Bezpečnost UN*Xových OS

David Košťál

4. listopadu 1998

Úvod

Proč vlastně zabezpečujeme a chráníme počítače a počítačové sítě? Důvodů je mnoho. Počínaje „účtováním“ za procesorový čas, diskový prostor nebo paměť a konče ochranou osobnich či firemních dat a ochranou každého uživatele systému. Síť i počítače se musí chránit i pro zachování funkčnosti, protože někdy i krátký výpadek může způsobit velké škody nebo ztráty.

Bezpečnost počítačového systému se skládá z mnoha prvků. Některé z nich si probereme v následujících kapitolách.

Bezpečnostní politika

Pod pojmem bezpečnostní politika rozumíme souhrn pravidel a opatření, které určují chování lidí (respektive zaměstnanců, správců, návštěvníků,...) k počítačům a/nebo k počítačové síti. Jsou to hlavně:

- Úloha jednotlivých osob, jejich rozčlenění do skupin.
- Práva jednotlivých skupin vůči manipulaci s HW.
    - Kdo má nebo nemá právo otevírat počítače,
    - připojovat periferie,
    - používat modemy pro vzdálený přístup,
    - nebo zapojovat počítače do poč. sítě.
- Práva jednotlivých skupin k užívání, instalaci a údržbě SW.
    - Kdo je odpovědný za instalaci patchů,
    - metodika zálohování systému a
    - výběr nainstalovaných programů.
- Které stroje mají nárok na UPS.
- Jaké budou smlouvy s dodavateli HW a SW o supportu v případě poruchy.
- Odkud budou které stroje dostupné.
- A spousta jiných bodů.

Bezpečnostní politika bývá velice podceňována a přitom právě na ní záleží, jestli budou ostatní bezpečnostní opatření účinná. K čemu je v síti oddělovací firewall, když každý připojený počítač má modem a jde se k němu možno dostat zvenčí?

Samostatný počítač

O zabezpečení (provozu) počítače je potřeba uvažovat už při jeho instalaci. Je potřeba rozdělit disky podle toho, co od stroje očekáváme. Důvody proč mít na různé části souborového systému zvláštní svazky jsou např. ty, že UN*Xy umožňují mít mnohá omezení pouze po jednotlivých svazcích. Pro nás může mít význam např.:

- Svazek `/` je systémový a je dobé nemíchat ho s ostatními.
- `/var` je potřeba mít rw, a zároveň jeho velikostí určujeme maximální velikost logů a to, že místo pro logy nám např. nezaberou uživatelé svými home adresáři.
- `/usr` bývá oddělován spíše z historických důvodů, případně pro zvýšení výkonu systému.
- `/home` bývá montován s quotami a omezujeme mu celkové místo.
- `/tmp` je dobré mít bez quot, a montovan nos[ug]id, nodev, nofollowsymlinks atd.

Dále je třeba pavidelně kontrolovat přístupová práva na filesystému, kontrolní součty (třeba MD5) souborů a množství volného místa na jednotlivých svazcích.

Pro zjištění nefunkčnosti nebo napadení počítače je dobré logovat co nejvíce událostí a logy pravidelně kontrolovat. Je dobré logovat i na zařízení nebo počítač, které bude případnému útočníkovi nepřístupné. To může být třeba jiný počítač na síti nebo po séiové lince nebo tiskárna. Zde je ale potřeba kompromis, protože podrobné logy mohou zahltit disk, kde jsou uloženy a pak se nemusí zaznamenat události, které by jsme potřebovali. Zahlcení logů může být i jeden z možných útoků (nebo příprav na útok) na systém.

Pro zotavní z HW či SW chyb a případně i napadení je pořeba systém zálohovat. Zálohovací místo (disk, páska, ZIP), frekvence (2x týdně, 1x za hodinu, jednou měsíčně) i způsob (úplný, inkrementální) zálohování záleží na typu a aktuálnosti dat.

Jaké jsou možné útoky na systém, kde v něm bývá njčastěji chyba?

- s[ug]id pogramy – přetečení/podtečení bufferů, práce se soubory v `/tmp`, přístupová práva (pracovních) souborů.

Je potřeba když už ne přímo kontrola zdrojových textů, tak alespoň včasné a pravidelné upgrady těchto programů. Na ochranu před přetečením nebo podtečením bufferů mohou pomoci i setuid-wrappery. Je dobré mít co nejméně setuid programů a speciální práva uživatelů dělat pomocí skupin nebo přes program *sudo*.

- Programy spouštěné root-em.

Mohou se zde vyskytnout chyby typu špatná práva pomocných souborů, špatná práce s dočasnými soubory,...

- Přístupová práva na filesystému.

K čemu je nám jinak dokonalé zabezpečení, když každý může změnit binárku jádra? :-)

- Účty bez hesel a nepoužívání `/etc/shadow`.

Když nepoužíváme `/etc/shadow`, může si každý zjistit všechna zakódovaná hesla a spustit si (třeba i na Vašem poočítači) jejich hádání, resp. dekódování.

- Špatná hesla. Zde pomůže např. program *Crack*.

Je vhodné pravidelně kontrolovat (nejen) uživatelská hesla. Je dobré mít kontrolu hesel přímo při jejich změně.

- DoS útoky: zalcení místa na disku, místa pro logy, počtu procesů. Zde částečně pomohou quoty, správné partišnování disků, pravidelná kontrola logů (z části třeba i automatická), omezení velikosti a počtu procesů.
- Bezpečné bootování systému. Je potřeba zajistit, aby nikdo nemohl nabootovat jádro se speciálními parametry, nebo zamezit bootování do single-user módu.

Počítačová síť

Dostupnost počítače zvenčí s sebou přináší i další způsoby, jak kompromitovat náš počítač. Na serveru (a nebo i stanici) nám běží spousta démonů, kteří zajišťují chod sítě. Od superdémona `inetd`, přes poštovní servery, sdílení disků až po služby zajišťující vzdálené přihlášení. (Nejen) skrze ně lze získat neoprávněná přístupová práva nebo způsobit tzv. nedostupnost nebo odepření služby – to znamená docílit toho, aby počítač přestal vykonávat svěřené úkoly.

Opět zde platí pravidlo, že mají běžet jen ty služby které jsou opravdu potřeba, případně zajistit, aby některé služby bylo dostupné jen z lokální sítě.

Jaké jsou možné útoky, kde bývá nejčastěji chyba?

- Špatná konfigurace programů. Dovolíme např. ftp démonovi aby zapisoval na celý disk nebo umožní zaplnit disky zbytečnými hlášeními (viz. odstavec o rozdělování disků).
- Chyby v programech.
  - Neošetřená nebo nesprávně ošetřená práce s parametry.
  - Klasické přetečení bufferů.
- Chyby v jádře, které umožní některé DoS útoky na TCP/IP stack. Např. útoky *nestea, teardrop,...*
- Zbytečně mnoho služeb, které mohou v sobě potenciálné mít díry (viz. body výše) a které nejsou potřeba.

V jakých konkrétních programech můžeme chyby očekávat? Ve všech :-) No dobře, např. v těchto:

- **sendmail** – je velice rozsáhlý a komplexní program, takže chyba se do něj zavleče velice rychle. Určitě je i ve vaší (předpokládám, že nejnovější) verzi. Nápravou může být rychlý upgrade v případě že se objeví chyba nebo použít alternativní poštovní servery: **qmail, zmailer**.

- **NFS** a po (nejen) siti montované disky. Je dobré si uvědomit, co exportujeme a na které stroje. Jsou dost důvěryhodné? Totéž při montování cizích svazků (ať již přes NFS nebo třeba ZIP mechaniku). Je vhodné nepovolit při montování set[ug]id, speciálních zařízení či dokonce ani spouštění programů. Ostatně existují mnohem bezpečnější varianty sdílení souborů. Namátkou jmenujme **AFS, Coda,** které navíc umožní spolupracovat s autentizačním mechanismem jako je **Kerberos**.
- **NIS, NIS+** – dvě služby pro sdílení uživatelských jmen a hesel mezi spoustou strojů. Mají (zvláště NIS) několik bezpečnostních nedostatků. Určitě existují bezpečnější varianty: **Kerberos, SESAME**.
- **Imapd, Pop3d** – služby pro vzdálenou práci s poštou. Hmm, jestli si budete moct vybrat jen jednu z těchto služeb, vyberte pop3. Rozhodně je ale dobré omezit přístup na tyto služby jen z vybraných stanic nebo sítí.
- Vzdálené přihlášení, případně vzdálené iXy. Omezte telnet-ové přihlašování z jině než lokální sítě. Stejně jako v případě iXů jdou hesla po síti nešifrovaně, takže je možný jejich odposlech. Určitě se pomocí telnet-u nepřihlašujte jako root. Pro vzdálený přístup použijte třeba **ssh, SSL-telnet** nebo jiné šifrované kanály.
- A každý další program dostupný přes síť.

Opět zde platí pravidlo logujte, logujte, logujte. Spusťte si `identd`, aby bylo možné dohledávat kdo z Vašich uživatelů co způsobil. Logy ze všech počítaču je možno směrovat na jeden centrální, a zde uchovávat. A nejen to, je potřeba je i kontrolovat! Základem může být třeba automatická kontrola, která Vás bude o všech „špatných“ věcech ihned informovat mailem nebo přes SMS, ale v každém případě je potřeba logy procházet ručně. Je taky dobré si na logy vyhradit nějaký větší svazek, aby se tam všechno vešlo a nedocházelo ke ztrátám logů.

Firewall?

Ano, je dobrý, ale nespraví všechno. Stále je potřeba dodržovat předchozí pravidla (a nejen ty) a navíc je potřeba starat se o zabezpečení firewallu a o správnost jeho filtrovacích pravidel. Navíc je nutné zvolit vhodnou topologii sítě, aby byl Váš firewall vůbec co platný. Ne vždy je firewall nutné řešení, v mnoha případech může podobnou úlohu plnit **tcpd**, případně doplněný filtrovacími pravidly týkajícími se jen tohoto jednoho stroje.

Tcpd je nástroj pro omezení přístupu k lokálním portům (ve smyslu jak je definuje TCP/IP) jen z vybraných adres počítačů nebo sítí. Typické použití je v souboru `/etc/inetd.conf`:

```
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
```

Tcpd si konfiguraci bere ze souborů `/etc/hosts.allow` a `/etc/hosts.deny`:

```
/etc/hosts.allow:
```

```
ALL:.fi.muni.cz
```

`/etc/hosts.deny:`

`ALL:ALL`

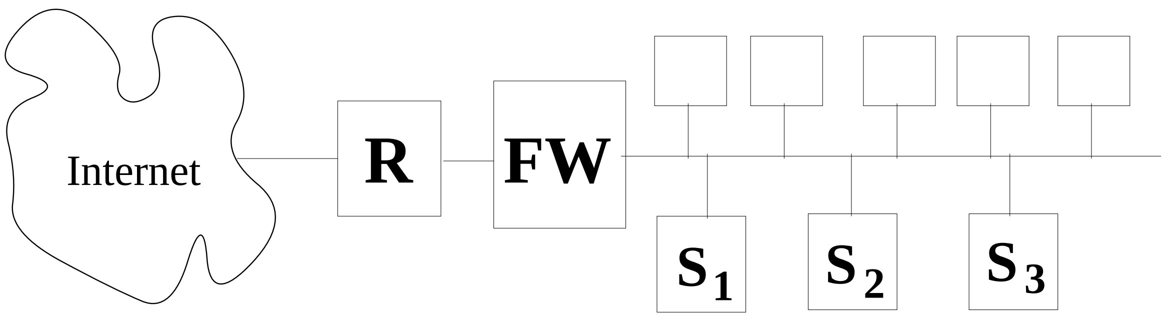
je jednoduchý příklad, který povolí přístup ke všem službám jen z domény `.fi.muni.cz`.

Tcpd navíc existuje jako knihovna, kterou lze přilinkovat k programům nespouštěným z inetd.

K dalšímu omezování pro přístup k počítači nebo jako firewall můžeme použít v Linuxu buď **ipfwad** nebo **ipchains**. Zvláště ipchains je velice mocný nástroj, který nám umožňí víc, než leckterý komerční firewall na bázi paketového filtru. Pokud chceme aplikační firewall, je možné použít třeba **TIS firewall toolkit**.

Nyní si ukážeme tři nejtypičtější topologie pro zapojení firewallu.

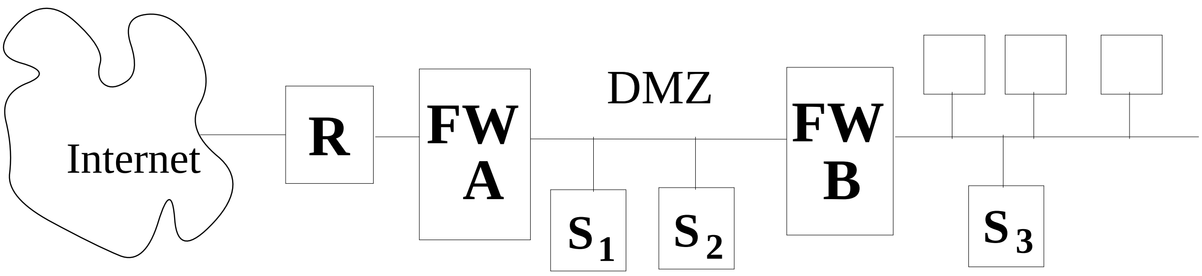
První je topologie, kdy firewall odděluje celou síť bez rozdílu, ať již se jedná o pracovní stanice nebo o servery.



Obr. .1: Síť oddělená jedním firewallem a bez DMZ

Nevýhodou této topologie je, že pokud se někomu podaří prolomit na server S1, dostane automaticky přístup k celé vnitřní síti.

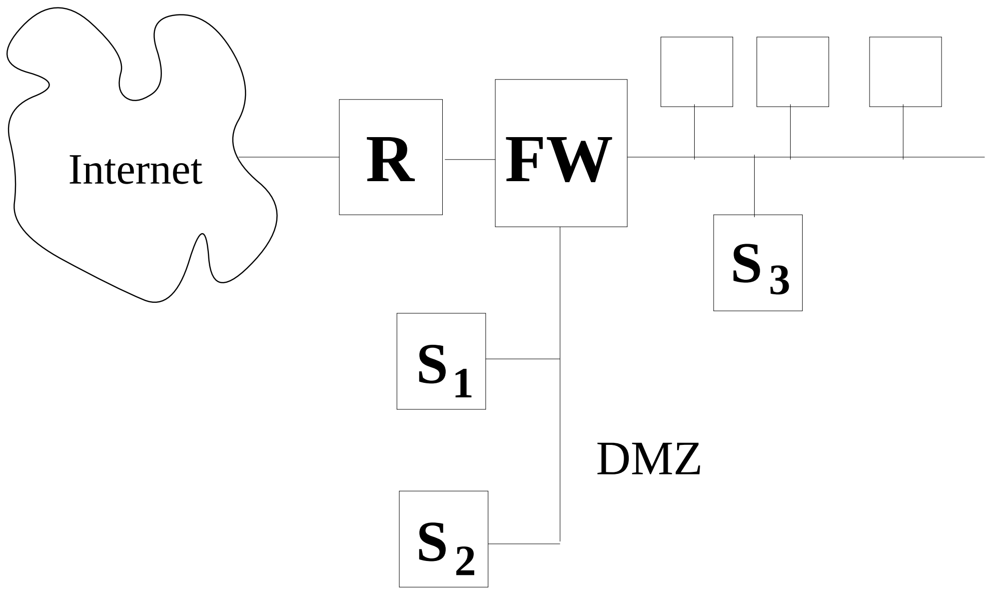
Druhá topologie již tuto nectnost odstraňuje.



Obr. .2: Síť se dvěma firewally a DMZ

Jedná se ale o mnohem nákladnější řešení, protože jsou potřeba firewally dva.

Třetí topologie také odděluje servery od lokálních pracovních stanic, ale pokud dojde k prolomení na firewall, je opět celá vnitřní síť napadnutelná.



Obr. .3: Síť s jedním fw a DMZ

Druhá a třetí toppologie je také vhodná pro použití např. s modemovým serverem. Nechceme dát každému po telefonní lince přístup do lokální sítě, ale také nechceme, aby byl modemový server lehce napadnutelný.

Ke všem těmto topologiím je potřeba určit bezpečnostní politiku a podle ní vypracovat vhodná filtrovací pravidla na firewally. Bezpečnostní politika je (opět opakuji) velice důležitá, protože všechna bezpečnostní opatření jsou k nepotřebě, když si někdo připojí modem ke své stanici a nepřítel zjistí ono telefoní číslo.

Nepomohlo to, jsme napadeni!

Ne vždycky je nejhůř :-) Pokud zjistíte, že se někdo snaží dostat na Váš server (nebo se tam již dostal a Vy máte server opět v provozu) je možné na útočníka polícit past. Mohl by to být jednoduchý prográmek nebo skript, který necháte (třeba přes inetd) poslouchat na portu místo služby, přes kterou se k Vám útočník prolomil. Tento prográmek bude simulovat základní komunikaci s útočníkem (reagovat na příkazy EHLO nebo VRFY) a všechno pečlivě zaznamenávat do logů. Pokud zjistíte odkud se útočník snaží prolomit a jaký program nebo způsob k tomu používá a informujte správce onoho stroje a případně i CERT a naši linuxovou komunitu.

V případě že se útočníkovi podařilo na Váš počítač prolomit, je dobré co nejrychleji odpojit počítač od sítě (počítačové, ne elektrické :-), nabootovat z diskety do single-user módu (ale nemontovat disk jako /, je potřeba použít něco nedotčeného, třeba disketu) a pokusit se zjistit, kudy k prolomení došlo. Pokud je server potřeba rozjet co nejrychleji, tak buď vyměnit disky nebo tyto staré disky někam nakopírovat a podrobit zkoumání později. Poté disk přeformátovat (případně přepártišnovat) a obnovit systém ze zálohy resp. znovu nainstalovat a obnovit konfigurační soubory a data ze zálohy. Vypnout všechny služby co nejsou potřeba (jak to, že jste je nevypli už dříve?), upgradovat všechny balíky, políčit pasti a stroj opět zapojit do sítě.

Pro hledání kde si útočník nechal zadní vrátka je dobré mít znalosti několika základních hackerských balíků, jako je třeba **rootkit**.

Závěr

Co dodat? Nebezpečí číhá všude a proto je dobré na bezpečnost opravdu dbát. Udržujte si zálohy, studujte logy a upgradujte balíky. A pozor! Nebezpečí hrozí nejen od záškodníků na Síti, ale i od Vašich uživatelů!