

# Firewall pre pracovnú stanicu s OS Linux

Jaroslava Kokavcová

Školiteľ: RNDr. Jaroslav Janáček, PhD

# iptables

- Firewall v Linuxe
- Reťaze
- Tabuľky
  - Filter
  - IP adresa, port, protokol...
  - Chýba PID

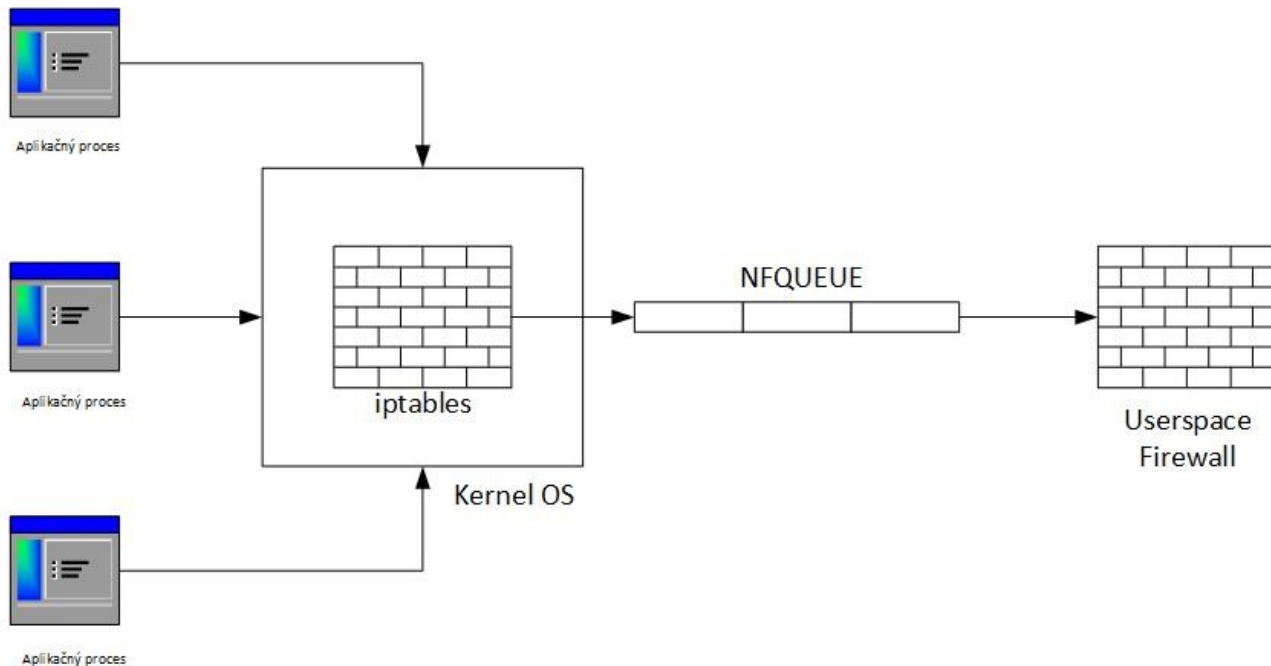
# Ciele práce

- analýza požiadaviek na kontrolu komunikácie aplikácií
- preskúmanie súčasného stavu problematiky
- analýza možností riešenia
- návrh a implementácia riešenia
- porovnanie riešenia s existujúcim stavom a demonštrovať jeho prínos pre bezpečnosť

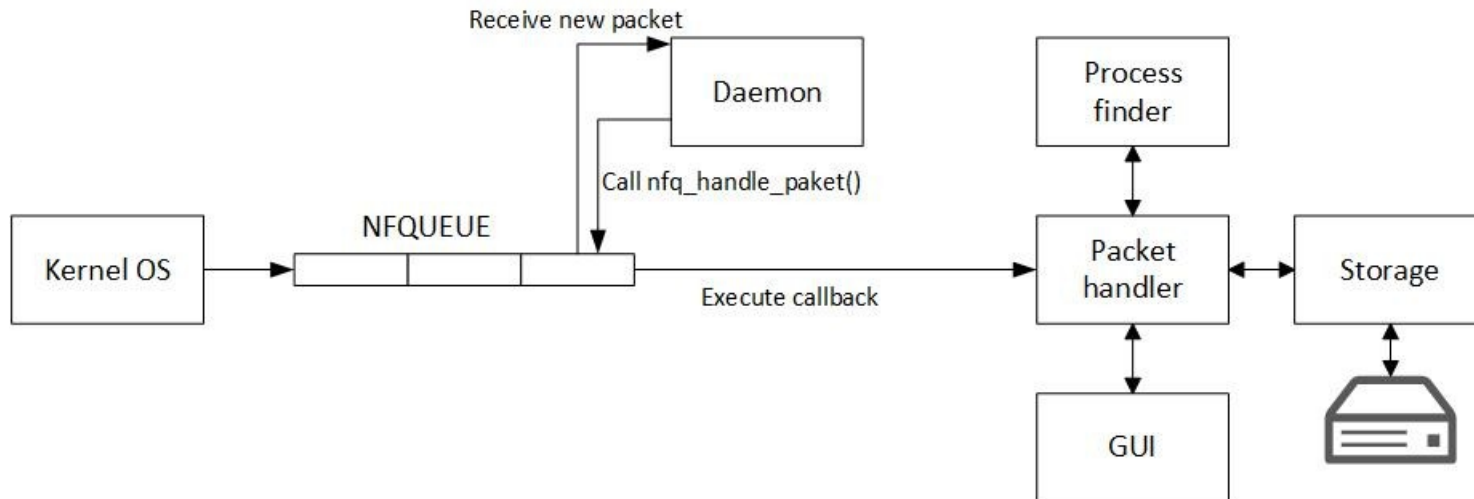
# Požiadavky

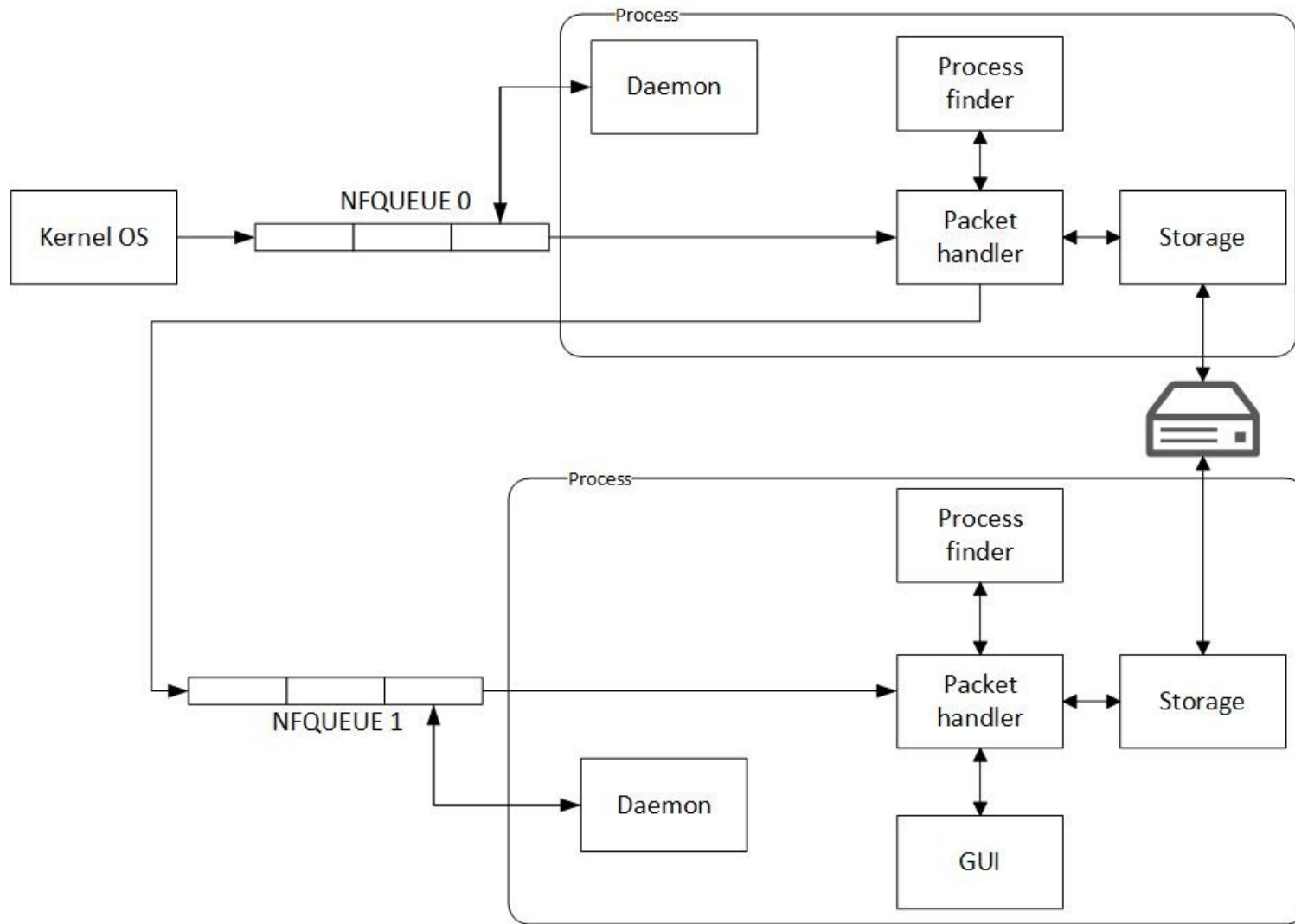
- Sledovanie paketov
  - IP adresa, port, protokol
  - Aplikácia
- Filtrovanie
- Ovládanie pomocou grafických prvkov
- Minimálne práva

# High-level architektúra



# Architektúra firewallu





# Hľadanie procesu

- Chýba informácia o PID
- IP hlavička
- /proc/net/tcp    /proc/net/udp
- /proc/<PID>/fd/\*



# Pravidlá

```
UNKNOWN 127.0.0.1 35059 tcp ACCEPT
UNKNOWN 127.0.0.1 53470 tcp ACCEPT
/opt/google/chrome/chrome 198.252.206.25 443 tcp ACCEPT
/opt/google/chrome/chrome 35.190.41.116 443 tcp ACCEPT
/opt/google/chrome/chrome * * * ACCEPT
UNKNOWN 192.168.1.254 4353 igmp ACCEPT
UNKNOWN 224.0.0.251 0 igmp ACCEPT
UNKNOWN 192.168.1.101 37892 igmp ACCEPT
/lib/systemd/systemd-resolved 192.168.1.254 53 udp ACCEPT
/lib/systemd/systemd-resolved 127.0.0.1 32781 udp ACCEPT
UNKNOWN 127.0.0.53 64405 icmp ACCEPT
/lib/systemd/systemd-resolved 127.0.0.1 43311 udp ACCEPT
/usr/sbin/NetworkManager 34.122.121.32 80 tcp ACCEPT
UNKNOWN 127.0.0.53 64484 icmp ACCEPT
UNKNOWN 127.0.0.1 771 icmp ACCEPT
UNKNOWN 127.0.0.53 64439 icmp ACCEPT
```

# Práva

- Princíp najmenších práv
- Používateľ firewall
- Privilegované práva
  - Pripojenie k NFQUEUE
  - Prechádzanie priečinkom /proc
  - Rozhodnutie

# Synchronizácia procesov

- Čítanie / zápis do súboru
  - Zamykanie
- Spoločné ukončenie procesov

# Služba

```
[Unit]
Description=Firewall service
After=network.target
StartLimitIntervalSec=0

[Install]
WantedBy=graphical.target

[Service]
Type=simple
Restart=always
RestartSec=1
User=root
Environment=DISPLAY=:0
Environment=XAUTHORITY=/home/jarka/.Xauthority
Environment=USER=jarka
ExecStart=/home/jarka/firewall/firewall
WorkingDirectory=/home/jarka/firewall
```

# Administrátorské centrum

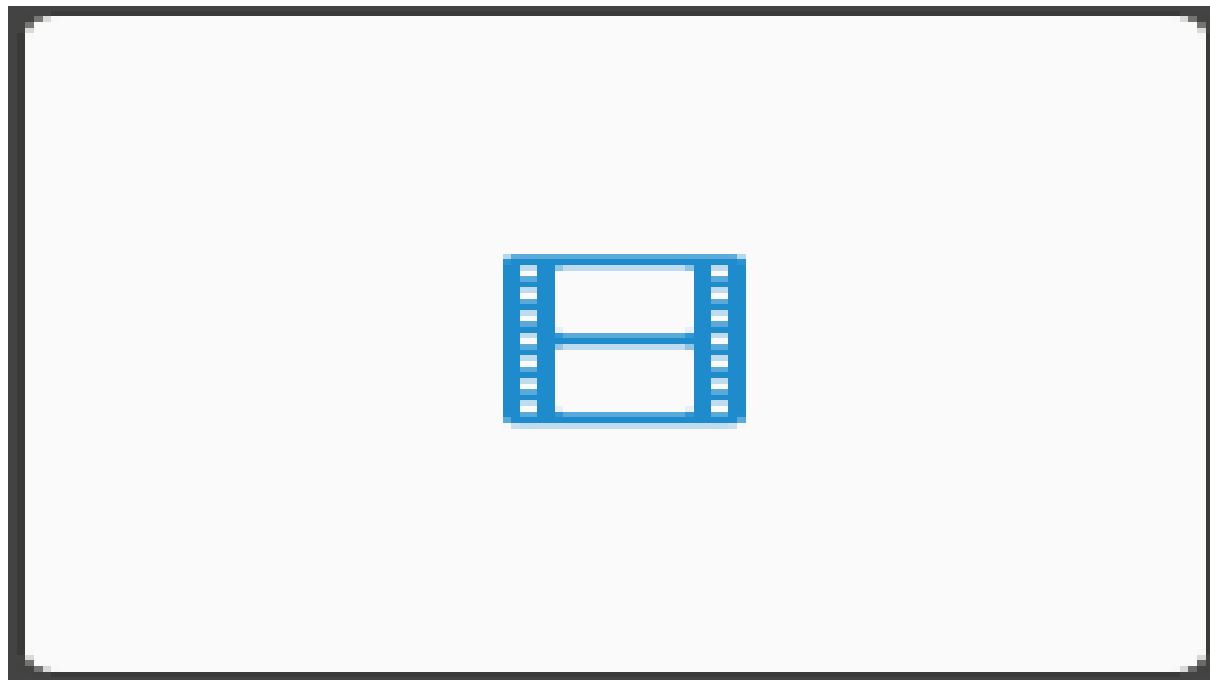
Firewall Admin Center

Select	Path	IP Address	Port	Protocol	Action
<input type="radio"/>	texstudio	127.0.0.1	8081	tcp	ACCEPT
<input type="radio"/>	/lib/systemd/systemd-re	192.168.1.254	53	udp	ACCEPT
<input type="radio"/>	/usr/sbin/NetworkManag	127.0.0.53	53	udp	ACCEPT
<input type="radio"/>	/lib/systemd/systemd-re	127.0.0.1	58604	udp	ACCEPT
<input type="radio"/>	/lib/systemd/systemd-re	127.0.0.1	49984	udp	ACCEPT
<input type="radio"/>	/usr/lib/snapd/snapd	127.0.0.53	53	udp	ACCEPT
<input type="radio"/>	/usr/sbin/NetworkManag	35.232.111.17	80	tcp	ACCEPT
<input type="radio"/>	/lib/systemd/systemd-re	127.0.0.1	46126	udp	ACCEPT
<input type="radio"/>	/lib/systemd/systemd-re	127.0.0.1	50168	udp	ACCEPT
<input type="radio"/>	/lib/systemd/systemd-re	127.0.0.1	44731	udp	ACCEPT
<input type="radio"/>	/opt/google/chrome/chro	127.0.0.53	53	udp	ACCEPT
<input type="radio"/>	/opt/google/chrome/chro	192.168.1.101	5353	udp	ACCEPT

Add Delete Move up Move down Reload

Save

# Ukážka



# Testovanie

- Google Chrome
- Mozilla Firefox
- Signal
- Thunderbird
- systemd-resolved,
- Texstudio
- NetworkManager
- Systemd-timesyncd
- Clion
- Xbrlapi
- Node
- Snapd
- http a https methods pre APT
- Git-remote-https
- MintUpdate
- Lsof
- Gvfsd-smb-browse
- cupsbrowsed

# Latencia

- Najhorší prípad
- 700 pravidiel
- 500 pravidiel



# OpenSnitch



# Zhrnutie

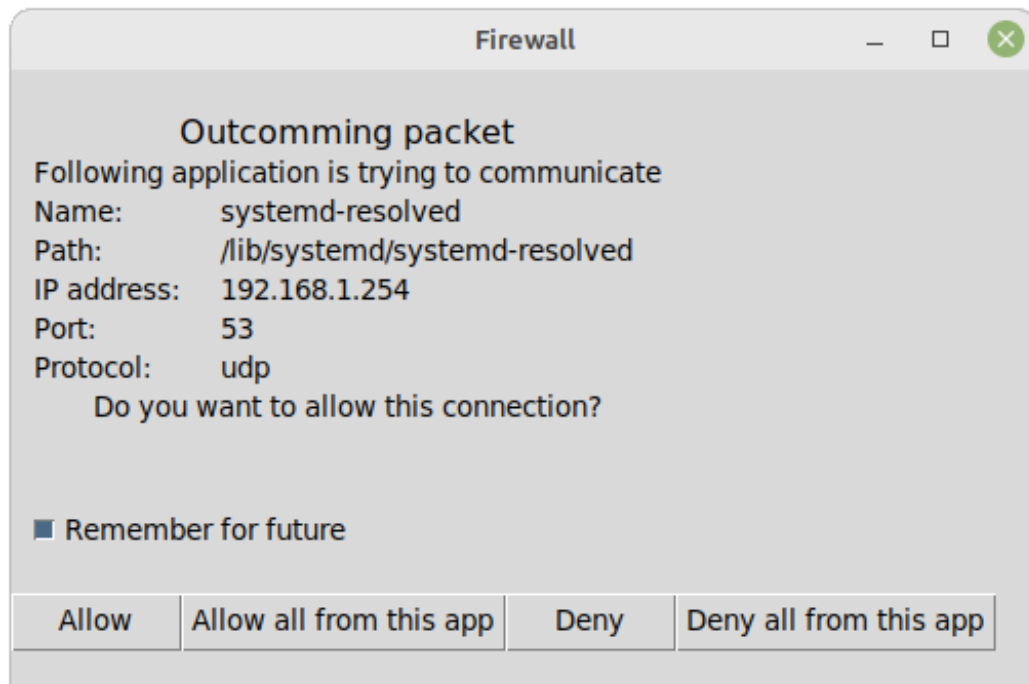
- Firewall pre Linux
- Návrh
- Implementácia
- Testovanie

Ďakujem za pozornosť

# Otázky od školiteľa

- Samostatný proces pre GUI
- Isov 127.0.0.53 53 udp
- Pravidlá v pamäti
  - Binárne stromy, heš. tabuľky

# Otázky od oponenta



# Otázky od oponenta

- Správna konfigurácia firewallu
- iptables vs nftables