Uniwersytet Mikołaja Kopernika w Toruniu

Wydział Matematyki i Informatyki

Wydział Fizyki, Astronomii
i Informatyki Stosowanej

Agnieszka Holka
Nr albumu: 187396

Praca magisterska
na kierunku Informatyka

Międzyplatformowy interfejs systemu FOLANessus wykonany przy użyciu biblioteki Qt4

Praca wykonana pod kierunkiem
dra hab. J. Kobusa
Zakład Mechaniki Kwantowej

TORUŃ 2009

Spis treści

Wstęp **4**

1 Graficzne interfejsy użytkownika **7**

1.1 Krótka historia GUI 8

1.1.1 Pierwszy interfejs graficzny 8

1.1.2 Xerox Alto 9

1.1.3 Apple 10

1.1.4 GUI lat 80. 11

1.1.5 X Window System 13

1.1.6 Spojrzenie w przyszłość 15

1.2 Projektowanie aplikacji graficznych 16

1.2.1 Podstawowe zasady 17

1.2.2 Wskazówki techniczne 20

2 Architektura systemu **26**

2.1 Instalator 27

2.2 Serwer 29

2.3 Aplikacja kliencka FOLANessus 30

2.3.1 Rozpoczęcie pracy 31

2.3.2 Definiowanie zestawu wtyczek i ich preferencji 31

2.3.3 Określanie parametrów skanowania 33

2.3.4 Tworzenie nowego skanu 34

2.3.5 Otwarcie zdefiniowanego zadania 36

2.3.6 Zarządzanie skanami 37

2.3.7 Przeglądanie i porównywanie raportów 37

2.3.8 Ustawienia programu 38

3 Implementacja **40**

3.1 Rozdzielenie warstw aplikacji 41

3.2 Komunikacja z serwerem 41

3.3 Projektowanie GUI 42

3.4 Mechanizm sygnałów i gniazd 43

3.5 Wykorzystanie XML-a 44

3.5.1 Parser DOM 45

3.5.2 XQuery i XPath 46

3.6 Użycie plików konfiguracyjnych 48

3.7 Internacjonalizacja 49

3.7.1 Wymagania dotyczące kodu aplikacji 50

3.7.2 Przygotowanie plików dla tłumacza 50

3.7.3 Wygenerowanie plików wczytywanych przez aplikację 51

Bibliografia **52**

A Wymagania systemowe **54**

Wstęp

Projekt FOLANessus stanowi kontynuację systemu stworzonego przez Karola Zygmunta i omówionego przez niego w pracy magisterskiej *Bezpieczeństwo sieci komputerowych w oparciu o skaner luk sieciowych Nessus* [1]. Jest to oprogramowanie służące do monitorowania odporności hostów w sieci na ataki. Wykorzystuje skaner Nessus [3], rozszerzając jego działanie o możliwość definiowania i zapisywania zadań skanowania oraz ich cykliczne wykonywanie. Najistotniejszym punktem pierwszej wersji systemu była koncepcja raportów różnicowych. Przyjęto założenie, że po zdefiniowaniu parametrów oraz zakresu używanych testów odporności użytkownik wykona pierwsze wzorcowe skanowanie. To skanowanie ma służyć za podstawę do określenia, jaki poziom zabezpieczeń jest dla administratora satysfakcjonujący. Przeprowadzane cyklicznie testowe ataki nie dostarczają już szczegółowych informacji o znalezionych lukach, lecz jedynie informują o zmianach, jakie zaszły w stosunku do wyniku przyjętego za wzorzec. Takie podejście ogranicza czas konieczny na analizę wyników oraz ułatwia administratorowi zauważenie niepokojących zmian.

Pierwsza wersja systemu FOLANessus została w całości zaimplementowana w języku Perl. Po stronie serwera umieszczono skrypty odpowiedzialne za zarządzanie zbiorem zadań należących do danego użytkownika oraz przeprowadzanie pojedynczych skanowań i przekazywanie na bieżąco ich postępu. Aplikację kliencką stanowiły zaś dwa skrypty, z których pierwszy pozwalał na określenie parametrów skanowania oraz jego przeprowadzenie. Drugi natomiast dawał możliwość przeglądania raportów wygenerowanych podczas testowania poszczególnych grup komputerów. Do stworzenia tych skryptów wykorzystano moduł perlowy *Curses* pozwalający na rysowanie w terminalu graficznych kontrolek. Taki interfejs uznać należy za spore udogodnienie w porównaniu do pracy wyłącznie za pośrednictwem komend tekstowych. Trzeba jednak przyznać, że moduł *Curses* posiada spore ograniczenia i nie pozwolił

na w pełni wygodne korzystanie z możliwości oferowanych przez serwer FOLANessus. Dlatego też zdecydowano się na wydanie drugiej edycji systemu, której główny cel stanowi stworzenie interfejsu graficznego pozwalającego jeszcze bardziej ułatwić pracę administratorowi monitorującemu bezpieczeństwo hostów. Jednocześnie zdecydowano się podjąć próbę automatyzacji zadań, jakie trzeba wykonać podczas instalacji serwera FOLANessus. Oba te moduły zaimplementowane zostały w języku C++ z użyciem biblioteki Qt4. Dzięki tym technologiom udało się stworzyć graficzne narzędzie, mogące konkurować choćby z dostarczanym przez Tenable Network Security[1] [2] oprogramowaniem NessusClient[2] [3].

Pierwszy rozdział pracy poświęcony jest historii graficznych interfejsów użytkownika oraz zasadom ich projektowania. Analiza rozwoju systemów okienkowych pozwala zrozumieć, jak wielki wkład miały w przybliżenie komputerów szerokiemu gronu ludzi i jak bardzo usprawniły wiele zadań wykonywanych wcześniej za pośrednictwem konsoli. Drugi rozdział stanowi opis architektury stworzonego systemu. Nacisk położony został na omówienie zmian w stosunku do pierwszej wersji projektu. Opisano działanie instalatora, którego powstanie pozwoliło na automatyzację większości zadań wymaganych do uruchomienia centralnego serwera systemu FOLANessus. Dalej omówione zostały funkcje spełniane przez serwer, w szczególności skrypty języka Perl stanowiące interfejs dostępowy. Najważniejszą część tego rozdziału stanowi jednak opis aplikacji klienckiej FOLANessus, gdyż właśnie ona jest centralnym elementem nowej wersji projektu. Przybliżono więc możliwości programu ze szczególnym uwzględnieniem kolejnych kroków, jakie należy wykonać celem zdefiniowania zadania skanowania hostów, jego przeprowadzenia, zapisania na serwerze i przeglądania wyników. Zapoznanie się z tym opisem powinno pozwolić na rozpoczęcie korzystania z aplikacji klienckiej FOLANessus.

Wreszcie ostatni rozdział poświęcony został szczegółom implementacyjnym. Skupiono się na wykorzystanej w projekcie bibliotece Qt4 i narzędziach z nią dostarczanych. Przede wszystkim zostały opisane te moduły, które w znaczący sposób wpłynęły na kształt aplikacji lub ułatwiły proces programowania. Przedstawiono moduł dostarczający komponentów graficznych, moduł umożliwiający przetwarza-

[1] Tenable Network Security – firma dostarczająca rozwiązania do badania bezpieczeństwa sieci, w tym skaner Nessus.

[2] NessusClient – aplikacja kliencka dla skanera Nessus.

nie dokumentów XML, a także omówiono obsługę połączeń z serwerem oraz internacjonalizację interfejsu. Zobrazowano również podział aplikacji na warstwy biznesową i prezentacji oraz klasy odpowiedzialne za realizację poszczególnych zadań.

Projekt FOLANessus dostępny jest na licencji GNU GPL [14]. Do pracy dołączona została płyta CD, zawierająca kod źródłowy projektu FOLANessus wraz z niniejszą pracą w formacie PDF oraz LaTeX.