

Programy skanujące

Programy skanujące (skanery portów) służą do automatycznego wykrywania słabych stron zabezpieczeń systemów – zarówno na serwerach lokalnych jak i zdalnych. Dzięki ich zastosowaniu użytkownik w Los Angeles może wykryć słabości w systemie ochrony na serwerze w Japonii.

Skanery działają wysyłają zapytania do portów TCP/IP i zapisują odpowiedź otrzymaną z serwera. Gromadzą one cenne informacje na temat wybranego serwera poprzez ustalanie:

- Usług udostępnianych przez serwer
- Właścicieli procesów serwerów tych usług
- Czy serwer zezwala na anonimowe logowanie
- Czy dla wybranych usług stosowane są procedury autoryzacji użytkownika

Pierwsze programy skanujące pisane były wyłącznie dla platformy UNIX. Obecnie wiele systemów operacyjnych korzysta z protokołów TCP/IP, toteż pojawiły się liczne programy skanujące przeznaczone na inne platformy, w szczególności pod Windows NT – w związku ze wzrostem znaczenia tego systemu.

Wymagania systemowe zależą od programu skanującego. Przeważająca większość, tych przeznaczonych dla UNIX-a, jest bezpłatna (freeware). Zazwyczaj są one rozprowadzane w formie kodu źródłowego, nie zaś w postaci binarnej – stąd wymagania systemowe są bardzo rygorystyczne.

Trzeba więc korzystać z:

- Systemu operacyjnego UNIX
- Kompilatora C
- Plików typu include protokołu IP.

Narzędzia tego typu nie są dostępne powszechnie. Poza tym, niektóre programy skanujące nakładają na użytkowników dodatkowe, specyficzne ograniczenia – takim właśnie programem

jest SATAN, który wymaga do pracy uprawnień administratora. Zatem rozsądnym wyjściem jest testowanie programów tego rodzaju na serwerze wyposażonym w pełną instalację Linux-a.

Inne wymagania skanerów portów to:

- Pamięć operacyjna RAM. Wiele programów skanujących ma w tym względzie znaczne potrzeby. Dotyczy to zwłaszcza skanerów pracujących w środowiskach graficznych lub generujących złożone raporty wyjściowe.
- Nie wszystkie programy skanujące działają identycznie na różnych platformach. Na jednych brakować może pewnych opcji, na innych niedostępne okazać się mogą niektóre z funkcji podstawowych.
- Podstawowym wymogiem jest – co oczywiste – połączenie z siecią.

Legalność programów skanujących podlega nieustannej dyskusji. Niektórzy porównują ich działanie do używania łomu w celu sprawdzenia wytrzymałości cudzych okien i drzwi, i uważają to za niedozwolone wtargnięcie na teren prywatny. Inni utrzymują, iż posiadanie serwera z połączeniem do Internetu wiąże się z przyzwoleniem na poddanie się skanowaniu. (adres internetowy można porównać do numeru telefonu – każdy ma prawo na dany numer zadzwonić.)

Prawo nie uwzględnia żadnego z tych poglądów, ponieważ, jak dotąd programy skanujące znajdują się poza obszarem jego zainteresowania. Należy zatem przyjąć, że programy skanujące są legalne.

Programy skanujące uczyniły bardzo wiele dla poprawienia bezpieczeństwa Internetu. Aby zrozumieć ten mechanizm należy wziąć pod uwagę, że dla każdej platformy znanych jest co najmniej kilkaset słabych punktów. Zwykle dotyczą one konkretnej usługi sieciowej – ręczne sprawdzenie serwera pod kątem jego słabych punktów zajęłoby kilka dni. należałoby pobrać, skompilować i uruchomić setki programów

wykorzystujących pojedyncze luki systemowe. Byłby to proces powolny, żmudny i podatny na błędy, a i tak w rezultacie ograniczony do jednego serwera. Co gorsza, po „ręcznej” weryfikacji serwera pozostałaby ogromna ilość niejednorodnych danych, znacznie różniących się strukturalnie. Każdy haker pisze swoje kody indywidualnie i niestandardowo, zatem raporty działania poszczególnych programów są zróżnicowane. Dlatego uporządkowanie danych po testach manualnych zajęłoby wiele dni. Programy skanujące definitywnie eliminują te problemy. Dane przez nie wygenerowane sformatowane są jednolicie – co ułatwia zarówno dostęp do nich jak również analizę. Większość z nich pozwala na skanowanie nieograniczonej liczby domen. Programy skanujące są doskonałymi narzędziami testowania wstępnego, zapewniają szybką i „bezbolesną” metodę odkrywania słabych punktów w zabezpieczeniach sieci.

W serwisie dyplom.com.pl prezentujemy obronione prace dyplomowe, które mogą służyć za wzór do napisania własnej pracy - gdyby potrzebowali jeszcze Państwo konsultacji to polecamy stronę [pisanie prac](http://pisanieprac.pl) - fachowa pomoc w pisaniu prac.