Generátor zabezpečovacího skriptu

Filip Hašek

Záměr

- Vytvořit skript pro síťové zabezpečení
- Jednoduchá obsluha
- „Neprůstřelný firewall“
- Optimalizace síťové části kernelu
- Samospustitelný (tedy démon)

Mechanismy

- Iptables
- Konfigurace jádra přes sysctl
  → alternativně přes zápis do /proc
- Bash
  → Skript generující skript pro zavádění
- Linux démoni
- Agregace záznamů pro iptables do funkcí a množin
- Typická nastavení pro PC/Server/Router

Co se podařilo

- Převést mnoho služeb na související pravidla pro iptables
- Každé přiřadit do množiny
- Rozdělit je dle rolí
- Zobecnit je pro většinu užití
- Přidávat uživatelské služby (dle portu)
- Vytvořit skript s kompletními iptables pomocí jednoho příkazu s argumenty

Co se nepodařilo

- Vytvořit pravidla pro nesíťovou část linuxu

Jak dál?

- Vytvořit autokonfigurační mechanismus postavený na PHP a databázi ze kterého by se stroje samy nastavovaly.
- Umožnit alespoň částečnou zpětnou vazbu.

Konec

- Díky za váš čas