



LINUX

postavte si počítačovou síť

Petr Krčmář

- ❑ Výběr linuxové distribuce
- ❑ Bezpečnost počítačových sítí
- ❑ Síťové vrstvy a síťová rozhraní
- ❑ Instalace a konfigurace Samby
- ❑ Webový server Apache



GRADA

Upozornění pro čtenáře a uživatele této knihy

Všechna práva vyhrazena. Žádná část této tištěné či elektronické knihy nesmí být reprodukována a šířena v papírové, elektronické či jiné podobě bez předchozího písemného souhlasu nakladatele. Neoprávněné užití této knihy bude **trestně stíháno**.

Používání elektronické verze knihy je umožněno jen osobě, která ji legálně nabyla a jen pro její osobní a vnitřní potřeby v rozsahu stanoveném autorským zákonem. Elektronická kniha je datový soubor, který lze užívat pouze v takové formě, v jaké jej lze stáhnout s portálu. Jakékoliv neoprávněné užití elektronické knihy nebo její části, spočívající např. v kopírování, úpravách, prodeji, pronajímání, půjčování, sdělování veřejnosti nebo jakémkoliv druhu obchodování nebo neobchodního šíření je zakázáno! Zejména je zakázána jakákoliv konverze datového souboru nebo extrakce části nebo celého textu, umísťování textu na servery, ze kterých je možno tento soubor dále stahovat, přitom není rozhodující, kdo takovéto sdílení umožnil. Je zakázáno sdělování údajů o uživatelském účtu jiným osobám, zasahování do technických prostředků, které chrání elektronickou knihu, případně omezují rozsah jejího užití. Uživatel také není oprávněn jakkoliv testovat, zkoušet či obcházet technické zabezpečení elektronické knihy.



Copyright © Grada Publishing, a.s.



Copyright © Grada Publishing, a.s.



Copyright © Grada Publishing, a.s.

Obsah

Slovo úvodem	11
Část I: Úvod do problematiky počítačových sítí	15
1. Historie počítačů, Unixu a internetu.....	17
1.1 Počítače a Unix	17
1.2 Historie internetu	20
2. Síťové vrstvy.....	23
2.1 Hardwarová vrstva.....	24
2.2 IP vrstva	25
2.3 Protokol TCP a UDP	26
2.4 Aplikační vrstva	28
3. Síťová rozhraní	29
3.1 Adresa a maska	29
3.2 Příkaz ifconfig.....	30
3.3 Routovací tabulka	31
3.4 PLIP	32
3.5 Ethernet	33
Ethernetové prvky	34
Nastavení karet.....	35
ARP protokol	35
4. Výběr linuxové distribuce	39
4.1 Distribuce vhodné pro server	40
Debian.....	40
Gentoo.....	41
Slackware.....	41

4.2 Distribuce vhodné pro desktop	42
Ubuntu.....	42
Fedora Core	42
Mandriva	42
5. Bezpečnost	43
5.1 Mýty a pověry	43
5.2 Nejběžnější druhy útoků	44
5.3 Jak se bránit	45
Část II: Praktická realizace sítě	47
6. Paketový filtr a firewall.....	49
6.1 Tabulky a řetězce	50
6.2 Syntaxe příkazu iptables	51
6.3 Filtrujeme	52
6.4 Tvorba vlastních řetězců	54
6.5 Překlad adres	54
6.6 Předávání paketů	56
6.7 Propouštění souvisejících spojení	57
7. Superserver xinetd	59
7.1 Konfigurace služeb	61
7.2 Kontrola přístupu	63
7.3 Ochrana před přetížením systému	63
7.4 Příklad konfiguračního souboru	64
8. Automatické přidělování IP adres	67
8.1 Konfigurace DHCP serveru	68
8.2 DHCP klient	70

9. Nameserver aneb DNS	71
9.1 Resolver	72
9.2 Druhy DNS serverů	73
9.3 Konfigurace DNS cache	74
9.4 Konfigurace primárního DNS serveru	76
10. FTP server	79
10.1 Postup připojení	80
Aktivní režim	80
Pasivní režim	81
10.2 FTP klienti	81
10.3 FTP server ProFTPD	82
10.4 Konfigurace ProFTPD	84
10.5 Spuštění ProFTPD	85
10.6 Omezení FTP uživatelů	86
11. Vzdálený terminál a protokol SSH	87
11.1 Historie a fakta o SSH	88
11.2 Klíče a fingerprinty	89
11.3 Konfigurace SSH serveru	89
11.4 Použití SSH klienta	91
11.5 Autorizace uživatele pomocí RSA klíčů	93
11.6 Další možnosti SSH	95
12. Síťový souborový systém (NFS)	97
12.1 NFS na straně klienta	98
12.2 NFS na straně serveru	99
13. Samba	101
13.1 Instalace Samby	102
13.2 Konfigurace Samby	103

13.3 Spouštění Samby	105
13.4 Správa uživatelů	106
13.5 Samba na straně klienta	106
smbget	107
smbmount	108
smbumount	109
14. Webový server	111
14.1 Protokol HTTP	111
14.2 Webový server Apache	115
14.3 Konfigurace webového serveru Apache	117
Global Environment	117
Main server configuration	119
.htaccess	122
14.4 Virtuální servery	123
14.5 Moduly Apache	125
Modul PHP	127
mod_perl a mod_python	127
mod_cband	128
Další moduly	129
15. Poštovní server	131
15.1 MUA, MTA a MDA	132
15.2 Protokol SMTP	132
15.3 Jak pošta putuje	134
15.4 Vyzvednutí pošty	135
15.5 Poštovní server Postfix	139
Konfigurace Postfixu	140
Antispam	141
15.6 POP3 a IMAP4	142
16. Virtuální privátní síť (VPN)	145
16.1 OpenVPN	147
16.2 Konfigurace jednoduchého tunelu	148

16.3 Práce s certifikáty	149
16.4 Vytvoření klient-server VPN	151
17. Tiskový systém CUPS.....	153
17.1 Konfigurace CUPS	154
17.2 Správa tiskáren	156
Ruční editace souborů	157
Webové rozhraní	158
Softwarové nástroje	159
17.3 Instalace ovladačů.....	161
17.4 CUPS a Samba	162
Slovo závěrem.....	165
Přílohy	167
Příloha A: Seznam TCP portů.....	167
Příloha B: Seznam doporučené literatury.....	174
Příloha C: Doporučené internetové zdroje.....	176
Rejstřík	179

Slovo úvodem

Operační systém Linux je mezi administrátory serverů velmi oblíbený a jeho zastoupení na trhu stále roste. Dnes v podstatě sotva naleznete středně velkou firmu, v níž by nebyl nasazen alespoň na firewallu. Jeho výhodou jsou oproti komerčním systémům především nižší náklady, robustnost, škálovatelnost, přizpůsobivost a vysoký výkon. Stejně klady ale dokáže nabídnout i „domácím“ uživatelům, kteří by si chtěli postavit vlastní počítačovou síť. Obvykle chtějí sdílet připojení k internetu v rámci jednoho domu, nabídnout své soubory ke sdílení nebo si jen tak vyzkoušet, co správa takového serveru obnáší.

V mnoha diskusních fórech pak najdeme příspěvky jako: „Ahoj, chci připojit náš panelák k internetu a slyšel jsem, že ten Linux je na to vhodný. Kde mám začít?“ Podobnými dotazy se diskuse jen hemží a tato tematika se v pravidelných intervalech objevuje vždy znovu a znovu.

Držíte v ruce knihu, která by vám měla na podobnou otázku dát jasnou a přesnou odpověď. Dozvíte se, co budete potřebovat, jak se na vše připravit a především se naučíte jednotlivé služby zprovoznit. Velkou výhodou této publikace je, že od čtenáře neočekává v podstatě nic. Nepředpokládám, že víte, co je to TCP, jak se nastavuje v Unixu IP adresa, ani proč potřebujete DNS a co to vlastně je. Vše bude postupně vysvětleno na mnoha

příkladech z praxe a do celé problematiky tak proniknete velmi přirozenou a nenásilnou cestou.

Přestože je vše psáno na míru systému GNU/Linux, měla by být většina postupů použitelná i v ostatních systémech unixového typu. Pro všechny podobné systémy je k dispozici mnoho softwaru, a proto by neměl být problém jej provozovat i v jiném prostředí. Můžete tak místo Linuxu sáhnout třeba po NetBSD, OpenSolaris a podobně.

Ke knize můžete přistupovat jednak jako k učebnici, ale také jako k manuálu. Doporučuji kombinovat obojí. Nejprve si přečtete hlavní části postupně jako učebnici a pak se k jednotlivým kapitolám vracíte, jak budete sami potřebovat.

Struktura knihy

Knihy je rozdělena do tří částí. První vás uvede do obecné problematiky počítačových sítí, vysvětlí teorii, kterou budete potřebovat později, a naučí vás některé základní operace potřebné k administraci Linuxu. Doporučuji tuto část přečíst pozorně a postupně jako učebnici, tedy od začátku do konce.

Druhá část se pak zabývá praxí, a to v míře, jak jen to je možné. Zde se naučíte to hlavní, tedy konfigurovat server, spouštět jednotlivé služby a řídit provoz celého vytvořeného systému. Tato část připomíná více než ta předchozí manuál. Můžete se v ní pohybovat podle potřeby a zajímat se o jednotlivé služby. Kapitoly jsou provázány jen minimálně, a tak není potřeba číst je všechny.

Poslední část knihy tvoří přílohy, ve kterých naleznete seznam nejběžnějších TCP portů, doporučenou literaturu k dalšímu studiu a internetové odkazy. Samozřejmě nechybí ani vředy tak důležitý rejstřík.

Typografické konvence

V knize jsou využívány různé typografické prvky, jako zvláštní druhy písma nebo speciální odstavce, označené piktogramem či ikonou. Jejich cílem je usnadnit čtenářům orientaci v textu a celkově usnadnit práci s knihou při studiu i při hledání odpovědi na konkrétní problém. Jedná se o následující věci:

- ✓ *Kurziva* označuje názvy internetových adres a odkazů.
- ✓ **Tučně** jsou označeny případné názvy karet, dialogových oken, příkazů z nabídek programů a obecně texty, které považujeme za důležité.
- ✓ Pro názvy kláves a klávesových zkratk jsou použity KAPITÁLKY.
- ✓ Počítačové kódy a názvy součástí operačního systému Linux jsou konečně sázeny neproporcionálním písmem.

Dále najdeme v knize tyto speciální odstavce:



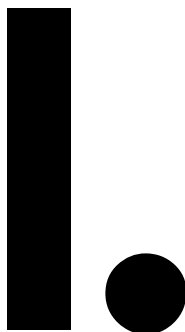
Tento symbol označuje odstavec, který rozšiřuje probíranou problematiku o nějakou zajímavost či výjimečnost. Poznámka není nezbytná k pochopení dané problematiky, většinou upozorňuje na další používané termíny označující stejnou skutečnost a prozrazuje další souvislosti.

Vykřičník zase upozorňuje na fakta, která byste měli určitě vědět, na situace, na něž byste měli dávat pozor, a na komplikace, se kterými se můžete při práci setkat.



Poděkování

Poděkování patří především mé ženě Petře, která přehlíží mnoho mých nedostatků a je mi v životě silnou oporou. Děkuji také celé své rodině, která, ač rozeseta po celé republice, je stále se mnou. Nesmím zapomenout ani na všechny své věrné přátele a fanoušky. A pochopitelně děkuji i vám, čtenářům – je to především vaše kniha!



Úvod do problematiky počítačových sítí

Na počátku bylo slovo. Tedy v tomto případě chuť postavit si vlastní počítačovou síť. Předpokládám, že jste se někde dočetli, že ten „Linux“ by na to mohl být to pravé, a proto jste si pořídili tuto knihu a nyní byste rádi začali. Kromě techniky, kabeláže a trochy šikovnosti budete především potřebovat alespoň základní znalosti o sítích, jejich funkci a GNU/Linuxu jako takovém.

Právě o tom bude následující teoretická část knihy. Vysvětlí vám, co je to síť, jak přes ní data putují, kdo je řídí a kam by asi měla dorazit. Pochopíte pojmy jako TCP/IP, paket, router, Ethernet, aplikační vrstva a podobně. Poznáte také operační systém GNU/Linux, zjistíte, co jsou to distribuce, a vyberete si tu pravou.

Vysvětlíme si také, jak celou síť realizovat po technické stránce, jaký hardware k tomu budeme potřebovat a jak můžeme vše propojit tak, aby to mohlo společně komunikovat. Na konci první části se budeme zabývat také jedním z aktuálních témat, kterým je bezpečnost. Pokud toho o sítích moc nevíte, doporučuji teoretickou část přečíst od začátku do konce. V opačném případě by vám totiž mohly uniknout důležité detaily, jimiž se v praktické části už nebudeme zabývat a budeme je považovat za samozřejmost.

1.

Historie počítačů, Unixu a internetu

1.1 Počítače a Unix

Počítačové sítě za sebou mají poměrně dlouhou a bouřlivou historii. Abychom pochopili jejich smysl a důvod jejich existence, musíme se ohlédnout zpět a podívat se, jak a proč vlastně přišly na svět.

V dávných dobách výpočetní techniky byly počítače vlastně samostatné oddělené jednotky, které pracovaly na svých stejně samostatných a oddělených úkolech. Počítače byly velmi drahé a složité, a proto jich existoval jen poměrně omezený počet. Tehdy se jednalo převážně o velké sálové počítače. Ty dokázaly plnit různé úkoly na základě složitě vloženého programu, který vždy připravovala na míru skupina programátorů. Abyste ovšem správně chápali jejich funkci: technicky se jednalo o něco, co připomíná dnešní programovatelné kapesní kalkulačky. Bavíme se ale o padesátých letech dvacátého století.

Už v té době ale počítače dokázaly urychlit mnoho složitých a náročných výpočtů, které by často bez jejich pomoci nebylo možné vůbec realizovat. Pomáhaly rovněž při praktických operacích u akcí, jako je například sčítání lidu.



Obrázek 1.1: Počítač Vax ze sedmdesátých let



Každý počítač obsahoval řadu relé pro přepínání signálů. Tato relé byla však velmi náchylná na různé druhy poruch. Aby fungovala bezchybně, musela být zajištěna naprostá čistota spínaných kontaktů. Při rozloze počítače, která dosahovala až stovek metrů čtverečních, to ale představovalo velmi obtížný úkol. Největším nepřítelem kontaktů byl mrtvý hmyz. Tělíčka mušek padala do obvodů a relé a vytvářela tak izolaci. U každého počítače tedy asistovala skupinka lidí, kteří se štěpali v ruce obíhali stále dokola všechna relé a vymetali z nich prach a hmyz. Takto vznikl pojem debugger, který by se dal přeložit jako „odhmyzovač“.

Počítače padesátých let byly složeny z tisíců elektronek, stykačů, diod a z kilometrů drátů. Počátkem šedesátých let se však začaly ve větší míře vyrábět a prosazovat integrované obvody. Ty umožnily prudký rozvoj počítačů a nebývalé vylepšení hardwaru. Začaly se objevovat stále složitější a rychlejší počítače, které se ale zároveň zmenšovaly. Další nezanedbatelnou výhodou použití integrovaných obvodů byl ohromný nárůst spolehlivosti počítačů. Elektronky byly velmi poruchové a u starých počítačů jich bylo denně potřeba vyměnit i několik stovek.

S rostoucí složitostí a dostupností počítačů bylo potřeba zajistit také jejich jednoduchou programovatelnost. Šedesátá léta proběhla ve znamení prudkého rozvoje programovacích jazyků. Objevily se jazyky Fortran, Cobol, Algol, Basic a další. Situace na poli programovacích jazyků byla v té době velmi nepřehledná, téměř každý obor využití počítačů používal vlastní jazyk.

V polovině šedesátých let se objevily první víceuživatelské počítače, které díky svému výkonu umožňovaly, aby na nich pracovalo více lidí zároveň. Každý uživatel byl připojen vlastním jednoduchým terminálem, jehož pomocí s počítačem komunikoval.

1. Historie počítačů, Unixu a internetu