



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

VIZUALIZACE SÍŤOVÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

VISUALIZATION OF NETWORK SECURITY EVENTS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

PETR STEHLÍK

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. PAVEL KROBOT

BRNO 2016

Abstrakt

Do tohoto odstavce bude zapsán výtah (abstrakt) práce v českém jazyce.

Abstract

Do tohoto odstavce bude zapsán výtah (abstrakt) práce v anglickém jazyce.

Klíčová slova

Sem budou zapsána jednotlivá klíčová slova v českém jazyce, oddělená čárkami.

Keywords

Sem budou zapsána jednotlivá klíčová slova v anglickém jazyce, oddělená čárkami.

Citace

Petr Stehlík: Vizualizace síťových bezpečnostních událostí, bakalářská práce, Brno, FIT VUT v Brně, 2016

Vizualizace síťových bezpečnostních událostí

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Ing. Pavla Krobota. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....

Petr Stehlík

5. dubna 2016

Poděkování

V této sekci je možno uvést poděkování vedoucímu práce a těm, kteří poskytli odbornou pomoc (externí zadavatel, konzultant, apod.).

© Petr Stehlík, 2016.

Tato práce vznikla jako školní dílo na Vysokém učení technickém v Brně, Fakultě informačních technologií. Práce je chráněna autorským zákonem a její užití bez udělení oprávnění autorem je nezákonné, s výjimkou zákonem definovaných případů.

Obsah

1 Úvod	2
2 Monitoring síť	3
2.1 Nemea	3
2.2 IDEA	4
2.3 Další monitorovací systémy	4
3 Technologie	5
3.1 Dostupné technologie	5
3.2 Výběr technologií	5
3.3 Zvolené technologie	5
4 Architektura aplikace	6
4.1 Případy užití	6
4.2 REST API	6
4.3 Databáze událostí	6
4.4 GUI	6
5 Implementace	7
5.1 Backend	7
5.2 Frontend	7
5.3 Zabezpečení	7
5.4 Distribuce	7
6 Dosažené výsledky	8
6.1 Názory uživatelů	8
6.2 Nasazení v praxi	8
7 Závěr	9
Literatura	10
Přílohy	11
Seznam příloh	12

Kapitola 1

Úvod

Počítačové sítě, zejména Internet, v dnešním světě zaujímají jednu z nejvýznamnějších rolí. Počínaje výzkumem a vědeckými experimenty, konče běžným životem většiny lidí. Jen za posledních deset let se počet uživatelů Internetu více než ztrojnásobil z cca jedné miliardy lidí na tři miliardy. Počítačové sítě propoují celý svět a jsou neustále rozšiřovány, vylepšovány a modernizovány. To vede k větším nárokům na použité technologie a zdroje.

Avšak se zvyšujícím počtem uživatelů roste i počet útoků na různé počítačové sítě, kterými se útočníci snaží získat informace či poškodit oběť. Síťový útok[1] je definován jako záměrný akt, kde se entita snaží překonat bezpečnostní služby a porušit bezpečnost systému. Vznikají tím pádem systémy na detekci takovýchto útoků, aby správci sítí dokázali reagovat na vzniklou situaci.

Jeden z těchto systémů vznikl ve sdružení CESNET s názvem Nemea. Tento framework analyzuje síťový provoz a zaznamenává podezřelé toky jako agregované události do databáze. Na větší síti (stovky až tisíce připojených zařízení) je takovýchto událostí vytvořeno až několik tisíc denně. S tím nastává problém jak dané události jednoduše analyzovat a rozpoznat na jaké události se zaměřit a na které nebrát zřetel.

Cílem této bakalářské práce je vytvořit aplikaci pro vizuální analýzu bezpečnostních událostí na síti monitorované s pomocí frameworku Nemea, tak aby správce sítě dokázal rychle a jednoduše rozpoznat významný útok na síť. Důležitým aspektem vytvořené aplikace je důraz na použití moderních knihoven podporující tvorbu dynamických webových aplikací, které jsou dostupné na různých typech zařízeních. Společně s tím je kladen důraz na uživatelskou přívětivost a jednoduchost prostředí, ve kterém bude probíhat vizuální analýza událostí.

Aplikace bude pracovat s konkrétním formátem dat nazvaný IDEA. Tento formát dat je specifikován sdružením CESNET a slouží jako prostředek pro sdílení dat bezpečnostních událostí mezi různými systémy. Díky tomu lze systém kdykoliv přenést na jiný zdroj databáze než je systém Nemea, např. v rámci sdružení CESNET na systém Warden.

Celou aplikaci navíc bude možno libovolně přizpůsobit tak, aby vyhovovala potřebám daného správce sítě. V aplikaci bude zavedena i technika zvaná *drill-down*, která napomáhá rychlé a přehledné analýze velkého množství dat bez ztráty informací o analyzované události.

Aplikace bude integrována do současného Nemea frameworku pod názvem Nemea Dashboard a bude s ním společně distribuována jako front end celého systému.

Kapitola 2

Monitoring sítě

V majoritních sítích jako např. páteřní či firemní síť je téměř nutností monitorovat provoz na síti, abychom byli informováni o jejím aktuálním stavu.

Monitoring lze rozdělit do dvou částí. Aktivní a pasivní způsob.

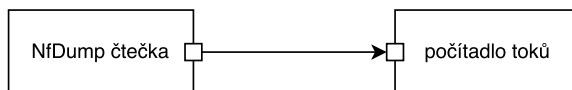
2.1 Nemea

Network Measurements Analysis, zkráceně Nemea, je framework, který dovoluje seskládat systém pro automatizovanou analýzu toků získaných ze síťového monitoringu v reálném čase. Systém se skládá z oddělených stavebních bloků nazývané moduly. Tyto jednotlivé moduly jsou následně propojeny pomocí rozhraní.

Moduly jsou nezávislé pracovní jednotky, které obecně přijímají proud dat na svých vstupech, zpracují či zanalyzují daná data a následně je odešlou ze svých výstupních rozhraní jako proud dat pro další moduly. Modul může například tvořit statistiky o přijatých datech a na základě těchto statistik detekovat určité typy síťového útoku. Detekovaný útok je popsán datovým záznamem, který je odeslán přes výstupní rozhraní dalším modulům, které s daným záznamem dále pracují, např. jej uloží v IDEA formátu (viz sekce 2.2) do databáze nebo ze získaných statistik dokáží detekovat anomálie v síťovém provozu a dokáží tak jednotlivé pokusy od jednoho útočníka agregovat a zpracovat jej jako jediný útok skládající se z několika desítek až stovek pokusů o útok, které odděleně nemají význam a administrátor sítě by je snadno přehlédl nebo ignoroval.

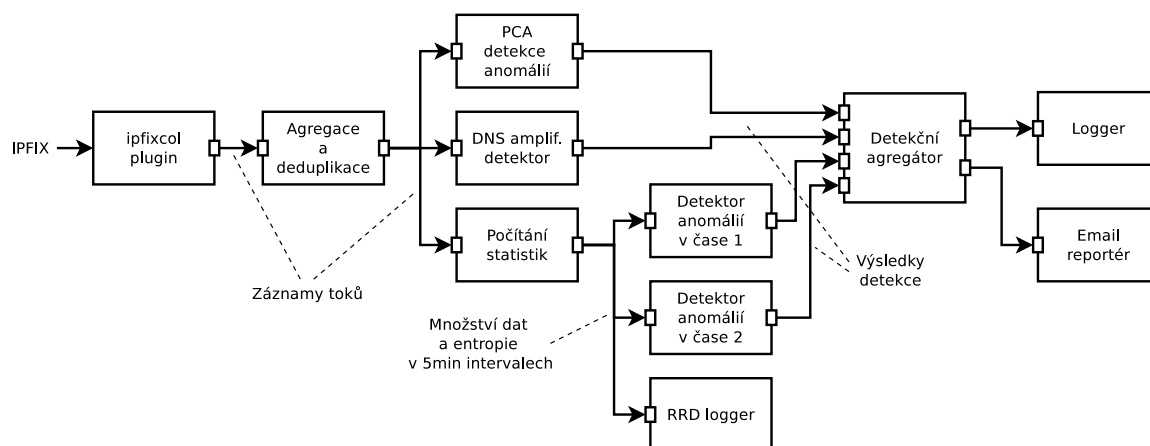
Jednotlivé moduly nemají osamoceně velký význam, ale pokud tyto moduly spojíme ve složitější systém, získáme komplexní nástroj na aktivní analýzu síťových dat schopný detekovat a identifikovat útoky na monitorovanou síť, který následně detekované útoky uloží do databáze a webová aplikace, kterou v této práci navrhujeme, uložené útoky zobrazí.

Nemea je také schopná přístupu “store-and-ex-post”, který lze vidět na obrázku 2.1. Jsou zde dva moduly spojené jedním rozhraním. První modul čte záznamy toků ze souboru a druhý modul počítá statistiky těchto přečených toků.



Obrázek 2.1: Minimální příklad Nemea systému

Z takto základních bloků lze postavit i velmi komplexní systém jak je vidět na obrázku 2.2, kde jsou data přijímána v reálném čase z IPFIX[2] kolektoru



Obrázek 2.2: Minimální příklad Nemea systému

Hlavní komponenty

Modul

libtrap

UniRec

2.2 IDEA

2.3 Další monitorovací systémy

Kapitola 3

Technologie

3.1 Dostupné technologie

3.2 Výběr technologií

3.3 Zvolené technologie

Kapitola 4

Architektura aplikace

4.1 Případy užití

4.2 REST API

4.3 Databáze událostí

4.4 GUI

Kapitola 5

Implementace

5.1 Backend

5.2 Frontend

5.3 Zabezpečení

5.4 Distribuce

Kapitola 6

Dosažené výsledky

6.1 Názory uživatelů

6.2 Nasazení v praxi

Kapitola 7

Závěr

Závěrečná kapitola obsahuje zhodnocení dosažených výsledků se zvlášť vyznačeným vlastním přínosem studenta. Povinně se zde objeví i zhodnocení z pohledu dalšího vývoje projektu, student uvede náměty vycházející ze zkušeností s řešeným projektem a uvede rovněž návaznosti na právě dokončené projekty.

Literatura

- [1] Shirey, R.: Internet Security Glossary, Version 2. RFC 4949, RFC Editor, Srpen 2007.
URL <https://tools.ietf.org/html/rfc4949>
- [2] Velan Petr, K. R.: Flow Information Storage Assessment Using IPFIXcol. In *Lecture Notes in Computer Science 7279*, Springer, 2012, ISBN 978-3-642-30632-7.

Přílohy

Seznam příloh