۱۰ ابزار برتر امنیت شبکه

نویسنده : مریم حیدري

ناشر : شرکت مهندسي شبکه و راهبري تحقیقات همکاران سیستم (مشورت)

تاریخ انتشار : ۸۸/۱۲/۱۷

کلمات کلیدي : امنیت شبکه، ابزارهاي امنیتي

در این مقاله سعی شده است تا ۱۰ ابزار برتر امنیت شبکه معرفي شوند . مدیران و حتی کاربران عادی با استفاده از این ابزار می‌توانند امنیت سیستم و شبکه خود را تا حد قابل قبولی تضمین نمایند.

۱. **Nessus**

Nessus محبوبترین اسکنر آسیب پذیری تا سال ۲۰۰۵ بود، این ابزار تا آن زمان open source بود اما از سال ۲۰۰۵ این ویژگي با انتشار نسخه‌ی جدید از بین رفت. این ابزار تنها برای استفاده در شبکه‌های خانگی مناسب است.

این ابزار مناسب محیط Unix می‌باشد و هنوز هم سرآمدترین ابزار امنیتی مناسب این محیط است.

۲. **Wireshark**

Wireshark یک ابزار تحلیل پروتکل شبکه open source است که برای محیطهای Unix و Windows مناسب است. این ابزار این امکان را فراهم می‌اورد تا داده‌های بدست امده از یک شبکه آنلاین مورد تجزیه و تحلیل قرار بگیرد. البته می‌توان داده‌های آفلاین که بر روی دیسکها ذخیره شده‌اند را نیز با استفاده از این ابزار تحلیل کرد.

ابزار Wireshark انواع پروتکلها را تحت پوشش قرار داده است و تمامی داده‌های شبکه را می‌تواند در سطح بسته‌های داده‌ای و سرآیند بسته‌ها تحلیل کند.

۳. **Snort**

Snort یک ابزار کشف مداخله در شبکه و یک سیستم پیشگیری از مداخله است. این ابزار با ثبت و تحلیل ترافیک گذرنده از شبکه کار خود را انجام می‌دهد. Snort از طریق تحلیل پروتکل، جستجوی محتوا و پیش پردازشهای بسیار، می‌تواند بسیاری از کرمها، آسیب پذیریها و دیگر رفتارهای مشکوک را کشف کند. Snort از یک زبان انعطاف پذیر و مبتنی بر قاعده برای توصیف ترافیک استفاده می‌کند.

Snort برای استفاده تمامی کاربران عادی، تجارتهای کوچک و بخشهای مختلف یک سازمان مناسب است.

۴. **Netcat**

این ابزار داده‌ها را از طریق ارتباطات شبکه‌ای UDP و TCP می‌خواند و می‌نویسد.Netcat ابزار قابل اعتمادی است که به صورت مستقیم می‌تواند استفاده شود و به همراه بسیاری برنامه‌ها و اسکریپتهای مختلف در دسترس قرار دارد. البته Netcat یک ابزار قوی در تحلیل شبکه و رفع مشکل در شبکه هست و می‌تواند هر نوع ارتباط مورد نیاز را برقرار کند.

۵. **Metasploit Framework**

Metasploit یک زیربناي open-source برای توسعه، تست و استفاده از کد افشا می‌باشد. این ابزار،مدل انعطاف پذیری است که بسیاری از افشاها و آسیب پذیریهای موجود در شبکه را کشف می‌کند. این ابزار هم برای کشف اسیب پذیری در سیستمهای عادی و هم براي سیستم هاي سازمانی مناسب است و این امکان را در اختیار کاربران قرار

می‌دهد تا اسیب پذیریهای مورد نظر خود را بنویسند و انها را تست کرده و درصدد رفع ان بر آیند.

۶. Hping2

این ابزار بسته‌های ICMP، UDP و یا TCP را اسمبل می‌کند و انها را می‌فرستد و هر بسته‌ای را که در پاسخ آنها دریافت می‌شود، نمایش می‌دهد. همچنین این ابزار دارای مد ردگیری مسیر بسته و تقسیم بندی بسته‌های IP می‌باشد. این نرم افزار زمانی مفید است که قصد ردیابی مسیر، ping و تحلیل میزبانها، از پشت یک فایروال وجود دارد. Hping در نگاشت و تطابق قوانین فایروال کمک می‌کند. این ابزار برای یادگیری بیشتر در مورد TCP/IP بسیار مناسب است.

۷. Kismet

Kismet یک سیستم کشف مداخله شبکه و کشف کننده شبکه است که با گوش دادن به ترافیک آفلاین شبکه سعی در شناسایی اختلالات و آسیب پذیریهای موجود در شبکه دارد. همچنین این ابزار،به صورت اتوماتیک می‌تواند ترافیک را مسدود کند و یا با استفاده از Wireshark/TCPDump آن را ثبت نماید.

۸. Tcpdump

Tcpdump یک ابزار برای گوش دادن به ترافیک IP هست که کاری شبیه به Wireshark انجام می‌دهد با این تفاوت که این ابزار قبل از Wireshark وارد عرصه شده و از یک محیط Console استفاده مي كند.

۹. Cain and Abel

کاربران Unix می‌توانند از این ابزار رایگان امنیتی استفاده کنند که البته برای محیط windows نیز مناسب است. کاربرد اصلی این ابزار کشف کلمات عبور از طریق گوش دادن به ترافیک شبکه است. البته این نرم افزار، کاربردهای دیگری نیز دارد که شامل شکستن کلمات عبور رمز شده با استفاده از دیکشنری، حملات brute-force، بدست اوردن کلمات عبور ذخیره شده، مسیریابی پروتکلها و آشکار کردن بسته‌های مربوط به کلمات عبور مي شود.

۱۰. John the Ripper

John the Ripper، ابزار قدرتمند، انعطاف پذیر و سریع شکننده کلمات عبور می‌باشد که ابتدا برای بدست اوردن کلمات عبور ضعیف در محیط Unix ساخته شد و هم اکنون در تمامی محیطها نیز کاربرد دارد.

مراجع

[۱] www.nmap.org