STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**/Uviesť názov práce/**

/uviesť podtitul, ak ho práca má, inak riadok vynechať/

**Juraj Petrina**

2013

Obsah (štýl Nadpis Kapitoly, bez čísla)

Úvod 4

1 Jadro práce 5

1.1 Názov podkapitoly 5

1.1.1 Názov časti podkapitoly 5

2 Ilustrácie, tabuľky, rovnice 6

2.1 Ilustrácie 6

2.2 Tabuľky 6

2.3 Zdrojový kód programu 7

2.4 Rovnice, vzorce 7

3 Záver 8

Zoznam použitej literatúry 9

Prílohy 10

Príloha A – CD médium 10

Príloha B – Metodické listy 10

Príloha C – Dotazník 10

Poznámka: Obsah formátujte tak, aby sa zmestil celý na stranu 2

Anotácia (štýl Nadpis Kapitoly, bez čísla)

Tento projekt sa zaoberá vytvorením sieťového monitoru s vizualizáciou na osobnom počítači s využitím nástrojov Wireshark a Grafana. Cieľom projektu je sledovanie sieťového prevozu, analýza dát a vizualizácia v reálnom čase pomocou interaktívnych grafov a panelov.

Na začiatku projektu bol nainštalovaný a konfigurovaný nástroj Wireshark na sledovanie sieťového prevozu. Pomocou Wiresharku boli zachytávané dáta, ktoré následne slúžili ako vstup pre monitorovanie a vizualizáciu.

Následne bol nainštalovaný a konfigurovaný nástroj Grafana, ktorý slúžil na vizualizáciu sieťového prevozu. Grafana bola pripojená k databáze zachytávaných dát a umožňovala vytváranie interaktívnych grafov a panelov na základe týchto dát.

Po nastavení boli vytvorené notifikácie, ktoré upozorňovali na neobvyklý sieťový prevoz a anomálie. Taktiež bolo nastavené periodické měření síťového provozu a zabezpečenie nástrojov Wireshark a Grafana.

Výsledkom projektu je funkčný sieťový monitor s vizualizáciou, ktorý umožňuje sledovať a analyzovať sieťový prevoz a detekovať potenciálne problémy v reálnom čase.

**Annotation**

This project deals with the creation of a network monitor with visualization on a personal computer using Wireshark and Grafana tools. The goal of the project is to monitor network traffic, analyze data and visualize it in real time using interactive graphs and panels.

At the beginning of the project, Wireshark was installed and configured to monitor network traffic. Data was captured using Wireshark, which subsequently served as input for monitoring and visualization.

Subsequently, the Grafana tool was installed and configured, which was used to visualize the network transport. Grafana was connected to the database of captured data and enabled the creation of interactive graphs and panels based on this data.

Once set up, notifications were created to warn of unusual network traffic and anomalies. Periodic measurement of network traffic and provision of Wireshark and Grafana tools were also set.

The result of the project is a functional network monitor with visualization that allows you to monitor and analyze network traffic and detect potential problems in real time.

Použité nástroje a ďalšie informácie

WireShark

Popis

Wireshark je open-source nástroj na analýzu sieťovej prevádzky. Umožňuje zachytávanie a analýzu dátových paketov v reálnom čase a je k dispozícii pre rôzne operačné systémy.

Dôvody výberu:

* Bohaté funkcie: Wireshark poskytuje širokú škálu funkcií pre analýzu sieťovej prevádzky, vrátane filtrovania, dekódovania protokolov a sledovania prenosových rýchlostí.
* Open-source a zadarmo: Wireshark je open-source projekt, čo znamená, že je zadarmo na použitie a má širokú podporu komunity.
* Flexibilita: Je kompatibilný s rôznymi operačnými systémami a umožňuje analýzu sieťovej prevádzky na rôznych úrovniach abstrakcie.

Nevýhody:

* Vysoká náročnosť na systém: Pri dlhodobom sledovaní môže Wireshark spotrebovať značné množstvo systémových prostriedkov, najmä pamäte.

Funkčnosť

Wireshark je veľmi podobný tcpdump, ale má grafický front-end a integrované možnosti triedenia a filtrovania.

Wireshark umožňuje používateľovi uviesť ovládače sieťového rozhrania do promiskuitného režimu (ak to ovládač sieťového rozhrania podporuje), takže môžu vidieť všetku premávku viditeľnú na tomto rozhraní vrátane jednosmernej prevádzky, ktorá nie je odoslaná na MAC adresu radiča sieťového rozhrania. Avšak pri zachytávaní pomocou analyzátora paketov v promiskuitnom režime na porte sieťového prepínača nie je všetka prevádzka cez prepínač nevyhnutne odoslaná do portu, kde sa zachytávanie vykonáva, takže zachytávanie v promiskuitnom režime nemusí nevyhnutne postačovať na zobrazenie celej siete. dopravy. Zrkadlenie portov alebo rôzne sieťové klepnutia rozšíria zachytávanie do akéhokoľvek bodu v sieti. Jednoduché pasívne kohútiky sú mimoriadne odolné voči manipulácii

História

Koncom 90-tych rokov pracoval Gerald Combs, absolvent informatiky na University of Missouri-Kansas City, pre malého poskytovateľa internetových služieb. Komerčné produkty na analýzu protokolov v tom čase mali cenu okolo 1500 $[6] a nebežali na primárnych platformách spoločnosti (Solaris a Linux), takže Gerald začal písať Ethereal a prvú verziu vydal okolo roku 1998.[7] Ochrannú známku Ethereal vlastní spoločnosť Network Integration Services.

V máji 2006 Combs prijal prácu v CACE Technologies u Lorisa Degioanniho. Combs stále držal autorské práva na väčšinu zdrojového kódu Etherealu (a zvyšok bol redistribuovateľný pod GNU GPL), takže ako základ pre úložisko Wireshark použil obsah úložiska Ethereal Subversion. Nevlastnil však ochrannú známku Ethereal, a tak zmenil názov na Wireshark.

Funkcie

Wireshark je program na zachytávanie dát, ktorý „rozumie“ štruktúre (zapuzdreniu) rôznych sieťových protokolov. Dokáže analyzovať a zobraziť polia spolu s ich významom, ako je špecifikované rôznymi sieťovými protokolmi. Wireshark používa pcap na zachytávanie paketov, takže môže zachytávať pakety len na typoch sietí, ktoré pcap podporuje.

Dáta je možné zachytiť „z drôtu“ zo živého sieťového pripojenia alebo prečítať zo súboru už zachytených paketov.

Živé dáta je možné čítať z rôznych typov sietí vrátane Ethernetu, IEEE 802.11, PPP a spätnej slučky.

Zachytené sieťové dáta je možné prehliadať cez GUI alebo cez terminálovú (príkazový riadok) verziu utility, TShark.

Zachytené súbory je možné programovo upravovať alebo konvertovať pomocou prepínačov príkazového riadku do programu „editcap“.

Zobrazenie údajov je možné spresniť pomocou filtra zobrazenia.

Na rozoberanie nových protokolov je možné vytvoriť zásuvné moduly.[23]

VoIP hovory v zachytenej prevádzke môžu byť detekované. Ak je zakódovaný v kompatibilnom kódovaní, možno tok médií dokonca prehrať.

Je možné zachytiť surovú prevádzku USB.[24]

Bezdrôtové pripojenia môžu byť tiež filtrované, pokiaľ prechádzajú cez monitorovaný Ethernet.[potrebné vysvetlenie]

Je možné nastaviť rôzne nastavenia, časovače a filtre, aby sa zabezpečilo filtrovanie výstupu zachytenej prevádzky.

Natívne formáty súborov sledovania siete Wireshark sú formát libpcap, ktorý čítajú a zapisujú libpcap, WinPcap a Npcap

Grafana

* 1. Popis

Grafana je open-source platforma pre vizualizáciu dát a monitorovanie. Umožňuje vytváranie interaktívnych grafov, panelov a dashboardov na základe dát z rôznych zdrojov.

Dôvody výberu:

* Flexibilita: Grafana podporuje mnoho rôznych typov databáz a zdrojov dát, čo umožňuje jednoduchú integráciu s rôznymi systémami a nástrojmi.
* Vizuálna atraktivita: Grafana poskytuje širokú škálu vizualizačných možností, vrátane grafov, tabuliek, panelov a dashboardov, ktoré je možné ľahko prispôsobiť podľa potrieb užívateľa.
* Široká podpora komunity: Grafana má veľkú a aktívnu komunitu užívateľov, čo znamená, že je ľahké nájsť pomoc, tutoriály a rozšírenie.

Nevýhody:

* Zložitejšie nastavenia: Nastavenie Grafany môže byť zložitejšie, najmä pri integrácii s niektorými typmi databáz.

História

Grafana bola prvýkrát vydaná v roku 2014 Torkelom Ödegaardom ako odnož projektu na Orbitz. Zamerala sa na databázy časových radov, ako sú InfluxDB, OpenTSDB a Prometheus, ale vyvinula sa na podporu relačných databáz, ako sú MySQL, PostgreSQL a Microsoft SQL Server.

V roku 2019 spoločnosť Grafana Labs zabezpečila financovanie série A vo výške 24 miliónov dolárov. V kole financovania série B v roku 2020 získala 50 miliónov dolárov. V kole financovania Labs Series C v roku 2021 Grafana zabezpečila 220 miliónov dolárov.

Produkty

Open source

* Loki – platforma na agregáciu protokolov založená na Prometheus prvýkrát sprístupnená v roku 2019
* Mimir – nástroj na metrickú vizualizáciu vydaný v roku 2022, ktorý nahradil Cortex
* Tempo - nástroj na sledovanie protokolov, vydaný v roku 2021

SNMP

Jednoduchý manažérsky protokol siete alebo jednoduchý protokol manažérstva siete (angl. Simple Network Management Protocol), skr. SNMP, je protokol umožňujúci monitorovanie a správu zariadení v IP sieti. Primárne bol navrhnutý pre účely správy siete a týkal sa základných sieťových prvkov, napr. smerovačov čomu zodpovedala štandardná MIB báza. Protokol sa však nakoniec uplatnil aj pri správe a monitorovaní ďalších zariadení pripojených v sieti, napríklad sieťových tlačiarní, serverov či koncových užívateľských staníc

**Architektúra**

Architektúra SNMP rozoznáva prinajmenšom 2 komponenty:

Spravovaný objekt (SNMP agent, napr. na prepínači)

Spravovacia stanica (napr. SNMP platforma)

Môže obsahovať subagentov (slave).

**Verzie SNMP protokolu**

SNMPv1

Prvá verzia SNMP protokolu bola definovaná v roku 1988

SNMPv2

Verzia 2 SNMP protokolu sa snažila odstrániť nedostatky SNMPv1. Vzniklo mnoho jej odnoží ktoré riešili bezpečnosť a rozšírenia protokolu. Nakoniec sa stala prakticky štandardom SNMP v2c

SNMPv3

Internet Engineering Task Force (IETF) ustanovuje od roku 2004 verziu SNMPv3

Záver

Záver obsahuje vecné závery, sumarizáciu, vlastný prínos alebo pohľad autora, odporúčania pre prax (výučbu). Záver je uvedený na maximálne 1 stranu.

Zoznam použitej literatúry (Nadpis Kapitoly, bez čísla)

Všetky dokumenty, ktoré v práci použijete, je potrebné zoradiť do zoznamu pozostávajúceho z  bibliografických odkazov, ktorý označujeme **Zoznam použitej literatúry**. Pre tvorbu zoznamov použitej literatúry platia štandardy. Cieľom je, aby zo zoznamu použitej literatúry bolo možné jasne identifikovať použitý zdroj a aby ho bolo možné bez ťažkostí opäť vyhľadať.

Hlavným zdrojom údajov pre tvorbu bibl. odkazov je **titulný list** (tzn. prvý list v knihe, kde sú uvedené údaje o názve autorovi atď.), príp. jeho rub. Odkazy sa môžu týkať knižných, časopiseckých a iných zdrojov informácií (zborníky z konferencií, patentové dokumenty, normy, odporúčania, kvalifikačné práce, osobná korešpondencia a rukopisy, odkazy cez sprostredkujúci zdroj, elektronické publikácie), ktoré boli v práci použité.

**Technika citovania** určuje spôsob, akým označujeme citácie v dokumente, pričom podľa normy (pozri STN ISO 690) existuje viacero spôsobov citovania. Pri metóde **číselných citácií** sa v zozname bibliografických odkazov každé citované dielo uvádza v tom poradí, v akom bolo uvedené a číslované v texte. Číslované odkazy v texte sú uvedené v zátvorkách [3] a odkazujú na dokumenty v takom poradí, v akom sa citujú po prvýkrát. Nasledujúce citácie dostávajú také isté číslo, ako má prvá citácia. Ak sa citujú osobitné časti dokumentu, môžu sa za číslom citácie uviesť čísla strán.

**Príklad zoznamu použitej literatúry:**

1. KALAŠ, Ivan – BLAHO, Andrej: *Tvorivá informatika. 1. zošit z programovania.* Bratislava: SPN - Mladé letá, 2007. 48. s. ISBN 80-10-01723-2
2. CIMBALA, Roman – BALOGH, Jozef – DŽMURA, Jaroslav: Diagnostika výkonových transformátorov s využitím prvkov umelej inteligencie 1. In: *Elektrotechnický magazín ETM*. roč. 14, č. 1 (2004), s. 8-9.
3. Kolektív autorov: *Štátny vzdelávací program*. [online] Bratislava: ŠPU v Bratislave, 2008. Aktualizované 14.2.2010 [cit. 2010-02-17]. Dostupné na internete: <http://new.statpedu.sk/sk/filemanager/download/987>
4. Elektronické diplomové a dizertačné práce SR: ETD SK. [online]. Košice : ETD SK, 2004. Aktualizované 14-2-2005 [cit 2005-03-10]. Dostupné na internete: <http://www.etd.sk/>.
5. KATUŠČÁK, Dušan: *Ako písať záverečné a kvalifikačné práce*. Nitra: Enigma, 2004. 162 s. il. ISBN 80-89132-10-3

Prílohy (štýl Nadpis Kapitoly, bez čísla)

Zoznam príloh záverečnej práce:

* Príloha A – CD médium
* Príloha B – <názov prílohy>
* Príloha C – <názov prílohy>

Táto časť záverečnej práce obsahuje zoznam všetkých príloh. Číslovanie strán príloh nadväzuje na číslovanie strán v hlavnom texte.

Príloha A – CD médium (štýl PodNadpis Kapitoly, bez čísla)

Priložené CD médium **povinne** obsahuje text záverečnej práce vo formáte PDF. CD môže obsahovať edukačný hypertext, metodické listy, dotazníky a ukážky projektov atď. CD médium zabalené do papierového obalu sa vlepí na vnútornú stranu zadnej obálky záverečnej práce.

Príloha B – <názov prílohy>

<popis prílohy>

Príloha C – <názov prílohy>

<popis prílohy>