



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

POKROČILÝ FTP SERVER

ADVANCED FTP SERVER

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

Jan Matoušek

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Tomáš Horváth, Ph.D.

BRNO 2018



Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Jan Matoušek

ID: 186137

Ročník: 3

Akademický rok: 2017/18

NÁZEV TÉMATU:

Pokročilý FTP server

POKYNY PRO VYPRACOVÁNÍ:

Cílem bakalářské práce je konfigurace glFTPd démonu pro přenos datových souborů s kontrolou kontrolních součtů v reálném čase. Student dále implementuje potřebné balíčky pro tvorbu požadavků o nahrání souborů a průběžnou správou statistik. Veškerou datovou komunikaci zabezpečte před neznámějšími útoky.

DOPORUČENÁ LITERATURA:

[1] CHARALABIDIS, Alexander. The book of IRC. Berkeley, Calif.: Publishers Group West [distributor], c2000. ISBN 978-1886411296.

[2] GIFTpD :: We make files transfer! [online]. ©2017. Dostupné z: <https://glftpd.eu/>

Termín zadání: 5.2.2018

Termín odevzdání: 29.5.2018

Vedoucí práce: Ing. Tomáš Horváth, Ph.D.

Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Tato bakalářská práce se zabývá protokolem FTP a jeho možnostmi ověřování kontrolních CRC součtů, třídění multimediálních dat podle autorů, žánrů, roků a tvorbě statistik přenosu. Tyto možnosti byly ukázány na FTP serveru GIFTPd. Do GIFTPd byl nainstalován plugin PZS-NG umožňující další nastavení. Byl také nainstalován IRC robot Eggdrop, který při použití skriptu ngBot z PZS-NG umožní vypsát informace o nahrávaných souborech a serveru na IRC kanál. GIFTPd byl nainstalován na fyzický stroj s linuxovou distribucí Debian.

KLÍČOVÁ SLOVA

Eggdrop, GIFTPd, Linux, ngBot, PZS-NG

ABSTRACT

This bachelor thesis deals with the FTP protocol and its possibilities to verify CRC checksums, to sort multimedia data by authors, genres, years and to create transmission statistics. These options were shown on FTP server GIFTPd. A PZS-NG plugin has been installed in GIFTPd for further setup. An IRC bot Eggdrop has also been installed. It allows the displaying of the information about the uploaded files and the server information to an IRC channel when using the ngBot script from PZS-NG. GIFTPd has been installed on a physical machine with a Debian Linux distribution.

KEYWORDS

Eggdrop, GIFTPd, Linux, ngBot, PZS-NG

MATOUŠEK, Jan. *Pokročilý FTP server*. Brno, 2018, 57 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Tomáš Horváth, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Pokročilý FTP server“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno

.....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu Ing. Tomáši Horváthovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno

.....

podpis autora

Obsah

Úvod	8
1 FTP	9
1.1 Řídící spojení	9
1.2 Datové spojení	9
1.3 Aktivní režim	9
1.4 Pasivní režim	10
1.5 Adresace	10
1.6 Reprezentace dat	11
1.7 Možnosti přenosu	12
1.8 Příkazy FTP	12
1.9 Odpovědi FTP	13
1.10 Příklad použití příkazů a odpovědí	14
1.11 Modifikace FTP	14
2 IRC	16
3 Eggdrop	18
3.1 Instalace	18
3.2 Konfigurace	18
4 Debian	21
4.1 Iptables	22
4.2 SSH	22
5 FTP démoni	24
5.1 GFTPd	24
5.1.1 Instalace	24
5.1.2 Konfigurace	24
5.1.3 PZS-NG	26
5.2 Konfigurace pomocí SITE příkazů	29
6 Postup realizace	32
6.1 Firewall	32
6.2 GFTPd	33
6.2.1 Zabezpečení	33
6.2.2 Tvorba požadavků	34
6.3 Propojení s IRC	34

6.3.1	Eggdrop	34
6.3.2	NgBot	37
6.4	Zavedení SSL do mIRC a FTP Rush	38
6.5	Ukázka funkčnosti GIFTPd	38
7	Závěr	43
	Literatura	44
	Seznam symbolů, veličin a zkratk	46
	Seznam příloh	47
A	Změněné konfigurační soubory	48
A.1	glftpd.conf	48
A.2	zsconfig.h	50
A.3	robot.conf	52
A.4	ngBot.conf	54
B	Obsah DVD	57

Úvod

V této bakalářské práci je představen jeden z protokolů pro přenos souborů, a to FTP. Tento protokol je v dnešní době hojně používaný pro přenos souborů například na úložiště webových serverů. Některé programy mají na tzv. FTP serverech s anonymním přihlášením zveřejněny například své instalační soubory.

Dále je vybrán FTP démon GFTPd, který bude nainstalován na distribuci GNU/Linuxu nesoucí název Debian. Jsou popsány vlastnosti, instalace a konfigurace GFTPd. Dalším cílem je ověřit, zdali je démon schopen třídít soubory dle žánrů nebo ověřovat kontrolní součty nahrávaných souborů za použití pluginů.

První kapitola obsahuje informace o protokolu FTP, popisuje jeho režimy a možnosti přenosu, reprezentaci dat, příkazy a odpovědi a také modifikace FTP, které přidávají zabezpečení přenosu v podobě šifrování.

Další kapitola obsahuje informace o IRC, například o možných příkazech nebo oprávněních. Dále je popsána instalace a konfigurace IRC robota Eggdrop, který je použit pro vypisování informací o nahrávaných souborech na kanál vybraného IRC serveru. V kapitole Debian jsou uvedeny základní informace o této distribuci a několik příkazů používaných v této distribuci. Jsou zde také uvedeny informace o firewallu a protokolu SSH.

Následně je popsána instalace a konfigurační volby FTP démona GFTPd. V této kapitole je uveden i plugin umožňující třídění a ověřování kontrolních součtů nahrávaných souborů. Dále jsou uvedeny informace o skriptu ngBot, který umožňuje vypisování údajů o třídění na IRC kanál.

Poslední kapitola je věnována realizaci. Pro samotnou realizaci bylo nezbytné vybrat i vhodné zabezpečení pomocí firewallu, nastavení některých voleb GFTPd démona, konfigurace Eggdrop a konfigurace ngBot a jeho začlenění do Eggdrop.

1 FTP

FTP (File Transfer Protocol) je aplikačním protokolem vrstevného modelu TCP/IP (Transmission Control Protocol/Internet Protocol). Využívá dvě TCP spojení transportní vrstvy označované jako řídicí (kontrolní) a datové.[1, 2] Jedná se o textově orientovaný protokol pracující na principu klient-server, tzn. existuje server, kam jsou připojeni jednotliví klienti (například osobní počítače). Textové příkazy jsou posílány v paketech, které mohou být odchyceny a bez větších problémů přečteny. Nejedná se o nový protokol. FTP byl definován v RFC 114 (Request for Comments) dostupný například na: tools.ietf.org/html/rfc114. Aktuální je definice v RFC 959 [1], které vyšlo v říjnu roku 1985 a s použitím aktualizací RFC je dnes stále využíváno převážně ke sdílení souborů.[1]

1.1 Řídicí spojení

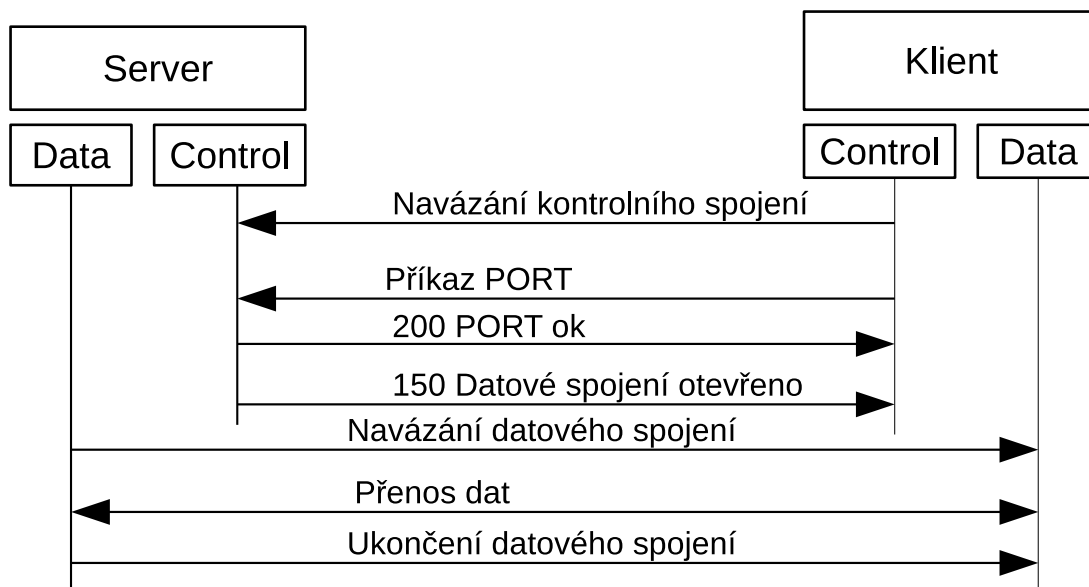
Toto spojení je standardně navázáno na portu TCP/21. Po tomto spojení jsou zasílány veškeré příkazy, které jsou předem definované s požadavky na server, a také jsou tímto spojením vráceny odpovědi. Se serverem je navazováno z klienta jen jedno řídicí spojení.[2]

1.2 Datové spojení

Toto spojení je používáno pro přenos souborů, kdy za pomoci řídicího spojení jsou dohodnuty parametry přenosu. Následně je sestaveno TCP spojení pomocí metody zvané three-way handshake. Je složen ze tří paketů, které mají postupně příznaky SYN (Synchronize sequence numbers), SYN a ACK (Acknowledgement), ACK. Následně se přenesou data a spojení je ukončeno pakety s příznaky FIN (end of connection) a ACK. Datových spojení může být i více. Pro každý soubor může být vytvořeno vlastní datové spojení. Pro přenos dat jsou používány dva režimy přenosu – a to aktivní a pasivní.[2]

1.3 Aktivní režim

Jedná se většinou o preferovaný režim přenosu, jelikož server nemusí otevírat porty a nemůže být přetížen mnoha žádostmi o data. Jak je zobrazeno na obr. 1.1. Přes řídicí spojení je mezi klientem a serverem dohodnuto, na jaké IP adrese a portu budou data k dispozici (pomocí příkazu PORT). Spojení je navázáno ze serveru na



Obr. 1.1: Aktivní režim přenosu[2]

sdělenou IP a port, kde se stáhne nebo nahraje soubor. Role serveru a klienta jsou tedy pro datové spojení vyměněny.[2]

Tento režim však může být problematický při používání NAT (Network Address Translation) nebo firewallu, kdy je bráněno otevření portu na klientovi a následnému připojení serveru.[2]

1.4 Pasivní režim

Problém NATu, který je způsoben nemožností připojení na klienta, a firewallu je vyřešen přenosem v pasivním režimu, kdy si klient se serverem nevymění role, ty zůstanou zachovány. Připojení je realizováno z klienta na FTP server.

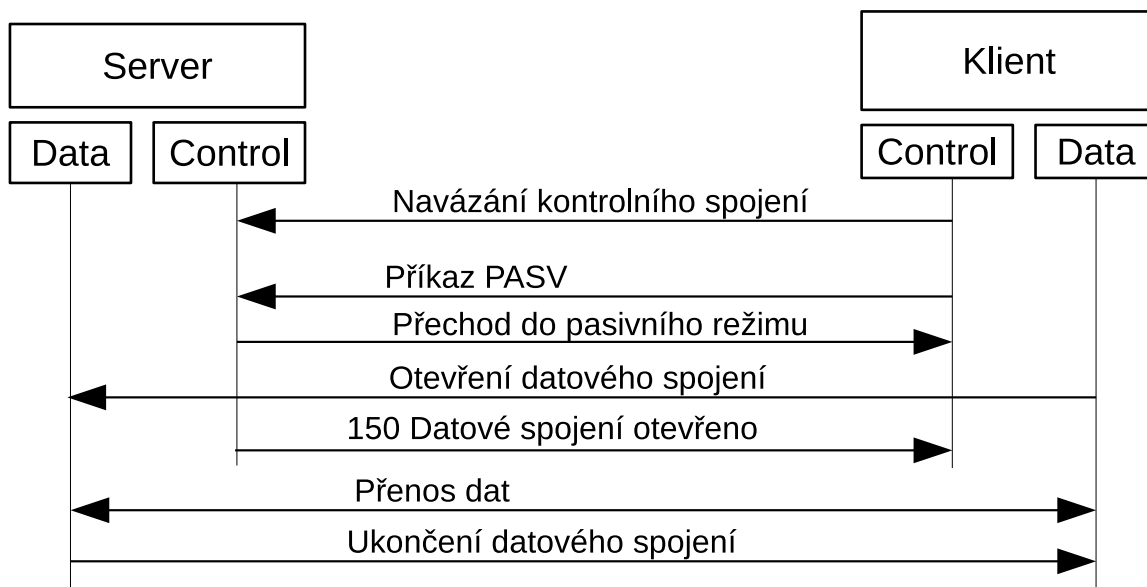
Jak je ukázáno na obr. 1.2. Příkaz PASV, kterým je oznámeno serveru, že bude komunikováno v tomto režimu, je odeslán klientem. Od serveru se nazpět zašle informace o IP adrese a portu, na kterém jsou data vystavena a kde je očekáváno spojení od klienta.[2]

1.5 Adresace

Adresa se skládá z několika částí a může vypadat následovně [3]:

`protokol://user:pass@host:port/path`

protokol definuje typ spojení, které může být FTP, FTPS (File Transfer Protocol over SSL/TLS) atd.



Obr. 1.2: Pasivní režim přenosu[2]

user reprezentuje uživatelské jméno

pass označuje heslo, které přísluší uživatelskému jménu, pokud jde o účet bez hesla, nepíše se ani dvojtečka

host značí adresu serveru sloužící k připojení

port pokud tato volba chybí, použije se výchozí port TCP/21

path obsahuje cestu do složky nebo k souboru uloženém na FTP

Položky, které jsou definovány jako povinné, jsou protokol a host. Ostatní jsou volitelné, avšak špatný port znemožní připojení. Na jméno a heslo je v případě potřeby vygenerován dotaz.

1.6 Reprezentace dat

V FTP je umožněno několik možností reprezentace dat, z nichž jsou pravděpodobně nejpoužívanější reprezentace ASCII a IMAGE.[1, 2]

ASCII má využití při přenosu textových dat přes síť (textových souborů), kdy je nutné přenášená data převést na osmibitovou sekvenci v ASCII reprezentaci.

IMAGE má binární podobu, lze jím přenášet například obrázky ve formátu JPEG (Joint Photographic Experts Group) a jiné soubory nepřevoditelné do textové podoby. Odesílá se jako proud bitů.

LOCAL slouží pro přenos dat v definované velikosti bitů (například 36 bitů).

V dnešní době nebývá implementován.

EBCDIC lze použít, pokud je na obou stranách spojení použito toto kódování.

1.7 Možnosti přenosu

Protokol také umožňuje nastavit způsob přenosu dat mezi klientem a serverem. Existují tři možnosti.[1, 2]

STREAM MODE – odesílá proud bajtů přes internet. Pro signalizaci začátku a konce souboru se používá otevření a uzavření datového spojení, případně pomocí dvojice EOR EOF. V dnešní době je tato možnost preferována.

BLOCK MODE – data jsou odesílána za sebou v blocích, kdy každý blok obsahuje hlavičku, kde je uvedeno, o kolikátý blok se jedná.

COMPRESSED MODE – přenos probíhá v komprimované podobě.

1.8 Příkazy FTP

Příkazy jsou přenášeny v textovém formátu, jelikož FTP používá NVT (Network Virtual Terminal), který je používán i protokolem Telnet. Všechny příkazy jsou zasílány na server z klienta přes řídicí spojení ve formátu NVT.[1]

příkaz parametr1 parametr2 <CRLF>

Příkazy nemusí mít žádný parametr nebo jich mohou mít více, ale ve většině případů mají pouze jeden parametr. Klávesa Enter je reprezentována značkou <CRLF>, jde o netisknutelný znak. V dalším textu budou představeny vybrané příkazy z [1].

Příkaz PORT se používá k předání parametrů pro datové spojení, jeho parametrem je šest desítkových čísel oddělených čárkou. První čtyři čísla reprezentují IP adresu a zbývající dvě představují port, kde je klientem nasloucháno a čekáno na připojení od serveru.

PASV slouží k informování serveru, že klient chce pracovat v pasivním režimu. Od serveru je následně zaslána informace, na jaké IP adrese a portu naslouchá.

USER odešle na server uživatelské jméno použité pro přihlášení k serveru. Pokud je vyžadováno heslo, je odesíláno jako parametr příkazu PASS. Oba příkazy slouží k přihlášení. QUIT ukončuje spojení s FTP serverem.

Vytvářet resp. mazat adresáře je umožněno příkazy MKD resp. RMD s parametrem reprezentujícím cestu k adresáři, který má být vytvořen resp. smazán. Příkazem STOR se na server uloží soubor specifikovaný parametrem. RETR umožňuje získat soubor ze serveru určeného cestou k souboru v parametru. DELE příkaz zařídí smazání souboru na serveru.

Pokud chce klient změnit pracovní adresář, použije příkaz CWD a jako parametr uvede cestu k novému adresáři. Pokud potřebuje znát adresář, ve kterém se právě nachází, tak tuto informaci získá při odeslání příkazu PWD.

Následující příkazy TYPE a MODE umožňují volbu reprezentace dat a typu přenosu datového spojení. TYPE slouží k nastavení reprezentace dat. Většinou jsou implementovány jen možnosti ASCII a IMAGE. MODE nastavuje, jakým způsobem budou data přenesena. Z možností STREAM, BLOCK nebo COMPRESSED MODE je používáno jako výchozí STREAM MODE.

HELP přenáší užitečné informace ze serveru k jednotlivým příkazům. Jde ve své podstatě o nápovědu. Server odpovídá například výpisem příkazů, které podporuje. NOOP nemá žádný parametr a je používán k udržení aktivního spojení se serverem.

1.9 Odpovědi FTP

Na každý příkaz je odpovězeno formou číselného kódu a většinou i pro uživatele čitelným textem. Každá ze tří číslic v odpovědi má specifický význam.[1] Pokud není uvedeno jinak, jsou kódy převzaty z [1].

1. číslice

- 1 – Předběžně pozitivní odpověď. Příkaz je prováděn a bude následovat ještě jedna odpověď informující o výsledku příkazu.
- 2 – Příkaz byl úspěšně proveden a lze pokračovat dalším příkazem.
- 3 – Přejídně pozitivní odpověď. Informace o provedení dosud obdržených příkazů.
- 4 – Přejídně negativní odpověď. Příkaz nebyl proveden, ale je možné ho zopakovat.
- 5 – Negativní odpověď. Příkaz nebyl úspěšně proveden a už by neměl být použit.
- 6 – Odpovědi týkající se zabezpečení. [4]

2. číslice

- 0 – Došlo k syntaktické chybě.
- 1 – Odpověď na příkaz, který požadoval informaci. (HELP)
- 2 – Odpověď, která souvisí se spojeními se serverem (datové a řídicí).
- 3 – Odpovědi při přihlašování.
- 4 – Nespecifikováno.
- 5 – Odpovědi souvisí se stavem souborového systému.

3. číslice označuje ještě jemnější dělení odpovědí, například kód 221 informuje o korektním odhlášení a ukončení spojení nebo kód 226 nese informaci o ukončení datového spojení.

1.10 Příklad použití příkazů a odpovědí

V této kapitole je zobrazen výpis komunikace serveru a klienta při přihlášení uživatele, stažení souboru a odhlášení klienta ze serveru. Přenos probíhá v aktivním režimu.

```
220 MY SITE NAME
---> USER xmatou27
331 Password required for xmatou27.
---> PASS XXXX
230 User xmatou27 logged in.
---> SYST
215 UNIX Type: L8
---> TYPE A
200 Type set to A.
---> PORT 10,0,6,4,237,71
200 PORT command successful.
---> RETR test.txt
150 Opening ASCII mode data connection for test.txt (84 bytes).
226- [Ul: 20.7MB] [Dl: 0.0MB] [Speed: 0.00K/s] [Free: 13223MB]
226 [Section: DEFAULT] [Credits: 76.8MB] [Ratio: UL: 1:4 | DL: 1:1]
87 bytes received in 0.00 secs (86.4302 kB/s)
---> QUIT
221- Goodbye
221
```

Server na pokus o připojení odpovídá odpovědí s číselným kódem 220. Na příkaz USER je odpovězeno kódem 331 spadajícím do kategorie odpovědí při přihlašování. Nejedná se o konečnou odpověď, ale je ještě požadováno heslo. To je odesláno na server a ten odpovídá kódem 230, což označuje úspěšné přihlášení. Následně je zaslán dotaz na typ operačního systému, odpovědí je kód 215, neboť se jedná o úspěšnou odpověď a příkaz žádal informace. Poté dojde k nastavení parametru ASCII a je odeslán příkaz PORT pro navázání spojení. Na oba příkazy je odpovězeno kódem 200. Otevření spojení je označeno odpovědí 150 a ukončení 226. Při odhlášení je vygenerována odpověď 221, neboť jde opět o kategorii pro přihlašování.

1.11 Modifikace FTP

Protokol FTP vzhledem k době, kdy byl definován v dokumentech RFC, postrádá jakékoliv zabezpečení jak proti odposlechu, tak i proti změně dat. Proto vzniklo

několik modifikací FTP protokolu, které přidávají dodatečnou vrstvu šifrování, aby byl přenos informací skryt před potencionálními útočníky. Je používáno především SSL (Secure Socket Layer), TLS (Transport Layer Security) a SSH (Secure Shell).[5]

Při použití FTP over SSL/TLS je FTP spojení skryto do protokolu transportní vrstvy SSL nebo TLS, čímž je zajištěno zabezpečení, následně je možné přenést data bezpečně přes síť a dále je dešifrovat na klientovi nebo serveru. Tato varianta může fungovat ve dvou režimech, a to v explicitním a implicitním režimu.[6, 7]

V explicitním režimu musí klient požádat o aktivaci zabezpečení. Na nezabezpečeném spojení je tento režim aktivován pomocí AUTH TLS nebo AUTH SSL. Případně lze žádat již při připojování. Spojení je navázáno na standardních portech pro FTP. Zda bude šifrováno řídicí, datové nebo obě spojení je určeno klientem. V implicitním režimu jsou použity jiné porty pro zabezpečené připojení z důvodu možné nekompatibility s nezabezpečeným FTP. Šifrování se aktivuje již na začátku spojení, kdy dochází k šifrování všech kanálů a není možné to změnit.[6, 7]

V FTP over SSH je pro zabezpečení použit tzv. tunel vytvořený za pomoci protokolu SSH. Skrze tento tunel je následně navázáno FTP spojení. Je nutné, aby datová spojení byla navazována v pasivním režimu. Vyskytuje se zde problém, který způsobují dvě TCP spojení (dva porty), kdy SSH musí o FTP přenášeném tunelem vědět, aby nemohlo dojít k navázání datového spojení mimo tento tunel. Tato modifikace FTP je často zaměňována s SFTP (SSH File Transfer Protocol), který kromě použití pro přenos souborů nemá s FTP nic společného, neboť jde o jiný protokol.[5]

2 IRC

IRC (Internet Relay Chat) je aplikační protokol typu klient-server, který slouží pro interaktivní komunikaci mezi uživateli (chatování). Používá protokol transportní vrstvy TCP.

Server je složen z tzv. kanálů (místností), ve kterých mohou uživatelé komunikovat všichni se všemi, ale lze komunikovat i s vybraným uživatelem.[8]

Několik IRC serverů může být sdruženo do tzv. IRC sítě. Mezi tyto sítě patří například EFnet, Undernet, DALnet a další.

Pro používání IRC serveru je vhodné znát některé příkazy, například pro změnu uživatelského jména nebo připojení se k vybranému kanálu. Příkazy pro IRC server začínají lomítkem a vybrané příkazy jsou uvedeny níže[8]:

/nick slouží pro změnu uživatelského jména.

/join se použije pro připojení k existujícímu kanálu. Pokud kanál tohoto názvu neexistuje, pak jej vytvoří.

/mode se použije například při změně oprávnění kanálu nebo uživatele.

/invite umožňuje pozvat uživatele do kanálu, kde byl příkaz zadán.

/msg slouží například k odeslání zprávy jednomu uživateli nebo k registraci a podobně.

V rámci kanálu lze nastavit různá oprávnění. Například je možné omezit přístup do kanálu jen pro zvané uživatele. Tato oprávnění lze změnit příkazem **/mode**. Zvolenou možností je možné přidat pomocí znaku **+** a odebrat znakem **-** před oprávněním. Vybraná jsou uvedena dále[8]:

o umožňuje specifikovat, který uživatel bude správcem kanálu. Ve výchozím stavu, kdy není tato volba nastavena, se správcem stane první uživatel, který kanál vytvořil. Po jeho odchodu se správcem stává jiný účet, který zůstane správcem, i pokud by původní uživatel znovu vstoupil.

i uzavře kanál pouze pro pozvané uživatele.

t umožní při nastavení změnit téma kanálu jen správcům. Pokud není tato volba nastavena, mohou téma měnit všichni uživatelé.

n zakazuje vkládat zprávy do kanálu uživatelům, kteří nejsou právě připojeni na tento kanál.

k umožňuje nastavit heslo, které je nutno zadat při připojování ke kanálu.

Některé IRC sítě umožňují zaregistrovat si svoje uživatelské jméno nebo název kanálu. K registraci uživatelského jména slouží příkaz, jehož parametrem je heslo pro aktuálně zvolené uživatelské jméno a případně i e-mailová adresa. Přihlášení se provede zvolením uživatelského jména pomocí **/nick** a druhým příkazem se ověří heslo k tomuto uživatelskému jménu.[8]


```
/msg NickServ REGISTER <heslo>  
/msg NickServ IDENTITY <heslo>
```

Pro registraci IRC kanálu se používá místo služby NickServ služba ChanServ. Příkaz pro registraci je následující.[8]

```
/msg ChanServ REGISTER <#jméno kanálu> <heslo> <popis kanálu>
```

3 Eggdrop

Jedná se o nejstaršího IRC (Internet Relay Chat) robota, který byl vytvořený Robey Pointerem v roce 1993.[9] Je možné jej nainstalovat na Linux, BSD (Berkeley Software Distribution) a další systémy (například SunOS). Je napsán v jazyce C a TCL (Tool Command Language) a je šířen pod svobodnou licencí.

Mezi jeho vlastnosti patří zejména:

- Možnost rozšíření pomocí modulů za použití jazyka C a skriptů v jazyce TCL (bude využito při následném propojení s GIFTpd),
- základní administrativa IRC kanálu,
- možnost použití zabezpečení SSL.

3.1 Instalace

Pro bezproblémovou instalaci je nutnost mít nainstalovány balíčky pro podporu TCL jazyka, stažení a rozbalení souborů například pomocí wget a dále použití příkazu níže ve složce s rozbaleným archivem.

```
./configure
```

Tento příkaz automaticky rozpozná, zda je v systému přítomna vývojová knihovna pro SSL podporu a pokud ano provede se překlad s podporou SSL. Dále je nutné zkompileovat moduly. Pro kompilaci výchozích se použije první příkaz. Pokud se mají kompilovat jen některé, použije se druhý, který nabídne možnost vybrat, které mají být kompilovány.

```
make config  
make iconfig
```

Pro překlad a instalaci se použije následující příkaz. U `make install` lze pomocí `DEST=<install directory>` zvolit složku, kam bude eggdrop nainstalován. Výchozím adresářem je domovská složka uživatele v podadresáři eggdrop.

```
make && make install
```

3.2 Konfigurace

Po instalaci jsou konfigurační soubory dostupné ve vybraném adresáři. Je možné si výchozí konfiguraci zkopírovat a použít k úpravám. Některé volby jsou uvedeny níže:

listen určuje, na kterém portu bude eggdrop naslouchat pro případnou dynamickou konfiguraci.

channel add přidává kanál do konfigurace eggdrop. Bližší syntaxe je v dokumentaci. [9]

channel set nastavuje možnosti kanálu. Například, že přístup je povolen jen zvaným uživatelům. Zda se práva přidávají nebo odebírají určuje + nebo - před právem.

set servers obsahuje servery, kam se má připojovat, včetně uvedení portu za dvojtečku. Pokud se nepovede připojení k prvnímu serveru, zkusí se další. Pokud se před číslem portu použije znak +, znamená to použití zabezpečení mezi robotem a serverem.

set nick nastavuje jméno robota na IRC serveru.

set altnick viz výše. Tento název účtu se použije v případě, že hodnota v set nick nebude na daném serveru volná.

loadmodule umožňuje nahrát další moduly do robota, například modul pro uptime stroje.

source umožní nahrát skript TCL jazyka.

Pokud byla konfigurace provedena, je nutné spustit v adresáři s konfigurací eggdrop příkaz níže:

```
./eggdrop -m <nazev-konf-souboru>
```

Tento příkaz provede vytvoření několika dalších souborů a spuštění robota. Pro další spuštění se používá stejný příkaz, ale bez -m, nebo lze nastavit soubor s konfigurací jako spustitelný a spouštět robota odkazem přímo na tento soubor. Podmínkou však je, že konfigurační soubor musí mít definovanou cestu k programu eggdrop a musí být nastaven jako spustitelný.

Robota lze také konfigurovat pomocí vzdáleného přístupu na jeho port ze systému Linux, to lze provést pomocí příkazu:

```
nc <adresa serveru> <port-robota>
```

Při prvním připojení se server zeptá na uživatelské jméno správce, které lze zvolit libovolně, a následně také na heslo. Po zobrazení příkazového řádku je možné dynamicky měnit nastavení robota. Lze například přidat kanál, změnit práva na daném kanále nebo změnit server. Aby se změny projevíly, je nutné provést příkaz **.rehash**, který načte nastavení, nebo příkaz **.restart**, který celého robota restartuje, a tím dojde opět k načtení aktuální konfigurace. [9]

Všechny příkazy v tomto režimu jsou uvozeny tečkou a dále může následovat + nebo -, které určují přidání nebo zrušení hodnoty. Vybrané volby jsou uvedeny níže [9]:

- .chan** slouží k nastavení kanálu na IRC serveru. Tato volba je používána se znaky + nebo -.
- .chanset** nastavuje práva kanálu. Například lze přidat možnost vstoupit jen pozvaným uživatelům atd.
- .chaninfo** zobrazí veškerá nastavení současného kanálu na IRC serveru.
- .user** přidá nebo odebere uživatele z robota. Lze uživatele přidávat nebo mazat pomocí modifikátorů výše.
- .chpass** nastaví uživateli z předchozí volby heslo.

4 Debian

Debian je jednou z distribucí Linuxu, který umožňuje používat i jiná jádra než Linuxové, například jádro ze systému FreeBSD. Debian je složeninou tohoto jádra a sady programů potřebných k provozu počítače.[10] Je možné ho rozšířit o další programy z tzv. repositářů nebo kompilací zdrojových kódů konkrétního programu.[11] Systém umožňuje práci v textovém nebo v grafickém prostředí, kterých existuje více. Pro server se více hodí právě textový přístup, neboť nevyžaduje tolik systémových prostředků. Pro komunikaci se systémem se v tomto případě používá příkazů psaných do textového rozhraní. Některé příkazy jsou uvedeny níže a některé z nich jsou používány v této práci:

man při použití `man` příkazu se vypíše manuálová stránka se všemi dostupnými parametry.

cd je používán pro změnu adresáře na adresář uvedený za tímto příkazem.

cp slouží ke kopírování souborů.

make použitý bez parametru provede překlad zdrojových kódů v aktuálním adresáři.

wget umožňuje stažení souborů z internetu do uvedené složky.

chmod provede změnu práv na souborech nebo adresářích na nastavená práva.

chown mění vlastníka souborů a adresářů.

tar rozbaluje archivy tar. Mohou být i komprimované některými metodami (gzip, bzip).

unzip rozbaluje zip archivy.

iptables, **ip6tables** jsou příkazy pro stavové firewally používané v Linuxových distribucích pro IPv4 a IPv6 (druhý jmenovaný).

nano, **vi**, **vim** jsou textové editory, například pro editaci konfiguračních souborů.

apt-get s parametrem `install` a názvem balíčku jej nainstaluje.

ftp jednoduchý FTP klient pro nešifrované spojení. Lze použít například pro vytvoření uživatelů na FTP serveru přes lokální smyčku.

Některé příkazy mají parametr `--help`. Při použití s příkazem dojde k výpisu zkrácené nápovědy k příkazu.

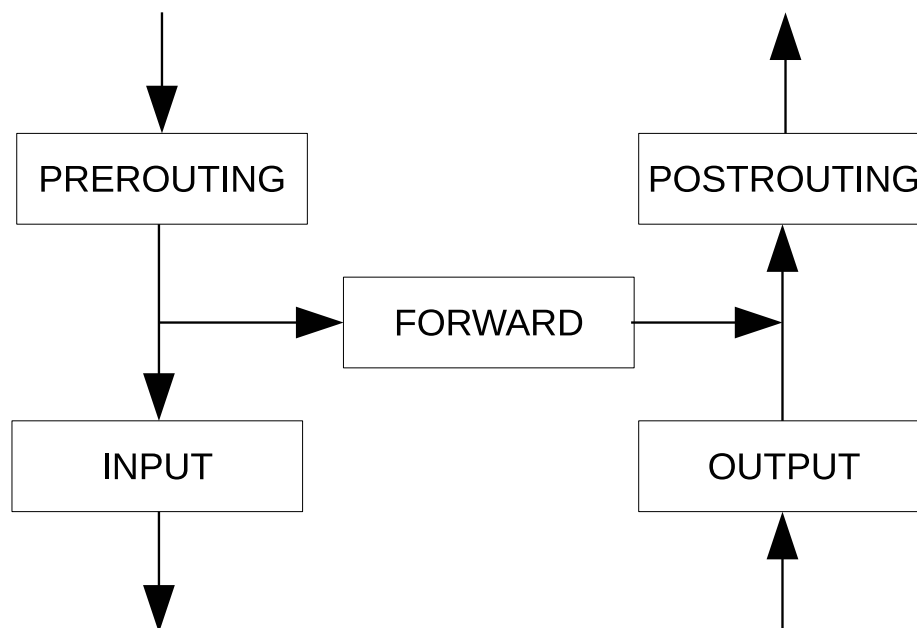
Adresářová struktura má podobu stromu, který začíná v tzv. kořenovém adresáři označovaným lomítkem (/) a dále se větví podle adresářů, například na `home`, `etc` atd. Systém rozlišuje malá a velká písmena, proto adresáře `plocha` a `Plocha` jsou dva různé.[11]

4.1 Iptables

Iptables je nástroj pro konfiguraci firewallu pro IPv4 (Internet Protocol verze 4) v systému Debian.[10] Používá se tzv. stavový firewall, který rozlišuje spojení a příznaky TCP paketů. Firewall se skládá z několika tzv. chainů, které určují, odkud a kam paket směřuje. Pravidla v chainech se procházejí sekvenčně od shora dolů. Použití pravidel z jednotlivých chainů je uvedeno níže[11]:

- INPUT – použije se při příchodu paketů určených přímo pro tento stroj.
- OUTPUT – použije se při odeslání paketů ze stroje s firewallem.
- FORWARD – najde uplatnění na routerech, neboť se uplatní při přeposílání paketů mezi rozhraními.
- PREROUTING – umožní změnu IP adresy nebo portu u příchozích paketů.
- POSTROUTING – viz výše, ale uplatní se na odchozí pakety.

Lze vytvářet i vlastní chainy a následně do nich vstupovat z výchozích chainů. Rozložení defaultních chainů ukazuje obr. 4.1.



Obr. 4.1: Rozložení chainů ve firewallu [11]

Pro konfiguraci firewallu pro IPv6 (Internet Protocol verze 6) se používá nástroj ip6tables.

4.2 SSH

Jde o protokol pro vzdálený přístup na stroj. SSH (Secure Shell) používá oproti protokolu Telnet šifrování. Debian používá variantu OpenSSH. Generuje si vlastní otisk,

který může uživatel zkontrolovat, aby zjistil, zda se připojuje na server, který předpokládá. Tento protokol umožňuje bezpečné připojení ke vzdálenému stroji a také přenos souborů. Dále umožňuje použití veřejného a tajného klíče k ověření namísto použití hesla. Výhoda klíčů je, že lze mít jeden tajný klíč pro několik serverů. V nastavení OpenSSH lze zvolit i uživatelské účty, na které se lze pomocí tohoto protokolu přihlásit. SSH pracuje standardně na portu 22.

5 FTP démoni

Tato část práce se věnuje vybranému démonu GIFTpD, jeho konfiguraci, vlastnostem a využití. Konfigurace byla provedena na fyzickém stroji.

5.1 GIFTpD

GIFTpD (GreyLine File Transfer Protocol Demon) je pojmenován po prvním vývoji GreyLine. První verze vyšla v roce 1998. Je volně šiřitelný pod vlastní licenci, která je přiložena v instalačním balíčku.[12]

Tento démon může být nainstalován na různé operační systémy založené na UNIXu, například GNU/Linux, systémy BSD atd. Má nezávislou databázi uživatelů a skupin, lze tedy vytvářet jiné uživatele a přihlášení uživatelé jsou uzavíráni v jejich domovských adresářích.[12]

Mezi jeho vlastnosti patří podle [12] například:

- Virtuální uživatelé a skupiny oddělené od systémových.
- Omezení šířky přenosového kanálu.
- Možnost nastavení Upload/Download poměru.
- Výpočet CRC pro nahrávané soubory.
- Možnost spravovat uživatele a skupiny online (přes SITE příkazy).
- Integrace SSL/TLS.
- Široká konfigurovatelnost aj.

5.1.1 Instalace

Před instalací je vhodné zkontrolovat, zda systém obsahuje vše potřebné pro její hladký průběh. Je především nutná znalost hesla administrátora (root), systém z rodiny UNIX a minimálně 30 MB místa na disku. Lepší je více, neboť se na běžícím serveru budou ukládat logy, nahrávané soubory atd.[13]

Nyní může být stažen balíček pro instalaci ze stránek GIFTpD. Archiv je nutné rozbalit na disk a nyní jsou dvě možnosti, buď lze spustit script `installgl.sh`, nebo manuální instalaci.[13, 14]

5.1.2 Konfigurace

Struktura adresářů se dělí vzhledem k adresáři s instalací na spustitelné soubory v adresáři `bin`, adresář `docs` obsahující dokumentaci, `etc` konfiguraci, `ftp-data` obsahuje vše pro FTP démon (logy, soubory uživatelů atd.), v adresáři `site` se nachází ve výchozí konfiguraci úložiště souborů nahraných na server.

Základní konfigurační soubor se jmenuje `glftpd.conf` a je umístěn v adresáři, který byl zvolen při instalaci (nejčastěji `/etc/glftpd.conf` nebo v adresáři s instalací GIFTPd). V souboru je obsažena spousta konfiguračních voleb, některé z nich jsou uvedeny níže a převzaty z [13].

V konfiguračním souboru je umístěno několik položek, které určují cesty k nějakým datům. Položka `rootpath` ukazuje na místo, kde je umístěna instalace GIFTPd, a další položky s cestami jsou od ní odvozeny.

Volba `datapath` určuje, kde se nachází soubory démona, kterými jsou soubory s nastavením uživatelů, skupin, logy, informační zprávy a další.

Dále jsou tu položky `welcome_msg` a `goodbye_msg`. První je určena pro cestu k souboru s textem, který se zobrazí po přihlášení uživatele, a druhá je určena pro cestu k textu zobrazovanému při odhlášení ze serveru. Cesta umístěná v `banner` se zobrazuje ještě před zadáním uživatelského jména.

Položka `min_homedir` má ve výchozím stavu nastaveno `/site` a označuje nejnižší složku, kam se standardní uživatelé dostanou bez administrátorských oprávnění. Po přihlášení na server je složka viditelná pro klienty jako kořenová.

Konfigurační volba `total_users` určuje maximální počet registrovaných uživatelů. Položka `master` říká, který uživatel má být tzv. master. Volba `banned_users` obsahuje v parametrech seznam uživatelských jmen, které nemohou být použity pro nové uživatele.

Pokud by bylo nutné zavést restriktce na uživatelská hesla, bylo by nutné použít volbu `secure_pass`. První parametr obsahuje minimální počet znaků, kolik velkých/malých písmen nebo číslic má minimálně heslo obsahovat. Druhý parametr určuje, kde se má toto omezení uplatnit.

Volby `pre_check` respektive `post_check` umožňují spustit externí příkazy (např. `dupecheck`, `zipscript`) reprezentující první parametr. Zda bude příkaz spuštěn před (pre) resp. po (post) nahrání souboru na server rozhoduje, která volba je použita. Volba `calc_crc` slouží k počítání kontrolních součtů nahrávaných souborů.

Volba `requests` slouží k nastavení cesty k souboru, kde se mají ukládat požadavky na nahrání dat a jejich maximální počet.

Volba `cscript` umožňuje spustit uživatelské skripty před nebo po spuštění příkazu. Volbou `site_cmd` se definují vlastní SITE příkazy a pomocí `custom-<název site příkazu>` se definuje, kdo jej může spustit.

K zabezpečení pomocí SSL/TLS slouží volby `ALLOWED_PROTOCOLS` určující použité protokoly, `userrejectsecure`, `userrejectinsecure` umožňují zakázání zabezpečeného nebo nezabezpečeného spojení a `denydiruncrypted`, `denydatauncrypted` určují, které části spojení mají být zabezpečeny, jakým protokolem. Také musí být zvolen typ a umístění klíče na serveru. Lze také zvolit, jak silné šifry budou použity.

Pro konfiguraci přes FTP klienta má démon k dispozici uživatelský účet `glftpd` s heslem stejným jako uživatelské jméno. Tento účet je však přístupný pouze z lokální smyčky.[13]

5.1.3 PZS-NG

PZS-NG (Project ZS – Next Generation) je rozšíření, které je napsáno v jazyce C. Tento doplněk (plugin) je kompatibilní s FTP démony GFTPD verze 1.x, 2.x a `cuftpd` verze 1.x. [15]

Mezi podporované operační systémy je zařazen Linux, FreeBSD, OpenBSD, dále pak OSX, AIX nebo Solaris. [15]

Níže jsou popsány vybrané vlastnosti podle [15]:

- Logování informací o souborech `sfv`, `mp3`.
- Záznam informací o prvním nahraném souboru.
- Logování informací o kompletnosti dat.
- Vytváření souborů *-missing* pro jednodušší určení, které soubory chybí, například dle informací v `sfv` souboru.
- Vytváření odkazů na nekompletní soubory nebo adresáře. Spouštění skriptů na základě typu souboru při nahrávání souboru aj.

PZS-NG umožňuje ověřovat CRC a pokročile třídít audio soubory dle tvůrce, žánru, zadaného roku apod. Je však nutné povolit tuto funkcionalitu pomocí voleb. Lze také umožnit nahrávání například jen povolených žánrů, nebo naopak některé zakázat.[17] Dále je rozebírána instalace a propojení s GFTPD.

Jako prerekvizity před instalací se instaluje balíček `curl`, podpora pro SSL a také TCL jazyk pro roboty. [14] Následně je nutné stáhnout soubory PZS-NG, provést příkaz, který má volbu pro specifikaci cesty k instalaci FTP.[14, 16]

```
./configure
```

Pro konfiguraci je používán soubor `zsconfig.h` pro `zipscript`. Jedná se o hlavičkový soubor jazyka C obsahující tzv. direktivy určující chování `zipscriptu`. Lze například zvolit, ve kterých adresářích se bude kontrolovat integrita dat tzv. CRC podle souboru `sfv`, v němž je uložen správný kontrolní součet.[17]

Direktiva (makro) má tvar `#define option value`. Znak `#` označuje direktivu, nejedná se o komentář. Vybrané direktivy jsou uvedeny v následujícím textu a jejich kompletní seznam je uložen v adresáři s instalačními soubory, konkrétně v souboru `README.ZSCONFIG`, kde se také nachází výchozí volby.[17]

`sitepath_dir` označuje umístění nahrávaných dat na serveru. Standardně je nastaveno `/site/`. Volba je udávána vzhledem k adresáři s instalací GFTPD.

sfv_dirs tato volba definuje složky, v nichž se mají kontrolovat kontrolní součty s údaji v sfv souboru. Cesty k adresářům jsou uváděny oddělené mezerou.

force_sfv_first tato volba při nastavení na TRUE neumožní nahrát jiný soubor do složek v **sfv_dirs**, dokud nebude nahrán soubor sfv. Ve výchozí konfiguraci je nastaveno na FALSE, lze tedy nahrát na server datové soubory, poté soubor sfv a dodatečně zkontrolovat CRC.

create_missing_files nastavení na TRUE vytvoří na serveru chybějící soubory s velikostí 0 B ve tvaru název_souboru-missing. Tyto soubory budou odstraněny po nahrání přírodních dat do adresáře.

create_m3u hodnota TRUE vytvoří po nahrání kompletních dat soubor M3U.

crc_algo určuje, který algoritmus bude použit pro CRC. Standardní pořadí je sliceby8, sliceby4, standard.

debug_mode její použití je v případě, že něco nefunguje, jak by mělo. Například nedochází k ověřování CRC součtů. Hodnota TRUE povolí ladící režim a vytvoří soubory s označením **.debug**.

gl_userfiles označuje cestu k souborům, ve kterých jsou uloženy informace o uživatelských účtech. Standardně **/ftp-data/users/**.

ignored_types hodnota zde umístěná definuje soubory, které není možné nahrát, soubory jsou proto ignorovány. Defaultně jsou zde uloženy soubory debug message html atd. Hodnota je uvedena ve tvaru **,debug,message**.

incompleteislink vytvoří zástupce na nekompletní složku. Lze vybrat buď symlink (zástupce) při hodnotě TRUE nebo jako soubor při hodnotě FALSE.

log ukazuje na soubor, kde lze nalézt tzv. log (soubor o činnostech, aktivitě atd.)

noforce_sfv_first_dirs umožní v zadaných adresářích, které jsou odděleny mezerou, při nastavení volby **force_sfv_first** na TRUE tuto volbu potlačit, aby bylo možné nahrát sfv soubor dodatečně.

storage určuje adresář, kde si může PZS-NG ukládat údaje jako jsou statistická data o tom, ze kterého účtu bylo nahráno, kolik souborů atd. Výchozí hodnota: **/ftp-data/pzs-ng/**.

audio_podle-čeho-třídít_sort umožňují třídění dle roku, žánru, autora, jazyka atd. Znaky podle-čeho-třídít označují, které třídění má být nastaveno na TRUE/FALSE (genre, artist, year, language atd.).

audio_podle-čeho-třídít_path určuje, v jakém adresáři budou vytvořeny odkazy na audio data. Opět podle-čeho-třídít označuje typ třídění (genre, artist atd.) a k němu se vážou cesty k adresáři. Tyto adresáře je nutné vytvořit předem.

allowed_podle-čeho-třídít umožňuje povolit jen některé autory, žánry pro třídění. Hodnotou jsou povolení autoři, žánry (dle volby podle-čeho-třídít) oddělené čárkou. Podle čeho-třídít opět určuje vztah k adresáři, nebo zda je třídění

dle této volby povoleno.

banned_podle-čeho-třídít vyjadřuje opak předchozí volby, lze zakázat autory, roky, žánry atd.

enable_nfo_script hodnota TRUE umožní použít script v `nfo_script`.

Po ukončení editace souboru `zsconfig.h` je třeba provést překlad zdrojových souborů a instalaci v adresáři se staženými soubory příkazy (nutné oprávnění root)

```
make && make install
```

a následně ještě zkopírovat knihovny pomocí skriptu `libcopy.sh`, který se nachází v `pzs-ng/scripts/libcopy/`. [16, 18]

Zipscript z PZS-NG je nyní nainstalován ve složce s GIFTpd démonem. Jeho konfigurační soubor musí obsahovat minimálně odkaz na binární soubor `zipscript-c` a musí být povoleno počítat kontrolní CRC součty, což zajistí vložení následujících řádků do `glftp.conf`. [16]

```
calc_crc *
post_check /bin/zipscript-c *
```

Dále je vhodné přidat následující dva řádky pro funkci i při smazání dat. [16]

```
cscript DELE post /bin/postdel
cscript RMD post /bin/datacleaner
```

Volitelně lze přidat i následující řádky, které slouží například k odstranění neplatných odkazů nebo jejich vytváření. Dále je těmito volbami umožněno znovu ověřit CRC nebo znovu provést třídění manuálně.

```
cscript SITE{:space:]NUKE post /bin/cleanup
cscript SITE{:space:]WIPE post /bin/cleanup
cscript SITE{:space:]UNNUKE post /bin/cleanup
site_cmd RESCAN EXEC /bin/rescan
custom-rescan !8 *
cscript RETR post /bin/dl_speedtest
site_cmd AUDIOSORT EXEC /bin/audiosort
custom-audiosort !8 *
```

Pokud se nainstaluje i skript `psxc-imdb`, pak lze stahovat i informace o video souborech.

ngBot

V adresáři s instalačními soubory se nachází i složka `sitebot`, kde jsou umístěny skripty a moduly pro IRC robota, který rozumí programovacímu jazyku TCL a také konfigurační soubory. Konfigurační soubor `ngBot.conf.defaults` je vhodné překopírovat s názvem `ngBot.conf` a upravovat konfiguraci v tomto souboru, neboť defaultní soubor by mohl být přepsán. [19] Vybrané konfigurační volby jsou uvedeny níže:

set location(param) jsou volby ukazující například na umístění souborů s uživateli, konfigurací `glftpd` atd. Hodnota `param` určuje, o jaký údaj se jedná.

set binary(parametr) určuje cestu k jednotlivým spustitelným programům, například `df`. Parametr opět určuje, ke které hodnotě parametru patří uvedená hodnota.

set device(pořadí) určuje disk, kde jsou uložena data. Lze zvolit i více disků pomocí hodnoty pořadí, která začíná od nuly. Dole se definuje, pro které sekce je tento volný prostor platný.

set invite_channels označuje kanál na IRC, kam má být uživatel pozván.

set stats(parametr) touto volbou je možné skrýt uživatele nebo skupiny ve statistikách. Parametr nabývá hodnot `hide_zeros`, `hide_users`, `hide_groups`.

set format_time, **set format_date** nastavují formát data a času.

set cmdpre určuje uvozující znak pro robota. Za tímto znakem následuje příkaz pro robota (například `free`).

set mainchan definuje název kanálu na IRC serveru.

set glroot určuje cestu k umístění instalace `GlFTPd` serveru.

set announce(THEMEFILE) definuje styl zobrazených informací na IRC kanále. Hodnota obsahuje cestu k této definici.

Pro propojení s IRC robotem je nutné nakopírovat soubory na místa, kde s nimi bude IRC robot počítat. [19]

5.2 Konfigurace pomocí SITE příkazů

Přidat uživatele na server nebo upravit jeho vlastnosti je možné buď úpravou souboru definujícího uživatele, nebo pomocí `SITE` příkazů. Některé z těchto příkazů nemusí být implementovány v každém serveru. Jejich přístupnost se řídí také nastavením oprávnění k jednotlivým příkazům. [13]

Přidat uživatele `username` s heslem `password` lze provést příkazem:

```
site adduser username password
```

Uživatelské jméno a heslo mohou mít nastaveno omezení, například pro heslo minimálně jedno velké písmeno atd. Volitelný parametr příkazu je IP adresa nebo rozsah adres, odkud se uživatel smí připojit. Například *@* značí připojení odkudkoliv, *@127.0.0.1 jen z lokální smyčky atd.

Přidávání/odstraňování adres lze provádět také dodatečně příkazy:

```
site addip username *@127.0.0.1
site delip *@127.0.0.1
```

První příkaz přidá adresu a druhý ji odebere. Lze přidávat/odebírat i více adres najednou, maximálně však 10 v jednom příkazu.

Pro změnu nastavení uživatele/uživatelů slouží příkaz `site change`. Tento příkaz má spoustu voleb. Lze pomocí něj změnit například poměr upload/download, nastavit, kolik si smí uživatel stáhnout dat (credits), změnit tzv. flags atd. Parametr flags také umožňuje zvýšit některým uživatelům oprávnění apod. Více informací o syntaxi lze získat následujícím příkazem.

```
site change
```

Zobrazí se také informace, co vše lze změnit tímto příkazem.

Pomocí dalšího příkazu lze zobrazit názvy všech SITE příkazů. Pokud je název příkazu napsán za `help`, zobrazí se informace k tomuto příkazu.

```
site help
```

Uživatelské účty na serveru lze také přejmenovávat, rozdělovat do skupin nebo jim měnit hesla, případně je odebírat.

```
site renuser old_username new_username
```

Tímto příkazem lze účet `old_username` přejmenovat na `new_username`. Přidání do skupiny se provede pomocí příkazu níže. Opětovné použití odebere účet ze skupiny.

```
site chgrp username group
```

Ke změně hesla dojde při použití prvního z příkazů níže, který změní heslo přihlášeného uživatele. Změna hesla jiného uživatelského účtu lze provést druhým příkazem.[13]

```
site passwd new_password
site chpass username new_password
```

Pokud má být uživatel odstraněn ze serveru, lze toho docílit pomocí:

```
site deluser username
```

6 Postup realizace

V této kapitole není uvedena instalace, která byla uvedena dříve v jednotlivých kapitolách. Tato kapitola se zaměřuje na provedené nastavení určitých voleb na serveru.

6.1 Firewall

V dnešní době je zvykem vše zabezpečovat, a proto bude i zde uvedeno nastavení firewallu. Například zde řešené FTP běží standardně na portu 21. Pokud není provozováno na tomto portu, není nutné, aby byl port na firewallu přístupný.

Jak již bylo uvedeno, konfigurace firewallu se v systému Debian provádí pomocí příkazu `iptables`. Zvláště při vzdálené konfiguraci je nutno dbát opatrnosti, neboť chybným nastavením nebo posloupností pravidel může dojít k zablokování přístupu.

```
iptables -i lo -j ACCEPT
iptables -m state --state INVALID -j DROP
iptables -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -p icmp -m icmp --icmp-type 8 -j ACCEPT
iptables -p icmp -m tcp --dport 1337 -j ACCEPT
iptables -p icmp -m tcp --dport 6000:6100 -j ACCEPT
iptables -P FORWARD DROP
iptables -P INPUT DROP
```

První příkaz povoluje komunikaci na lokální smyčce. Druhý zahazuje pakety, které nejsou validní, nebo nepatří žádnému spojení. Třetí naopak povoluje již vytvořená spojení (ESTABLISHED) a také spojení, která souvisí s momentálně aktivními (RELATED) například pro FTP. Další povoluje ping. Pátý a šestý povolují přístup pomocí TCP protokolu na port 1337 na tomto severu (GIFTPd) a také k pasivním portům FTP serveru v rozsahu 6000-6100.

Poslední dva určují tzv. výchozí politiku. Ta se uplatní, pokud paket projde všemi pravidly až na konec. Chainy FORWARD i INPUT jsou nastaveny na DROP (zahození paketu). Chain OUTPUT není nijak omezován a jeho politika je tedy ACCEPT.

Po zadání těchto příkazů do konzole nebo nahráním pomocí skriptu, jsou tato pravidla uložena jen do restartu systému. Pro uložení pravidel v paměti na disk do souboru `iptables.rules` v adresáři `/etc` je třeba zadat příkaz

```
iptables-save > /etc/iptables.rules
```


a následně v `/etc/network/if-pre-up.d/` vytvořit soubor libovolného názvu s obsahem:

```
#!/bin/sh
/sbin/iptables-restore < /etc/iptables.rules
```

Toto zajistí nahrání pravidel při startu systému po použití následujícího příkazu, který nastaví souboru příznak spustitelnosti.

```
chmod +x /etc/iptables.rules
```

Analogicky se nastavuje firewall pro IPv6 pomocí `ip6tables`.

6.2 GFTPD

6.2.1 Zabezpečení

Démon GFTPD je ve výchozím nastavení nastaven na možnost připojení uživatelů bez šifrování a bez restrikcí na délku hesla, počet velkých písmen v hesle a podobně. V konfiguračním souboru `glftpd.conf` je možné toto chování změnit. Pro zabezpečené připojení byly použity volby níže.

```
CERT_FILE /glftpd/etc/ftpd-ecdsa.pem
ALLOWED_PROTOCOLS TLSv1.2 TLSv1

userrejectsecure    !-glftpd *
userrejectinsecure -glftpd !*
denydiruncrypted   -glftpd !*
denydatauncrypted  -glftpd !*
```

První z nich určuje umístění certifikátu, druhá povolené protokoly a následující čtyři volby určují, která spojení se mají šifrovat. Parametr těchto voleb určuje, pro které uživatele je volba nastavena. Znakem minus (-) je uvozen uživatel, hvězdička (*) označuje všechny uživatele. Vykřičník zde slouží pro negaci. Například u `userrejectsecure` bude odmítnuto zabezpečené spojení pouze uživateli `glftpd`.

Pro nastavení restrikcí na hesla slouží volba `secure_pass`. Zde počet malých a velkých písmen a číslic určuje minimální počet těchto znaků v hesle. Tečka určuje libovolný znak a lze takto definovat minimální délku hesla.

```
secure_pass aA2.. *
```

V ukázce výše bude toto omezení použito na všechny uživatele při pokusu o změnu hesla nebo vytvoření nového uživatele. Heslo musí obsahovat minimálně jedno velké a malé písmeno, jedno číslo a zároveň musí být alespoň pět znaků dlouhé.

Jelikož je použit firewall, je nutné definovat i porty pro pasivní přenos, které musí odpovídat povoleným portům ve firewallu. Byl definován rozsah portů 6000-6100, což určuje následující řádek.

```
pasv_ports 6000-6100
```

6.2.2 Tvorba požadavků

Povolení tvorby požadavků pro nahrání dat lze provést nastavením volby `requests` v souboru `glftpd.conf`.

```
requests /ftp-data/misc/requests 10
```

První parametr určuje, do kterého souboru se budou požadavky ukládat a odkud budou následně odebírány. Číslo 10 označuje počet záznamů, které se zobrazí. Pomocí následujících SITE příkazů jde vložit/vymazat požadavek a třetí příkaz umožní zobrazit seznam požadavků o délce maximálně deseti záznamů. Viz předchozí volba.

```
site request <název požadavku>  
site reqfilled <číslo požadavku v seznamu>  
site request
```

6.3 Propojení s IRC

6.3.1 Eggdrop

Před instalací byl doinstalován balíček `libssl-dev` pro podporu zabezpečeného připojení k serveru. Příkaz nutno spustit jako administrátor (`root`).

```
apt-get install libssl-dev
```

Pro instalaci byl vytvořen nový účet s názvem `ircbot` a do jeho domovského adresáře do podadresáře `irc-bot` byl Eggdrop nainstalován způsobem uvedeným dříve v této práci. Instalován byl pod tímto uživatelem.

Konfigurační soubor může být libovolného jména. V tomto případě byl vytvořen soubor `robot.conf`, který vznikl kopií souboru `eggdrop-basic.conf`.

První řádek tohoto souboru odkazuje na spustitelný program eggdrop (bude využito dále). Dále bylo zvoleno uživatelské jméno pro IRC, alternativní jméno a určen název souboru, kam bude ukládáno číslo procesu robota.

```
#! /home/ircbot/irc-bot/eggdrop

set nick "ngrobot"
set altnick "ngrobot_"

set pidfile "robot.pid"
```

Dále bylo nutné specifikovat IRC server, kam se má připojit. Znak plus u portu za dvojtečkou značí šifrované připojení. Byl vybrán server irc.link-net.org. Poslední volba určuje, zda se jedná o některou z uvedených sítí. Hodnota 5 značí jinou síť.

```
set servers {
irc.link-net.org:+7000
}

set net-type 5
```

Další volby specifikují názvy souborů pro nastavení kanálu a uživatelů registrovaných na robotovi Eggdrop. Volba `listen` slouží k nastavení portu pro připojení protokolem Telnet pro dynamickou správu robota (viz dále). Tento port je však na firewallu zablokován pro přístup z internetu.

```
set userfile "robot.user"
set chanfile "robot.chan"
listen 33333 all
```

Nastavení DNS serverů nezávisle na nastavení systému umožní první volba, druhá pak nastavuje ověřování SSL certifikátů serverů.

```
set dns-servers "8.8.8.8 8.8.4.4"
set ssl-verify-server 0
```

Nyní může být soubor uložen a robot spuštěn pomocí následujícího příkazu, který nejprve provede přesun do složky s eggdrop a následně z této složky spustí robota. Dojde k vytvoření souborů pro uživatele a kanály.

```
cd /home/ircbot/irc-bot/ ; ./eggdrop -m robot.conf
```

Pro další spuštění stačí vypustit parametr `-m`. Nebo nastavit soubor s konfigurací jako spustitelný pomocí příkazu `chmod` a následně jej spustit odkazem na tento soubor (druhý příkaz).

```
chmod +x /home/ircbot/irc-bot/robot.conf
cd /home/ircbot/irc-bot/ ; ./robot.conf
```

Pro určení, na který IRC kanál se má robot připojit, bylo využito dynamické konfigurace pomocí protokolu Telnet. Tento port je blokován pro přístup z internetu firewallem a je přístupný jen z lokální smyčky. Připojení se provede pomocí programu `nc`.

```
nc 127.0.0.1 33333
```

Dojde k dotazu na uživatelské jméno budoucího správce a poté na jeho heslo. Zde byl nastaven název IRC kanálu a jeho přístupová práva. Poslední příkaz provede ukončení spojení s robotem.

```
+.chan #considerabant
.chanset #considerabant mode +itn
.save
.quit
```

Spouštění po startu systému

Eggdrop jde spouštět při startu systému, pokud bude vytvořen tzv. unit soubor a nahrán do umístění pro uživatelem definované soubory v `/etc/systemd/system/`. Soubor nese název `eggdrop.service` a jeho obsah je uveden níže.

```
[Unit]
Description=EGGDROP with ngBot
After=network.target
Requires=network.target
[Service]
WorkingDirectory=/home/ircbot/irc-bot/
ExecStart=/home/ircbot/irc-bot/robot.conf
User=ircbot
PIDFile=/home/ircbot/irc-bot/robot.pid
[Install]
WantedBy=multi-user.target
```

V sekci [Unit] je definován popis, který se zobrazí v systémových záznamech při spuštění/ukončení a také požadavky na závislosti. Například, že má dojít ke spuštění až po spuštění sítě.

Sekce [Service] obsahuje informace nutné pro spuštění samotného robota. Pracovní adresář, cesta ke spustitelnému souboru, uživatel, pod kterým bude program spuštěn a umístění souboru, kde je uloženo číslo procesu.

[Install] označuje, do které složky bude vložen odkaz, aby byl soubor spuštěn při startu.

Po uložení souboru je nutné obnovit databázi těchto souborů a povolit spuštění při startu.

```
systemctl daemon-reload
systemctl enable eggdrop.service
```

6.3.2 NgBot

Soubory ngBot byly nakopírovány do vytvořené složky pzs-ng v adresáři s eggdrop. Zkopírování souborů bude provedeno pomocí příkazů níže. Poslední příkaz kopíruje skript, který umožňuje pozvání do IRC kanálu z FTP serveru.

```
mkdir -p /etc/ircbot/irc-bot/pzs-ng/
cd <cesta k~adresáři s~instalačními soubory pzs-ng>/sitebot/
cp -R ngBot.* plugins themes modules /home/ircbot/irc-bot/pzs-ng/
cp ngBot.conf.dist /home/ircbot/irc-bot/pzs-ng/ngBot.conf
cd extra ; cp invite.sh /glftpd/bin/
```

Soubor ngBot.conf je konfigurační soubor, ve kterém je nutné uvést IRC kanál, uvozující znaky pro příkazy robota, kontrola umístění binárních souborů a cesty k některým souborům a položku set device označující disky pro určení volného místa.

```
set cmdpre      "!"
set mainchan    "#considerabant"
set device(0)  "/dev/sda2 DEFAULT"
```

Pro spolupráci s eggdrop je nutné do jeho konfigurace uvést odkaz na skript ngBot.tcl přidáním do robot.conf tohoto řádku.

```
source pzs-ng/ngBot.tcl
```

Následně musí být proveden restart robota, aby se změna projevila.

Pro možnost zvat uživatele pomocí GIFTpD připojení byl do `/glftpd/bin/` zkopírován soubor `invite.sh`. Opět je nutné informovat GIFTpD, že jej má zařadit mezi své SITE příkazy. Do `glftpd.conf` byly vloženy následující řádky.

```
site_cmd INVITE EXEC /bin/invite.sh
custom-invite !8 *
```

Nyní po zadání příkazu níže v konzoli FTP klienta dojde k pozvání uživatele s tímto nickem na IRC serveru do kanálu s robotem.

```
site invite <irc-nick>
```

6.4 Zavedení SSL do mIRC a FTP Rush

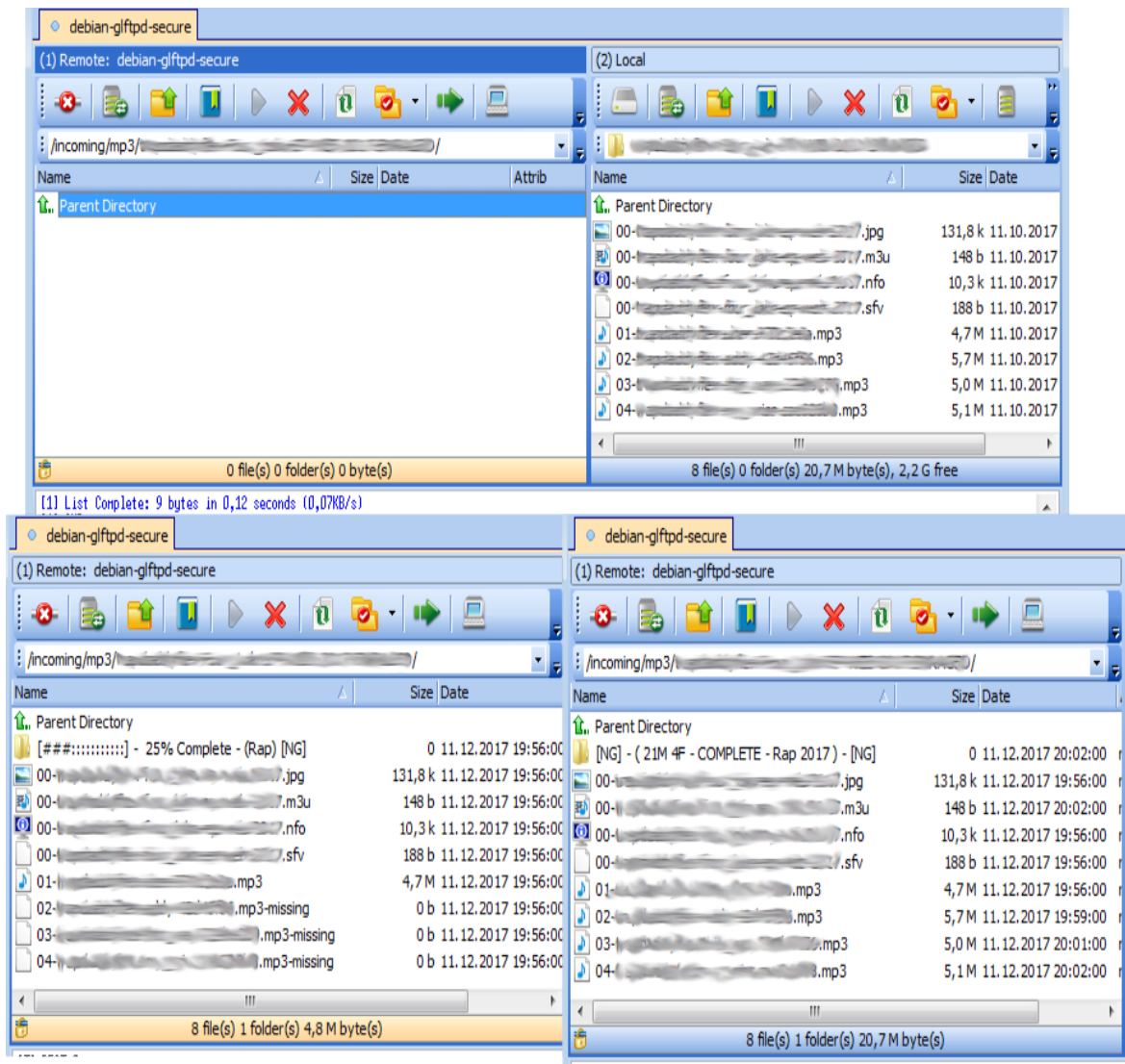
Pro vyzkoušení funkčnosti byly použity programy FTP Rush pro připojení k GIFTpD a program mIRC, který slouží pro připojení a komunikaci na IRC serverech, instalované na systému Windows 7. Při pokusu použít zabezpečené spojení s GIFTpD a IRC serverem `irc.net-link.org` nebyly k dispozici šifrovací algoritmy. Bylo proto nutné provést instalaci programu OpenSSL a zkopírovat dva soubory z této instalace do adresářů s instalací programu FTP Rush a mIRC. Tyto soubory nesou název `libeay32.dll` a `ssleay32.dll`

6.5 Ukázka funkčnosti GIFTpD

GIFTpD bylo nainstalováno na fyzický stroj. Jako operační systém byla zvolena distribuce linuxu Debian v 64bit variantě. Fyzický stroj obsahuje CPU: i3-6100 taktovaný na 3,7 GHz, 16 GB RAM, 500 GB HDD a gigabitovou síťovou kartu.

Na následujícím obrázku (obr. 6.1) a výpisech je ukázána funkčnost GIFTpD v uvedené konfiguraci. Postupně je ukázáno úspěšné přihlášení, nahrání souborů, ověřování CRC součtů, informace o nahrávaných souborech a údaje vztahující se k parametru `ratio`. K otestování byl použit operační systém Windows 7 a FTP klient FTP Rush, který umožňuje zabezpečené připojení na server, odeslat některé soubory dříve než jiné a tak dále.

Na obr. 6.1 je znázorněna funkčnost ověření CRC, které provádí server. V horní části obrázku je zobrazena prázdná složka serveru a adresář na lokálním disku počítače obsahující data nahrávaná na server (čtyři mp3 soubory, `sfv`, `m3u` a `nfo` soubor). Po nahrání souboru `sfv` a jednoho souboru mp3 (vlevo dole) je vidět vytvoření tzv. status baru zobrazujícího, že je nahráno 25 % ověřovaných dat a tří souborů označených `filename-missing` s nulovou velikostí. Tyto označují soubory chybějící na



Obr. 6.1: Ověřování CRC

serveru. V pravé dolní části obrázku je zobrazen stav po kompletním nahrání souborů. To je signalizováno změnou hodnot status baru. Zároveň je zde uvedeno, že se jedná o žánr Rap a rok je uveden 2017, který byl získán z metadat souborů. Tyto hodnoty dokazují funkčnost třídění a také ověřování CRC.

Vedení statistik o přenesených datech pocházejících od pluginu PZS-NG je uvedeno níže. Pořízeno po nahrání všech čtyř mp3 souborů. Ze serveru je tento výpis přijat jako odpověď s kódem 250 následovaná textem.

```

250- .-----===== PZS-NG v1.2.0 =====.
250- |--[ U~S~E R T O~P ]-----.
250- |                                     '-----|
250- |      1 xmatou27/NoGroup           20.5M   4F 100.0%   7950KBs |

```

```

250- |-----|
250- | 1 Total                20.5M   4F 100.0%   7950KBs |
250- |
250- |--[ G R 0~U~P T 0~P ]=----. |
250- |
250- | 1 NoGroup              20.5M   4F 100.0%   7950KBs |
250- |-----|
250- | 1 Total                20.5M   4F 100.0%   7950KBs |
250- |
250- |--[ I~D 3 - T A~G ]=-----. |
250- |
250- | Artist : trapdaddyflex |
250- | Album  : Four Loko     |
250- | Genre  : Rap           | Rate   : 320kbit/s |
250- | Tracks : 4             | Year   : 2017 |
250- | Encoder: NA           | Preset: NA |
250- |-----|

```

Je vidět, že PZS-NG vede statistiku o množství nahraných dat pro každého uživatele a skupinu. Také vede záznamy o autorovi, albu, žánru atd.

Kolik lze nahrát nebo stáhnout dat je uvedeno v následujícím výpisu, který se zobrazí po zadání příkazu `site stat`. Byl nastaven parametr `ratio` na hodnotu 4, což vyjadřuje, že z každého 1 MB nahraných dat lze stáhnout 4 MB. Kolik server umožňuje stáhnout přihlášenému uživateli je uvedeno v položce Credits.

```

226- [Ul: 15.6MB] [Dl: 0.0MB] [Speed: 0.00K/s] [Free: 13228MB]
226  [Section: DEFAULT] [Credits: 56.4MB] [Ratio: UL: 1:4 | DL: 1:1]

```

Tento výpis byl pořízen před započítáním nahrávání dat. Následně bylo nahráno 20,7 MB dat. Jak je vidět níže, hodnota Credits zvýšila svoji hodnotu o čtyřnásobek množství nahraných dat.

```

226- [Ul: 36.3MB] [Dl: 0.0MB] [Speed: 0.00K/s] [Free: 13207MB]
226  [Section: DEFAULT] [Credits: 139.1MB] [Ratio: UL: 1:4 | DL: 1:1]

```

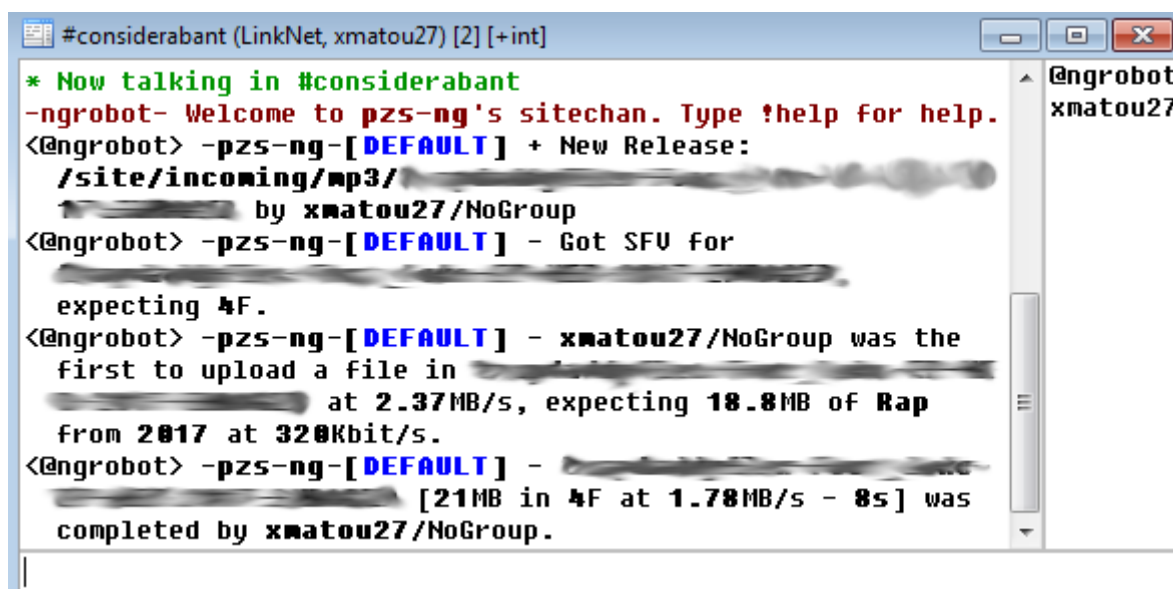
Pro přihlášení na IRC server byl použit program mIRC ve zkušební verzi (trial). IRC kanál na serveru je pouze pro zvané, což je možné ověřit pokusem o připojení. Pokud je do řádku hlavního okna serveru v mIRC zadán následující příkaz, objeví se informace o přístupu pouze pozvaným uživatelům. Odpověď je zobrazena pod příkazem.


```
/join #considerabant  
#considerabant unable to join channel (invite only)
```

Proto je nutné uživatele nejprve pomocí SITE příkazu zadaného do FTP Rush pozvat. Příkaz pro pozvání uživatele se jménem xmatou27 na IRC serveru je následující.

```
site invite xmatou27
```

Po zadání tohoto příkazu se objeví pozvánka na IRC kanál spravovaný nakonfigurovaným robotem. Po kliknutí dojde k připojení do kanálu. Při nahrávání stejných dat jako výše se na IRC kanále zobrazují informace o nahrávaných datech a jejich kompletnosti.



Obr. 6.2: Zobrazení informací o datech na IRC kanále

Jak je vidět na obr. 6.2, na IRC kanále s názvem #considerabant se nacházejí nakonfigurovaný robot a pozvaný uživatel xmatou27. Robot zaregistroval vytvoření nové složky na FTP serveru uživatelem, dále nahrání souboru sfv a nahrání prvního souboru do tohoto vytvořeného adresáře. Také je zde záznam o kompletnosti dat ve složce dle sfv souboru. Také je zde uvedeno označení žánru nahrávaných dat, údaj o roce a také bitové rychlosti. Text DEFAULT označuje sekci, ve které se adresář nachází. Může existovat více sekcí dle konfigurace.

Příkazy určené robotovi jsou uvozeny vykřičníkem (!), po kterém následuje požadovaný příkaz. Například zadání příkazu !free vypíše volný prostor na serveru, například uvedeným způsobem.

```
<@ngrobot> -pzs-ng-[FREE] + [DEFAULT: 414.71GB free of 441.79GB]  
<@ngrobot> -pzs-ng-[FREE] + [TOTAL: 414.71GB free of 441.79GB]
```

7 Závěr

V této bakalářské práci byl představen protokol FTP. Bylo uvedeno, jaké podporuje režimy přenosu. Dále byly vypsány vybrané příkazy a odpovědi definované v FTP, následované modifikacemi přidávajícími šifrování k tomuto protokolu, konkrétně jde o modifikace založené na SSL, TLS a SSH protokolu.

Další kapitola pojednává o některých příkazech IRC a oprávněních. Pro FTP server je možné využít robot Eggdrop, který zajistí přímé spojení mezi serverem a IRC kanálem. Byly vypsány základní informace o distribuci linuxu Debian, například používané příkazy, informace o iptables nebo zabezpečeném vzdáleném připojení.

FTP démon GFTPD, který byl spolu s Eggdrop nainstalován na fyzický stroj s distribucí Debian. Bylo poukázáno na jeho vlastnosti, instalaci a možnost konfigurace. Byl představen i plugin pro pokročilejší třídění hudby PZS-NG a také skript ngBot, který po začlenění do Eggdrop vypisuje údaje o nahrávaných souborech na IRC kanál vybraného serveru.

GFTPD s pluginem PZS-NG zvládá kontrolovat CRC součty v reálném čase a porovnávat je s údaji v sfv souborech. Po nahrání souboru sfv a následnému nahrávání datových souborů na server se zkontrolují kontrolní součty a případně se upraví statistiky. Plugin PZS-NG v závislosti na konfiguraci umožňuje pokročilejší třídění hudby do složek dle definovaných autorů, žánru, roku atd. Je rovněž možné například určit, které žánry se nemají nahrávat. FTP server ve spolupráci s PZS-NG buď upozorní, nebo neumožní soubor nahrát.

V rámci řešení bakalářské práce byly prezentovány dílčí výsledky na studentské konferenci EEICT.

Literatura

- [1] POSTEL, J. a J. REYNOLDS. RFC 959 - File Transfer Protocol. *IETF Tools* [online]. 1985 [cit. 8. 11. 2017]. Dostupné z: <https://tools.ietf.org/html/rfc959>
- [2] KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 9788025122365.
- [3] BERNERS-LEE, T., L. MASINTER a M. MCCAHERILL. RFC 1738 - Uniform Resource Locators (URL). *IETF Tools* [online]. 1994 [cit. 7. 11. 2017]. Dostupné z: <https://tools.ietf.org/html/rfc1738>
- [4] HOROWITZ, M. a S. LUNT. RFC 2228 - FTP Security Extensions. *IETF Tools* [online]. 1997 [cit. 14. 11. 2017]. Dostupné z: <https://tools.ietf.org/html/rfc2228>
- [5] KRČMÁŘ, Petr. Jak nahradit FTP pomocí SFTP a zamknout uživatele. *Root.cz* [online]. 2010 [cit. 16. 11. 2017]. Dostupné z: <https://www.root.cz/clanky/jak-nahradit-ftp-pomoci-sftp-a-zamknout-uzivatele/>
- [6] FORD-HUTCHINSON, P. RFC 4217 - Securing FTP with TLS. *IETF Tools* [online]. 2005, [cit. 17. 11. 2017]. Dostupné z: <https://tools.ietf.org/html/rfc4217.html>
- [7] FTPS - Obsolescent Secure FTP. *Company home Page - SSH Communications Security | SSH.COM* [online]. 2017 [cit. 17. 11. 2017]. Dostupné z: <https://www.ssh.com/ssh/ftp/ftps#sec-FTPS-Combining-FTP-and-SSL>
- [8] CHARALABIDIS, Alexander. *The book of IRC*. Berkeley, Calif.: Publishers Group West [distributor], c2000. ISBN 978-188-6411-296.
- [9] *Eggheads* [online]. [cit. 20. 4. 2018]. Dostupné z: <https://eggheads.org/>
- [10] *Debian – Univerzální operační systém* [online]. ©1997-2016 [cit. 24. 4. 2018]. Dostupné z: <https://www.debian.org/>
- [11] *AbcLinuxu.cz - Linux na stříbrném podnose* [online]. ©1999-2015 [cit. 26. 4. 2018]. Dostupné z: <http://www.abclinuxu.cz/ABCLinuxu>
- [12] *GlFTPd :: We make files transfer!* [online]. ©1997-2012 [cit. 21. 11. 2017]. Dostupné z: <https://glftpd.eu/>
- [13] GlFTPd Docs for v2.07. *GlFTPd :: We make files transfer!* [online]. 2017 [cit. 27. 11. 2017]. Dostupné z: <https://glftpd.eu/latest/docs/glftpd.docs>

- [14] *Mewbies.com Tutorials for the Installation and Usage of Softwares for Linux, Mac, Windows and iOS* [online]. 2014 [cit. 28. 11. 2017]. Dostupné z: <http://mewbies.com/>
- [15] Pzs-ng/README at master · pzs-ng/pzs-ng · GitHub. *The world's leading software development platform · GitHub* [online]. 2012 [cit. 28. 11. 2017]. Dostupné z: <https://github.com/pzs-ng/pzs-ng/blob/master/README>
- [16] Pzs-ng/INSTALL at master · pzs-ng/pzs-ng · GitHub. *The world's leading software development platform · GitHub* [online]. 2012 [cit. 28. 11. 2017]. Dostupné z: <https://github.com/pzs-ng/pzs-ng/blob/master/INSTALL>
- [17] Pzs-ng/README.ZSCONFIG at master · pzs-ng/pzs-ng · GitHub. *The world's leading software development platform · GitHub* [online]. 2015 [cit. 28. 11. 2017]. Dostupné z: <https://github.com/pzs-ng/pzs-ng/blob/master/README.ZSCONFIG>
- [18] MATOUŠEK, Jan. Advanced FTP server. In: *Proceedings of the 24 th Conference STUDENT EEICT 2018*. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2018, 135 – 137. ISBN 978-80-214-5614-3. Dostupné také z: http://www.feec.vutbr.cz/EEICT/archiv/sborniky/EEICT_2018_sbornik.pdf
- [19] Pzs-ng/sitebot at master · pzs-ng/pzs-ng · GitHub. *The world's leading software development platform · GitHub* [online]. 2017 [cit. 8. 5. 2018]. Dostupné z: <https://github.com/pzs-ng/pzs-ng/tree/master/sitebot>

Seznam symbolů, veličin a zkratek

ACK	Acknowledgement
BSD	Berkeley Software Distribution
FIN	end of connection
FTP	File Transfer Protocol
FTPS	FTP over SSL/TLS
GIFTPd	GreyLine File Transfer Protocol Demon
IPv4	Internet Protocol verze 4
IPv6	Internet Protocol verze 6
IRC	Internet Relay Chat
JPEG	Joint Photographic Experts Group
NAT	Network Address Translation
NVT	Network Virtual Terminal
PZS-NG	Project ZS – Next Generation
RFC	Request for Comments
SFTP	SSH File Transfer Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
SYN	Synchronize sequence numbers
TCL	Tool Command Language
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security

Seznam příloh

A	Změněné konfigurační soubory	48
A.1	glftpd.conf	48
A.2	zsconfig.h	50
A.3	robot.conf	52
A.4	ngBot.conf	54
B	Obsah DVD	57

A Změněné konfigurační soubory

Zde jsou přiloženy změny v konfiguračních souborech pro GLFTPd, Eggdrop, PZS-NG a ngBot

A.1 glftpd.conf

Tento soubor se nachází v adresáři /etc. Jsou uvedeny provedené změny a některé další vybrané volby.

```
CERT_FILE /glftpd/etc/ftpd-ecdsa.pem
#DHPARAM_FILE /glftpd/ftpd-dhparam.pem

ALLOWED_PROTOCOLS TLSv1.2 TLSv1

rootpath /glftpd

# Path relative to the ROOTPATH.
datapath /ftp-data

# TLS enforcements.
userrejectsecure -glftpd !*
userrejectinsecure !-glftpd *
denydiruncrypted !-glftpd *
denydatauncrypted !-glftpd *

# PASV configuration
pasv_ports 6000-6100

#####
# SECTION # KEYWORD DIRECTORY SEPARATE CREDITS #
#####
stat_section DEFAULT * yes

#####
##### THE RIGHTS SECTION BEGINS HERE #####
#####
# (you can use a ! in front of any group/user/flag to negate it) #
# The default is no, you don't need to add "!" at the end #
```



```

#                                                                 #
# Function          Path          =GROUP or -username or X (flag)  #
#####
upload      *          *
resume     *          *
mkdir      *          *
download   *          *
dirlog     *          *
rename     *          1 =STAFF
filemove   *          1 =STAFF
renameown  *          *
nuke       *          *
unnuke    *          *
delete     *          1
deleteown *          *

#####
#####          THE RIGHTS SECTION ENDS HERE          #####
#####

secure_pass      a2..  *

show_totals      *          *
show_diz .message *
show_diz .date   *
show_diz .imdb   *

free_space 20
max_users 15 5
total_users 300

dl_incomplete 1
noretrieve passwd passwd- group group-

min_homedir      /site

```

```

calc_crc *

post_check      /bin/zipscript-c *

cscript        DELE post      /bin/postdel
cscript RMD post /bin/datacleaner

cscript        SITE[:space:]NUKE  post  /bin/cleanup
cscript        SITE[:space:]UNNUKE post  /bin/postunnuke
cscript        SITE[:space:]WIPE  post  /bin/cleanup
site_cmd      RESCAN            EXEC /bin/rescan
custom-rescan  !8 *

cscript        RETR            post /bin/dl_speedtest
site_cmd      AUDIOSORT        EXEC      /bin/audiosort
custom-audiosort !8 *

##### Location ##### Max number of lines in Display #
requests      /ftp-data/misc/requests      10
#####

site_cmd RULES          TEXT      /ftp-data/misc/site.rules
site_cmd LOCATE         EXEC      /bin/locate.sh

site_cmd INVITE         EXEC      /bin/invite.sh
custom-invite          !8 *

custom-rules          !8 *

```

A.2 zsconfig.h

Tento soubor je umístěn v adresáři se zdrojovými kódy v podadresáři `zipscript/conf/`. Některé řádky byly rozděleny z důvodu jejich délky. Každý řádek, pokud nezačíná znakem #, je pokračováním předchozího. Nejsou zde uvedeny všechny volby.

```

/* DO NOT USE WILDCARDS HERE! */
#define sitepath_dir      "/site/"
#define group_dirs        "/site/groups/"
#define zip_dirs          "/site/test/ /site/incoming/0day/"
#define sfv_dirs          "/site/test/ /site/incoming/mp3/"

```

```

/site/incoming/games/ /site/incoming/apps/
/site/incoming/musicvideos/ /site/incoming/requests/"
#define nocheck_dirs          "/site/private/"
#define noforce_sfv_first_dirs "/site/incoming/requests/"
#define audio_nocheck_dirs "/site/groups/ /site/incoming/requests/"
#define allowed_types_exemption_dirs "/site/incoming/musicvideos/"
#define check_for_missing_nfo_dirs  "/site/incoming/games/
                                   /site/incoming/apps/"
#define cleanupdirs  "/site/test/ /site/incoming/games/
                    /site/incoming/apps/ /site/incoming/musicvideos/"
#define cleanupdirs_dated          "/site/incoming/0day/%m%d/
                                   /site/incoming/mp3/%m%d/"

#define check_for_missing_sample_dirs "/site/incoming/movies/"
#define create_missing_sample_link  FALSE

#define short_sitename            "NG"

#define debug_mode                 FALSE
#define debug_altlog               TRUE

#define status_bar_type            BAR_DIR
#define incompleteislink          TRUE

#define ignored_types              ",date,diz,debug,message,
                                   imdb,html,url,m3u,metadata"

#define deny_double_sfv            FALSE
#define force_sfv_first           FALSE

#define audio_genre_path           "/site/incoming/music.by.genre/"
#define audio_artist_path         "/site/incoming/music.by.artist/"
#define audio_year_path           "/site/incoming/music.by.year/"
#define audio_group_path          "/site/incoming/music.by.group/"
#define audio_language_path       "/site/incoming/music.by.language/"
#define allowed_constant_bitrates "160,192,320"
#define allowed_years              "2007,2008,2009,2010,2011,2012,2017"
#define banned_genres              "Christian Rap,Christian Gangsta Rap,
                                   Contemporary Christian,Christian Rock"

```

```

#define allowed_genres          "Top 40,Pop Funk,Rock,Pop"
#define audio_genre_sort      FALSE
#define audio_year_sort      FALSE
#define audio_artist_sort    FALSE
#define audio_group_sort     FALSE
#define audio_language_sort  FALSE
#define audio_cbr_check      TRUE
#define audio_cbr_warn       TRUE
#define audio_year_check     TRUE
#define audio_year_warn     TRUE
#define audio_banned_genre_check TRUE
#define audio_allowed_genre_check FALSE
#define audio_genre_warn     TRUE

#define enable_nfo_script    TRUE
#define nfo_script          "/bin/psxc-imdb.sh"

```

A.3 robot.conf

Tento konfigurační soubor je umístěn v adresáři, kam byl Eggdrop nainstalován. Jsou uvedené jen některé volby z konfiguračního souboru, neboť tento soubor je velmi dlouhý.

```

#! /home/ircbot/irc-bot/eggdrop
# ^- This should contain a fully qualified path to your Eggdrop
# executable.

## More detailed descriptions of all these settings can be found in
## doc/settings/.

loadmodule dns      ; # Asynchronous DNS support
loadmodule channels ; # Channel support
...
loadmodule uptime   ; # Centralized uptime stat collection
# (http://uptime.eggheads.org)

##### BASIC SETTINGS #####
set nick "ngrobot"

```

```

set altnick "ngrobot_"

set username "lamest"

set pidfile "robot.pid"

set servers {
irc.link-net.org:+7000
}

set prefer-ipv6 0

##### LOG FILES #####
set log-forever 0

## Code to set settings based on the above setting, do not edit this.
if {${log-forever}} {
    set switch-logfiles-at 2500
    set keep-all-logs 0
}

##### FILES AND DIRECTORIES #####
set userfile "robot.user"

set help-path "help/"

listen 33333 all

set ssl-verify-server 0

set dns-servers "8.8.8.8 8.8.4.4"

set chanfile "robot.chan"

#### SERVER MODULE ####
## What is your network?
## 0 = EFnet
## 1 = IRCnet
## 2 = Undernet

```

```

## 3 = DALnet
## 4 = +e/+I/max-modes 20 Hybrid
## 5 = Others. See eggdrop.conf for settings related to this.
set net-type 5

## This is a Tcl script to be run immediately after connecting
## to a server.
bind evnt - init-server evnt:init_server

proc evnt:init_server {type} {
    global botnick
    putquick "MODE $botnick +i-ws"
}

set default-port 6667

set notefile "robot.notes"

source scripts/alltools.tcl
source scripts/action.fix.tcl
source scripts/dccwhois.tcl

source pzs-ng/ngBot.tcl

source scripts/userinfo.tcl
loadhelp userinfo.help

```

A.4 ngBot.conf

Tento soubor je v adresáři s instalací Eggdrop v podadresáři `pzs-ng/`. Jsou uvedeny pouze některé volby.

```

set debugmode           "TRUE"
set cmdpre              "!"
set sitename            "pzs-ng"
set mainchan            "#considerabant"
set glroot              "/glftpd/"
set announce(THEMEFILE) "themes/classic.zst"

```

```

#####
# Bins, Logs & Paths Check this lines.
#####
set location(GROUP)          "$glroot/etc/group"
set location(PASSWD)         "$glroot/etc/passwd"
set location(USERS)          "$glroot/ftp-data/users/"
set location(GLCONF)         "/etc/glftpd.conf"
set glftpdlog(NORMAL)        "$glroot/ftp-data/logs/glftpd.log"
set loginlog(NORMAL)         "$glroot/ftp-data/logs/login.log"
set sysoplog(NORMAL)         "$glroot/ftp-data/logs/sysop.log"
set binary(GLFTPD)           "$glroot/bin/glftpd"
set binary(INCOMPLETE)       "$glroot/bin/incomplete-list.sh"
set binary(PASSCHK)          "$glroot/bin/passchk"
set binary(SHOWLOG)          "$glroot/bin/showlog"
set binary(STATS)            "$glroot/bin/stats"
set binary(WHO)              "$glroot/bin/sitewho"
set binary(DF)               "/bin/df"
set binary(PING)             "/bin/ping"
set binary(UPTIME)           "/usr/bin/uptime"

#####
# Misc. Settings
#####
set bindnopro                "FALSE"
set speed(INCOMING)          12500
set speed(OUTGOING)          12500
set device(0)                "/dev/sda2 DEFAULT"
set local_devices_only       "TRUE"
set device_size               "AUTO"

#####
# Stats Settings
#####
set stats(hide_zeros)        "TRUE"
set stats(hide_users)         "glftpd"
set stats(hide_groups)       "glftpd"

#####

```

```

# Sections
#####

set denypost          "/site/groups/* /site/private/*"
set sections          "MV"
set paths(ODAY)       "/site/incoming/Oday/*"
set paths(MV)         "/site/incoming/musicvideos/*"
set chanlist(MV)      $mainchan
set chanlist(DEFAULT) $mainchan
set chanlist(WELCOME) $mainchan
set statsection(0)    "DEFAULT"
set statsection(1)    "PRE"

#####

# Invite
#####

set enable_irc_invite "FALSE"
set invite_channels   $mainchan
set invite_channels_rights "!6 *"

set splitter(CHAR)    "\n"

```


B Obsah DVD

```
/ ..... kořenový adresář přiloženého DVD
├── BP_Pokrocily_FTP_server.pdf ..... elektronická verze práce
├── zdrojove_soubory ..... zdrojové soubory BP ze systému LATEX
│   ├── loga ..... loga školy a fakulty
│   ├── obrazky ..... obrázky použité v práci ve formátech png, eps a pdf
│   ├── pdf ..... pdf stránky generované informačním systémem
│   ├── text ..... zdrojové textové soubory
│   └── BP_Pokrocily_FTP_server.tex ..... hlavní soubor pro sazbu BP
├── lab_uloha ..... soubory pro laboratorní úlohu
│   ├── zdrojove_soubory ..... zdrojové soubory návodu ze systému LATEX
│   │   ├── lab_uloha_student.tex ..... soubor pro sazbu studentského návodu
│   │   └── lab_uloha_ucitel.tex ..... soubor pro sazbu učitelského návodu
│   ├── lab_uloha_ucitel.pdf ..... elektronická verze návodu pro učitele
│   ├── lab_uloha_student.pdf ..... elektronická verze návodu pro studenty
│   └── Lab_glftpd ..... složka s virtuálním strojem pro Virtualbox
└── konfigurace ..... konfigurační soubory
```