1. Wprowadzenie

Szybki rozwój dziedziny nowoczesnych technologii sprawił, że dostęp do globalnych zasobów sieci Internet stał się możliwy praktycznie w każdym zakątku ziemi. Już dziś trudno sobie wyobrazić funkcjonowanie oddziałów nowoczesnych przedsiębiorstw, często umiejscowionych w oddalonych od siebie miastach a nawet i różnych kontynentach bez wzajemnej komunikacji.

W dzisiejszych czasach kwestia cyber-bezpieczeństwa stała się kwestią priorytetową, nie tylko dla wielkich korporacji i banków lecz także - lub może raczej przede wszystkim - dla małych firm i zwykłych użytkowników komputerów. W celu zapewnienia pewnego pewnego stopnia bezpieczeństwa sieci niezbędne jest wcześniejsze zbadanie istniejących luk i błędów w jej aktualnym stanie zabezpieczeń. W tym celu bardzo często wykorzystuje się skanery portów sieciowych lub też bardziej rozbudowane narzędzia, przedstawiające dodatkowe informacje o badanej siecji jak na przykład wersja systemu operacyjnego na komputerach w sieci czy też działające usługi sieciowe. Taki oględny skan jest nie tylko wstępem do ataku na daną sieć, lecz może być także świetnym punktem startowym w przypadku, gdy chcemy stworzyć lub wzmocnić zabezpieczenia już istniejące. Aktualnie na rynku znajduję się sporo narzędzi, które można wykorzystać w tym celu, w tej pracy jednak nacisk położony zostanie na zobrazowanie wydajności poszczególnych metod skanowania sieci oraz na przystępną wizualizaję przeprowadzonej analizy sieci z wykorzystaniem interaktywanych diagramów, wykresów i map sieci.

Konieczne zatem stało się zapewnienie poufności oraz auten- tyczności, jednym słowem bezpieczeństwa przesyłanych tym medium danych. Mam na myśli zapobiegnięcie ich podsłuchaniu, nieautoryzowanemu spreparowaniu, przejęciu se- sji lub też uniemożliwieniu w ogóle komunikacji sieciowej (Atak DoS - Deny Of Service). Skutki takich ataków podczas komunikacji np. z bankiem, czy też wewnątrz firmy mogą być paraliżujące na dużą skalę, w konsekwencji - wyjątkowo kosztowne.

1.1. Cele pracy

Celem poniższej pracy jest zaprojektowanie i stworzenie rozbudowanego narzędzia do prowadzenia testów penetracyjnch na sieciach komputerowych małych i średnich rozmiarów, opartych na skanowaniu obecności usług sieciowych z wykorzystaniem jak największej ilości protokołów sieciowych i technik wyszukiwania. Dodatkowo ńależyśtworzyć podsystem wizualizacji wyników (w postaci diagramów lub map topologii sieci), umożliwiający interaktywne prowadzenie dalszych testów penetracyjnych na wybranych jednostkach. Dodatkowo należy dokonać analizy porównawczej wyników procesów skanowania

prowadzonych z przyjęciem różnych priorytetów i kryteriów (czas, wydajność, ąnonimowośćśkanera, poziom ingerencji).

Wybrane rozwiązania zostaną zaprojektowane, wdrożone i zweryfikowane w przykładowej sieci korporacyjnej firmy mającej 6 oddziałów

1.2. Zawartość pracy

W rodziale 2 przedstawiono podstawowe informacje dotyczące struktury dokumentów w LaTeXu. Alvis [**?**] jest językiem

Praca niniejsza składa się z 11 rozdziałów. W rozdziale pierwszym zaprezentowano genezę sieci komputerowych, opis technologii używanych do budowy sieci rozległych, Internetu i protokołu IP. Rozdziały drugi i trzeci poruszają tematy związane z zagrożeniami przesyłania danych poprzez sieć publiczną oraz opis procesów bezpieczeństwa. W rozdziale czwartym znajdują się szczegółowe informacje o technologiach umożliwiających zabezpieczenie danych podczas tranzytu.

2. Pierwszy dokument

W rozdziale tym przedstawiono podstawowe informacje dotyczące struktury prostych plików LaTeXa. Omówiono również metody kompilacji plików z zastosowaniem programów *latex* oraz *pdflatex*.

2.1. Struktura dokumentu

Plik LaTeXowy jest plikiem tekstowym, który oprócz tekstu zawiera polecenia formatujące ten tekst (analogicznie do języka HTML). Plik składa się z dwóch części:

1. Preambuły – określającej klasę dokumentu oraz zawierającej m.in. polecenia dołączającej dodatkowe pakiety;
2. Części głównej – zawierającej zasadniczą treść dokumentu.

```
\documentclass[a4paper,12pt]{article}        % preambuła
\usepackage[polish]{babel}
\usepackage[utf8]{inputenc}
\usepackage[T1]{fontenc}
\usepackage{times}

\begin{document}                             % część główna

\section{Sztuczne życie}

% treść
% ąśężźćńłóĘŚĄŻŹĆŃÓŁ

\end{document}
```

Nie ma żadnych przeciwskazań do tworzenia dokumentów w LaTeXu w języku polskim. Plik źródłowy jest zwykłym plikiem tekstowym i do jego przygotowania można użyć dowolnego edytora tekstów, a polskie znaki wprowadzać używając prawego klawisza `Alt`. Jeżeli po kompilacji dokumentu polskie znaki nie są wyświetlane poprawnie, to na 95% źle określono sposób kodowania znaków (należy zmienić opcje wykorzystywanych pakietów).

2.2. Kompilacja

Załóżmy, że przygotowany przez nas dokument zapisany jest w pliku `test.tex`. Kolejno wykonane poniższe polecenia (pod warunkiem, że w pierwszym przypadku nie wykryto błędów i kompilacja zakończyła się sukcesem) pozwalają uzyskać nasz dokument w formacie pdf:

```
latex test.tex
dvips test.dvi -o test.ps
ps2pdf test.ps
```

lub za pomocą PDFLaTeX:

```
pdflatex test.tex
```

Przy pierwszej kompilacji po zmiane tekstu, dodaniu nowych etykiet itp., LaTeX tworzy sobie spis rozdziałów, obrazków, tabel itp., a dopiero przy następnej kompilacji korzysta z tych informacji.

W pierwszym przypadku rysunki powinny być przygotowane w formacie eps, a w drugim w formacie pdf. Ponadto, jeżeli używamy polecenia `pdflatex test.tex` można wstawiać grafikę bitową (np. w formacie jpg).

2.3. Narzędzia

Do przygotowania pliku źródłowego może zostać wykorzystany dowolny edytor tekstowy. Niektóre edytory, np. Emacs, mają wbudowane moduły ułatwiające składanie tekstów w LaTeXu (kolorowanie składni, skrypty kompilacji, itp.).

Jednym z bardziej znanych środowisk do składania dokumentów LaTeXa jest *Kile*. Aplikacja dostępna jest dla środowiska KDE począwszy od wersji 2. Zawiera edytor z podświetlaną składnią, zestawy poleceń LaTeXa, zestawy symboli matematycznych, kreatory tabel, macierzy, skrypty kompilujące i konwertujące podpięte są do poleceń w menu aplikacji (i pasków narzędziowych), dostępne jest sprawdzanie pisowni, edytor obsługuje projekty (tzn. dokumenty składające się z wielu plików), umożliwia przygotowanie i zarządzanie bibliografią, itp.

Na stronie `http://kile.sourceforge.net/screenshots.php` zamieszczono kilkanaście zrzutów ekranu środowiska *Kile*, które warto przejrzeć, by wstępnie zapoznać się z możliwościami programu.

Bardzo dobrym środowiskiem jest również edytor gEdit z wtyczką obsługującą LaTeXa. Jest to standardowy edytor środowiska Gnome. Po instalacji wtyczki obsługującej LaTeXa, edytor nie ustępuje funkcjonalnościom środowisku Kile, a jest zdecydowanie szybszy w działaniu. Lista dostępnych wtyczek dla tego edytora znajduje się pod adresem `http://live.gnome.org/Gedit/Plugins`. Inne polecane wtyczki to:

– Edit shortcuts – definiowanie własnych klawiszy skrótu;

– Line Tools – dodatkowe operacje na liniach tekstu;

– Multi-edit – możliwość jednoczesnej edycji w wielu miejscach tekstu;

– Zoom – zmiana wielkości czcionki edytora z użyciem rolki myszy;

– Split View – możliwość podziału okna edytora na 2 części.

2.4. Przygotowanie dokumentu

Plik źródłowy LaTeXa jest zwykłym plikiem tekstowym. Przygotowując plik źródłowy warto wiedzieć o kilku szczegółach:

– Poszczególne słowa oddzielamy spacjami, przy czym ilość spacji nie ma znaczenia. Po kompilacji wielokrotne spacje i tak będą wyglądały jak pojedyncza spacja. Aby uzyskać *twardą spację*, zamiast znaku spacji należy użyć znaku *tyldy*.

– Znakiem końca akapitu jest pusta linia (ilość pusty linii nie ma znaczenia), a nie znaki przejścia do nowej linii.

– LaTeX sam formatuje tekst. **Nie starajmy się go poprawiać**, chyba, że naprawdę wiemy co robimy.

Nessus nmap