How to automate iptables rules

Erran Carey

~~@ipwnstuff~~

@errancarey

Agenda

- iptables
- ipset
- NAT
- Custom DNS nameserver ✨
- Takeaways

iptables(8)

administration tool for IPv4 packet filtering and NAT

iptables

- NAT
  - Masquerade
- Filter
  - Forward
  - Log
  - Drop

ipset(8)

administration tool for IP sets

ipset

- Save multiple rule sets
- Enable TTL iptables extension

NAT

- Network address translation
- Public IP to private IP translation

Custom DNS nameserver ✨

- A configuration format to whitelist domains/IPs

- A cron task to update IP sets

Takeaways

- LOG anything you DROP.
- ~20-300 dropped packets for 2-3 million packets.