# Essence

Kadlecsik József
KFKI RMKI

# Tartalom

- Motiváció
- Konfigurációs file szintaxisa
- Scriptek és argumentumaik
- Működés

# Motiváció

- Miért kell még egy iptables script?
  - példa script-ek sokasága
  - karakteres, grafikus, webes konfiguráló programok
- Mert
  - virágozzék minden virág
  - érdekes feladat
  - fun!

# Motiváció folyt.

- Szabály-generátor
- Egyszerű szintaxis
- IPv4 és IPv6 támogatás
- Leggyakoribb és nem a szofisztikált, egyedi eseteket fedje le
- Használja az ip[6]tables/netfilter “legújabb” képességeit
- Természetes belső logika

# Szintaxis

- Kulcsszó, érték párok:

```
# comment
keyword = value0, value1 value2 ,
    value3 # comment
```

- Kulcsszavak csoportokba rendezettek, kontextustól függően használhatóak
- Azonosító értékű toplevel kulcsszavak:
  - general, zone, template, filter, nat, mangle, raw

# Protokoll I.

- Legszélesebb értelemben használjuk
  - azonosító a protocol-numbers.txt file-ból:
    - tcp, udp, icmp, icmpv6, ospf, stb.
  - azonosító a port-numbers.txt file-ból:
    - ftp, ssh, http, https, stb.
  - azonosító az icmp-names.txt file-ból
    - ping, destination-unreachable, host-unknown, stb.
  - azonosító az icmpv6-names.txt file-ból
    - ping, destination-unreachable, no-route, stb.

# Protokoll II.

- tcp:8888, udp:9898
- tcp:1024..65535, udp:33434..33523
- icmp:1, icmpv6:1
- icmp:1/2, icmpv6:1/2
- any, all

# general

- Általános beállítások

```
tcpudp = domain
udp = ntp, talk
module = nf_conntrack
    modparam = hashsize=65536
module = nf_conntrack_ftp
    modparam = ports=21,1121
```

# general

- Naplózó modul beállításai: LOG

```
logmodule = log
    level = warning
    tcp-sequence = no
    tcp-options = no
    ip-options = no
```

# general

- Naplózó modul beállításai: ULOG

```
logmodule = ulog
    nlgroup = 1          # default
    cprange = 68         # default: 0
    qthreshold = 8       # default: 1
```

# general

- Naplózó osztályok beállítása: accepted, denied, spoofed, banned

```
logclass = denied
    limit = 10/second
    burst = 12
    prefix = DENIED
    reject = ident
```

# general

- Naplózás bekapcsolása (yes, no, accepted, denied), általános kivételek

```
logging = yes

service = ping

    logging = denied

client = ping

    logging = no
```

# zone

- Hálózati topológia: ki mely interfész(ek) “mögött” van?

```
zone = external
    interface = eth0, eth1
    network = 10.10.10.0/24
zone = internal
    interface = eth2
    network = 10.10.0.0/16,
              2001:DB8:85::/60
```

# nat

- NAT szabályok: SNAT, DNAT, MASQUERADE, REDIRECT, ACCEPT, SAME, NETMAP

```
nat = typical
    target = snat
    options = 1.2.3.4
    out = eth0, eth1
    # in, srcip, dstip, proto
```

# mangle

- mangle szabályok: ECN, IPV4OPTSSTRIP, TCPMSS, TOS, TTL

```
mangle = typical
    target = tcpmss
    # options = 1460
    chain = forward
    out = eth0, eth1
    # in, srcip, dstip, proto
```

# raw

- raw szabályok: NOTRACK, TARPIT, DROP

```
raw = banned
    target = drop
    ip = 192.168.0.0/16
    logging = no
    # in, out, srcip, dstip, proto
```

# filter

- Szűrési szabályok: tűzfalra magára

```
filter = localhost
    service = ping
    service = ssh
        access = 10.10.10.0/24,
                 !10.10.10.1,
                 2001:DB8:85::1
    client = any
```

# filter

- Szűrési szabályok

```
filter = http servers
    ip = 10.10.10.1, 2001:DB8:85::2
    service = http, https

filter = clients
    ip = 10.10.0.0/16, 2001:DB8:85::/60
    client = any
```

# essence script

```
essence [-v] [-d] \
    -4 <file> -6 <file> -m <file> \
    -- config file ...
```

# fw script

```
fw create
fw start
fw stop
fw restart
fw reconfig
```

# Működés

- naplózó szabályok
- zone beállításokból IP cím hamisítás elleni szabályok a raw táblában
- banned lánc a raw táblában
- raw, mangle, nat táblák: egyszerű *most specific first* sorrendezés

# Működés, filter tábla

- naplózó szabályok definiálása
- protokollok alapján láncok
  - láncokban most specific first sorrendezés
- localhost implicit engedélyezési szabályokkal:
  - IPv4/IPv6 loopback traffic
  - IPv6 ND

# Letöltési cím

- http://www.kfki.hu/cnc/projekt/securefilter