

Zapory sieciowe Firewall. Cel pracy

Niewielu internautów zdaje sobie sprawę, że beztrioskie przeglądanie stron WWW niekiedy niesie ze sobą wiele niespodziewanych niebezpieczeństw. W gąszczu światowej pajęczyny można trafić na kogoś, kto dla pieniędzy, zaspokojenia swojej ciekawości albo po prostu dla sportu będzie próbować złamać najbardziej wyrafinowane systemy zabezpieczeń i zagrozić naszemu komputerowi, który podświadomie uważamy za twierdzę nie do zdobycia.

Podłączenie do sieci publicznej jest dwukierunkowe: pozwala użytkownikowi nie tylko odbierać, ale i dostarczać informacje, co może odbywać się bez jego wiedzy i pozwolenia. Pracując w sieci należy liczyć się chociażby z tak zwanymi atakami Denial of Service, których celem nie jest zdobycie jakichkolwiek informacji, lecz unieruchomienie lub chwilowe zablokowanie serwera bądź stacji.

Podstawową zasadą działania wszelkich systemów ochronnych jest: „To co nie jest jawnie dozwolone – jest zakazane”. Firewall (zapory ogniowe) są instalowane między sieciami w celu wymuszenia kontroli dostępu między nimi. Generalnie rzecz ujmując, firewalle zabezpieczają przed nieautoryzowanym dostępem z zewnątrz do sieci lokalnej. Niektóre nawet mogą całkowicie blokować ruch pakietów z zewnątrz – dopuszczając ewentualnie pakiety poczty elektronicznej – zezwalając jednakże na swobodne komunikowanie się użytkowników sieci ze światem zewnętrznym. Inną pożyteczną cechą firewalli jest możliwość wykorzystania ich do rejestrowania i śledzenia wszelkich przychodzących pakietów (auditing).

Stacje umieszczane w pierwszej linii obrony, określane również jako bastion host, są punktami przez które przechodzą wszystkie informacje do sieci lokalnej i na zewnątrz. Dzięki

takiemu scentralizowaniu dróg dostępu do sieci w jednym komputerze można łatwo zarządzać systemem ochrony.

2. Cel pracy.

Celem pracy jest przedstawienie i omówienie wybranych zagadnień związanych z bezpieczeństwem sieci komputerowych i zastosowaniem w nich zapor firewall. W pracy zostały opisane szczegółowo sposoby konfiguracji systemu Linux tak, by spełniał podstawowe zadania i funkcje stawiane przed skuteczną zaporą ogniową a także poruszono najważniejsze zagadnienia związane z podłączeniem i instalacją w sieci Internet komputera pracującego pod kontrolą systemu Windows.

W sierpniu 1996 r. miało miejsce jedno z najbardziej znanych i upokarzających włamań dotyczące Departamentu Sprawiedliwości USA. Hakerom udało się podmienić stronę Web na elektroniczne graffiti składające się z portretów Hitlera i golizny. We wrześniu tego roku, na liście „zdobytych” znalazły się strony Web Brytyjskiej Partii Konserwatywnej, Nation of Islam, Amerykańskiego Stowarzyszenia Psychoanalitików, Sił Powietrznych USA oraz Centralnej Agencji Wywiadowczej, której nazwę zmieniono na Central Stupidity Agency (Centralna Agencja

Głupoty/Bezsensu) [\[1\]](#).

Ten przykład pokazuje jak bardzo na niebezpieczeństwo narażone są serwery, dane i strony www publikowane w sieci internet . Ochrona systemów komputerowych, budowa i konfiguracja zapór sieciowych oraz innych systemów zabezpieczeń są tematami niezwykle złożonymi (aktualnymi), których nie sposób wyczerpać w jednej publikacji czy książce.

[\[1\]](#) rekonstrukcje włamań do Departamentu Obrony, CIA oraz U.S. Air Force: <http://www.260.com>

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](#) - fachowa pomoc w pisaniu prac.