
UNIwersytet MIKOŁAJA KOPERNIKA
W TORUNIU

Wydział Matematyki i Informatyki

Wydział Fizyki, Astronomii
i Informatyki Stosowanej

Piotr Szubiakowski

Nr albumu: 168543

Praca magisterska
na kierunku informatyka

**Bezpieczeństwo systemów komputerowych
i lokalnej sieci komputerowej**

Praca wykonana pod kierunkiem
dr hab. Jacka Kobusa
Zakład Mechaniki Kwantowej

TORUŃ 2007

Spis treści

| | |
|--|-----------|
| Wstęp | 4 |
| 1 Sieci komputerowe | 5 |
| 1.1 Model OSI | 5 |
| 1.2 Protokół ARP | 9 |
| 1.2.1 Działanie protokołu ARP | 10 |
| 1.2.2 Zatrutowanie tablicy ARP i metody ochrony | 12 |
| 1.2.3 Zarządzanie tablicami ARP | 14 |
| 1.3 Netfilter i iptables | 16 |
| 1.3.1 Tablice i łańcuchy | 16 |
| 1.3.2 Protokół IP | 19 |
| 1.3.3 Protokoły TCP i UDP | 22 |
| 1.3.4 Moduł conntrack i śledzenie stanu połączeń | 25 |
| 1.3.5 Budowa reguł filtrowania | 25 |
| 2 Architektura modułu FOLA::Security 2.0 | 29 |
| 2.1 Zadania serwera i klientów | 29 |
| 2.2 Struktura katalogów | 31 |
| 2.3 Komunikacja między serwerem i klientami | 33 |
| 2.4 Narzędzia i biblioteki | 33 |
| 2.5 Konfiguracja | 35 |
| 2.5.1 Konfiguracja serwera | 35 |
| 2.5.2 Konfiguracja klienta | 36 |
| 3 Implementacja modułu FOLA::Security 2.0 | 38 |
| 3.1 Instalacja | 38 |
| 3.2 Rejestracja klienta | 40 |
| 3.3 Zarządzanie tablicami ARP | 41 |
| 3.3.1 Definiowanie zleceń | 42 |
| 3.3.2 Wykonywanie zleceń | 44 |
| 3.4 Konfiguracja zapory ogniowej | 45 |
| 3.4.1 Definiowanie zapory ogniowej | 46 |
| 3.4.2 Definiowanie superusług | 48 |
| 3.4.3 Tworzenie i wykonywanie zleceń | 49 |
| Podsumowanie | 50 |

| | |
|-------------------------------|----|
| Spis literatury | 52 |
| A Dokumentacja FOLA::Security | 53 |
| B CD-ROM | 61 |

Wstęp

Celem projektu FOLA (ang. *the Friend of a Lazy Administrator*) jest stworzenie platformy wspomagającej pracę administratorów sieci. Składa się na nią szereg modułów, z których każdy realizuje część zadań związanych z automatyzacją zarządzania siecią oraz systemami komputerowymi. Platforma ta jest przeznaczona dla systemu GNU/Linux.

Celem tej pracy jest rozbudowa modułu `FOLA::Security`, który jest odpowiedzialny za zapewnienie odpowiedniego poziomu bezpieczeństwa komputerom osobistym oraz stacjom roboczym pracujących w lokalnej sieci komputerowej. W skład systemu `FOLA::Security` wchodzi serwer oraz stacje klienckie. Serwer jest odpowiedzialny za bezpieczeństwo stacji klienckich. Główną funkcją poprzedniej wersji modułu było nadzorowanie nienaruszalności wybranych plików i katalogów na stacjach klienckich. Obecna wersja modułu dostarcza narzędzi, które ułatwiają korzystanie ze statycznych tablic ARP (ang. *Address Resolution Protocol*) oraz konfigurowanie zapory ogniowej na maszynach klienckich. Oprogramowanie `FOLA::Security` zostało napisane w języku Perl i udostępniane jest na zasadach ogólnej licencji publicznej GNU GPL (ang. *General Public License*).

Plan pracy jest następujący. Rozdział pierwszy zawiera opis protokołu ARP oraz systemu `netfilter`, który jest filtrem pakietów w systemie Linux. W rozdziale tym znajdują się również podstawowe informacje na temat funkcjonowania sieci komputerowych. Rozdział drugi opisuje architekturę modułu `FOLA::Security`, w tym sposób komunikacji między serwerem a stacjami klienckimi, strukturę katalogów oraz zadania realizowane przez serwer i klientów. Rozdział trzeci opisuje sposób zarządzania statycznymi tablicami ARP oraz zaporą ogniową. Zawiera on również informacje na temat instalacji programów klienta i serwera oraz rejestracji klienta w systemie `FOLA::Security`. Dodatek A zawiera dokumentację oprogramowania, a Dodatek B opisuje zawartość płyty CD-ROM dołączonej do niniejszej pracy.