Building a dynamic firewall with iptables

Andreas Herz
andi@geekosphere.org

Linogate GmbH

29.06.2016

LINOGATE
INTERNET TECHNOLOGIES

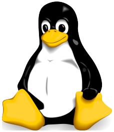
Concept

Extend the stateful firewall with dynamic blocking of bad IPs

- block malicious traffic and add penalty
- several sensors detect suspicious behavior
- Whitelist and Blacklists
- different blocking duration

Procedure

- Sensor detects something -> srcip added to badset with timeout X or increased timeout by Y
- Good behavior -> srcip added to goodset with same logic
- Afterwards comparison between badset and goodset
- Threshold of bad behavior reached -> srcip blocked for Z minutes
- For longtime observation srcip added to xt_recent set as well
- Increased timeouts in blacklistset based on longtime behavior



Sensors

- Portscan/sweep
- DOS
- traceroute
- pingfake
- restricted rules

ipset

Modifications made for ipset 6.16

- TARGET: –increase
- MATCH: –compare-set –threshold

Examples:

```
iptables -A FOO -j SET –add-set badset src –exist –timeout
300 –increase
```

```
iptables -A BAR -j CHECKING -m set –compare-set badset src
goodset src –threshold 1000
```

portscan/portsweep

- using xtables_addons psd with patches from Florian
- added portsweep detection and syslog output
- adding mixed mode in the future

traceroute and pingfake

- detect traceroute with basic iptables
- reply icmp requests instead of forwarding them

prospects

- switch to nftables
- get as much as possible into upstream
- improve IPv6 coverage
- conjunction with IDS/IPS Suricata
- longtime analytics

Suggestions

Any suggestions?