Linux – Server

1 Slovo úvodem

V této MO se dá použít mnoho věcí (znalostí) z jiných MO (jak tomu obvykle bývá). Takže veškeré služby popíšu jen krátce, popř. se rozepíšu u SSH – jinde není, ale zase jsme jej neprobírali, tak jen trošku.

Linux je hojně využíván jako WWW servery, MAIL servery, Databázové servery, routery, …

2 Služby a aplikace

2.1 Databázové servery

Linux může sloužit jako databázový server. Například MySQL, Postgres, Oracle, Firebird, …

2.2 Web a poštovní servery

Mezi nejvýznamnější linuxové web-servery patří jistě Apache, mezi light servery kraluje LightHTTPd a dále nginx a Litespeed. Podle statistik netcraft.net má Apache 50% podíl, IIS od Microsoftu pouze 35%
více http://news.netcraft.com/archives/2008/04/14/april_2008_web_server_survey.html

U poštovních serverů se odstupuje od děravého a složitého sendmailu a nahrazuje se Postfixem (dnes asi nejrozšířenější), Qmailem popř. Eximem (z těch nejrozšířenějších). Tyto servery jsou nazývány MTA (Mail Transfer Agent) a vždy na linuxovém stroji musí být nějaký MTA nainstalován (třeba i jednoduchý ssmtp – pouze předávání pošty).

2.3 FTP

FTP služba užívaná pro přenos souborů (ukládání na server). Hojně užívaný deamon je pure-ftpd, proftpd, wsftpd.

2.4 SSH

Secure Shell. Služba pro vzdálené ovládání unixového stroje pomocí šifrovaného spojení. Nahrazuje dříve užívaný telnet. Užívá tcp:22. Pokrývá tři základní oblasti bezpečné komunikace: autentizaci obou účastníků komunikace, šifrování přenášených dat a integritu dat. Označení „Secure Shell“ je mírně zavádějící, protože nejde ve skutečnosti o shell ve smyslu interpret příkazů. Název byl odvozen z existujícího programu rsh, který má podobné funkce, ale není zabezpečený. SSH je většinou implementováno jako OpenSSH.

2.4.1 Užití

- Náhrada protokolu Telnet, práce na vzdáleném počítači přes nezabezpečenou síť
- Náhrada protokolu Rlogin, přihlášení na vzdálený počítač
- Náhrada protokolu Rsh, spouštění příkazů na vzdáleném počítači
- Tunelování spojení
- Přesměrování TCP portů a X11 spojení zabezpečeným kanálem
- Bezpečný přenos souborů pomocí SFTP nebo SCP

2.4.2 OpenSSH

OpenSSH je opensource implementace protokolu SSH. Původně vyvinuto jako součást OpenBSD.

Skládá se z:

- Ssh — Samotný klient. Nahrazení telnetu.
- Scp — Užívá se pro kopírování. Náhrada FTP
- Sshd — SSH deamon (server)
- Ssh-keygen — Vytváří RSA a DSA klíče, které se používají pro ověřování uživatele
- Ssh-agent a ssh-add — pomůcky k ulehčení ověřování držených klíčů. Klíč nevyžaduje heslo při každém jeho užití

- Ssh-keyscan skenuje seznam hostitelů a sbírá jejich veřejné klíče.

2.5 Souborové servery

Nativní linuxový NFS (Network File Systém) je užíván pro sdílení souborů napříč unixovými stroji. Vyžaduje podporu v jádře. Dříve fungoval na UTF, nyní i TCP.

SMB – Samba je primárně užívána pro sdílení mezi windows a linux stroji. Používá protokol SMB (z dílny MS). Dnes se používá i pro sdílení linux a linux. Může fungovat jako tiskový i autentifikační server – toto jest užíváno, pokud je Samba nasazována ve Windows sítích jako PDC (Primary Domain Controller).

2.6 DNS

V souboru /etc/host.conf je definováno, zda se má jako první prozkoumávat hosts soubor nebo se má užít DNS (volba bind). Soubor hosts.conf se nachází v /etc/hosts a má strukturu: IP hostname. Lokální revolver (stará se o překlad DNS) se konfiguruje pomocí /etc/resolv.conf. Nastavují se zde servery, kterým budou posílány dotazy.

Mezi nejpoužívanější servery patří Bind, TinyDNS, MyDNS.
http://mydns.bboy.net/survey/

MyDNS neumožňuje rekurzivní překlad. Tudíž lze jej užít pouze jako autoritativní server, nikoliv jako cache server, proto se na firemních serverech téměř nepoužívá.

2.7 DHCP

DHCP (Dynamic Host Configuration Protocol) server slouží k automatické konfiguraci počítačů ve vnitřní síti. Pomocí DHCP lze PC přidělit nějakou nepoužívanou IP adresu (z definovaného rozsahu), sdělit masku sítě, adresu implicitní brány, DNS serveru a mnoho dalších podrobností. Celá konfigurace DHCP serveru je uložena v souboru /etc/dhcp/dhcpd.conf. Tento soubor po instalaci dhcpd nemusí existovat (je to ochrana proti tomu, aby někdo nevědomky nespustil v LAN další DHCP server, což by mělo za následek zmatení síťových adres). Konfigurační soubor pro DHCP server může také obsahovat i pevně stanovené IP adresy pro vybrané počítače, které se navážou na MAC adresu síťového rozhraní.

3 Firewall - zabezpečení

Iptables je nástroj, který umožňuje linuxovému nebo unixovému systému plně pracovat se síťovou komunikací. Pomocí něj si můžeme snadno postavit různé druhy firewallů (stavový, transparentní…) nebo sdílet internet (NAT)

Pravidlo pro iptables má následující obecnou syntaxi:

```
iptables "oč se jedná" "umístění pravidla" "podmínka" "co provést"
```

Firewall je síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti nebo zabezpečení. Zjednodušeně se dá říct, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Tato pravidla historicky vždy zahrnovala identifikaci zdroje a cíle dat (zdrojovou a cílovou IP adresu) a zdrojový a cílový port, což je však pro dnešní firewally už poměrně nedostatečné – modernější firewally se opírají přinejmenším o informace o stavu spojení, znalost kontrolovaných protokolů a případně prvky IDS. Firewally se během svého vývoje řadily zhruba do následujících kategorií:

3.1.1 Paketové filtry

Nejjednodušší a nejstarší forma firewallování, která spočívá v tom, že pravidla přesně uvádějí, **z jaké adresy a portu na jakou adresu a port** může být doručen procházející paket, tj. kontrola se provádí na třetí a čtvrté vrstvě modelu síťové komunikace OSI.

Výhodou tohoto řešení je **vysoká rychlost zpracování**, proto se ještě i dnes používají na místech, kde není potřebná přesnost nebo důkladnější analýza procházejících dat, ale spíš jde o vysokorychlostní přenosy velkých množství dat. Nevýhodou je **nízká úroveň kontroly** procházejících spojení

3.2 Aplikační brány

Jen o málo později, než jednoduché paketové filtry, byly postaveny firewally, které na rozdíl od paketových filtrů zcela oddělily sítě, mezi které byly postaveny. Říká se jim většinou Aplikační brány, někdy také Proxy firewally. Veškerá komunikace přes aplikační bránu probíhá formou dvou spojení – klient (iniciátor spojení) se připojí na aplikační bránu (proxy), ta příchozí spojení zpracuje a **na základě požadavku klienta otevře nové spojení** k serveru, kde klientem je aplikační brána. Data, která aplikační brána dostane od serveru, pak zase v původním spojení předá klientovi. Kontrola se provádí na sedmé (aplikační) vrstvě síťového modelu OSI (proto se těmto firewallům říká aplikační brány).

3.3 Stavové paketové filtry

Stavové paketové filtry provádějí kontrolu stejně jako jednoduché paketové filtry, navíc si však ukládají informace o povolených spojeních, které pak mohou využít při rozhodování, zda procházející pakety patří do již povoleného spojení a mohou být propuštěny, nebo zda musí znovu projít rozhodovacím procesem. To má dvě výhody – jednak se tak urychluje zpracování paketů již povolených spojení, jednak lze v pravidlech pro firewall uvádět jen směr navázání spojení a firewall bude samostatně schopen povolit i odpovědní pakety a u známých protokolů i další spojení, která daný protokol používá. Například pro FTP tedy stačí nastavit pravidlo, ve kterém povolíte klientu připojení na server pomocí FTP a protože se jedná o známý protokol, firewall sám povolí navázání řídícího spojení z klienta na port 21 serveru, odpovědi z portu 21 serveru na klientem použitý zdrojový port a po příkazu, který vyžaduje přenos dat, povolí navázání datového spojení z portu 20 serveru na klienta na port, který si klient se serverem dohodli v rámci řídícího spojení a pochopitelně i odpovědní pakety z klienta zpět na port 20 serveru. Zásadním vylepšením je i možnost vytváření tzv. virtuálního stavu spojení pro nestavové protokoly, jako např. UDP a ICMP.

3.4 Stavové paketové filtry s kontrolou známých protokolů a popř. kombinované s IDS

Moderní stavové paketové filtry kromě informací o stavu spojení a schopnosti dynamicky otevírat porty pro různá řídící a datová spojení složitějších známých protokolů implementují něco, co se v marketingové terminologii různých společností nazývá nejčastěji Deep Inspection nebo Application Intelligence. Znamená to, že firewally jsou schopny kontrolovat procházející spojení až na úroveň korektnosti procházejících dat známých protokolů i aplikací. Mohou tak například zakázat průchod http spojení, v němž objeví indikátory, že se nejedná o požadavek na WWW server, ale tunelování jiného protokolu, což často využívají klienti P2P sítí (ICQ, gnutella, napster, apod.), nebo když data v hlavičce e-mailu nesplňují požadavky RFC apod.

Intrusion Detection System (zkráceně IDS, v češtině se obvykle používá termín "Systémy pro odhalení průniku") je obranný systém, který detekuje nepřátelské aktivity na síti (a nejenom tam!). Klíčové je na IDS hlavně to, že by tyto činnosti měl být schopen nejenom odhalit, ale pokud možno proti nim aktivně zasáhnout a zabránit tak všemu, co by mohlo kompromitovat bezpečnost operačního systému. Jedná se tedy nejenom o finální pokusy o hacknutí/průnik do systému, ale i odhalení akcí, které tomu předcházejí, jako je například shromažďování potřebných informací a dat pro útok, typicky třeba port scaning. IDS by na základě své schopnosti zachytit neobvyklou aktivitu měl být schopen vygenerovat varování (alert), který upozorní administrátora na tuto činnost a případně zabrání jejímu dalšímu pokračování.
Případná definice by mohla znít asi takto:
Intrusion detection je proces identifikace a reakce na podezřelé aktivity, které se odehrávají na počítačových a síťových prostředcích.

4 Směrování

Pojmem směrování (routing, routování) je označováno hledání cest v počítačových sítích. Jeho úkolem je **dopravit datový paket určenému adresátovi**, pokud možno co nejefektivnější cestou. Síťová infrastruktura mezi odesílatelem a adresátem paketu může být velmi složitá. Směrování se proto zpravidla nezabývá celou cestou paketu, ale řeší vždy jen jeden krok – **komu data předat jako dalšímu**. Ten pak rozhoduje, co s paketem udělat dál. Každý počítač v síti Internet (přesněji každé jeho rozhraní, např. ethernetová karta) má přidělenu IP adresu. Adresa je 32bitové číslo, které se obvykle zapisuje jako čtveřice čísel.
Např. 192.168.10.8

4.1 Směrování (IP Adresa)

Lokální síti vždy odpovídá **rozsah IP adres, který je dán adresou sítě a maskou**. Maska je čtyřbajtové číslo (v bitech určující adresu sítě má samé jedničky a v ostatních bitech samé nuly) a slouží k získání adresy sítě, ve které je stanice o dané IP adrese - určuje, které bity v IP adrese tvoří adresu sítě. Maska má stejný tvar jako síťová adresa, ale

podmínkou je, že horních několik bitů jsou jedničky a zbytek nuly. Do rozsahu patří ty IP adresy, jejichž logický AND s maskou dá adresu sítě. Síť se pak zapisuje ve tvaru adresa / maska.

Například síť:
213.168.177.64 / 255.255.255.192
obsahuje adresy 213.168.177.64 až 213.168.177.127.

Krajní dvě adresy mají speciální význam:

- 213.168.177.64 se používá jako označení sítě
- 213.168.177.127 pro adresování paketů určených všem uzlům v síti (broadcast).

Protože maska je určena počtem nenulových bitů, zapisuje se síť často zkráceně ve tvaru 213.168.177.64/26

4.2 Potřebné programy

- *Ifconfig* - nastavení parametrů síťové karty
- *iwconfig* - nastavení wifi
- *route* - nastavení routingu
- *IP* - nastavení parametrů síťového spojení (nahrazuje ipconfig a route)
- *Pin* - diagnostika spojení
- *traceroute* – zjištění, kde na cestě mezi uzly dochází k problémům

5 Obsah