Univerzita Karlova v Praze
Pedagogická fakulta

Katedra informačních technologií a technické výchovy

Zabezpečení školní počítačové sítě na bázi operačního systému Linux

Autor: Vladimír Svoboda
Aprobace: RV-TIV

Vedoucí práce: PhDr. Jan Víšek

Praha 2009

ABSTRAKT:

Předmětem diplomové práce je zmapovat současné možnosti připojení školních počítačových sítí k internetu a navrhnout jejich vhodné zabezpečení. Jsou zde probírána možná nebezpečí počítačových útoků a nastíněna možná řešení obrany proti nim. V práci je zdůvodněno nasazení ochrany školní počítačové sítě na bázi operačního systému Linux. Na modelovém příkladu je ukázán způsob instalace a nastavení služeb tak, aby mohli práci použít správci školních počítačových sítí. Tento model byl v rámci práce vyzkoušen v praxi na dvou školách. Toto testování v reálném prostředí prokazuje vhodnost zvolených prostředků pro řešení tohoto typu úkolu.

SUMMARY:

Subject of this thesis is to describe contemporary possibilities in connecting school computer networks to the Internet and design appropriate security system. There are discussed possible threats of computer attacks and relevant ways of defese against them. Thesis gives reasons to choose security solution based on Linux operating system in school computer networks. Model example shows installation and services settings in order to the thesis is being usable by school computer network administrators. This model have been tested in real enviroment of two schools. That real life test have proven that chosen means can solve the given situation.

Poděkování

Chtěl bych tím to poděkovat vedoucímu diplomové práce PhDr. Janu Víškovi za vedení a za zajímavé podněty, jenž přispěly k výsledné podobě práce.

Zároveň chci poděkovat své rodině a blízkým přátelům za veškerou podporu při studiu.

Prohlašuji, že jsem diplomovou práci vypracoval samostatně pod vedením PhDr. Jana Víška. V práci jsem použil informační zdroje uvedené v seznamu.

Praha 24.4.2009

……..

podpis

1 Obsah

2 Úvod

V letech 2001-2005 probíhala realizace projektu Ministerstva školství, mládeže a tělovýchovy „SIPVZ PIII – Infrastruktura“, obecně známého pod názvem Internet do škol či INDOŠ, který byl součástí vládních podpůrných opatření realizovaných v rámci první etapy programu Státní informační politiky ve vzdělávání (SIPVZ). Během března až listopadu roku 2005 tento projekt skončil. V rámci tohoto projektu bylo k internetu připojeno 3620 škol. Po ukončení projektu byla nucena většina škol připojení k internetu řešit jiným novým způsobem, neboť způsob a platforma připojení zvolená v rámci projektu byla bez plné finanční podpory ministerstva školství nevýhodná. Úkolem této práce bylo zmapovat současný stav způsobů připojení na školách a navrhnout optimální řešení v poměru cena / bezpečnost. Práce se nezabývá samotnými technologiemi a cenovými variantami připojení, neboť toto se mění velmi rychle v závislosti na nabídce trhu a na technologickém vývoji přenosových tras.

3 Vymezení problematiky

Jedna ze vzdělávacích oblastí v Rámcově vzdělávacím programu (RVP), jenž nabyl platnosti 1.9.2005, se nazývá Informační a komunikační technologie. V rámci této vzdělávací oblasti je třeba umožnit žákům dosáhnout základních úrovní informační gramotnosti, které jdou definovány jako elementární dovednosti v ovládání výpočetní techniky, orientovat se ve světě informací, tvořivě s nimi pracovat a využívat je v dalším vzdělávání a praktickém životě.[1] Zde je definován i vzdělávací obsah oboru, kde očekávanými výstupy v části „Vyhledávání informací a komunikace" jsou znalosti při vyhledávání informací na internetu, vyhledávání informací na portálech, v knihovnách a databázích a komunikace pomocí internetu či jiných běžných komunikačních zařízeních. Z údajů Českého statistického úřadu z roku 2007 vyplývá, že počítač je k dispozici v pouhých 55,6 % domácností.[2] Má-li žák na konci povinné školní docházky ovládat komunikaci přes e-mail, chat, nebo má-li si osvojit zmíněné vyhledávání informací na internetu, musí mít možnost v rámci výuky přístupu k tomuto médiu v rámci školy.

V úvodu byl zmíněn projet „Internet do škol" Ministerstva školství (MŠMT), který skončil v průběhu roku 2005. Díky němu bylo připojeno 3620 škol k internetu dodanou technologií od generálního dodavatele Autocont. Tento celý projekt byl hrazen z rozpočtu ministerstva a příliš se nehledělo na ekonomičnost. Po skončení projektu byly mnohé školy nuceny vyřešit připojení k internetu jiným způsobem, neboť si nemohly dovolit stávající připojení hradit ze svého rozpočtu. Současně nutno podotknout, že na konci projektu bylo sice připojeno k internetu 3600 škol, ale většina rychlostí pouhých 64 kbit/sec, což na dobu konce roku 2005 bylo opravdu málo. Školy byly s průběhem projektu vcelku spokojeny, neboť v jeho rámci získaly zdarma mnoho počítačů a učeben, které by si jinak nemohly dovolit. Generální partneři projektu Internet do škol – Autocont On Line a.s. a Český Telecom (později Telefónica 02) - se rozhodli pokračovat ve službách školám a vytvořili nový projekt „Pokračování", ve kterém bylo školám zajištěno nové, technologicky vyspělejší a rychlejší připojení

[1] Rámcově vzdělávací program pro základní vzdělávání. Výzkumný ústav pedagogický v Praze 2005. str. 34-35

[2] Statistika rodinných účtů - vybavenost, Český statistický úřad. [citováno 10.4.2009]. Dostupné na WWW: http://www.czso.cz/csu/2008edicniplan.nsf/t/710027FB6E/$File/30010865.pdf

k internetu. MŠMT tento projekt dotovalo 70%. Počínaje listopadem 2007 ukončilo MŠMT všechny dotace připojení škol k internetu. Školy si další konektivitu k internetu musejí plně hradit. Pokud školy nechtěly ponechat služby ve stávajícím stavu, byly nuceny najít si „alternativního operátora“ a vrátit Telefónice 02 router, který zajišťoval technologické rozhraní mezi počítačovou sítí školy a poskytovaným internetem.

Tato diplomová práce se zabývá možností nasazení operačního systému Linux právě jako technologického rozhraní mezi připojením k internetu od libovolného poskytovatele a školní počítačovou sítí. V první části diplomové práce jsou zmíněny důvody pro jeho nasazení v porovnání s ostatními možnostmi. V této části jsou probrány i rizika bezpečnosti počítačových sítí z hlediska internetové konektivity a síťových útoků. Druhá část je zaměřena na praktickou ukázku konfigurace routeru na bázi operačního systému Linux v nasazení v modelové škole. Tento model byl vyzkoušen v provozu na dvou základních školách.

4 Cíl práce

Cílem diplomové práce bylo zmapování současné situace zabezpečení internetu ve školách, zmapování současné nabídky možností zabezpečení a nalézt optimální řešení zabezpečení školní počítačové sítě v poměru cena / bezpečnost s přihlédnutím na dostupnost, snadnost instalace a spravovatelnosti, zajištění aktualizací a možnost implementace uživatelských nadstaveb.

Součástí práce byl vývoj a otestování nadstavby řešící fenomén dnešní doby, kdy žáci při výuce v počítačové učebně v rámci výuky procházejí internet, prohlížejí a stahují videa, hrají síťové počítačové hry. To vše má za následek nižší soustředěnost na výuku. Dalším nevhodným použitím či skoro zneužitím školní počítačové sítě je to, že v době testů vyhledávají informace na internetu místo ve své paměti. Rozmáhá se též nový způsob napovídání pomocí IRC klientů (ICQ, chat). Nadstavba by měla umožňovat vypnout na žákovských počítačích zcela přístup na internet s tím, že případný přístup pro žáky na povolené sdílené prostředky tímto neměl být dotčen. Zbytek školní počítačové sítě by měl běžet bez omezení. Vyučující v učebně by měl mít možnost i v době, kdy mají žáci omezen přístup k internetu, na své učitelské pracovní stanici prezentovat práci s internetem.

5 Zhodnocení současného stavu a popis možností připojení škol k internetu

5.1 Šetření současného stavu vybavenosti škol a připojení škol k internetu

V rámci šetření současného stavu byly osloveny náhodně vybrané základní školy v rámci celé České republiky. Byl vypracován dotazník s otázkami zjišťujících základní stav vybavenosti školy a způsob připojení školy k internetu a s ním byly školy osloveny. Výsledkem šetření je, že všechny školy mají alespoň jednu počítačovou učebnu a všechny školy mají nějaké připojení k internetu. Toto připojení si školy zařizovaly v rámci kompetence dané MŠMT.

Výsledky způsobu připojení a technologie směrování (routeru) v tabulce 1.

Přehled způsobů připojení a zabezpečení školní počítačové sítě		
Technologie připojení	ADSL	9
	HDSL	15
	WiFi	5
	Jiné	1
Typ routeru	V rámci ADSL modemu	5
	Samostatný počítač s OS Windows	11
	Samostatný počítač s OS Linux	8
	Samostatný počítač s OS Novell	0
	Router Cisco	3
	Router SOHO "HW krabička"	3

5.2 Technologie používané pro připojení školní počítačové sítě do internetu

V dnešní době je možno počítačovou síť k internetu připojit několika způsoby.

- Pevným metalickým dedikovaným okruhem např. HDSL
- Pevným metalickým okruhem ADSL
- Připojením pomocí WiFi technologie
- Připojení metalickou vytáčenou linkou
- Připojení bezdrátovou technologií typu GPRS,EDGE,CMDA

Poslední dvě zmíněné se pro připojení školní počítačové sítě příliš nehodí. Mají nízkou přenosovou rychlost a vysoké náklady na provoz (metalická vytáčená linka). Proto již dále nebudou zmiňovány. Tato připojení lze doporučit pouze jako záložní spoj.
Připojení školy je možno realizovat pomocí prvních tří z výše uvedených způsobů a to nejlépe od nějakého renomovaného profesionálního poskytovatele. Například nabídka WiFi připojení od občanských sdružení typu CZFree Net je sice velmi finančně zajímavá, ale není zajištěna možnost získání veřejné statické IP adresy, důležité například pro dálkovou správu, nebo není většinou smluvně zajištěna přenosová rychlost, kvalita a dostupnost služby.

5.3 Routery / firewally používané pro připojení počítačové sítě k internetu

5.3.1 Router na bázi SOHO

Jedná se o router používaný při připojování malých a domácích sítí. V současné době bývá k němu integrován malý switch, většinou čtyřportový. Dalším doplňkem u SOHO routerů bývá WiFi rozhraní. To je možné u některých routerů nastavit jak v režimu klient – tedy WiFi rozhraní je jako vstupní rozhraní internetu nebo jako přístupový bod a poté je možnost se připojit nějakým dalším WiFi zařízením (notebook) v rámci lokální počítačové sítě. Poskytuje základní funkce firewallu, jako je překlad adres NAT, přesměrování portů, například pro některé služby a hry.

Výhody:

- malý
- jednoduchá instalace
- malá spotřeba
- levný

Nevýhody:

- pouze základní funkce
- nemožnost uživatelské nadstavby
- nestavový firewall
- nízká odolnost proti síťovým útokům (DOS, podvrhnutí adresy...)

5.3.2 Router v rámci ADSL modemu

Jedná se vlastně o kombinaci ADSL modemu a SOHO routeru v jednom pouzdře. Výstup ADSL modemu je zaveden přímo do SOHO routeru, tedy odpadá nutnost dalšího propoje. Klady a zápory jsou stejné jako u samostatného SOHO routeru.

5.3.3 Router jako samostatný počítač s OS Windows

Po hardwarové strance stránce se jedná o „klasický“ počítač se dvěmi síťovými kartami. Jako operační systém je instalován operační systém Microsoft Windows. Síťové služby jako firewall, překlad adres a jiné je potřeba k tomuto dokoupit jako nadstavbu. Náklady na pořízení takovéhoto nadstavbového systému jsou v řádech tisíců až desetitisíců a záleží na rozsáhlosti sítě a množství služeb, které má systém poskytovat. Další nadstavbou, která je třeba do routerů na bázi operačního systému MS Windows přidat, je antivir. Systémy MS Windows nevynikají přílišnou odolností prosti síťovým a virovým útokům a útočníkovi nedá příliš práce, když ne systém napadnout, tak alespoň vyřadit z provozu. Ze statistik vyplývá, že úspěšnost napadení stroje s operačním systémem Windows je o 75% vyšší než například s operačním systémem Linux.[1]

[1] Zone-H ORG – Unrestricred information. [citováno 5.4.2009]. Dostupné na www: www.zone-h.orh

Výhody:

- lehká „přehledná“ konfigurace pomocí grafického nástroje
- lokalizováno do češtiny
- sice omezená, ale možnost uživatelských nadstaveb

Nevýhody:

- náročné na HW
- už samotný OS Windows je licencovaný a placený
- nadstavby jsou licencované a placené a mnohdy časově limitované
- nízká odolnost proti síťovým útokům
- nízká odolnost proti virovým útokům
- nemožnost místní ani vzdálené správy v příkazovém řádku.
- velmi pomalá reakce na objevené chyby (řádově týdny, měsíce)

5.3.4 Router jako samostatný počítač s OS Linux

Po hardwarové strance stránce se jedná opět o „klasický“ počítač se dvěmi síťovými kartami. Jako operační systém je instalován operační systém Linux. V rámci jeho distribuce, která je zdarma, bývají k dispozici všechny potřebné programové nadstavby pro provoz síťových služeb jako firewall včetně překladu adres NAT, doménový server (DNS), dynamické přidělování IP adres (DHCP), sledování provozu, omezování šířky přenosového pásma atd..... V případě vyšších nároků, například grafické zpracování statistiky síťového provozu, grafické nastavovací rozhraní pro firewall a další služby, je možno zakoupit i komerční software. Některé právě zmíněné služby je možno zprovoznit i v rámci bezplatné distribuce, jen je k tomu potřeba příslušných znalostí. Velikou výhodou je možnost dálkové správy přes příkazovou řádku. V případě nějakého útoku, kdy útočník zabere celé přenosové pásmo, je grafická ovládací konzole z důvodu množství přenášených dat naprosto nepoužitelná. U Linuxu je třeba též vyzdvihnout jeho stabilitu a to, že na něj zatím neexistují viry.

Výhody:

- nepříliš náročné na HW
- samotný operační systém Linux je zdarma
- je možno vybrat si nadstavbu zdarma či komerční (placenou)
- možnost naprogramovat jednoduše nadstavbu vlastní
- při dobré konfiguraci slušná odolnost proti síťovým útokům
- neexistence virů
- možnost místní i vzdálené správy přes příkazový řádek
- velmi rychlá odezva na nahlášenou bezpečnostní závadu (řádově hodiny)
- stabilita
- není nutno při každé instalaci, updatu atd. dělat restart
- velmi rozsáhlá komunita ochotná zdarma pomoci
- mnoho diskusních fór a webů

Nevýhody:

- plně nelokalizováno do češtiny
- ke konfiguraci jsou zapotřebí základní znalosti z oblasti IT a poč. sítí
- dokumentace jen v elektronické formě

5.3.5 Router jako server s operačním systémem Novell

Po hardwarové stránce se jedná opět o „klasický“ počítač se dvěmi síťovými kartami. Jako operační systém je instalován operační systém Novell. Ten je sám o sobě určen a provozován spíš jako souborový, autorizační nebo aplikační server. V těchto oblastech je velmi stabilní a bezpečný. Možnost routování má sice v jádře systému zakomponovanou, ale jako router / firewall nelze toto řešení doporučit, protože jsou tyto funkce složitě konfigurovatelné. Navíc není rozumné z hlediska bezpečnosti použít vstupní bránu též jako souborový server.

Výhody:

- nenalezeny

Nevýhody:

- licenčně finančně náročnější
- systém routing zvládá, ale není k tomu určen
- dlouhá doba vydávání opravných balíčků (řádově roky)
- nemožnost uživatelských nadstaveb
- složitá a nepříliš přehledná konfigurace routingových služeb

5.3.6 Router (směrovač) Cisco

Zařízení od amerického výrobce Cisco patří na trhu k absolutní špičce v síťových službách. Je nasazováno jak v centrálních bodech sítí a internetu, tak i v obyčejných sítích, kde je však zapotřebí vysoké stability a propustnosti. Hardware Cisco používá svůj vlastní operační systém zvaný IOS. Zařízení jsou „statická“ a nelze do nich přidávat uživatelské nadstavby. Jejich ovládání je třeba svěřit školenému profesionálovi.

Výhody:

- vysoká stabilita a propustnost
- vysoká bezpečnost

Nevýhody:

- vysoká cena
- konfigurace pouze profesionální a placená
- nemožnost uživatelských nadstaveb

6 Bezpečnost školní počítačové sítě

6.1 Obecně o bezpečnosti

Bezpečnost počítačových sítí je samostatný a velmi obsáhlý obor, k jehož pochopení a zvládnutí je třeba řada zkušeností, které většinou lze získat pouze dlouhodobou praxí. Základ je však možno načíst z knih a dalších dostupných materiálů zabývajících se touto částí informačních technologií. K zajištění bezpečnosti systému není třeba jen instalace firewallu a antiviru. To je pouze jedna z možností nebo spíš částí, jak bezpečnosti systému dosáhnout. K zajištění celkové bezpečnosti systému je nutno stálého studia problematiky. Dodržováním bezpečnostní politiky, tj. zajištění pravidelné aktualizace systému a souborů ochran, je možné dosáhnout efektivního stavu ochrany spravovaného systému.

6.2 Důvody nutnosti ochrany školní počítačové sítě

V rámci způsobu připojení školní počítačové sítě k internetu není důležitá jenom technologická funkčnost, ale je třeba brát na zřetel i datovou bezpečnost vnitřní sítě před počítačovým útokem z internetu. Důvody, proč vlastně školní počítačovou síť chránit, jsou následující.

- Při útoku na prostředky sítě vždy dochází k nějakému poškození softwaru, případně i hardwaru. Škola pak musí vynakládat finanční prostředky na opravu.
- Pokud je technika v poruše, nelze jí použít jako učební pomůcku a pro některé předměty je její použití nezbytné.
- Dnes je mnoho agend ve škole vedeno v elektronické podobě. Je třeba mít na paměti zákon č 101, 2000 Sb., ochraně osobních údajů, kde v §13 je jasně definováno, že „Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich

jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.“[1]

6.3 Bezpečnost již nainstalovaného systému

V následující části bude probrána bezpečnost systému a to jak z pohledu síťového provozu, tak následně z podhledu lokálního (například umístění stroje, zajištění napájení).

6.4 Druhy útočníků

Většina začínajících administrátorů si klade jednoduchou otázku, kde nalezení správné odpovědi je zásadní pro pochopení smyslu ochrany systému. Tou otázkou je „Kdo by se chtěl do mého systému dostat a proč?“. Pokud uživatel tuto otázku použije jako argument pro nižší stupeň zabezpečení a nepříliš zásadové dodržování bezpečnostních pravidel, bude vystaven provozním problémům s možnými až fatálními následky. V oblasti školy by se dalo uvažovat o napadení zničení či změně informací ve studijním informačním systému, únik důvěrných informací o žácích a učitelích nebo o ekonomické situaci školy. Útočníky lze dělit do dvou skupin na „průzkumníky“ a „opravdové crackery“.

Průzkumníkem – hackerem - lze nazvat útočníka, jehož cílem není poškodit či zničit systém. Pokus o průnik je jen pro jeho dobrý pocit, že něčeho dosáhl, něco obešel, objevil slabé místo a dokázal své schopnosti. Jemu jedno kam se dostává. Průzkumníkovi nejde o zisk, dalo by se říci, že útočí lidově řečeno ze sportu. Většinou jde o studenty, kteří se tímto způsobem baví.

Crackerem je nazýván útočník, který si oběť vybírá cíleně, jehož cílem je zisk. Ten může být finanční nebo jiný. Stroj, který napadne, může být jen „odrazovým můstkem“ pro další činnost. Napadnutý systém používá například jako skladiště ilegálních dat. Často pracuje jako nájemný vyhledavač informací či likvidátor konkurence.

[1] Zákon o ochraně osobních údajů, Část 1, Hlava 2, §13. [cit 28.2.2009]. Dostupné na WWW: <http://business.center.cz/business/pravo/zakony/oou/cast1h2.aspx>

A zde je odpověď na druhou část otázky – proč? :

- útočník hledá něco zajímavého
- instaluje do stroje „zadní vrátka“, pro případné další použití stroje
- útočník napadá firewall, protože se potřebuje dostat do vnitřní sítě
- úročník chce použít stroj jako „přestupní stanici“, aby zmátl a zneprůhlednil vyšetřování jeho další nelegální činnosti
- útočník hledá konkrétní informace a data
- útočník chce využít diskovou kapacitu napadené sítě
- útočník chce využít výpočetní kapacitu napadené sítě
- útočník napadá webserver pro vystavení vlastních informací

6.5 Druhy síťových útoků

Vzhledem k tomu, že je třeba vědět, proti čemu bude systém vnitřní počítačovou síť chránit, následuje popis základních druhů síťových útoků.

6.5.1 Útok na webserver

Nejčastějším vstupem do systému se stávají PHP scripty. Největší chybou, kterou jejich autor může udělat, je neošetření vstupů, díky kterému může útočník místo očekávaných informací předávat příkazy, které mohou být interpretrem po té zpracovány, jako kdyby do scriptu opravdu patřily. Tak lze jednouše měnit informace v databázích i souborovém systému. To samé platí o CGI scriptech. Pokud jen útočník změní některou část zobrazovaných dat, lze problém vyřešit jednoduše obnovením ze zálohy. Pokud špatně napsaný PHP či CGI script dokáže zasáhnout do souborového systému, může běh serveru vážně ohrozit.

6.5.2 Odposlech komunikace

Dalším nejběžnějším útokem je odposlechnutí důležitých dat, která procházejí nešifrovaným kanálem v internetu. Stačí, aby kdekoliv po cestě někdo naslouchal a po té údaje zneužil např. k neoprávněnému vstupu. Jelikož je internet velmi složitý a data procházejí mnoha stroji, nemůžeme si být vždy jisti, zda jsou všechny stroje bezpečné. Proto je třeba vyvarovat se při komunikaci na „veřejném“ internetu použití například

služby telnet. Další služby používající nezabezpečenou komunikaci a posílající třeba uživatelské jméno i heslo nešifrovaně jsou autorizace HTTP, POP3, IMAP nebo FTP.

6.5.3 Denial of service (DoS útok)

DoS je druh útoku, který se přímo nepoužívá pro získávání dat, ale útočník jej může použít pro podporu svých plánů. Principem je zahlcení serveru daty. Server pak pod tíhou dat nevydrží a zkolabuje. Silnější variantou tohoto útoku je DDoS – distribuovaný DoS útok, který využívá útoku více strojů na jeden a tím se síla útoků zvyšuje. Lze tím vytvořit několikanásobně silnější provoz, než je obvyklé. Takovému útoku se odolává velmi špatně. K posílení ničivé síly se navíc většinou používají vadné pakety, nesmyslné dotazy nebo otevírání spojení, která pak nejsou uzavírána. Tím se zátěž ještě znásobí. Obrana proti tomuto útoku je nelehká, nikoliv však nemožná. Jedním ze způsobů je kontrola počtu spojení z jedné IP adresy, která při překročení limitu zakáže otevření dalšího spojení. Cílem takovéhoto útoku se mohou stát například autentizační nebo logovací servery. Logovací servery pak nezaznamenávají dění na síti a útočník je při dalších postupech „neviditelný“. Pokud je server jinak dobře zabezpečen, DoS útok je jediným způsobem, jak ho vyřadit z provozu.

6.5.4 Podvržení IP adresy (IP spoofing)

Některé stroje používají k ověření přístupu z jiného stroje pouze IP adresu. Firewally mohou být nastaveny, že určité služby povolí pouze z určité skupiny IP adres, které patří konkrétním strojům. IP adresu lze však podvrhnout a paket se tváří, jako by přicházel úplně od někoho jiného. Stejně tak lze podvrhnout i MAC adresu zařízení. Spoléhat se tedy na ověřování pouze na základě IP nebo MAC adresy je velmi nebezpečné.

6.5.5 Odcizení relace

Při odcizení relace se používá podobná technika jako při falšování IP adres. Navíc je potřeba poslouchat a analyzovat celý provoz na síti. Útočník počká, až někdo nešifrovaným způsobem otevře komunikační kanál, po té podvrhne IP adresu a může zadávat vzdálenému systému příkazy. Tento útok má však své slabiny. Pokud u druhého počítače sedí uživatel, vidí přicházet data, o které si neřekl a může nějak zareagovat.

Pokud ale předání dat je prováděno automatem mezi dvěma systémy a u nichž není nikdo přítomen, je pravděpodobné, že se útok zdaří.

6.5.6 Man-in-middle (muž uprostřed)

Tento druh útoku se využívá při použití ověřování identifikace pomocí IP adresy nebo DNS záznamu. Útočník směruje komunikaci od klienta k cílovému stroji přes svůj stroj, který pak zaznamenává komunikaci. Útočníkův stroj se vydává za originální cílový server a tím lze získat ověřovací autentizační údaje (jména, hesla…) Tyto útoky jsou oblíbené zvláště u internetového bankovnictví.

6.6 Možnosti ochrany před síťovým útokem

Na základě výše uvedených druhů útoků lze použít následující nástroje pro zvýšení bezpečnosti spravovaného systému.

6.6.1 SSH

SSH[1] – Secure SHell je bezpečnou alternativou k programům, které se používají pro vzdálenou správu systému (telnet, rlogin, rsh). Jako SSH je možno označovat obecný protokol či systém. SSH je v Linuxu poskytováno pod licencí GNU a má název OpenSSH. Umožňuje několik důležitých operací:

- Ověřování identity uživatele a tím je zabránit oklamání systémů identifikace na základě IP adres.
- Šifrování přenosu dat pomocí asymetrického klíče, včetně zadávání uživatelského jména a hesla. Tím pak zabránit odposlechu autorizace a komunikace.
- Vytvoření šifrovaného tunelu na úrovni aplikační vrstvy.

Systém je postaven na asymetrických šifrách. Ty se od symetrických liší tím, že pro jejich použití je třeba dvou klíčů. Jeden pro zakódování informace, druhý pro dekódování. Nazývají se veřejný a tajný klíč. Veřejným klíčem je informace kódována a tento klíč není nutno zásadně tajit. Naopak klíč k převodu informace zpět

[1] Popis protokolu SSH. [cit 23.4.2009]. Dostupné na WWW: http://www.ietf.org/rfc/rfc4251.txt

do původní podoby je třeba chránit. Klíče nelze zaměňovat a klíče nelze je od sebe odvodit. Samotná konfigurace a použití systému SSH je popsáno v samostatné kapitole v části popisující praktické nasazení OS Linux.

6.6.2 Firewall

Pomocí firewallů[1] lze dosáhnout nejbezpečnější možné připojení k internetu. Firewally kontrolují a poté schvalují či zamítají jednotlivé pokusy o připojení mezi vnitřní počítačovou sítí a externími sítěmi, například internetem. Firewally mohou chrání síť na všech vrstvách od linkové až po aplikační. Firewally jsou umístěny na hranicích sítě a jsou přímo připojeny k okruhům, zajišťujícím přístup k jiným sítím. Fungují na základě tří metod:

- Filtrování paketů – Odmítá pokusy o připojení od neautorizovaných uživatelů a neautorizovaných služeb.
- Překlad adres NAT – Překládá adresy interních hostitelských počítačů a skrývá je před monitorováním zvenčí. Tato funkce se označuje též jako maskování IP adres.
- Služby proxy – vytváří na základě požadavků interních hostitelských počítačů mezipřipojení na aplikační vrstvě s externími hostiteli . Tím úplně ruší propojení mezi interními a externími hostiteli na síťové vrstvě.

Další funkce, které mívají firewally implementované, jsou šifrovaná autentizace a propojování virtuálních privátních sítí. Tím zajišťuje uživatelům bezpečný přístup k interním informacím z externích lokalit.

6.6.3 Proxy server

Proxy server zajišťuje jakýsi požadavkový mezistupeň mezi interními hostitelskými a externími stanicemi. Nasazení proxyserveru má následující výhody:

- datová cache server si po určitý čas pamatuje zprostředkovávanou informaci a při dalším požadavku z interní sítě tuto informaci předá ze své paměti, aniž by zatěžoval příchozí linku

[1] Root.cz, Stavíme firewall. [cit. 23.4.2009]. Dostupné na WWW: http://www.root.cz/clanky/stavime-firewall-1/

- maskuje vůči externímu hostiteli konkrétní interní stanici
- umožňuje antivirovou a antispamovou kontrolu přenášených dat
- filtrování obsahu umožňuje zabránit prostup dat mezi sítěmi podle různých kategorií. Například pornografie, propaganda rasistických organizací, informace o hackerství, atd.

6.7 Fyzické zajištění serveru

Celá bezpečnost serveru sloužícího jako bezpečnostní brána či celého počítačového systému není jen závislá na správné volbě softwaru, nastavení firewallu a služeb, ale důležitou rolí, která je bohužel mnohdy podceňována, je i fyzické zajištění hardware. Většina popsaných praktik ochrany serveru se týká ochrany před síťovým útokem. Zde budou popsány základní body, které je třeba nepodceňovat. Dostane-li se útočník přímo ke stroji, existuje jen málo technik za zabránění průniku do systému. Tedy jedna z věcí, kterou není radno podceňovat je fyzické umístění serveru. Je vhodné mít pro tyto stroje buď zvláštní místnost nebo je umístit do místnosti s omezeným přístupem lidí. Ve školním případě např. archiv nebo ředitelna. Obzvláště nevhodným místem je například počítačová učebna, kde k severu mohou o přestávce žáci. S tímto souvisí i zajištění stroje jako majetku proti krádeži. Do školy si pro data nepřijde profesionál, ale obzvláště v malých školách v menších městech a vesnicích může dojít k odcizení techniky za účelem „přivýdělku“. Po té se tedy technika může dostat do nepovolaných rukou a může být odkryt způsob ochrany počítačové sítě. To dává případnému útočníkovi šanci po obnově systému k dalšímu útoku.

V dnešní době však nejsou pro počítače nebezpečím jen lidé (útočníci). Při fyzickém zajištění serveru je třeba dbát i na ochranu před fyzikálními vlivy jako jsou elektřina, voda, oheň, teplota a vlhkost vzduchu. Jednotlivá témata budou popsána následně.

6.7.1 Elektřina

Elektřina je pro chod veškeré výpočetní techniky klíčová. Počítače jsou závislé nejen na její existenci, ale jsou náchylné i na její výkyvy. Počítačový zdroj je konstruován tak, aby bez problému vydržel výpadek v řádu desetin sekundy. Není však nezničitelný a je

zbytečné ho vystavovat nebezpečí. Proto je doporučeno použití záložního zdroje napájení (UPS). Měl by to být zdroj s takovou kapacitou, aby vydržel dodávat napájení do té doby, než uživatel či aplikace nedokončí rozdělanou práci. O informaci o výpadku napájení dá UPS serveru vědět pomocí komunikace po rozhraní RS232 nebo USB. Nasazení UPS je vhodné i z důvodu ochrany zařízení před přepětím z elektrické sítě vzniklé poruchou či atmosférickými vlivy (blesk). Proti tomuto je UPS jediná možná ochrana.

6.7.2 Voda

Pokud budou pominuty živelné katastrofy typu záplavy, je obecně pro výpočetní techniku vhodné umístit jí do suché místnosti bez přítomnosti vedení či práce s vodou. Typickým příkladem špatně umístěného serveru je místnost uklízeček. Jiným případem je pak umístění stroje v kanceláři, kde nad (nebo dokonce přímo na) jsou umístěny květiny. Při jejich zalévání může dojít nejen k poškození stroje, ale i k úrazu elektrickým proudem.

6.7.3 Oheň

Zde je třeba mít na paměti standardní protipožární opatření.

6.7.4 Teplota a vlhkost vzduchu

Dalším nepříjemným a často podceňovaným nepřítelem elektroniky je teplo. Počítače jsou velkými výrobci tepla, ale sami teplo rádi nemají. Proto je vhodné servery umístit do místnosti s klimatizací nebo alespoň s odvětráváním. Doporučovaná teplota pro běh počítačů je kolem 20ti stupňů Celsia. Klimatizace řeší i problém vlhkosti vzduchu. Vlhkost vzduchu je doporučována 20 až 30 procent.

7 Výběr vhodného řešení

Při porovnání možností probraných v kapitole 6.3 Routery / firewally používané pro připojení počítačové sítě k internetu a k přihlédnutí finančním možnostem většiny škol, vychází jako nejlepší nasazení operačního systému Linux, jako vstupně výstupního bodu mezi školní počítačovou sítí a internetem (poskytovatelem internetu). Důvod výběru je patrný z tabulky, která obsahuje název možnosti, počet výhod a nevýhod. Počtu výhod odpovídá počet kladných bodů, počtu nevýhod počet záporných bodů. Poslední sloupec tabulky obsahuje následný matematický součet hodnocení dané možnosti.

Porovnání výhod a nevýhod routerů			
Název možnosti	**Výhody**	**Nevýhody**	**Výsledek**
Router na bázi SOHO	4	-4	0
Router na bázi OS Windows	3	-7	-4
Router na bázi OS Linux	12	-3	**9**
Router na bázi OS Novell	0	-5	-5
Router Cisco	2	-3	-1

7.1 Linux – základ ní popis

Jedná se o operační systém unixového typu, přesněji jádro operačního systému, vyvíjeného pod licencí svobodného softwaru (GNU[1]). Na rozdíl od proprietálních operačních systémů jako například Microsoft Windows nebo MacOS, jsou zdrojové kódy volně k dispozici a kdokoli je může bezplatně a svobodně používat, distribuovat a upravovat. Způsob tohoto licencování se nazývá GPL – General Public Licence.

Termínem Linux je označováno samotné jádro operačního systému, ale velmi často se tento název používá i pro celé unixové operační systémy používající Linuxové jádro. Jedná se o velké balíky aplikačních softwarů a podpůrných knihoven fungujících právě

[1] Stránky o svobodném software – GNU. [cit 28.2.2009]. Dostupné na WWW: <http://www.gnu.cz/article/37/>

nad tímto jádrem. Tyto balíky se nazývají též „distribuce“. Popis, rozdíly a využití distribucí je uveden v dalších kapitolách.

Linux byl z počátku vyvíjen a používán jednotlivými nadšenci. Díky své nezávislosti, flexibilitě, spolehlivosti a bezpečnosti jej začaly používat jako serverový operační systém renomované společnosti jako Novell, Hewlett Packard, IMB, Dell. V poslední době se díky vývoji grafického rozhraní a zpříjemnění uživatelského rozhraní začíná používat i na pracovních stanicích.

Linux byl v počátcích vyvinut pro počítače kompatibilní s architekturou i386. V současné době podporuje více počítačových architektur od superpočítačů až po neobvyklé embedded systémy používané v mobilních telefonech, robotech, multimediálních přehrávačích. Právě na superpočítačích je Linux zastoupen 85%[1]. Výhodou je možnost ovládání celého systému i z příkazové řádky, což umožňuje efektivní dálkovou správu systému.

7.2 Linux historie

Základním kamenem jádra operačního systému Linux bylo založení GNU projektu Richardem Stallamem v roce 1983. Cílem GNU projektu bylo vyvinout komplexní unixový operační systém složený výhradně ze svobodného softwaru. Začátkem 90. let dvacátého století byly v rámci GNU projektu vytvořeny a shromážděny všechny potřebné součásti základního operačního systému (knihovny, překladač GCC, shell - bash, textový editor a další), ovšem bez samotného jádra operačního systému. Toto jádro pro projekt GNU se začalo vyvíjet v roce 1990 pod názvem GNU Hurd. Od vývoje se později upustilo z důvodu špatné spolupráce programátorů.

V roce 1991 Linus Torvalds započal s vývojem vlastního jádra vycházejícího z Minixu. Autor Minixu však nedal souhlas k úpravám systému a tak Linus Torvalds začal psát náhradu Minixu a vzniklo jádro, které později dostalo název Linux. Torvalds započal vývoj jádra v dobách svých studií na helsinské univerzitě původně jako svůj koníček. První verze Linuxu byla vydána 17.9.1991 a byla k dispozici ke stažení na internetu

[1] Operating systém Family share 06/2008. [cit 28.2.2009]. Dostupné na WWW: <http://www.top500.org/stats/list/31/osfam>

pomocí FTP protokolu ze serveru ftp.funet.fi. Od té doby se na vývoji projektu podílejí vývojáři z celého světa.
Logem a maskotem Linuxu je tučňák Tux vycházející z obrázku L.Ewigna z roku 1996. Samotný název Linux nevychází od Torvaldse, ale od Ariho Lemmke, který byl správcem FTP serveru, kde byl Linux prvně k dispozici. Lemmkemu se nelíbil Torwaldsův název Freax a tak na severu vytvořil adresář Linux – jako zkratku „Linusův Minix“. V současné době je název Linux ochrannou známkou.

7.3 Distribuce Linuxu

Jak již bylo zmíněno, existuje více souborů knihoven a softwarových balíčků pracujících a společně poskytovaných s jádrem Linux. Jednotlivé takové soubory se nazývají distribuce a každá z nich má svou vlastní specializaci. Při volbě distribuce je třeba brát ohled například na snadnost instalace, autodetekce a podpora hardware, snadnost používání, snadnost údržby, snadnost upgrade, bezpečnost, rychlost vydávání oprav, podpora češtiny, množství softwarových balíčků, dostupnost dokumentace a technické podpory. Prostě výběr distribuce záleží na požadovaném uplatnění a zkušenosti správce. Některé distribuce, byť jsou GBU/GPL, jsou poskytovány komerčně. Je k nim možno získat např. tištěný manuál, je poskytována distribuční uživatelská podpora, atd… Za zmínku stojí i způsob primárního spouštění distribuce. Serverové distribuce se např. spouštějí téměř vždy z pevného disku, kdežto distribuce pro pracovní stanice je možno pouštět jak z pevného disku, tak z CD/DVDROM a USB datových nosičů. Distribuce na CD/DVD ROM se označují též jako Live distribuce.

V tabulce na další stránce jsou uvedeny nejznámější distribuce s jejich základním popisem, vhodnosti a způsobu použití a odkazem na jejich webové stránky.

Název distribuce	**Krátký popis a odkaz na informační zdroje distribuce**
Arch Linux	Nepříliš uživatelsky přívětivá, ale rychlá distribuce. http://www.archlinux.org
Danix	Česká distribuce založená na Debianu. Vhodná pro desktop. Možnost spouštění z CDROM, USB i HDD. http://www.danix.cz
Debian	Distribuce určená pro server. Na pracovní stanice je vhodná jen pro zkušené uživatele. Výborná správa balíčků. http://www.debian.org (http://www.debian.cz)
Fedora	Pokroková nekomerční odnož RedHatu. Vhodná jak pro server, tak i pracovní stanici. Výborná správa balíčků. http://www.fedoraproject.org (http://www.fedora.cz)
Tentok	Distribuce určená jak pro servery tak pracovní stanice. V základu rychlá distribuce. Nutná hlubší zkušenost s Linuxem. Poněkud nepřívětivá správa instalace softwarových balíčků. http://www.gentoo.org (http://www.gentoo.cz)
Knoppix	Oblíbená Live CD/DVD-ROM distribuce určená spíše pro prezentaci a testování. http://knoppix.de
Mandriva	Dřívější název Mandrake. Velmi uživatelsky přívětivá distribuce určená pro začátečníky, optimalizovaná pro pracovní stanice. http://www.mandrivalinux.com (http://www.mandrivalinux.cz)
Mint	Distribuce vycházející z distribuce Ubuntu http://www.linuxmint.com
Red Hat Enterprice	Komerční serverová výkonná distribuce. http://www.redhat.com
Slackware	Velmi rozšířená, stabilní a bezpečná distribuce určená stejně jak pro servery, tak pro pracovní stanice. http://www.slackware.org (http://www.slackware.cz)

Slax	Live CDROM a USB distribuce Slackware určená pro testování, správu a mobilní využití. http://www.slax.org (http://www.slax.cz)
Source Mage	Distribuce pro opravdové znalce Linuxu a vývojáře aplikací instalovaná ze zdrojových kódů. Možno ladit přímo na příslušný HW. http://www.sourcemage.com
SuSE	Komerční distribuce určená primárně pro servery a v současné době vlastněná a vyvíjená společností Novell. http://www.suse.com
Ubuntu	Distribuce určená jak pro pracovní stanice tak i servery. Má několik odnoží pro specifická použití – kubuntu (optimalizováno pro grafické prostředí KDE), xbuntu (s grafickým prostředím GNOME), edubuntu (optimalizováno pro školy) http://www.ubuntulinux.org (http://www.ubuntu.cz)
CentOS	Výkonná serverová distribuce určená pro běh firemních aplikací. http://www.centos.org

7.4 Hardwarové požadavky běhu Linuxu

Hardwarové požadavky pro provoz Linuxu se liší od distribuce a požadovaného typu aplikací, které mají být na příslušném stroji provozovány. Pokud pomineme jednočipové aplikace embedded typu (hardwarové routery či mobilní zařízení), které mají jádro i aplikace speciálně laděné, tak distribuce určené pro pracovní stanice i server dokáží běžet jak na standardním hardwaru typu Intel P3, 128MB RAM, tak i na nejmodernějším hardwaru typu superpočítače.

8 Modelový příklad nasazení operačního systému Linux

Následující kapitola popisuje konkrétní nasazení routeru na bázi operačního systému Linux. Tento konkrétní model byl úspěšně nasazen a vyzkoušen na dvou základních školách ve středočeském kraji.

8.1 Popis řešeného modelového připojení školní počítačové sítě

Bylo z důvodu bezpečnosti rozhodnuto, že stroj – server, řešící modelové zabezpečení školní počítačové sítě, bude vůči veřejnému internetu plnit funkci firewallu s překladem adres (NAT). Vnitřní síti bude poskytovat pouze základní služby a to dynamické přidělování adres (DHCP), lokální server pro překlad adres DNS a společně s firewallem bude umožňovat dočasné omezení přístupu na internet z předem daných adres (například z počítačové učebny v době zkoušení). Ovládání dočasného omezení přístupu na internet bude možno provádět po autorizaci přes webové rozhraní.

Ve škole bylo zapotřebí vytvořit počítačovou síť připojenou do internetu pro 12 žákovských počítačů a jeden učitelský v počítačové učebně a pro 6 počítačů v kancelářích školy. V síti byl zapojen i souborový server, ke kterému měli mít žáci přístup. Současně však mělo být zajištěno, aby se z počítačové učebny nebylo možno připojit ke kancelářským strojům, kde by učitel či jiný pracovník školy mohl při neopatrné manipulaci nasdílet část dat, ke kterým by žáci neměli mát přístup. Z druhé strany by mělo být zajištěno, aby žáci ze strojů v počítačové učebně nemohli požívat volně dostupné nástroje pro průnik do počítačů a snaze získání či poškození dat v učitelských PC. Tomu by mělo být zabráněno již na síťové úrovni. Dalším požadavkem byla i možnost řízeného zabránění přístupu na internet z pracovních stanic školní počítačové učebny v době zkoušení či výuky, ke které není přístup k internetu zapotřebí. Tím měla být zajištěna regulérnost při zkoušení a zvýšena pozornost žáků při standardní výuce. V neposlední řadě je to nástroj pro udržení kázně při oblíbených suplovaných hodinách, které mohou probíhat v počítačové učebně. Z důvodu topologie

sítě a nákladů není možno mít obě sítě odděleny pomocí síťových prvků (druhá síťová karta, dva switche jeden pro počítačovou učebnu, druhý pro kancelářské stroje).
Schéma řešené modelové školní počítačové sítě je na obrázku.

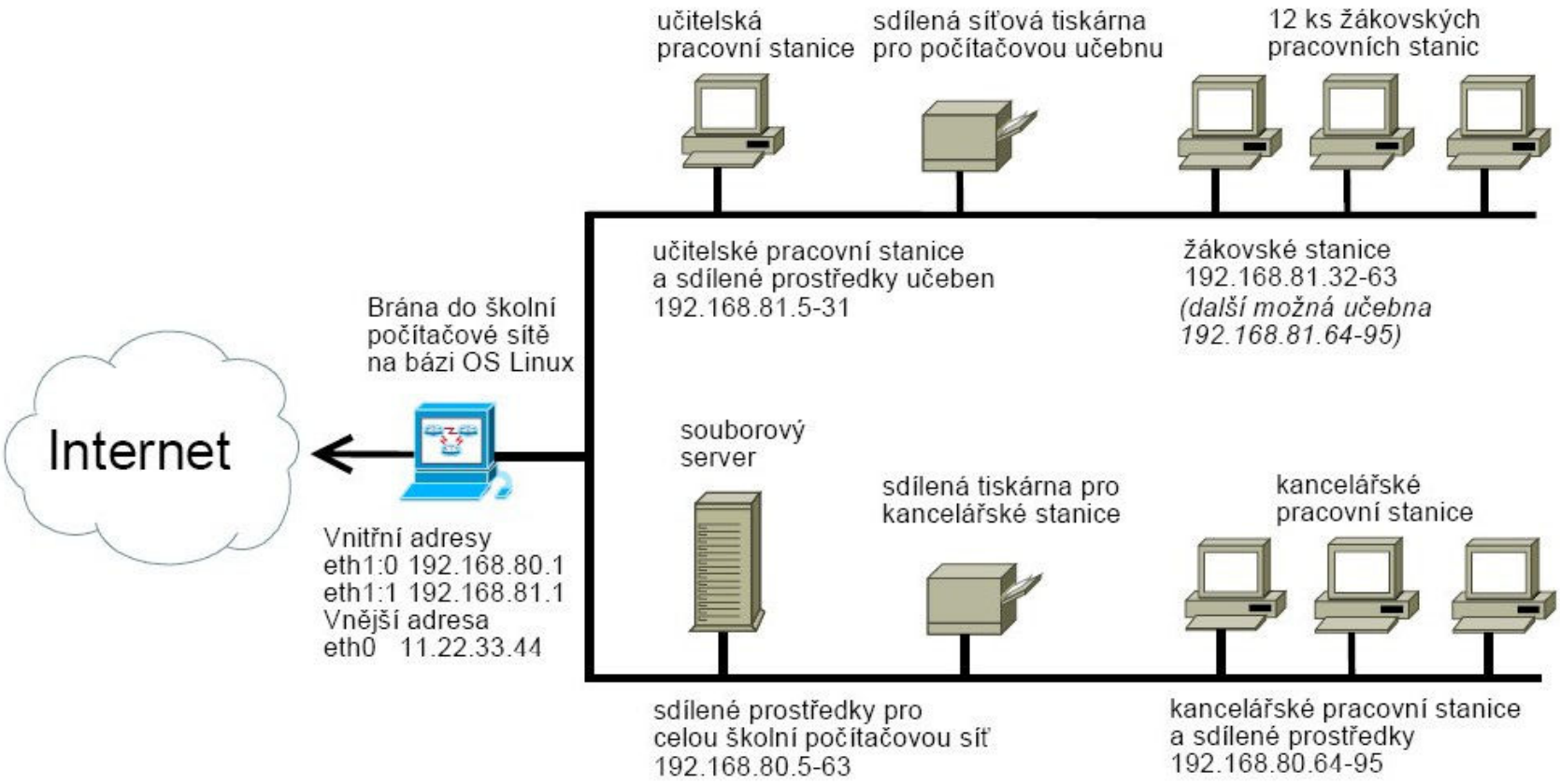


Schéma řešené modelové školní počítačové sítě

8.2 Konkrétní instalace operačního systému Linux

Základní instalace systému Linux byla provedena na stroji s hardwarovou konfigurací Intel Celeron 430 1,6 GHz, 512 MB RAM, 40 GB HDD, DVD+-RW. Nutno nezapomenout, že stroj musí mít dvě síťové karty. Například - jedna síťová karta je umístěna na základní desce a druhá bude do stroje přidána. Takový nebo podobný nový stroj lze v době realizace této diplomové práce (jaro 2009) pořídit do osmi tisíc korun. Samozřejmě je možno použít i stroj starší. V tomto konkrétním případě byl volen stroj nový z důvodu záruk.

Jako operační systém byla zvolena distribuce Fedora Core 10 a to pro její jednoduchou správu a údržbu. Tuto distribuci lze stáhnout ze stránek projektu http://www.fredora.cz. Na těchto stránkách je možno získat i česky psanou základní dokumentaci. Pro budoucí nasazení je možno již základní instalaci provést v textovém režimu. Instalaci je možno provést se třemi základními skupinami softwarových balíků. Kancelářské aplikace, webový server a vývojové prostředí systému. Vzhledem k tomu, že stroj bude plnit jen výše uvedené funkce, je instalace mnohých přednastavených komponent zbytečná (například kancelářského balíku, X-serveru). Další nastavení a pozdější správu serveru je možno provádět v textovém režimu z příkazové řádky přímo z konzole nebo přes zabezpečené terminálové připojení (SSH). Kompletní a podrobný popis instalace distribuce Fedora Cote 10 je v příloze.

V rámci instalace je vyžadováno heslo správce systému. Bezpečnost hesla je probrána ve zvláštní kapitole.

Během instalace je též vyžadována konfigurace síťových rozhraní. Je doporučeno použít rozhraní označené eth0 pro veřejnou část sítě – pro internet. Rozhraní eth1 pak pro vnitřní síť. Tedy rozhraní eth0 je nastaveno dle informací od poskytovatele internetu. Konkrétně IP adresa našeho rozhraní, IP adresa výchozí brány poskytovatele a v současné chvíli i doménové servery poskytovatele. Ty pak budou v rámci instalace dalších služeb změněny. V současné chvíli jsou třeba pro online update systému.

Na vnitřní rozhraní – tedy eth1 - je třeba nastavit adresu z rozsahu privátních adres[1]. Privátní rozsah adres je volen dle velikosti – rozsahu počítačové sítě. Vzhledem k tomu,

[1] IP adresa – Wikipedia. [cit 28.2.2009]. Dostupné na WWW: http://cs.wikipedia.org/wiki/IP_adresa , oddíl Vyhrazené adresy

že se bude jednat o výchozí bránu sítě, doporučuje se zvolit úplně první nebo poslední adresu daného rozsahu. Například z důvodu dalšího jednoduššího nastavení firewallu. (V řešeném případě škola, kde byl tento projekt realizován, neměla ještě žádné připojení k internetu a tedy adresní rozsah byl plně na výběru řešitele. Protože mnohá nová dodávaná síťová zařízení, tedy myšleno síťové tiskárny, managementovatelné switche, atd… mají z výroby přednastavenou adresu v rozsahu 192.168.0.X nebo 192.1689.1.X a též je tato adresa buď úplně na začátku či konci rozsahu, může tím dojít ke konfliktu IP adres a ochromení funkčnosti sítě. Proto je vhodné volit bloky adres rozsahu C buď 192.168.N.X, kde číslo N je vyšší než 10. Vodítkem může být třeba číslo popisné objektu, kde je síť umístěna.)

Po prvním restartu se provádí další základní nastavení systému, jako typ autorizace uživatelů, nastavení firewallu atd… Zde není třeba nic měnit. Tím je instalace hotova.

Rekapitulace stavu - systém je nainstalován, síťová rozhraní jsou nakonfigurovaná a stroj je připojen k internetu. Je tedy třeba se přihlásit ke stroji jako superuživatel root s heslem, které bylo zadáno během instalace a to přímo na konzoli serveru. Pokud byla při instalaci povolena možnost instalace s grafickým serverem (X server), tak se hned první spuštění provede do tohoto grafického rozhraní. Do textového režimu se přepneme pomocí klávesové kombinace Ctrl+Alt+1.

Kontrolu správného připojení je možno otestovat pomocí příkazu ping.

```
[root@gw.modelova-skola.cz ~]# ping -c 3 www.seznam.cz
```

Odpovědí by měl být následující výpis:

```
PING www.seznam.cz (77.75.76.3) 56(84) bytes of data.
64 bytes from www.seznam.cz (77.75.76.3): icmp_seq=1 ttl=248 time=2.50
ms
64 bytes from www.seznam.cz (77.75.76.3): icmp_seq=2 ttl=248 time=2.49
ms
64 bytes from www.seznam.cz (77.75.76.3): icmp_seq=3 ttl=248 time=2.41
ms

--- www.seznam.cz ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 2.415/2.472/2.508/0.057 ms
```

Důležitá je informace o počtu ztracených paketů v poslední části výpisu a to položka „packet loss“. Ta by měla být na nulové hodnotě. Pokud je tato hodnota vyšší (obzvláště pak 100%) je třeba hledat chybu v nastavení rozhraní směrem do internetu.

Pokud vše běží v pořádku, jsou vypsány odezvy, tak je třeba celý systém on-line aktualizovat. Toto je možno udělat pomocí příkazu

```
[root@gw.modelova-skola.cz ~]# yum –y update
```

Systém automaticky zkontroluje aktuálnost nainstalovaných softwarových balíčků a v případě existence novější verze příslušnou programovou část zaktualizuje.
Během aktualizace jsou vypisovány právě aktualizované softwarové balíčky a na obrazovce je možné vidět výpis podobný následujícímu:

```
---> Package bind.i386 31:9.3.4-7.P1.fc10 set to be updated
---> Package perl-Clone.i386 0:0.27-1.fc10 set to be updated
---> Package iptables.i386 0:1.3.8-2.1.fc10 set to be updated
…
(34/51): bind.i386 100%    |=========================| 8.6 MB    00:18
(35/51): perl-Clone.i386 100% |=====================| 4.6 MB    00:10
(36/51): iptables.i386 100% |=========================| 8.8 MB    00:19
…
Complete!
```

Nebo pokud je systém aktuální, tak je update zakončen halášením:

```
No Packages marked for Update/Obsoletion
```

8.3 Konfigurace síťových služeb

V následujících kapitolách bude popsáno konkrétní nastavení služeb běžících na modelovém stroji.

8.4 DHCP

„Dynamic Host Configuration Protocol. Protokol umožňující dynamické přidělování IP adres počítačům v síti po jejich připojení. Jednotlivá zařízení nemají svoji pevnou IP adresu, pokud nepotřebují být k síti připojeny, teprve v okamžiku potřeby připojení k síti je jim adresa přidělena. Při příštím přihlášení do sítě může, ale nemusí, být počítači přidělena jiná IP adresa.“[1]

Protokol vyvinula a spravuje společnost ISC[2] (Internet Software Consorcium). Dodává také příslušný software a to jak serverovou, tak klientskou část. V použitém systému Fedora Core je prezentován softwarovým balíkem dhcpd.i386. Pokud není nainstalován v rámci základní instalace, je možné ho doinstalovat pomocí příkazu

```
yum –y install dhcp
```

V řešeném modelovém případu bylo DHCP nastaveno tak, že přidělovalo konkrétní IP adresy dle MAC adres počítačů. Tím se zajistilo rozdělení počítačů do skupin „kanceláře“ a „počítačová učebna“. Přidělování konkrétních (statických) adres pomocí DHCP služby má tu výhodu, že pokud je třeba provést změnu ve směrování či nastavení jiného DNS serveru, lze toto učinit centrálně změnou jednoho centrálního konfiguračního souboru. Poté stačí počkat, až si stanice znovu nastavení načtou. Další výhodou statických adres přidělovaných pomocí DHCP je možnost jednoduššího dohledání případného problému či odhalení viníka nepovolené činnosti.

8.4.1 Popis fungování DHCP

Klient vyšle do sítě multicast UDP požadavek DHCPDISCOVER. Servery zachytí požadavky a zašlou zprávu DHCPOFFER (opět multicast). Klient si vybere ze všech

[1] Root.CZ Informace nejen ze světa Linuxu. [cit 2.4.2009]. Dostupné na WWW: http://www.root.cz/slovnicek/dhcp/

[2] ISC, Internetová prezentace – domácí stránky společnosti. [cit. 2.4.2009]. Dostupné na WWW: https://www.isc.org/

odpovědí tu nejvhodnější a pošle DHCPREQUEST. Server, který klient oslovuje, vše buď potvrdí (DHCPACK), nebo ne (DHCPNAK). Klient si to může ještě rozmyslet (DHCPDECLINE). Po vypršení lhůty (nebo pokud klient skončí před lhůtou a pošle DHCPRELEASE) se adresa může poskytnout jinému zájemci (existují i výjimky).

8.4.2 Konfigurace lokálního DHCP serveru

Obsah konfiguračního souboru služby DHCP je uložen v souboru /etc/dhcpd.conf .

Z důvodu přehlednosti je konfigurace rozdělena do více souborů. V souboru /etc/dhcpd.conf je základní konfigurace služby a jednotlivých sítí. V připojených souborech /etc/dhcpd_80.conf a /etc/dhcpd_81.conf jsou definice konkrétních pracovních stanic.

Obsah /etc/dhcpd.conf by měl být následující. Důležité volby mají český komentář. Jsou však psány bez diakritiky, aby bylo možné příklady rovnou použít.

```
/etc/dhcpd.conf
############################
###   OBECNA NASTAVENI   ###
############################


    # kdyz DDNS (dynamicke DNS) neni pouzito, nasledujici dva radky
    # by mely obsahovat toto
    ddns-update-style           none;
    ddns-updates                off;
    # nastaveni autoritativni ulohy toho DHCPD serveru
    authoritative;
    # zpusob predavani info do systemoveho logu
    log-facility                local7;

############################
###   SUBNET 80 + 81    ###
############################

shared-network site_eth1 {
    subnet 192.168.80.0 netmask 255.255.255.0 {
        ####################################
```

```
        ### servery a kancelarske stanice ###
        ######################################
        # adresa vychozi brany site
        option routers                  192.168.80.1;
        # adresa vychozi maska site
        option subnet-mask              255.255.255.0;
        # automaticka pripona domeny
        option domain-name              "modelova-skola.cz";
        # adresa serveru DNS
        option domain-name-servers      192.168.80.1;
  # doba v sec, po kterou bude „zapujcena“ IP adresa
        default-lease-time          600;
        # maximalni doba v sec, po kterou bude „zapujcena“ IP adresa
        max-lease-time              700;
  # pripojeni souboru s konfiguraci stanic v siti 192.168.80.0
  include "/etc/dhcpd_80.conf";
    }

    subnet 192.168.81.0 netmask 255.255.255.0 {
        ######################################
        ### stanice a prostredky  uceben  ###
        ######################################
        # adresa vychozi brany site
        option routers                  192.168.81.1;
        # adresa vychozi maska site
        option subnet-mask              255.255.255.0;
        # automaticka pripona domeny
        option domain-name              "modelova-skola.cz";
        # adresa serveru DNS
        option domain-name-servers      192.168.80.1;
  # doba v sec, po kterou bude „zapujcena“ IP adresa
        default-lease-time          600;
        # maximalni doba v sec, po kterou bude „zapujcena“ IP adresa
        max-lease-time              700;
  # pripojeni souboru s konfiguraci stanic v siti 192.168.81.0
  include "/etc/dhcpd_81.conf";
    }
}
```

Obsah připojeného souboru s konfigurací kakcelářských stanic.

```
/etc/dhcpd_80.conf

# adresa souboroveho serveru je pridelena fixne, zde je uveden
# jen pro uplnost seznamu a pro lepsi orientaci pri budoucim
# pridelovani IP pro sdilene prostredky
host server {
        hardware ethernet 00:50:FC:B2:36:47;
        fixed-address 192.168.80.10;
    }

###################################
# Definice kancelarskych tiskaren #
###################################
host pc80_20 { # tiskarna sborovna
        hardware ethernet 00:50:FB:E2:86:77;
        fixed-address 192.168.80.20;
    }
host pc80_21 { # tiskarna u zastupkyne
        hardware ethernet 00:50:FB:E2:86:88;
        fixed-address 192.168.80.21;
    }



#################################
# Definice kancelarskych stanic #
#################################
host pc80_65 {
        hardware ethernet 00:50:FB:E2:56:99;
        fixed-address 192.168.80.65;
    }
host pc80_66 {
        hardware ethernet 00:50:FB:E2:56:A2;
        fixed-address 192.168.80.66;
    }
```

```
### zde je mozno pokracovat v konfiguraci zbylych kancelarskych stanic
```

Obsah připojeného souboru s konfigurací stanic a sdílených prostředků počítačové učebny.

/etc/dhcpd_81.conf

```
#################################
# Definice tiskaren v ucebnach  #
#################################
host pc81_20 { # tiskarna ucebna1
        hardware ethernet 00:50:FB:E2:86:00;
        fixed-address 192.168.81.20;
    }


#################################
# Definice ucitelskych stanic   #
#################################
host pc81_25 { # ucitelska pracovni stanice – ucebna 1
        hardware ethernet 00:50:FB:E2:56:11;
        fixed-address 192.168.81.25;
    }

#####################################
# Definice zakovskych stanic ucebna 1#
#####################################
# IP rozsah zakovskych stanic ucebny 1 je 192.168.81.32-63
host pc81_33 {
        hardware ethernet 00:50:FB:E2:56:22;
        fixed-address 192.168.81.33;
    }
host pc81_34 {
        hardware ethernet 00:50:FB:E2:56:33;
        fixed-address 192.168.81.34;
    }
```

```
host pc81_35 {
        hardware ethernet 00:50:FB:E2:56:44;
        fixed-address 192.168.81.35;
    }

### zde je mozno pokracovat v konfiguraci zbylych zakovskych stanic
```

Po každé změně některého z konfiguračních souborů je třeba nezapomenout restartovat službu DHCP například z příkazového řádku pomocí příkazu:

```
service dhcpd restart
```

8.5 DNS server

„Domain Name System (nebo Service) je internetová služba zajišťující překlad doménových jmen (www.root.cz) na IP adresy (81.31.5.12) a obráceně.“ [1]

V použité distribuci Fedora Core je server DNS připraven a provozován pomocí softwarového balíku BIND. Pokud není instalován při základní instalaci, je možno ho doinstalovat pomocí příkazu

```
yum –y install bind*
```

Hvězdička za bind znamená požadavek na do/instalaci všeho co začíná na „bind“. V modelovém příkladu se doinstalovala například i nadstavba pro bind-chroot, jenž umožňuje provoz služby v režimu „chroot“. Příkaz /režim chroot se používá pro změnu kořenového adresáře (change root) u aktuálního procesu (včetně jeho dětí). Chrootnutý proces používá jako výchozí "jediný nejvyšší" adresář při vyhledávání v adresářovém stromu. Také se tento prvek používá pro omezení práv uživatele na prohlížení adresářové struktury a to konfigurací určité služby. Např. u přístupu na ftp účet vás tímto způsobem daemon může blokovat pouze na váš domovský adresář. A není možné změnit pozici směrem nahoru (/home, / apod.).[2]

[1] Root.CZ Informace nejen ze světa Linuxu. [cit 2.4.2009]. Dostupné na WWW: http://www.root.cz/slovnicek/dns/

[2] Root.CZ Informace nejen ze světa Linuxu. [cit 2.4.2009]. Dostupné na WWW: http://www.root.cz/slovnicek/chroot/

Po instalaci balíčku bind-chroot se konfigurační a datové soubory nacházejí v adresáři /var/named/chroot. V adresáři /var/named/chroot/etc jsou soubory upravující běh samotného DNS serveru a v adresáři /var/named/chroot/var/named jsou datové soubory definující odpovědi z tohoto DNS. Samotná serverová služba je prezentována daémonem s názvem named.

8.5.1 Popis fungování DNS

Klient odešle požadavek o překlad internetové adresy na IP (nebo obráceně) na adresu serveru, kterou má nastavenou ve své konfiguraci TCP/IP. Server z kontroluje, zda není správcem této domény. Pokud ano, projde lokální datový soubor s definicí domény a pokud najde požadovanou informaci, sdělí jí klientovi. V případě, že požadovanou informaci nezná, sdělí toto klientovi. Pokud server není správcem této domény, prohlédne datový soubor s kořenovými DNS servery (/var/named/chroot/var/named/named.ca) a u nich požadovanou informaci hledá. Postupuje přitom směrem od nejvyšší domény. Výsledek poté sděluje klientovi.
Příklad: místní lokální server dostal požadavek na překlad adresy www.seznam.cz. Není konfigurován jako správce domény seznam.cz, tedy zasílá kořenovým serverům požadavek o informaci, který server má na starosti doménu seznam.cz. Od jednoho z kořenových serverů se dozví, že správu seznam.cz má na starosti stroj ns.seznam.cz s IP 77.75.73.77. Na tento stroj se obrací s požadavkem o překlad adresy www.seznam.cz. Ten, pokud požadovanou adresu zná, sdělí jí místnímu lokálnímu DNS serveru a ten jí sdělí klientovi. Tedy lokální server pošle klientovi odpověď, že IP adresa www.seznam.cz je 77.75.72.3.

Důvody provozování lokálního DNS serveru jsou následující.
klienti místní sítě nezatěžují linku svými opakovanými dotazy na externí DNS při dotazu na stejnou adresu. Je možné provozovat vnitřní překlad adres – provoz intranetu, sdílené prostředky po TCP/IP oslovovat jménem (tiskarna1.modelova-skola.cz). Servery na vnitřní síti mají možnost zpětného překladu adres pro zápis do logů. Některé služby dokonce tento zpětný překlad vyžadují pro svůj správný běh (emailové služby například - sendmail, postfix, dovecot).

8.5.2 Konfigurace lokálního DNS serveru

Konfigurace bude probíhat v následujících bodech. Definice souboru pro překlad lokálních adres jmenných názvů do IP, reverzní překlad těchto adres (IP na jméno), úprava a doplnění hlavního konfiguračního souboru pro načtení lokálních konfigurací.

Vysvětlení struktury doménového konfiguračního souboru:

hlavička souboru - SOA záznam

```
$TTL    86400
@               IN SOA  jmeno_domeny spravce.jmeno_domeny (
                                        42          ; serial
                                        3H          ; refresh
                                       15M          ; retry
                                        1W          ; expiry
                                        1D )        ; minimum
```

`jmeno_domeny` – celé jméno spravované domény

`spravce.jmeno_domeny` – email na správce domény (mezi správcem a doménou je tečka místo @ - nejedná se o překlep)

`serial` – seriové číslo změn, musí být pokaždé vyšší pro synchronizaci se sekundárními DNS servery. Doporučuje se datum ve formátu YYYYMMDDXX, kde XX je pořadové číslo změny od 00-99. Nepočítá se s tím, že by se dělalo více jak 100 změn za den.

`refresh` – obnovovací frekvence v sec. pro sekundární DNS server

`retry` - čas v sec pro sekundární DNS server, kdy se pokusí o opětovné připojení k primárnímu DNS po neúspěšném připojení v době „refresh“

`expiry` – expirace datových tabulek na sekundárním DNS serveru v sec.

`minimum` – defaultní TTL doba v sec. pro záznamy, které nemají TTL nastaveno.

Datová část konfiguračního souboru domény může obsahovat následující záznamy:

`NS – adresa podřízeného DNS serveru`

```
MX – adresa serveru kam se doručuje pošta pro danou doménu. Následné
číslo udává prioritu doručovacího serveru.
A – přiřazuje jménu IP adresu – smí být pouze jedno dané IP
CNAME – přiřazuje alias k A záznamu
PTR – reverzní záznam – přiřazuje k IP jméno
```

Soubor pro překlad názvů lokální počítačové sítě bude umístěn v adresáři s datovými soubory DNS /var/named/chroot/var/named a bude mít pro přehlednost název dle provozované domény modelova-skola.cz.conf

Soubor: /var/named/chroot/var/named/modelova-skola.cz.conf

```
@            IN SOA  modelova-skola.cz root.modelova-skola.cz (
                                          2008122001  ; serial
                                          3H          ; refresh
                                         15M          ; retry
                                          1W          ; expiry
                                          1D )        ; minimum
                 IN NS localhost.
;definice mailserveru
                 IN MX 5 mail.modelova-skola.cz

; definice aliasu k domenovym jmenum
gw               IN CNAME pc80_1
ns               IN CNAME pc80_1
server           IN CNAME pc80_10
mail             IN CNAME pc80_10
prn-sborovna     IN CNAME pc80_20
prn-zastupkyne   IN CNAME pc80_21

prn-ucebna1      IN CNAME pc81_20

;definice A zaznamu pro sit 192.168.80.0
pc80_1           IN A  192.168.80.1
pc80-2           IN A  192.168.80.2
pc80-3           IN A  192.168.80.3
pc80-4           IN A  192.168.80.4
pc80-5           IN A  192.168.80.5
```

```
pc80-6            IN A  192.168.80.6
pc80-7            IN A  192.168.80.7
. . . . .
pc80_254          IN A  192.168.80.254

;definice A zaznamu pro sit 192.168.81.0
pc81_1            IN A  192.168.81.1
pc81-2            IN A  192.168.81.2
pc81-3            IN A  192.168.81.3
pc81-4            IN A  192.168.81.4
pc81-5            IN A  192.168.81.5
pc81-6            IN A  192.168.81.6
pc81-7            IN A  192.168.81.7
. . . . .
pc81_254          IN A  192.168.81.254
```

Soubor pro zpětný (reverzní) překlad IP na jméno má stejný formát jako standardní formát definující překlad jmenných adres na IP adresy, jen místo A záznamů jsou použity záznamy PTR. Tento typ záznamu slouží ke sdružení názvů v doméně in-addr.arpa s názvy hostitelů. Tento záznam se používá ke zpětnému mapování IP-adres na názvy hostitelů. Zadaný název hostitele musí být v kanonickém tvaru.

Soubor: /var/named/chroot/var/named/192.168.80.0.arpa

```
@            IN SOA  modelova-skola.cz root.modelova-skola.cz (
                                          2008122001  ; serial
                                          3H          ; refresh
                                         15M          ; retry
                                          1W          ; expiry
                                          1D )        ; minimum
1     IN PTR pc80_1.modelova-skola.cz.
```

```
2     IN PTR pc80_2.modelova-skola.cz.
3     IN PTR pc80_3.modelova-skola.cz.
4     IN PTR pc80_4.modelova-skola.cz.
5     IN PTR pc80_5.modelova-skola.cz.
6     IN PTR pc80_6.modelova-skola.cz.
. . . . .
254   IN PTR pc80_254.modelova-skola.cz.
```

Protože byly použity dva rozsahy sítě, bylo zapotřebí vytvořit in-addr.arpa záznamy i pro druhý rozsah

```
Soubor: /var/named/chroot/var/named/192.168.81.0.arpa

@            IN SOA  modelova-skola.cz root.modelova-skola.cz (
                                          2008122001  ; serial
                                          3H          ; refresh
                                         15M          ; retry
                                          1W          ; expiry
                                          1D )        ; minimum
1     IN PTR pc81_1.modelova-skola.cz.
2     IN PTR pc81_2.modelova-skola.cz.
3     IN PTR pc81_3.modelova-skola.cz.
4     IN PTR pc81_4.modelova-skola.cz.
5     IN PTR pc81_5.modelova-skola.cz.
6     IN PTR pc81_6.modelova-skola.cz.
. . . . .
254   IN PTR pc81_254.modelova-skola.cz.
```

Stav hlavního konfiguračního souboru po úpravě a doplnění

```
Soubor: /var/named/chroot/etc/named.conf
options {
        listen-on port 53 { 127.0.0.1; 192.168.80.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
```

```
        recursion yes;
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";

zone "modelova-skola.cz" IN {
        type master;
        file "modelova-skola.cz.conf";
};

zone "80.168.192.in-addr.arpa" IN {
        type master;
        file "192.168.80.0.arpa";
};
zone "81.168.192.in-addr.arpa" IN {
        type master;
        file "192.168.81.0.arpa";
};
```

Po každé změně některého z konfiguračních souborů je třeba nezapomenout zvýšit sériové číslo konfigurace a restartovat službu DNS serveru například z příkazového řádku pomocí příkazu:

```
service named restart
```

8.6 Firewall

Základem síťové bezpečnosti celé sítě a i počítače tvořícího bezpečnostní bránu mezi lokální počítačovou sítí a internetem je datagramový filtr. Je to služba, která umí prohlížet hlavičky ICP/IP datagramů a podle informací v nich uložených rozhodne o jejich dalším osudu, co s kterým datagramem udělá. Podle nadefinovaných filtrů může datagram pustit dál, zahodit, odmítnout, případně s ním provést nějakou složitější operaci. Přímo v jádře GNU Linuxu je tato služba zahrnuta a jmenuje se iptables.

8.6.1 Iptables

Pro pochopení funkce bude vhodné krátce shrnout vědomosti o TCP/IP datagramu. Ten se skládá ze dvou hlavních částí. Hlavička a přenášená data – vlastní informace. Pro pochopení funkce datagramového filtru je třeba dále rozebrat informace uvnitř hlavičky. Důležitými informacemi pro datagramový filtr jsou zdrojová IP adresa, zdrojový port, cílová IP adresa a cílový port.

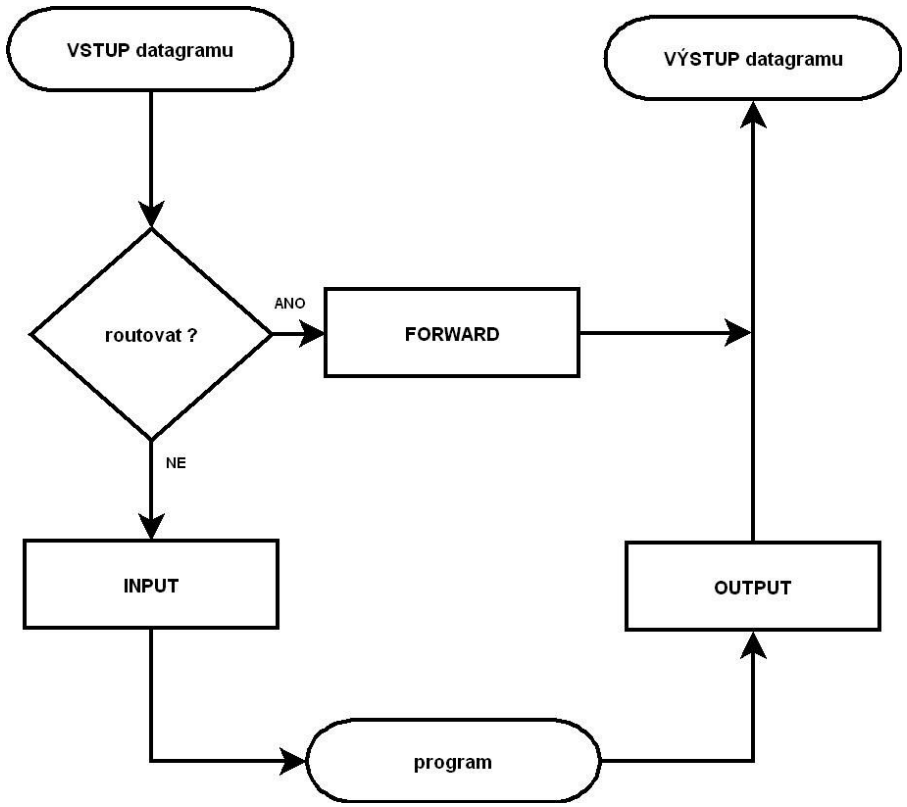
Služba iptables[1] pak rozdělí datagramy do různých kategorií podle toho, odkud a kam datagramy putují. V systému jsou definovány tři základní kategorie – řetězce, kterými datagramy prochází. Podle těchto řetězců se pak rozdělí jednotlivé datagramy. V každém řetězci se na každý datagram aplikuje řada předem definovaných pravidel. Řetězce se nazývají INPUT, OUTPUT a FORWARD.

Typ řetězce	**Funkce**
INPUT	do něj přicházejí datagramy, které jsou určeny přímo pro daný stroj. Většinou se jedná o datagramy pro nějakou službu běžící na daném stroji.
OUTPUT	Obsahuje datagramy generované přímo strojem, které se snaží odejít ven ze stroje.
FORWARD	Tímto řetězcem procházejí ostatní datagramy které vznikly mimo daný stroj a směřují jinam. Strojem tedy jen procházejí. INPUT a OUTPUT pravidla se

[1] The Netfilter.ORG project. [cit 23.4.2009]. Dostupné na WWW: http://www.netfilter.org/

	jich netýkají.

Pro lepší pochopení fungování datagramového filtru je k dispozici vývojový diagram základního průchodu datagramu strojem.



Vývojový diagram zpracování datagramu

Služba iptables má v sobě zabudovány ještě dva speciální průchodové řetězce PREROUTING a POSTROUTING. Ty jsou aktivní ještě těsně před a po průchodu zpracování datagramu. Nepoužívají se přímo pro filtraci datagramu, ale pro změnu jeho hlavičky. Své využití mají například při změně zdrojové IP adresy při překladu NAT. Kromě těchto pravidel je možné definovat si vlastní řetězce s libovolnými názvy a těm pak přiřazovat sady pravidel. Ty jsou ve zpracování předřazeny základním řetězcům.

Při průchodu řetězcem je datagram testován definovanou sadou pravidel a pokud narazí na pravidlo, kterému vyhovuje, je datagram přesunut na konec testovacího řetězce a bez dalšího testování je provedena zvolená akce. Po té probíhá kontrola dalšího paketu.
Pokud nerozhodne žádné z pravidel, stojí na konci řetězce poslední pravidlo, které se nazývá POLICY. To rozhodne o konečném osudu datagramu. Tedy standardní firewall má nastaveny povolené vyjímky a „…ostatní zahodit“. To přesně dělá pravidlo POLICY. Pravidla POLICY jsou definována jen u výše zmíněných třech základních řetězců.
Požadovaná akce, která následuje po zpracování datagramu může být z následujících možností:

- DROP datagram je tiše zahozen
- REJECT datagram je zahozen a odesilatel je informován chybovým hlášením
- ACCEPT datagram volně prochází skrz službu iptables
- LOG existence paketu je zaznamenána systémem syslogd a paket pokračuje cestou řetězcem.

Pro práci s datagramovým filtrem služby iptables se používá příkaz stejného jména, tedy iptables. Jeho syntaxe je složitější a pro její pochopení je doporučeno přečíst si manuálovou stránku na www.iptables.org.

Pro lepší pochopení následujícího příkladu scriptu jsou uvedeny použité základní volby příkazu iptables.

iptables –F ŘETĚZEC	vymaže pravidla řetězce
iptables –P ŘETĚZEC	nastaví POLICY řetězce
iptables –A ŘETĚZEC	vloží pravidlo na konec řetězce
iptables –I ŘETĚZEC	vloží pravidlo na začátek řetězce (použito ve scriptu s podmíněným zákazem přístupu na internet)

8.6.2 Script firewallu

Následuje bash script s nastavením firewallu v modelové škole. Plně odpovídá schématu řešené modelové školy a požadavkům na bezpečnost uvedeným v zadání v kapitole „Popis řešeného modelového připojení školní počítačové sítě“. Script je pro lepší orientaci doplněn o komentář. Script je uložen mezi ostatními scripty pouštějící služby a to v adresáři /etc/init.d . Jen pro připomenutí, vše co je za znakem # je považováno za komentář a interpret příkazů to nezpracovává. Script nastavující pravidla chování firewallu se automaticky spouští po každém zapnutí systému.

Soubor /etc/inir.d/firewalling

```
##### firewall modelove skoly #####
### nastaveni promennych ###
#cesta k programu iptables
IPTABLES='/sbin/iptables'
#venkovni rozhrani (internet)
INTETH='eth0'
#vnitrni rozhrani (lokalni sit)
LOCETH='eth1'
#IP segment site sdilenych prostredku kancelarskeho segmentu
#(prvnich 32 IP segmentu 192.168.80.0)
SHARE_K_NET='192.168.80.0/27'
#IP segment site sdilenych prostedku segmentu uceben
#(prvnich 32 IP segmentu 192.168.81.0)
SHARE_U_NET='192.168.81.0/27'
#IP adresa mail severu
SERVER_IP='192.168.80.10/32'


### reset vsech pravidel  a povoleni komunikace###
#vstupni pravidla
$IPTABLES -F INPUT
$IPTABLES -P INPUT ACCEPT
#vystupni pravidla
$IPTABLES -F OUTPUT
$IPTABLES -P OUTPUT ACCEPT
```

```
#predavaci – routovaci - pravidla
$IPTABLES –F FORWARD
$IPTABLES –P FORWARD ACCEPT
#pravidla pro preklad adres NAT
$IPTABLES –F –t nat


### nastaveni konecnych pravidel ###
#nastaveni konecneho pravidla pro retezec OUPUT neni provedeno,
#protoze stroj sam o sobe zadne pakety zbytecne nevysila.
$IPTABLES –P INPUT DROP
$IPTABLES –P FORWARD DROP

#povoleni pro ICPM pakety – (prikaz ping a servisni sluzby)
#0 "Echo reply", 3 "Destination unreachable", 8 "Echo request",
#11 "Time exceed"
$IPTABLES -A INPUT -p ICMP --icmp-type 0 -j ACCEPT
$IPTABLES -A INPUT -p ICMP --icmp-type 3 -j ACCEPT
$IPTABLES -A INPUT -p ICMP --icmp-type 8 -j ACCEPT
$IPTABLES -A INPUT -p ICMP --icmp-type 11 -j ACCEPT
$IPTABLES -A FORWARD -p ICMP --icmp-type 0 -j ACCEPT
$IPTABLES -A FORWARD -p ICMP --icmp-type 3 -j ACCEPT
$IPTABLES -A FORWARD -p ICMP --icmp-type 8 -j ACCEPT
$IPTABLES -A FORWARD -p ICMP --icmp-type 11 -j ACCEPT

### nastaveni vstupnich pravidel  - povoleni (vse ostatni zahodit)###
#povolit vse co jde z loklani site (vnitrni sit)
$IPTABLES –A INPUT –i $LOCETH –j ACCEPT
#povolit vse co jde na vnitrni smycku “lo” –j ACCEPT
$IPTABLES –A INPUT –i lo  –j ACCEPT
#povoleni protokolu SSH pro dalkovou spravu z internetu (port 22)
$IPTABLES –A INPUT –i $INTETH –p TCP –-dport 22 –j ACCEPT
#povolit pakety u existujicich spojeni pro externi rozhrani pro sluzby
# bezici na routeru – stavovy firewall
$IPTABLES -A INPUT -i $INTETH -m state --state ESTABLISHED,RELATED \
      -j ACCEPT

### nastaveni routovacich pravidel – povoleni (vse ostatni zahodit)###
#povoleni routingu ke sdilenym zarizenim
```

```
$IPTABLES –A FORWARD –d $SHARE_K_NET –j ACCEPT
$IPTABLES –A FORWARD –d $SHARE_U_NET –j ACCEPT

#povoleni pristupu na internet na www stranky pro vsechny stanice
#podmineny zakaz pro ucebnove stanice je resen v ramci jineho scriptu
$IPTABLES –A FORWARD –i $LOCETH –p TCP --dport www –j ACCEPT
$IPTABLES –A FORWARD –i $LOCETH –p UDP --dport www –j ACCEPT

#povoleni pristupu na internet pro souborovy server, protoze na nem
#bezi postovni server
$IPTABLES –A FORWARD –d $SERVER_IP -j ACCEPT

##zrizeni prekladu adres NAT pro vsechny stanice na vnitrni siti....
$IPTABLES -A POSTROUTING -t nat -o $INTETH -j MASQUERADE

### bezpecnostni prvky proti DOS utokum a podvrhnuti adresy IP ###
### ochrana pred IPspoofing
echo "1" > /proc/sys/net/ipv4/conf/$INTETH/rp_filter
$IPTABLES -N spoofing
$IPTABLES -A spoofing -s 192.168.0.0/16 -j DROP
$IPTABLES -A spoofing -s 172.16.0.0/12 -j DROP
$IPTABLES -A spoofing -s 10.0.0.0/8 -j DROP
$IPTABLES -A INPUT -i $INTETH -j spoofing
$IPTABLES -A FORWARD -i $INTETH -j spoofing

### ochrana pred SYN flooding (hromadny utok paketu)
#prijde-li max "1000" paketu za 1/s - propustit, zbytek filtrovano
$IPTABLES -N syn_flood
$IPTABLES -A INPUT -i $INTETH -p tcp --syn -j syn_flood
$IPTABLES -A syn_flood -m limit --limit 1/s --limit-burst 1000 \
      -j RETURN
$IPTABLES -A syn_flood -j DROP

### ochrana pred DoS - Ping of death
$IPTABLES -A INPUT -p icmp --icmp-type echo-request -m limit \
      --limit 1/s --limit-burst 5 -j ACCEPT
```

8.7 Automatické spouštění programů

Pro zajištění automatického spouštění programů jako je aktualizace systému nebo zálohování, jež jsou popsány v dalších kapitolách, je možno použít program cron, který je většinou součástí základní instalace systému. Systém ho používá například pro pravidelné „rotování logů“, což zajišťuje rozumnou velikost aktuálního textového souboru se záznamem událostí (log) a současně šetří místo, protože starší logy komprimuje nějakým dostupným algoritmem. Program cron dokáže pouštět programy s rozlišovací schopností jedné minuty. Samotný program běžící v paměti počítače a zajišťující spouštění programů se jmenuje crond. Program sloužící pro manipulaci se spouštěnými úlohami se jmenuje crontab (tabulka pro cron).
Výpis aktuálních programů spouštěných programem cron pro aktuálního uživatele je možno získat z příkazové řádky pomocí příkazu:

```
crontab -l
```

Výpis koresponduje s formátem konfiguračního souboru pro crontab. Je doporučeno pro lepší orientaci správce systému, mít tento konfigurační soubor v domácím adresáři uživatele, tedy např. v adresáři /root a s názvem crontab.conf. Ten je možné poté editovat oblíbeným textovým editorem.

Formát souboru crontab.conf

```
m h D M T spoustený_příkaz
```

Položky m h D M T mohou nabývat číselných hodnot od nuly do čísla dle významu položky, nebo * pro každou platnou hodnotu
m – minuty – 0 – 59
h – hodiny – 0 – 23
D – dny v měsíci – 1- 28, 30, 31 (dle příslušného měsíce)
M – měsíc – 1 – 12
T – den v týdnu 0 = neděle, 1 = pondělí, ... 6 = sobota

Příklad zápisu pro spouštění programu každou minutu je

* * * * * nazev_programu

Příklad programu pro spouštění programu v 1:15 každý pracovní den v dubnu je:

15 1 4 1-5 nazev_programu

Načtení nové aktuální konfigurace pro program cron se provede z příkazové řádky zadáním:

```
crontab /root/crontab.conf
```

8.8 Automatický update systému

Vzhledem ke stálému vývoji jádra operačního systému Linux, opravy nalezených chyb v softwarových balíčcích a zvyšování bezpečnosti a nasazení nových technologických standardů, jsou stále vydávány aktualizace. Ty jsou dostupné volně a zdarma na internetu na stránkách příslušné distribuce. Pro zjednodušení a možnou automatizaci jak jádra operačního systému, tak instalovaných softwarových aplikačních programů, je možné tyto updaty stáhnout z on-line distribučních serverů („repozitoří“). K tomuto je třeba zajistit, aby měl server na bázi OS Linux přístup k internetu. V případě nasazení Linuxu jako routeru je toto zajištěno z principu. Update je možné provádět ručně z příkazové řádky nebo pomocí nějakého nástroje automatické spouštění programu v uvedený čas, například programem cron. Jen pro úplnost je nutno uvést, že uživatel či automatizační proces provádějící update systémových částí musí být přihlášen s právy superuživatele root.

8.8.1 Ukázky ručních aktualizací

Například, vejde-li ve známost možnost či nutnost aktualizace programového balíčku SSH z důvodu vylepšení šifrovacího algoritmu přenosu, je možné toto udělat z příkazového řádku následujícím příkazem:

```
yum –y update ssh
```

Pokud je třeba provést kompletní aktualizaci systému, je možno použít příkaz:

```
yum –update all
```

8.8.2 Ukázka nastavení automatických aktualizací

Jak jíž bylo zmíněno, pro automatické spuštění aktualizace jednou za den například ráno v 5:00, stačí přidat do konfiguračního souboru programu crontab následující zápis:

```
0 5 * * *   yum –y upadate all
```

8.9 Zálohování

Pro případ havárie disku, živelné události, nutné reinstalace systému z jakéhokoli důvodu (například po úspěšném průniku útočníka do systému), nebo případně krádeže routeru, je třeba mít pro rychlou obnovu běhu routeru provedenu zálohu nastavení systému a případně uživatelských nadstaveb a dat. Zároveň je třeba dbát na to, aby zálohy probíhaly automatizovaně a bez zásahu člověka. Je prokázáno, že je-li do zálohovacího systému včleněn lidský faktor, zálohovaný systém selže ihned po selhání faktoru lidského. Zálohu proti havárii disku je možno provést na druhý disk fyzicky namontovaný v routeru. Toto řešení má výhodu v jednoduchosti a rychlosti provádění záloh, avšak nezabrání ztrátě dat v případě živelné události či krádeže zařízení. Pokud to je možné, je doporučeno mít zálohovací prostor (datové úložiště) fyzicky oddělen od ostatních zálohovaných systémů. V praxi se toto řeší například umístěním síťového zálohovacího zařízení mimo technologickou místnost se servery, například kabinet vyučujícího výpočetní techniku nebo do bytu školníka.

Pro systém zálohování systému je možno použít následujících možností:

8.9.1 FTP

Pomocí FTP[1] (File Transfer Protokol) je možné zkopírovat příslušné adresáře s nastavením a data na někde v síti zprovozněný FTP server. Tento způsob je vhodný pro automatické nasazení zálohování. Jediná záporná vlastnost je v bezpečnosti provozu FTP, neboť nepoužívá pro autorizaci ani samotný přenos přenášených dat žádné kryptování. Pro zjednodušení zálohovacího scriptu je možné použít programový balík ncftp, jehož hlavní výhodou je možnost rekurzivního kopírování souborů.

8.9.2 SCP

Program SCP (Secure Copy) je součástí nadstavby SSH, která je obsažena v základní instalaci distribuce. Umožňuje pomocí šifrovaného kanálu kopírovat data do příslušného úložiště. Tento systém zálohování je možné spouštět automatizovaně. Nevýhodou je složitější prvotní konfigurace zálohovacího systému, neboť je třeba vygenerovat RSA bezpečnostní klíče a ty používat k autorizaci vůči datovému úložišti záloh.

8.9.3 RSYNC

Program rsync[2] bývá součástí základní distribuce. V případě potřeby je ho možné doinstalovat. Dokáže věrně synchronizovat obsahy zálohovaných adresářů, tedy je-li nějaký soubor ve zdrojovém stroji smazán, je v rámci zálohy smazán i v zálohovacím prostoru. Jeho funkce spočívá ve spočtení kontrolního součtu zálohovaných souborů a jejich komparace s kontrolním součtem souborů v datovém úložišti záloh. V případě změny pouze části souboru je toto detekováno algoritmem a je přenesena pouze změněná část souboru. Tato funkce přináší výhody obzvláště při přenosu záloh na pomalejších přenosových cestách. Samotný RSYNC má v základu podobnou

[1] Ietf.org, Popis protokolu FTP. [cit. 2.4.2009]. Dostupné na WWW: http://www.ietf.org/rfc/rfc959.txt
[2] RSYNC, domácí stránka projektu. [cit 2.4.2009].http://rsync.samba.org/

bezpečnostní nevýhodu jako protokol FTP, ale je možné ho tunelovat přes šifrovaný kanál SSH.

8.10 Řešení krizových situací

Nejjednodušší způsob řešení krizových situací je jejich předcházení.
V rámci ztráty dat je základním kamenem předcházení krizových situací aktualizace systému a jeho zálohování. Způsoby řešení jsou popsány v předcházejících kapitolách. Bohužel se může stát, že útočník provede zdařilý útok na systém. Pokud bude útok veden tak, aby stroj vyřadil z provozu, je záhy zdařilý útok patrný na první pohled. Následuje reinstalace systému, update a obnova dat ze zálohy. Větším nebezpečím je však tichý a nenápadný zdařilý průnik do systému, kdy útočník následně začne využívat napadnutý stroj jako úložiště nelegálních dat, k prezentaci svých dat (útok na webserver) nebo jako přestupní bod pro další nelegální činnost. Zmíněná nelegální činnost může být vedena vůči dalším prostředkům vnitřní sítě nebo napadený stroj bude použit k útokům na cíle v internetu. Např. příprava DOS útoku nebo ztížení dohledávání útočníka. Následuje popis dvou způsobů, jak objevit průnik do systému. Oba lze automatizovat a hlášení o nestandardní situaci zajistit třeba zasláním varovného mailu či SMS. Prvním způsobem je analýza logů a druhým je zavedení detekce průniku.

8.10.1 SWATCH

V dobře spravovaném systému vždy běží služba, která zachytává chybové hlášky jádra systému a běžících programů. Většinou tato hlášení ukládá v textové podobě do tzv. log souborů. Je sice možné provádět kontrolu manuálně, ale toto je časově náročné, neboť na středně vytíženém stroji mohou logy dosáhnout i několika stovek kilobytů. Jedním z nástrojů umožňujícím analýzu informací z logu je program Swatch. Jedná se o program vyvinutý na Stanfordské univerzitě. Jedná se o program napsaný v jazyce Perl, který je multiplatformní a bude fungovat na všech linuxových distribucích. Program dokáže běžet buď jako dávkově spouštěný třeba právě programem cron, nebo v reálném čase, kdy načítá a vyhodnocuje on-line data zapisovaná do souboru logu.
Příklad konfigurace:

Do souboru /root/.swatchrc provedeme zápis

```
watchfor /Fail*pass/
      mail=root,subject=Autorizace selhala
      treshold    type=limit,count=1,seconds=300
```

Uvedený příklad prohledá soubor s logem na výskyt příslušného řetězce (například „authentication failure“) a zašle email uživateli root s předmětem „Autorizace selhala“. A to vše maximálně jednou za 5 min. Pokud se v nastaveném čase bude hláška opakovat, program bude pouze pokusy sčítat. V těle mailu se bude nacházet celá chybová hláška:

```
Apr 10 16:43:02 support sshd[18329]: Failed password for root from
192.168.85.178 port 38378 ssh2
```

Program spustíme buď z řádku nebo pomocí programu cron následujícím příkazem:

```
swatch –f /var/log/secure
```

Tuto programovou nadstavbu můžeme použít i na jiná hlášení, než k nahlášení pokusu o neautorizovaný přístup. Dají se jím analyzovat například chyby na disku ještě před jeho totální havárií.

8.11 Systémy pro odhalení průniku

Pokud se povede zkušenému útočníkovi nenápadně prolomit přihlášení k serveru, tak jeho prvním úkolem je zabezpečit zastavení logování události nebo alespoň smazat informace o možném napadení a skrýt jeho další činnost. Jeden ze způsobů nenápadného průniku do systému, který není zaznamenán do logu jako chyba, je získání některého z uživatelských účtů například způsobem sociálního inženýrství. Pomocí tohoto způsobu nic netušící uživatel vyzradí útočníkovi své přihlašovací údaje. Dalším způsobem je vyzrazení přístupu nespokojeným, vyhozeným či jinak frustrovaným zaměstnancem. Pro skrytí své ilegální činnosti musí útočník například změnit funkci programu „ps“, který má za úkol výpis procesů běžících v počítači tak, aby jeho konkrétní běžící programy nezobrazoval. Podobnou úpravu provede i pro službu

logování událostí, aby jeho činnost nebyla nijak zaznamenávána. Administrátor poté nemá šanci jeho nekalou činnost standardními cestami odhalit. Řešením je po nainstalování a updatu systému udělat otisk kontrolních součtů systémových souborů do databáze a pravidelně kontrolovat jejich integritu komparací aktuálních kontrolních součtů se součty v databázi. Případná nahlášená změna může mít tři důvody.

- Správce nainstaloval nový program nebo jeho novou verzi. O tom by měl správce vědět a mimo aktualizace databáze s kontrolními součty souborů není nutno vyvolávat nějaká další opatření.
- Došlo k chybě na disku. Zde je třeba prohlédnout systémový log a začít se připravovat na možnou výměnu disku.
- Povedl se průnik do systému a útočník změnil některé programové či systémové soubory. Zde je třeba provést obnovu souborů například ze zálohy a zjistit, jakým způsobem se útočník do systému dostal. Po té učinit příslušná protiopatření. Metodika hledání způsobu průniku je velmi složitá a doporučuje se ji přenechat například specializované organizaci.

V rámci části práce týkající se bezpečnosti Linuxu jsou zmíněny dva zástupci programových nadstaveb řešící výše popsaný problém. Vzhledem ke složitosti instalace či konfigurace jsou tyto programy zmíněny pouze pro doplnění informací a popsány pouze principy fungování a jejich základní vlastnosti. V rámci zabezpečení školní počítačové sítě je možné si vystačit s analýzou logů.

8.11.1 Tripwire

Jedním z programů, který slouží k detekci průniku za použití kontroly integrity souborů je Tripwire. Tento program při prvním spuštění vyzve uživatele k zadání dvou hesel. Jedno heslo je ke čtení databáze a druhé k zápisu databáze. Po načtení programů v systémových oblastech a jejich kontrolních součtů vytvoří databázi. Poté databázi zašifruje klíčem k zápisu. V případě testování systémových oblastí je možno šifrovanou databázi otevřít heslem ke čtení. V případě updatu databáze je nutno zadat heslo pro

zápis. Program je v dnešní době na vysoké úrovni, ale jeho konfigurace není příliš jednoduchá. Bližší informace k projektu je možno nalézt na www stánkách projektu www.tripwire.com. Zde je možné stáhnout jak lite verzi zdarma, tak případně sofistikovanější komerční verzi.

8.11.2 LIDS – Linux Intruder Detection System

Jedná se o programovou nadstavbu přímo jádra operačního systému Linux.
LIDS je softwarová záplata linuxového jádra spadající pod licenci GPL, která umožňuje významně zvýšit bezpečnost Linuxu, a její hlavní vlastnosti jsou:

- Ochrana souborů a adresářů. Nikdo včetně administrátora nemůže modifikovat soubory chráněné pomocí LIDS. Soubory a adresáře mohou být i neviditelné.
- Ochrana procesů. Nikdo včetně administrátora nemůže ukončit pomocí signálu kill chráněné procesy. Procesy mohou být i neviditelné.
- *Access Control Lists (ACLs)* pro přístupová práva k souborům, adresářům (*File ACLs*) a ACLs, která omezují schopnosti a systémové možnosti procesů (*Capability ACLs*).
- Rozšířená schopnost kontrolovat celý systém.
- Bezpečnostní avíza od jádra operačního systému. SMTP klient se volitelně může stát součástí jádra.
- IDS - systém detekce průniku.

V názvu projektu je sice uveden systém odhalení průniku (IDS), ale největším přínosem softwarové záplaty LIDS je bezesporu jedinečná schopnost LIDS vynutit silná přístupová omezení pomocí ACLs.

Další informace a popis instalace a konfigurace je možné nalézt na stránkách projektu www.lids.org.

9 WWW rozhraní pro ovládání přístupu k internetu pro počítačové učebny

Pro provoz webového rozhraní je třeba mít nainstalovaný webový server. V použité distribuci Fedora Core je WWW server připraven a provozován pomocí softwarového balíku Apache HTTP Server – dále jen „httpd“. Pokud není instalován při základní instalaci, je možno ho doinstalovat pomocí příkazu

```
yum –y install httpd
```

Vzhledem k tomu, že se nebude jednat o provoz statických webových stránek, ale bude vyžadováno interaktivní nastavování systému, je třeba nainstalovat podporu pro scriptovací jazyk PHP. Pokud není nainstalována při základní instalaci, je možno jí doinstalovat příkazem:

```
yum –y install php
```

Httpd je velmi mocný nástroj a má místy složitou konfiguraci. Následuje popis změn a doplnění nastavení, které jsou potřeba pro správný a bezpečný běh služby.
Všechny konfigurační soubory se nacházejí v adresáři /etc/httpd. Hlavní konfigurační soubor je /etc/httpd/conf/httpd.conf.
V něm je třeba poupravit následující konfigurační volby:

V sekci 2 „Main server configuration“
Stávající položku

```
#ServerName: www.example.com:80
```

změnit na reálný název serveru. V řešeném případu má řádek následujíc tvar:

```
ServerName gw.modelova-skola.cz:80
```

Stávající položku

```
#DocumentRoot „/var/html“
```

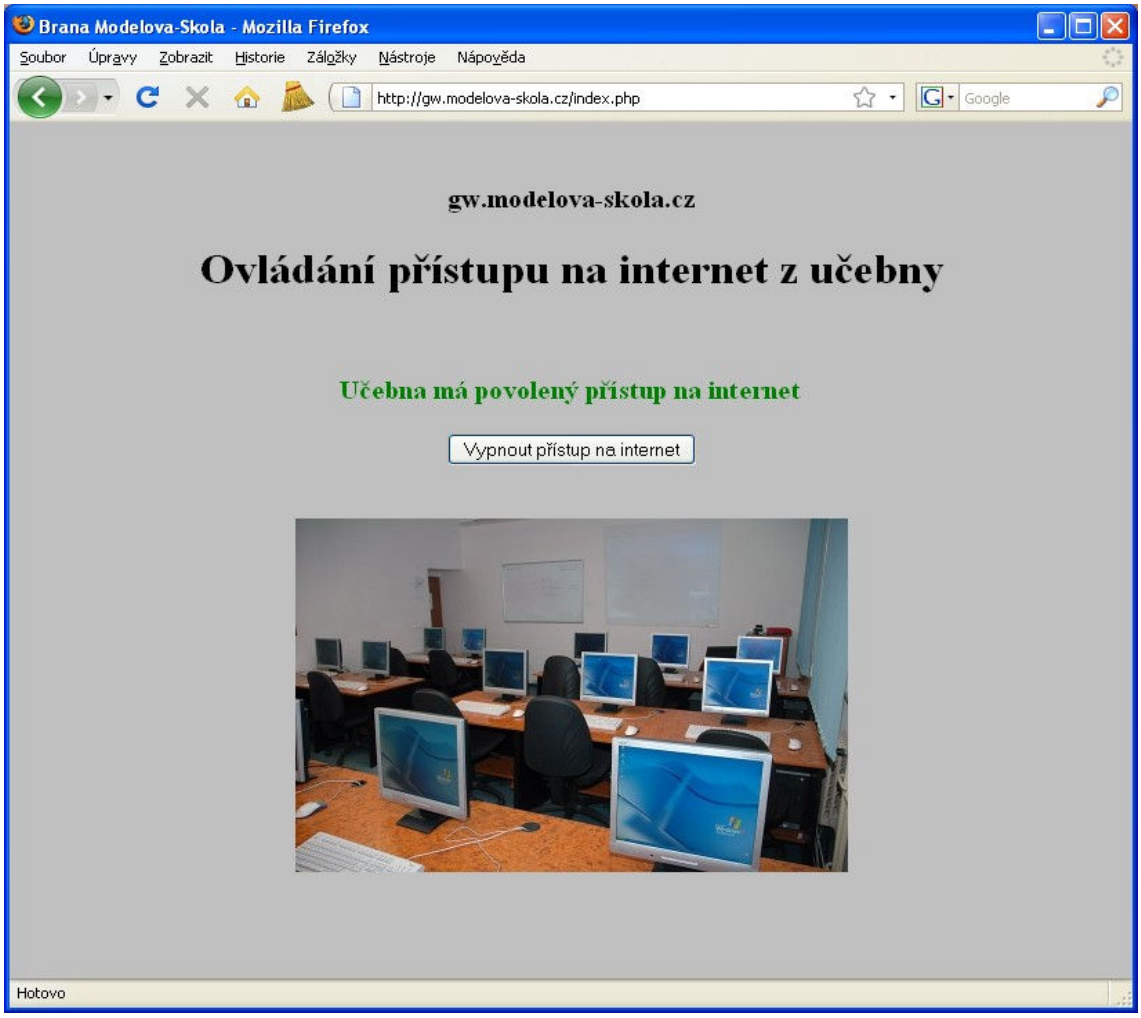
změnit na

```
DocumentRoot „/srv/www/gw“
```

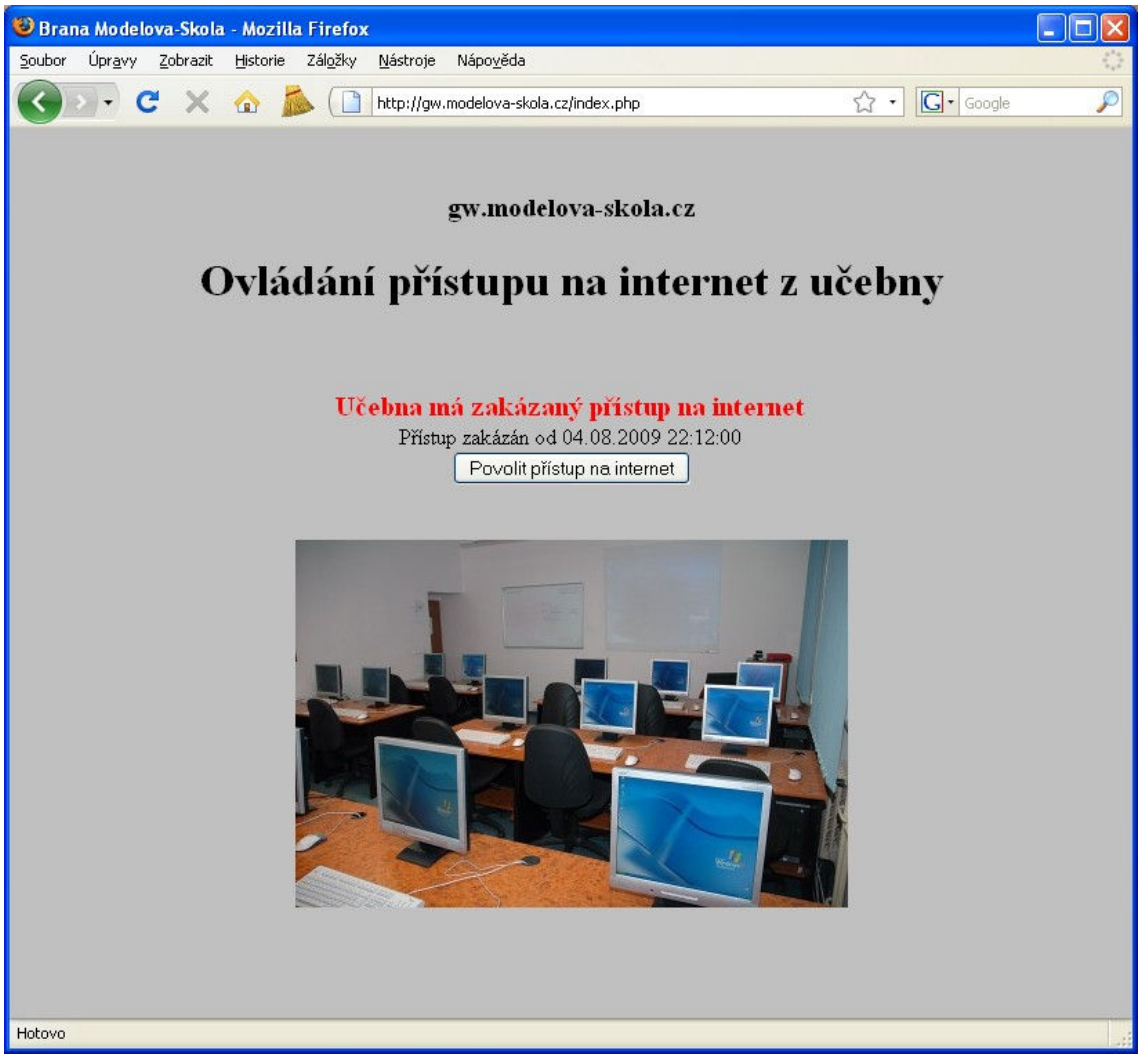
Tím je základní konfigurace webové služby pro ovládání přístupu na internet z počítačové učebny v modelové škole hotova.
Dále je třeba vytvořit adresář s výkonnou částí webového rozhraní /srv/www/gw a uložit do něj script a pokud je to požadováno, tak i například obrázek učebny.

Celý systém funguje následovně: Vyučující se připojí z učitelského počítače pomocí internetového prohlížeče na adresu brány.
V tomto případě to je http://gw.modelova-skola.cz

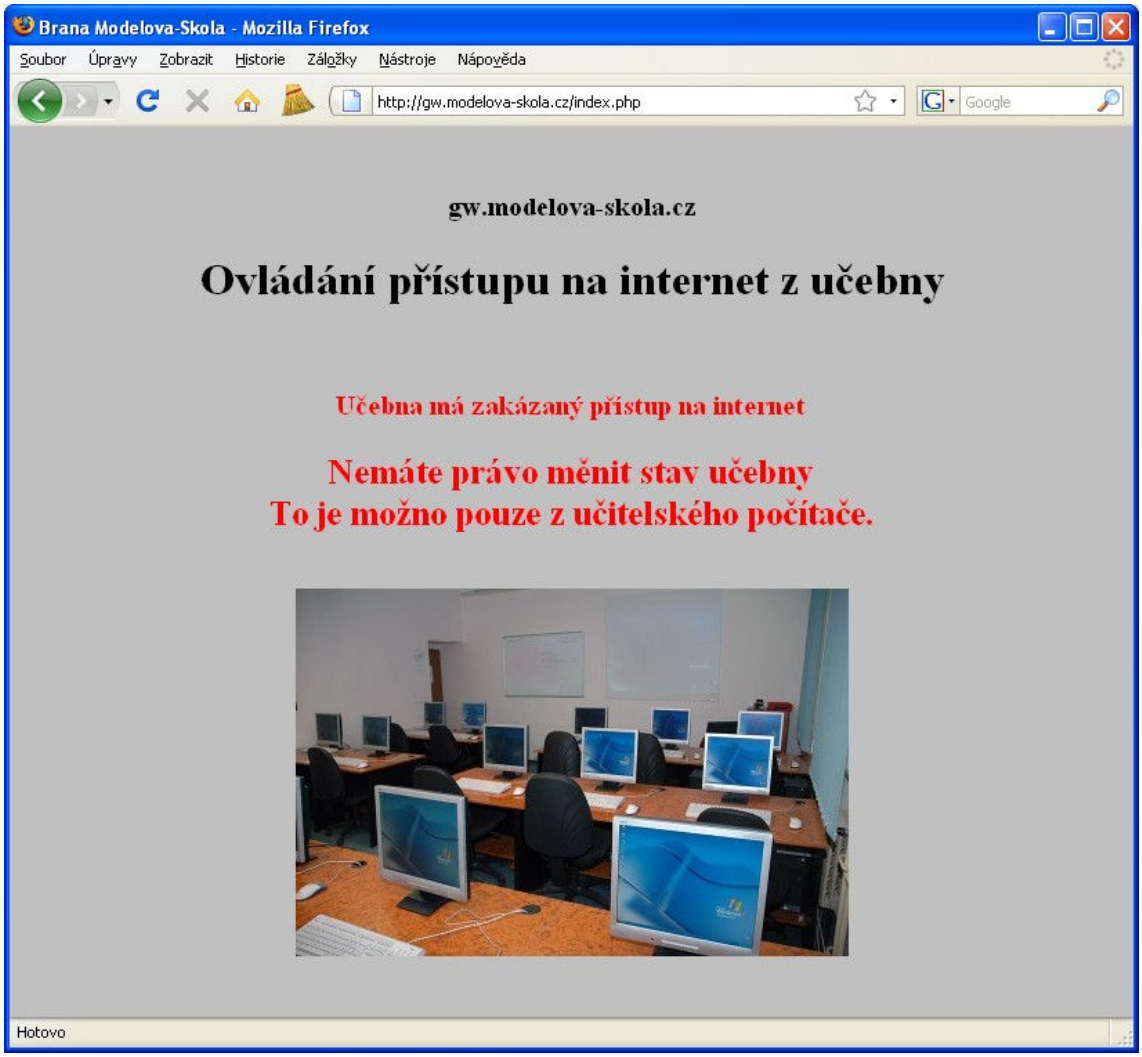
Pokud je povolen přístup na internet ze žákovských počítačů v učebně, bude zobrazena následující stránka, kdy se pomocí ovládacího tlačítka může stav učebny změnit – zakázat přístup.



Pokud není povolen přístup na internet ze žákovských počítačů v učebně, bude zobrazena následující stránka, kde se pomocí ovládacího tlačítka může stav učebny změnit – tedy povolit přístup.



Pokud se někdo pokusí připojit na ovládací stránku z jiného než učitelského počítače, zobrazí se mu stránka se statusem učebny a bez ovládacího prvku. Současně je vypsána chybová hláška, že stanice nemá právo měnit stav učebny. Oblast oprávněných učitelských počítačů lze definovat na začátku ovládacího scriptu. V našem případě dle zadání se jedná o stanice s IP rozsahem 192.168.81.5-192.168.81.31.



Toto webové rozhraní uloží do systému informaci o stavu učebny. Každou minutu se pak provádí kontrola požadavku změny stavu. V případě potřeby se spouští zvláštní script, který zakáže či povolí žákovským stanicím přístup na internet.

9.1.1 PHP script generující ovládací stránku nadstavby

Script je uložen v nadefinovaném root adresáři serveru, v konkrétním modelovém případě je to /srv/www/gw /index.php. Script je pro lepší orientaci komentován.

```
<?
//test, zda pozadavek jde z ucitelskeho PC
list($ip1,$ip2,$ip3,$ip4)=explode(".",$_SERVER['REMOTE_ADDR']);
if ( $ip1 == "192" && $ip2 == "168" && $ip3 =="38" && $ip4 < 32){
  $ucebna_pristup=1;
    } else { $ucebna_pristup=0;}


//volani funkce vypnuti a zapnuti pristupu na internet
if ($_POST['VYP'] != ''){ucebna_vyp($ucebna_pristup);}
if ($_POST['ZAP'] != ''){ucebna_zap($ucebna_pristup);}

//informace o stavu ucebny
if (file_exists("/tmp/ucebna.dat")){

  $ucebna_status="<span style=\"color: red; font-size: 20px; font-
weight: bold\">Učebna má zakázaný přístup na internet</span>";
  $ucebna_tlacitko="<input type=\"submit\" name=\"ZAP\"
value=\"Povolit přístup na internet\">";
  $soubor = fopen("/tmp/ucebna.dat","r");
  $vypnuto_od="Přístup zakázán od ".fread($soubor,100);
  fclose($soubor);

} else {

  $ucebna_status="<span style=\"color: green; font-size: 20px; font-
weight: bold\">Učebna má povolený přístup na internet</span>";
  $ucebna_tlacitko="<input type=\"submit\" name=\"VYP\"
value=\"Vypnout přístup na internet\">";

}
```

```
print "
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01//EN\">
<html><head>
<meta http-equiv=\"Content-Type\" content=\"text/html;charset=UTF-8\">
<META http-equiv=\"cache-control\" content=\"no-cache\">
<META http-equiv=\"pragma\" content=\"no-cache\">
<title>Brana Modelova-Skola</title>
</head>
<body style=\"background-color: silver;\">
<center>
<br>
<h3> gw.modelova-skola.cz</h3>
<h1>Ovládání přístupu na internet z učebny</h1>
<br><br>
$ucebna_status
<br>
";

if ($ucebna_pristup){
  print "
  <form action=\"index.php\" method=\"POST\">
  $vypnuto_od
  <br>
  $ucebna_tlacitko
  </form>
  ";
} else {

  print "
    <br>
    <div style=\"color:red; font-size: 25px; font-weight: bold;\">
      Nemáte právo měnit stav učebny<br>
      To je možno pouze z učitelského počítače.
      </div>
  ";
}
```

```
print "
<br>
<br>
<img src=\"ucebna1.jpg\" alt=\"učebna\">
</body>
</html>
";

####################################
# funkce pro povoleni internetu v ucebne
function ucebna_zap($ucebna_pristup){
    if (! $ucebna_pristup){return;} //neni-li povolen pristup, ukonci
funkci
    if (file_exists("/tmp/ucebna.dat")){unlink("/tmp/ucebna.dat"); }
}

# funkce pro zakazani internetu v ucebne
function ucebna_vyp($ucebna_pristup){
    if (! $ucebna_pristup){return;} //neni-li povolen pristup, ukonci
funkci
    if (! file_exists("/tmp/ucebna.dat")){
      $soubor = fopen("/tmp/ucebna.dat","w");
      fwrite($soubor, date("m.d.Y H:i:00"));
      fclose($soubor);
    }
}
?>
```

9.1.2 Script zajišťující zákaz či povolení přístupu na internet

Script je uložen v adresáři s ovládacím PHP scriptem a jmenuje se ucebna.sh .

Soubor /srv/www/gw/ucebna.sh

```
#!/bin/sh

# test na existenci pozadavku na zakaz provozu z ucebny
if [ -e "/tmp/ucebna.dat" ]; then
```

```
    #pokud nexexistuje informace o tom, ze byl pozadavek jiz vykonan
    if [ ! -e "/tmp/ucebna.lck" ]; then
        #nastavit ciste firewall
        /etc/init.d/firewaling
        #zakazat forward provozu pro zakovske stanice do internetu
        /sbin/iptables -I FORWARD -s 192.168.81.32/27 -d 0.0.0.0/0 \
            -j REJECT
        #vytvorit informaci o provedenem pozadavku
        touch "/tmp/ucebna.lck"
    fi
else
    #pokud nexexistuje informace o tom, ze byl pozadavek jiz vykonan
    #a neni pozadavek na zakaz
    if [ -e "/tmp/ucebna.lck" ]; then
        #nastavit ciste firewall
        /etc/init.d/firewaling
        #smazat informaci o provedenem pozadavku
        rm -f "/tmp/ucebna.lck"
    fi
fi
```

Pro správnou funkci nadstavby je třeba zajistit pravidelné spouštění scriptu ucebna.sh každou celou minutu například službou crond. Založíme například soubor /root/contab.conf a jeho obsahem bude řádka

```
* * * * * /srv/www/gw/ucebna.sh
```

Poté je třeba zajistit, aby služba novou konfiguraci načetla a tento příkaz začala provádět. To se provede z příkazové řádky pomocí

```
crontab /root/crontab.conf
```

Podrobně se službou crond zabývá kapitola Automatické spouštění programů.

Tím je nadstavba plně připravena k provozu.

10 Vyhodnocení zabezpečení Linux v testovaných školách

10.1 Technické vyhodnocení

Na základě konkrétního nasazení zabezpečení školní počítačové sítě na bázi operačního systému Linux popsaného v této diplomové práci a po následné analýze bezpečnostních logů za stejné období jednoho měsíce, je možné konstatovat, že bylo zabráněno celkem desetitisícům pokusům o získání neoprávněného přístupu k routeru. V tabulce „Neoprávněné přístupy“ jsou uvedeny tyto pokusy s rozdělením podle uživatele a unikátní zdrojové adresy. Následně pak byla provedena analýza logů se záznamem požadavků na neoprávněné připojení ke službám. Celkem bylo zaznamenáno alarmujících 337.213 zakázaných pokusů o neoprávněné připojení k službám routeru. Logy jsou k dispozici na přiloženém CDROM.

10.1.1 Metodika zpracování logů zamítnutých přihlášení.

Písmeno X v názvu souboru znamená pořadové číslo školy (tedy škola1 a škola 2):

Následujícím příkazem byly vybrány řádky pro neoprávněný přístup k administrátorskému účtu root a zapsány do zvláštního souboru:

```
grep „Failed password“ skolaX_secure | grep root >  skolaX_secure_root
```

Následujícím příkazem byly vybrány řádky pro neoprávněný přístup k neadministrátorskému účtu a zapsány do zvláštního souboru. Vzhledem k tomu, že na strojích nebyl aktivní jiný účet než administrátorský, vyhověly všechny záznamy nepatřící administrátorskému účtu.

```
grep „Failed password“ skolaX_secure | grep –v root > \
skolaX_secure_noroot
```

Následujícím příkazem byly spočteny všechny požadavky pro neoprávněný přístup k administrátorskému účtu root

```
cat skolaX_secure_root | wc –l
```

Následujícím příkazem byly spočteny všechny požadavky pro neoprávněný přístup k neadministrátorskému účtu root

```
cat skolaX_secure_noroot | wc –l
```

Následujícím příkazem byly spočteny všechny unikátní IP adresy, ze kterých byly vedeny požadavky pro neoprávněný přístup k neadministrátorskému účtu root

```
cat skolaX_secure_nroot | awk –F "from" {'print $2'} | \
awk –F "port" {'print $1'} | sort –u | wc –l
```

Následujícím příkazem byly spočteny všechny unikátní jména podvrhnutých uživatelských účtů, ze kterých byly vedeny požadavky pro neoprávněný přístup k neadministrátorskému účtu root

```
cat skolaX_secure_noroot | awk –F "from" {'print $2'} | \
awk –F "port" {'print $1'} | sort –u | wc –l
```

10.1.2 Metodika zpracování logu pokusů o neoprávněného připojení ke službám z hlediska typu paketu

Tento log je k dispozici pouze u školy1. U školy 2 nebylo možné log zachovat z důvodu množství místa na pevném disku. V rámci sledování provozu byly zaznamenávány veškeré pokusy o připojení k routeru. Z nich pak byly filtrem vybrány ty pokusy, které neměly s provozem routeru nic společného.

Tabulka pokusů zamítnutých přihlášení

Popis	**škola 1**	**Škola 2**
Počet útoků na účet root	9623	8363
Počet útoků na jiný účet	31400	27404
Celkem útoků na přístup	**41023**	**35767**
počet unikátních IP adres pro útok na účet root	57	119
počet unikátních IP adres pro útok na účet jiný účet než root	48	100
počet unikátních uživatelských jmen pro útok na účet jiný účet než root	8816	6419

Tabulka pokusů o neoprávněné připojení ke službám z hlediska typu paketu.

popis	**počet útoků**	**počet unikátních adres**
Útok paketem ICMP	115390	458
Útok paketem TCP	199327	1415
Útok paketem UDP	22496	1954
	337213	

10.2 Vyhodnocení ze strany správců a učitelů ICT

V závěru ověřovacího provozu na jednotlivých školách byl provedeno šetření spokojenosti metodou řízeného rozhovoru s použitím otevřených otázek. Díky nim bylo možno získat ucelenější náhled na výsledky ověřovacího provozu.
Na jedné škole byl jeden z učitelů současně správcem ICT. O Linux se zajímal i v rámci sebevzdělávání. Tento učitel-správce hodnotil projekt kladně, aktivně ze zajímal o jeho možná rozšíření. Do budoucna byla zjišťována možnost přidání ovládání další učebny do webové aplikace, možnost instalace a ovládání proxyserveru, který by měl sloužit pro filtrování obsahu www stránek.
Správce na druhé škole byl externím pracovníkem, který neměl s Linuxem zásadní zkušenosti. Jeho specializací byla oblast pracovních stanic na bázi operačního systému Windows. Z hodnotícího rozhovoru vyšlo najevo, že až na nezvyklé ovládání Linuxu přes příkazovou řádku, hodnotil ověřovací provoz kladně.

Ostatní učitelé pracujících v počítačové učebně hodnotili ověřovací provoz kladně. Obzvláště kladně hodnotili jednoduchost ovládání přístupu na internet pro žákovské stanice. Díky této nadstavbě se též dařilo udržet na vysoké úrovni kázeň při suplovaných hodinách, které probíhaly v počítačové učebně. Žáci se pod pohrůžkou vypnutí přístupu k internetu v případě kázeňských problémů a tedy znemožnění hraní her a či jiné zábavy založené na internetové komunikaci, chovali nezvykle klidně.

11 Závěr

Diplomová práce měla za úkol zmapovat současný stav a možnosti připojení školních počítačových sítí a navrhnout optimální způsob jejich zabezpečení. Výsledkem byla volba zabezpečit školní počítačovou síť na bázi operačního systému Linux.
Na základě této volby byl předložen modelový způsob instalace a nastavení operačního systému Linux tak, aby splňoval požadavky na bezpečnou komunikaci lokálních hostitelských stanic s okolním digitálním světem.

V práci jsou též shrnuta možná nebezpečí útoku na citlivá data a stabilitu počítačové sítě a navrhnuty možnosti řešení ochrany před těmito hrozbami. Toto shrnutí přináší ucelený pohled na základní metody počítačových útoků vedených po síti internet a obranu proti nim. Jako důkaz, že není radno tyto hrozby podceňovat, je i výsledek analýzy logů, kdy bylo zachyceno celkem 414.003 pokusů o nelegální přístup do sledované počítačové sítě. Každý z těchto útoků představoval potencionální hrozbu možné ztráty či zneužití dat, případně poškození zařízení a následně nemožnost zabezpečit výuku v počítačové učebně.

Požadovaná nadstavba pro řízení přístupu k internetu ze žákovských stanic vyvinuta a úspěšně otestována nadstavba.

Závěrem lze prohlásit, že cíle stanovené na počátku práce byly úspěšně splněny.

Diplomová práce může být výchozím materiálem pro další činnost, kterou lze realizovat např. v rámci doktorského studia. Je možné rozšířit předložené řešení o další bezpečnostní prvky jako třeba proxyserver s možností filtrace obsahu stahovaných webových stránek.

12 Použitá literatura

- BRDIČKA, B. Role internetu ve vzdělávání, Kladno : AISIS, 2003, ISBN 80-239-0106-0. Dostupné z: omicron.felk.cvut.cz/~bobr/role/
- BRDIČKA, B. Vzdělávání a internet 2. generace, Česká škola.cz, 2006, ISSN 1213-6018.
  Dostupné z: www.ceskaskola.cz/ICTveskole/Ar.asp?ARI=103468&CAI=2129
- Kopecký, K. E-learning (nejen) pro pedagogy. Olomouc: Hanex, 2006. ISBN 80-85783-50-9
- VÚP Praha, Rámcový vzdělávací program pro základní vzdělávání, VÚP Praha 2005
- VÚP Praha, Rámcový vzdělávací program pro gymnazijní zdělávání, VÚP 2004 pilotní verze
- VÚP Praha. Učební plán. Metodický portál RVP [online]. [cit. 2009-02-13]. Dostupné na WWW: http://www.rvp.cz/clanky
- DOMBROVSKÁ, M. Informační gramotnost z hlediska veřejné politiky : Jak definovat informační gramotnost? . Ikaros 2002, č. 12. Dostupné na WWW: http://www.ikaros.cz/Clanek.asp?ID=200211011. ISSN 1212-5075
- NEUMAJER,O. *ICT kompetence učitelů*. Praha : Pedagogická fakulta UK v Praze, 2007. 167 s. Dizertační práce
- *Klíčové kompetence* [online]. 2007 [cit. 2008-12-18]. Dostupné na WWW: http://cs.wikipedia.org/wiki/Kl%C3%AD%C4%8Dov%C3%A9_kompetence
- CAPPER, J.. *Teacher training and technology : An Overview of Case Studies and Lessons Learned* [online]. c2000 [cit. 2008-12-14]. Angličtina. Dostupné na WWW: http://www.techknowlogia.org/TKL_Articles/PDF/195.pdf
- STERNBERG. Kognitivní psychologie. 2002. PORTÁL. ISBN 80-7178-632-2.
- JENKINS, J. *Teaching for tomorrow : The changing role of teachers in the connected classroom* [online]. 1999 [cit. 2008-12-17]. Angličtina. Dostupné na WWW: http://www.eden-online.org/papers/jenkins.pdf
- Internetový portál ABCLinuxu, http://www.abclinuxu.cz

- PERKINS, CH., STREBE, M. Firewally a proxy-servery, Computer Press, 2003
- AULDS, CH. Linux Apache, administrace serveru, Grada 2003
- KRČMÁŘ, P. Linux, tipy a triky pro bezpečnost, Grada 2004
- FLICKENGER, R. Linux server na maximum, 100tipů a řešení pro náročné, Computer Press 2005
- Internetový portál Root.CZ, http://www.root.cz
- The PHP Group. Dokumentace jazyka PHP. Php.net [online]. 2008 [cit. 2009-04-10]. Dostupný na WWW: http://www.php.net
- Popis protokolu SSH. [cit 23.4.2009]. Dostupné na WWW: http://www.ietf.org/rfc/rfc4251.txt
- The Netfilter.ORG project. [cit 23.4.2009]. Dostupné na WWW: http://www.netfilter.org/
- Root.cz, Stavíme firewall. [cit. 23.4.2009]. Dostupné na WWW: http://www.root.cz/clanky/stavime-firewall-1/
- ISC, Internetová prezentace – domácí stránky společnosti. [cit. 2.4.2009]. Dostupné na WWW: https://www.isc.org/
- Root.CZ Informace nejen ze světa Linuxu. [cit 2.4.2009]. Dostupné na WWW: http://www.root.cz/slovnicek/dns/
- Root.CZ Informace nejen ze světa Linuxu. [cit 2.4.2009]. Dostupné na WWW: http://www.root.cz/slovnicek/chroot/

13 Seznam příloh

Příloha č 1 – zadání DP

Příloha č. 2 – volně ložený optický disk obsahující elektronickou verzi diplomové práce, použité příklady nastavení, zdrojové kódy skriptů.