که فشرده شود را ذخیره نموده، لیستی از حروف تایپ شده بر روی کامپیوتر را تولید می‌کنند. این لیست سپس در اختیار فردی که برنامه را بر روی دستگاه نصب کرده قرار می‌گیرد. بعضی از Keylogger ها این امکان را دارند که گزارش حروف تایپ شده را به کامپیوتری دیگر بر روی شبکه ارسال کنند. امکان ارسال اطلاعات ذخیره شده از طریق e-mail هم وجود دارد.

علاوه بر ذخیره حروف تایپ شده، بعضی از Keylogger ها اطلاعات خاصی را به صورت جدای از سایرین ثبت و گزارش آنها را تولید می‌کنند. لیست URLهایی که توسط کاربر دستگاه مشاهده شده و یا پیام‌هایی که در جریان Chat بین کاربر و دیگران رد و بدل می‌شود، جزء این گروه از اطلاعات می‌باشند.

قابلیت جالبی که تعدادی از Keylogger ها دارند گرفتن عکس از صفحه کامپیوتر در فواصل زمانی قابل تنظیم است. به این ترتیب مشخص می‌شود که چه برنامه‌هایی بر روی کامپیوتر نصب و در حال اجرا می‌باشند، چه فایل‌هایی بر روی DeskTop دستگاه قرار دارد و چه فعالیت‌هایی بر روی دستگاه انجام می‌شود.

انواع Keylogger ها

شرکت‌های مختلف تولید کننده Keylogger محصولات خود را به دو صورت سخت‌افزاری و نرم‌افزاری ارائه می‌نمایند. نرم‌افزارهای Keylogger به صورت بسته‌های نرم‌افزاری توسط شرکت‌های مختلفی توسعه داده شده، با قابلیت‌های مختلف به صورت‌های تجاری و یا مجانی عرضه می‌گردند. با یک جستجوی ساده بر روی کلمه KeyLogger در یکی از موتورهای جستجو نمونه‌های زیادی از این ابزار یافته می‌شود که بعضی از آنها به صورت مجانی قابل دریافت می‌باشد. نکته‌ای که در همه نرم‌افزارهای Keylogger وجود دارد این است که هیچ یک از آنها در Task Manager و لیست فرایندهای دستگاه ظاهر نمی‌شوند. علاوه بر این فایلی که نرم‌افزار برای ثبت اطلاعات از آن بهره می‌گیرد نیز مخفی بوده و به سادگی قابل تشخیص نیست.

برای استفاده از قابلیت‌های keylogger باید یک نمونه از نرم‌افزار بر روی دستگاه مورد نظر نصب شود. این کار با داشتن مجوزهای مدیر سیستم امکان‌پذیر است. در این صورت حتی از راه دور هم می‌توان برنامه را نصب نمود. انتقال Keylogger از طریق e-mail هم ممکن است. در این روش نرم‌افزار به همراه با یک فایل پیوست برای قربانی ارسال می‌گردد. باز کردن نامه و گرفتن پیوست آن منجر به نصب و فعال شدن keylogger بر روی دستگاه می‌شود.

نمونه‌های سخت‌افزاری این ابزار که بین صفحه‌کلید و درگاه کامپیوتر وصل می‌شوند معمولا مشابه کابل اتصال می‌باشند. با توجه به اینکه اتصال این ابزار از پشت دستگاه انجام می‌شود لذا در معرض دید نبوده و احتمال اینکه کاربر به سرعت وجود آن را کشف کند پایین است. علاوه بر این نمونه‌هایی از Keylogger ها داخل خود صفحه کلید قرار می‌گیرند و امکان شناسایی شدن آن به سادگی وجود ندارد.

نمونه‌ای از Keylogger سخت‌افزاری

کاربردهای Keylogger

پس از آشنایی با مشخصات و قابلیت‌های Keylogger اولین چیزی که به ذهن هر کسی می‌رسد استفاده از آن برای یافتن کلمات عبور دیگران می‌باشد. با استفاده از این ابزار امکان دزدیدن شناسه‌های کاربری، کلمات عبور، شماره کارت اعتباری و ... بوجود

می‌آید. از جمله مواردی که Keylogger ها در کاربردهای منفی مورد استفاده قرار گرفته‌اند می‌توان به دو مورد زیر اشاره نمود:

در فوریه ۲۰۰۳ دیوید بودرو که دانشجوی دانشگاه بوستون بود اقدام به نصب Keylogger بر روی بیش از ۱۰۰ دستگاه کامپیوتر دانشگاه نمود. او با استفاده از اطلاعاتی که به این ترتیب در مورد اساتید، دانشجویان و کارکنان دانشگاه به دست آورد، توانست بیش از ۲۰۰۰ دلار به دست آورد. مورد دیگر مربوط به جولای ۲۰۰۳ است که در آن جوجو جیانگ اعتراف نمود بر روی کامپیوترهای بیست فروشگاه در نیویورک Keylogger نصب نموده و به مدت دو سال شناسه‌های کاربری و کلمات عبور کاربران را از این طریق سرقت می‌کرده است.

در کنار این کاربردها که همگی منفی بوده و به نوعی سوء استفاده از قابلیت‌های یک ابزار محسوب می‌شوند کاربردهای دیگری نیز برای این ابزار وجود دارد. بسیاری از والدین همواره نگران نحوه استفاده فرزندان خود از اینترنت هستند. با توجه به وجود انواع سایت‌ها و مراکز اطلاع رسانی، این والدین دوست دارند که کنترل بیشتری بر استفاده از اینترنت داشته باشند. حداقل خواسته آنها این است که بدانند فرزندانشان چه سایت‌هایی را مشاهده می‌نمایند و یا با چه کسانی چت می‌کنند. در چنین مواردی استفاده از این ابزار می‌تواند کمکی باشد برای والدینی که نگران سلامت روانی فرزندان خود بوده و نسبت به تربیت آنها دغدغه‌های خاص خود را دارند.

Anti- Keylogger

این نرم‌افزارها با هدف شناسایی و ردیابی Keylogger ها تولید می‌شوند. با توجه به اینکه Keylogger ها روش‌های مختلفی برای کار و مخفی کردن خود دارند شناسایی آنها به سادگی امکان پذیر نیست. نمونه‌هایی از این نرم‌افزارها از طریق جستجو در

اینترنت قابل دریافت می‌باشند. ولی واقعیتی که در رابطه با همه این نرم‌افزارها وجود دارد عدم کارآیی آنها در مواجه با Keylogger های متنوع است.

تولیدکنندگان Keylogger، عموما ابزارهایی هم برای ردیابی Keyloggerهای خود به مشتریان عرضه می‌کنند. این ابزارها جامع نیستند و با توجه به اینکه روش‌های مختلفی برای ثبت کلیدهای فشرده شده وجود دارد، نمی‌توانند همه Keylogger ها را شناسایی نمایند.

روش‌های مقابله

متاسفانه ردیابی Keylogger ها بر روی دستگاه بسیار دشوار بوده و anti Keylogger ها هم کارایی مطلوبی ندارند. تنها راهی که برای مقابله با این ابزارها و جلوگیری از دزدی اطلاعات و نقض حریم شخصی می‌توان پیشنهاد داد بهره گرفتن از روش‌های پیش‌گیرانه است. موارد زیر به کاربران کامپیوترهای متصل به شبکه و مدیران سیستم توصیه می‌شود:

۱. کاربران عادی کامپیوتر باید با اختیارات عادی به کامپیوتر وصل شده و مجوز نصب برنامه نداشته باشند.

۲. تعداد اعضای گروه مدیران سیستم باید محدود بوده و سیاست‌های دقیقی بر فرایند انتخاب و محافظت از کلمات عبور حاکم باشد.

۳. هیچ‌گاه نباید با شناسه کاربری مدیر سیستم به اینترنت (و حتی شبکه محلی) وصل شد. ممکن است در همین زمان هکرها به سیستم نفوذ کرده و با استفاده از اختیارات مدیران سیستم اقدام به نصب نرم‌افزار keylogger بر روی دستگاه نمایند.

٤. پورت صفحه‌کلید کامپیوتر باید هر چند وقت یکبار مورد بازرسی قرار گیرد و سخت‌افزارهای مشکوک بررسی شوند.

است. لذا باید نکات امنیتی e-mailها از طریق keyloggerیکی از روش‌های انتقال لازم رعایت شده، از باز کردن نامه‌های مشکوک اجتناب شود.

آشنایی با PGP

با استفاده از PGP (Pretty Good Privacy) شما می‌توانید محرمانگی پیغامها و فایلهایتان را حفظ کنید بطوریکه فقط دریافت‌کنندگان مورد نظر شما بتوانند آنها را بخوانند. بعلاوه می‌توانید پیامها و فایلهایتان را امضای دیجیتال کنید تا دریافت‌کنندگان از تعلق آنها به شما مطمئن شوید. یک پیام امضاءشده، عدم تغییر محتویات آن را نیز تایید می‌کند. البته PGP تنها نرم‌افزار ارسال و دریافت ایمیلهای امن نیست اما کاربرد آن در این زمینه نسبتا زیاد است.

PGP براساس رمزنگاری کلید عمومی عمل می‌کند که در آن از یک جفت کلید برای برقراری ارتباط امن استفاده می‌شود. برای ارسال ایمیل خصوصی به یک نفر، از کپی کلید عمومی آن شخص برای رمزنگاری اطلاعات استفاده می‌کنید و به این ترتیب تنها آن فرد می‌تواند با استفاده از کلید خصوصی خود ایمیل را رمزگشایی کند. بالعکس، چنانچه شخصی بخواهد برای شما ایمیل امن ارسال کند، از کلید عمومی شما برای رمز کردن متن نامه استفاده می‌کند و تنها شمایید که می‌توانید آن متن را با استفاده از کلید خصوصی خود رمزگشایی کنید. بنابراین شما دیگران را از کلید عمومی خودتان مطلع می‌کنید اما از کلید خصوصی خودتان، خیر!!!

همچنین از کلید خصوصی خود برای امضای ایمیلی که قصد ارسال آنرا دارید استفاده می‌کنید. دریافت‌کنندگان می‌توانند از کلید عمومی شما برای تعیین اینکه آیا واقعا خود شما آنرا ارسال کرده‌اید و آیا متن نامه در طول ارسال تغییر نکرده است، استفاده کنند. شما هم برای تایید امضای دیگران از کلید عمومی آنها برای رمزگشایی متن دریافت‌شده استفاده می‌کنید.

در ادامه به نحوه کار با نرم‌افزار PGP اشاره می‌شود،

۱- PGP را روی کامپیوتر خود نصب کنید:

با مراجعه به راهنمای نصب PGP که معمولا همراه این نرم‌افزار است با نحوه نصب آن آشنا خواهید شد. در صورت نبود این راهنما، خودتان دست بکار شوید. چندان مشکل نیست.

۲- یک جفت کلید خصوصی و عمومی ایجاد کنید:

قبل از اینکه بتوانید استفاده از PGP را آغاز کنید، نیاز به تولید یک جفت کلید دارید. می‌توانید اینکار را در طول نصب PGP انجام دهید یا زمان دیگری که این نرم‌افزار را اجرا می‌کنید. شما به جفت کلید برای موارد زیر نیاز دارید:

- رمزنگاری اطلاعات
- رمزگشایی اطلاعاتی که با کلید شما رمز شده‌اند.
- امضاء کردن اطلاعات

۳- مبادله کلیدهای عمومی با دیگران:

بعد از اینکه جفت‌کلید را ایجاد کردید، می‌توانید مکاتبه با دیگر استفاده‌کنندگان PGP را آغاز کنید. شما به یک کپی از کلید عمومی دیگران نیاز دارید. کلید عمومی شما بصورت بلوکی از متن است، بنابراین تبادل کلید با شخص دیگر آسان است. می‌توانید کلید عمومی خود را در ایمیل قرار دهید، آنرا در فایل کپی کنید یا آنرا به یک سرویس‌دهنده کلید ارسال کنید تا هرکسی بتواند به کپی آن در صورت نیاز دسترسی داشته باشد. (مراقب باشید که کلید خصوصی خود را برای دیگران ارسال نکنید، در ضمن مطمئن باشید که از کلید عمومی یک نفر نمی‌توان به کلید خصوصی وی پی برد)

۴- از اعتبار کلید عمومی دیگران مطلع شوید:

هنگامی که شما یک کپی از کلید عمومی شخصی را دارید، می‌توانید آنرا به جاکلیدی خود اضافه کنید. بعد از آن می‌توانید نسبت به تعلق این کلید به شخص مورد نظر اطمینان حاصل کنید و اینکه این کلید تغییر نکرده است. اینکار با مقایسه اثرانگشت

(fingerprint) یکتا که در کنار کپی کلید عمومی آن شخص دارید با اثرانگشت کلید اصلی که در اختیار صاحب اصلی کلید است، انجام می‌پذیرد. هنگامی که مطمئن شدید که کلید عمومی معتبری از آن شخص در اختیار دارید، به آن کلید نشانه معتبر بودن اضافه می‌کنید.

۵- امن‌کردن ایمیلها و فایلهایتان را آغاز کنید:

بعد از اینکه جفت کلیدهایتان را تولید کردید و کلیدهای عمومی را مبادله کردید، می‌توانید دست به کار رمزنگاری، امضاء، رمزگشایی و تایید ایمیلها و فایلها شوید. برای انجام یک عمل PGP باید فایل یا پیامی را که می‌خواهید امن کنید انتخاب کنید و سپس عمل مورد نظر خود را «رمزنگاری (Encrypt)، امضاء (Sign)، رمزگشایی (Decrypt) یا تایید (Verify) » از طریق منوی PGP انتخاب کنید. منوهای PGP از چند طریق در دسترس هستند؛ مثلا در Windows Explorer شما می‌توانید روی فایل مورد نظر کلیک راست کنید و سپس عمل مناسب را در قسمت PGP انتخاب کنید.

۶- فایلهای مورد نظر را پاک کنید.

هنگامی که احتیاج به پاک کردن دائمی یک فایل دارید، می‌توانید با استفاده از ویژگی Wipe این عمل را انجام دهید تا مطمئن شوید که فایل قابل بازیابی نیست. فورا در محل ذخیره فایل اطلاعاتی نوشته می‌شود تا نتوان فایل را با استفاده از نرم‌افزارهای بازیابی دیسک حاصل کرد.

ضمنا نرم‌افزار PGP به شما امکان رمزکردن، رمزگشایی و سایر اعمال را روی اطلاعاتی که روی clipboard قرار دارد، می‌دهد. سپس اطلاعات تغییریافته را روی همان clipboard قرار میدهد. حتما می‌دانید که با انتخاب گزینه copy ، متن انتخاب شده به clipboard و با انتخاب گزینه paste متن موجود در clipboard به پنجره فعال شما منتقل می‌شود.

Nessus : پویش‌گری ساده و قدرتمند

معرفی نرم افزاری قدرتمند با نام Nessus محصولی کد باز و رایگان که با قابلیت‌های ویژه‌اش خود را مبدل به یکی از به‌ترین ابزارها در سال‌های اخیر ساخته است، می‌رسد.

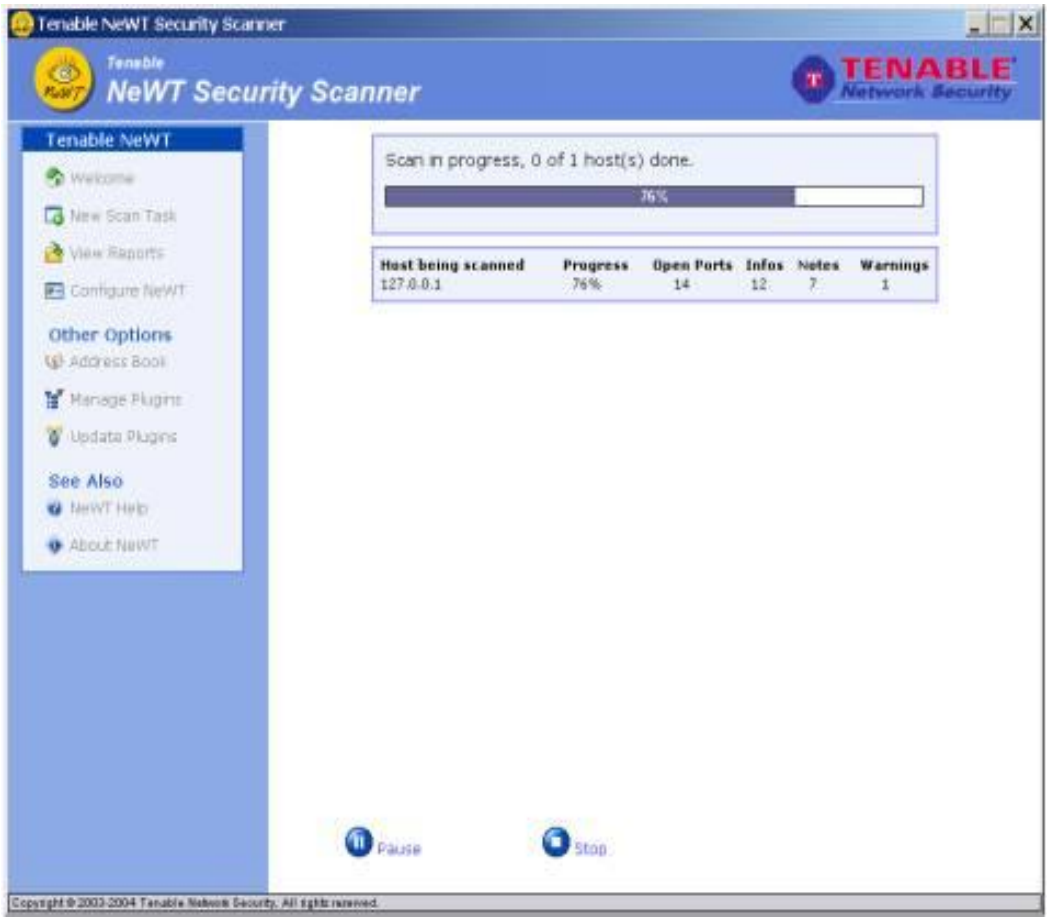
هرچند که این نرم‌افزار در واقع تنها برای محیط‌های Linux، BSD، Solaris و دیگر محیط‌های مشابه Unix نوشته شده است و در پایگاه www.nessus.org قابل دریافت است، ولی نگارشی از آن برای سیستم‌های عامل سری Windows با نام NeWT محصول Inc Tenable Network Security نیز موجود است که با مراجعه به پایگاه این شرکت، www.tenablesecurity.com، قابل دریافت است. مبنای این معرفی بر پایه‌ی نسخه‌ی تحت Windows این ابزار، یعنی NeWT، می‌باشد.

شکل زیر صفحه‌ی آغازین این نرم‌افزار را نشان می‌دهد :

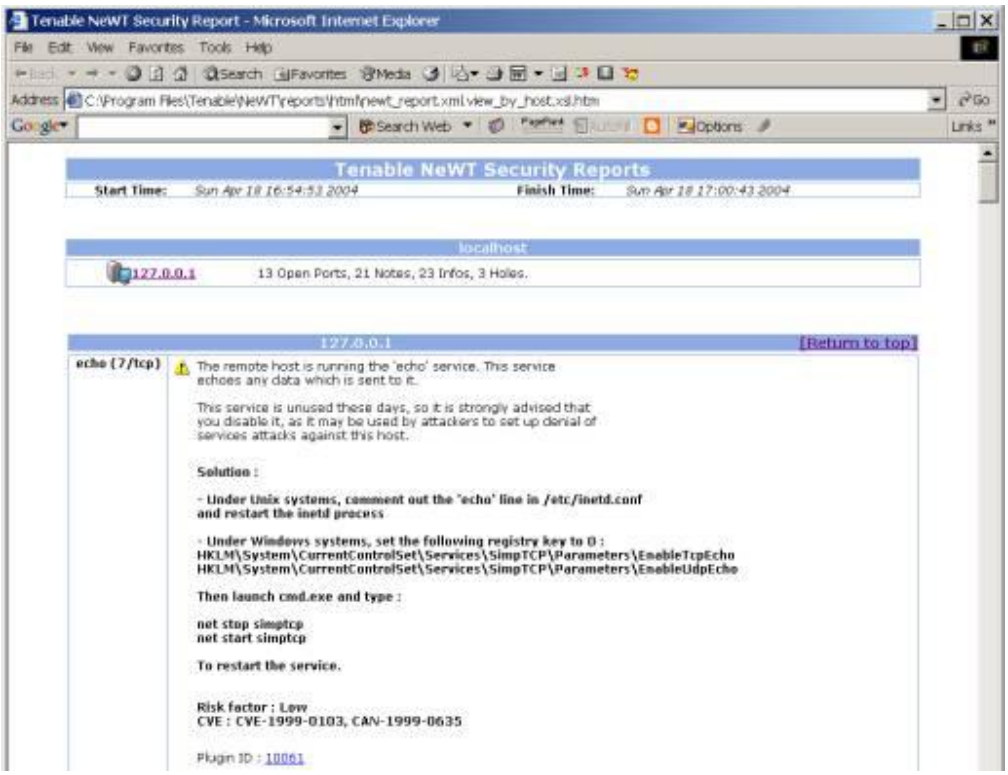
با انتخاب پویش جدید، نرم‌افزار آدرس یا آدرس‌های سیستم‌های مورد نظر برای پویش را به عنوان ورودی دریافت می‌کند. این آدرس‌ها می‌توانند در یک بازه‌ی آدرس نیز نباشند و در این صورت تک تک آنها به صورت مجزا باید ذکر شوند.

پیش از شروع پویش، از آن‌جاکه برخی از عملیاتی که در حین پویش توسط نرم‌افزار انجام می‌گیرد باعث ایجاد آسیب‌های امنیتی به سیستم مورد نظر می‌شوند، امکان تعیین زیربرنامه‌هایی که برای بررسی امنیت مورد استفاده قرار خواهند گرفت نیز وجود دارد.

پس از انتخاب حالت مورد نظر، که همان‌گونه که نرم‌افزار نیز پیش‌نهاد کرده است حالت اول امن‌ترین حالت برای پویش است، نرم‌افزار شروع به پویش کرده و در حین پویش اطلاعاتی همچون درصد پیشرفت پویش، تعداد پورت‌های باز، اخطارهای امنیتی و شکاف‌های موجود در سیستم مورد نظر ارایه می‌دهد. شکل زیر خروجی نرم‌افزار در حین پویش را نمایش می‌دهد.



پس از اتمام عمل پویش، نرم‌افزار گزارشی به‌صورت HTML تولید کرده و توسط مرورگر نمایش می‌دهد. شکل زیر نمونه‌ای از این گزارش را نشان می‌دهد.



در هر بخش از گزارش‌های ارایه شده توسط این نرم‌افزار، ضمن درج آسیب‌های امنیتی محتمل، آدرسی برای دریافت اطلاعات بیشتر در مورد ضعف امنیتی به‌همراه روش رفع آن نیز ذکر می‌شود.

همان‌گونه که در تصویر اول نیز مشاهده می‌شود، در این نرم‌افزار امکان مدیریت زیربرنامه‌هایی که توسط آن‌ها پویش انجام می‌گیرد نیز وجود دارد. از سوی دیگر در قسمت پیکربندی نیز می‌توان جزئیات پویش را نیز تعیین کرد. در این قسمت امکان تعیین کدهای کاربری به همراه رمز عبور برای پویش سرویس‌هایی که نیاز به احراز هویت دارند نیز فراهم شده است.