Uniwersytet Mikołaja Kopernika

Wydział Matematyki i Informatyki

Wydział Fizyki, Astronomii i Informatyki Stosowanej

Karol Zygmunt
Nr albumu: 168555

Praca magisterska
na kierunku Informatyka

Bezpieczeństwo sieci komputerowych w oparciu o skaner luk sieciowych Nessus

Praca wykonana pod kierunkiem
dra hab. Jacka Kobusa

Toruń 2007

Spis treści

1 Wstęp

Celem projektu FOLA[1] jest stworzenie wygodnej, funkcjonalnej platformy narzędziowej służącej do zarządzania grupami serwerów i stacji roboczych. W skład systemu wchodzą moduły odpowiedzialne za wykonywanie ściśle wyspecjalizowanych zadań automatyzujących codzienną pracę administratora lokalnej sieci komputerowej. Do zadań tych zaliczamy między innymi rejestrowanie nowych maszyn w sieci, monitorowanie ich funkcjonowania oraz integralności, zarządzanie kontami użytkowników, zarządzanie pakietami oprogramowania, tworzenie kopii zapasowych bądź udostępnianie scentralizowanych mechanizmów uwierzytelniania. Poszczególne moduły działają niezależnie korzystając czasami ze wspólnych baz danych i plików konfiguracyjnych. Ich architektura powinna jednak umożliwić stworzenie osobnego programu (modułu centralnego) stanowiącego jednolity interfejs oferujący dostęp do funkcjonalności każdego z nich [1] [2] [3].

Zasadniczym celem tej pracy jest zbudowanie narzędzia FOLANessus wchodzącego w skład systemu FOLA, które umożliwi wykonywanie zdalnych testów bezpieczeństwa, zbieranie wyników z ich przeprowadzenia oraz analizowanie zgromadzonych danych. Funkcjonalność obejmować powinna również tworzenie raportów oraz wszczynanie alarmów w przypadku wykrycia niebezpieczeństwa. Zasady i mechanizmy nadzorowania bezpieczeństwa rozwijają się tak szybko jak szybko następują zmiany w budowie i oprogramowaniu sieci komputerowych. Prawdziwie bezpieczna sieć definiowana jest jako wyidealizowany system, który poprawnie i w całości realizuje tylko i wyłącznie cele zgodne z intencjami administratorów i wymaganiami użytkowników. W praktyce jednak zapewnienie bezpieczeństwa sprowadza się do zarządzania ryzykiem. Różnorodność oprogramowania oraz jego dynamiczny rozwój, który niestety nie idzie w parze z bezpieczeństwem, powoduje, że administratorzy mają pełne ręce pracy. Dodatkowo wymagania użytkowników niejednokrotnie kłócą się z zastosowaną filozofią bezpieczeństwa, a uleganie oczekiwaniom użytkowników powoduje zwykle obniżenie poziomu zabezpieczeń. Należy także uświadomić sobie, że sieć jest na tyle bezpieczna, na ile bezpieczny jest jej najsłabszy punkt. Komplikuje to sprawę jeszcze bardziej, ponieważ w wielu przypadkach tymi najsłabszymi punktami są stacje robocze, nad którym administratorzy nie mają bezpośredniej kontroli. Niejednokrotnie maszyny te mają nieograniczony

1 FOLA (ang. *Friend of Lazy Administrator*) – przyjaciel leniwego administratora.

kontakt z siecią Internet tworząc tym samym pojedynczy punkt ataku, przez który z łatwością rozprzestrzeniać się mogą rozmaite zagrożenia, takie jak robaki i wirusy komputerowe. Powoduje to także, że stacje klienckie stają się celem zdalnych ataków polegających na wykradaniu danych, instalowaniu oprogramowania szpiegowskiego, itp. O tym na ile poważny jest problem bezpieczeństwa może świadczyć fakt ujawnionych przestępstw komputerowych, które dotyczyły włamań do systemów komputerowych najlepiej strzeżonych instytucji na świecie takich jak National Security Agency[2] czy AT&T[3]. Na skutek narastających tego typu incydentów powstał specjalny zespół do reagowania na zdarzenia naruszające bezpieczeństwo systemów komputerowych CERT (Computer Emergency Response Team) [4] [5].

Administrator lokalnej sieci komputerowej w celu zachowania odpowiedniego poziomu bezpieczeństwa zarządzanej przez siebie sieci powinien przeprowadzać testy sprawdzające jej podatność na poszczególne znane luki w zabezpieczeniach. Testy te powinny obejmować sprawdzania pod kątem najnowszych ujawnionych zagrożeń jaki i starszych, ale bardzo popularnych. Odpowiednio wcześnie wykryte zagrożenia sprawiają, że administrator jest o krok przed intruzami i ma możliwość naprawy niedoskonałości systemu.

System FOLANessus składa się ze serwera FOLANessus, który jest centralnym punktem odpowiedzialnym za rejestrowanie użytkowników, wykonywanie zleconych przez klientów zadań skanowania oraz zarządzanie zwracanymi raportami. Do procesu skanowania serwer FOLANessus wykorzystuje skanery Nessusa, będące ogólnodostępnym oprogramowaniem rozwijanym przez społeczność internetową [6]. W systemie występuje co najmniej jeden taki skaner, ale ich całkowita liczba zależy jedynie od architektury monitorowanej sieci. Serwerem FOLANessus zarządza centralny administrator sieci, natomiast klientami systemu są administratorzy poszczególnych podsieci lub użytkownicy stacji klienckich. Rejestracja klienta wiąże się z utworzeniem na serwerze FOLANessus specjalnego konta użytkownika oraz wygenerowaniem certyfikatów i kluczy zapewniających ustanowienie bezpiecznego kanału komunikacyjnego. Pozwala to na wygodne przekazywanie i pobieranie danych z

2 Agencja Bezpieczeństwa Narodowego (ang. *National Security Agency NSA*) - amerykańska wewnętrzna agencja wywiadowcza koordynująca m.in. zadania wywiadu elektronicznego, powstała w kwietniu 1952 roku na bazie struktury działającej od 1949 roku, Agencji Bezpieczeństwa Sił Zbrojnych (*Armed Forces Security Agency AFSA*).

3 AT&T (ang. *American Telephone and Telegraph)* – amerykańskie przedsiębiorstwo telekomunikacyjne. AT&T było przez pewien czas największym na świecie przedsiębiorstwem świadczącym usługi telefoniczne oraz największą siecią telewizji kablowej. W jego laboratoriach (Bell Labs) powstał m.in. system operacyjny UNIX i języki C i C++.

serwera FOLANessus.

Klient za pomocą odpowiedniego oprogramowania łączy się z serwerem i konfiguruje parametry zadań monitorowania. Parametry te określają zakres badanych maszyn, rodzaj przeprowadzanych testów oraz ich częstotliwość. Po wykonaniu wstępnego skanowania i zaakceptowaniu jego wyniku klient zapisuje go jako wzorzec na serwerze. Wzorcowy wynik będzie wykorzystywany później do porównania z raportami zwracanymi z cyklicznych skanowań. W przypadku, gdy kolejne porównanie ujawni różnice pomiędzy wzorcem, a zwróconym raportem zleceniodawca zadania zostanie o tym powiadomiony drogą pocztową. Klient oprócz zarządzania zleceniami skanowania może także przeglądać wszystkie raporty.

System FOLANessus został napisany w języku Perl, który umożliwia wygodne tworzenie narzędzi systemowych, dysponuje doskonałymi mechanizmami do obróbki tekstu, a także umożliwia korzystanie z ogromnej liczby modułów dostępnych w repozytoriach CPAN[4]. Na system składają się skrypty perlowe oraz liczne funkcje zgromadzone w oddzielnych bibliotekach. Zlecenia przekazywane są poprzez zdalne wywoływanie komend z użyciem protokołu SSH, a pliki raportów mają XML-ową strukturę. Przed rozpoczęciem instalowania serwera i skryptów klienckich należy zainstalować wymagane moduły perlowe. System FOLANessus udostępniony jest na zasadach ogólnej licencji publicznej GNU GPL[5].

Plan pracy jest następujący. Rozdział drugi opisuje różne formy zagrożeń oraz możliwe formy ataku. Przedstawiony jest tam również protokół *Nessus Transport Protocol* wykorzystywany w trakcie komunikacji ze skanerami Nessusa. Rozdział trzeci przybliża architekturę systemu FOLANessus, funkcje serwera i klientów oraz protokół komunikacyjny. Rozdział czwarty przedstawia szczegóły implementacji systemu, a piąty zawiera podsumowanie. Załączniki określają specyfikację dotyczącą wymagań systemu, szczegóły procesu instalacji serwera i rejestracji klientów, strukturę katalogów i XML-owych baz danych oraz dokumentację bibliotek funkcji. Do niniejszej pracy dołączona jest płyta CD-ROM, na której znajduje się oprogramowanie oraz dokumentacja w formie elektronicznej.

4 CPAN (ang. *Comprehensive Perl Archive Network*) – to źródło dokumentacji oraz modułów do języka Perl. Zgromadzone moduły mają bardzo wiele zastosowań (umożliwiają dostęp do baz danych czy protokołów komunikacyjnych, tworzenie obrazków, wykonywanie skomplikowanych operacji matematycznych) [7].

5 Powszechna Licencja Publiczna GNU (ang. *General Public License GNU*) jest jedną z licencji wolnego oprogramowania, która została sformułowana w 1988 przez Richarda Stallmana i Ebena Moglena na potrzeby Projektu GNU (projekt mający na celu stworzenie wolnego systemu operacyjnego), na podstawie wcześniejszej Emacs General Public License [8].