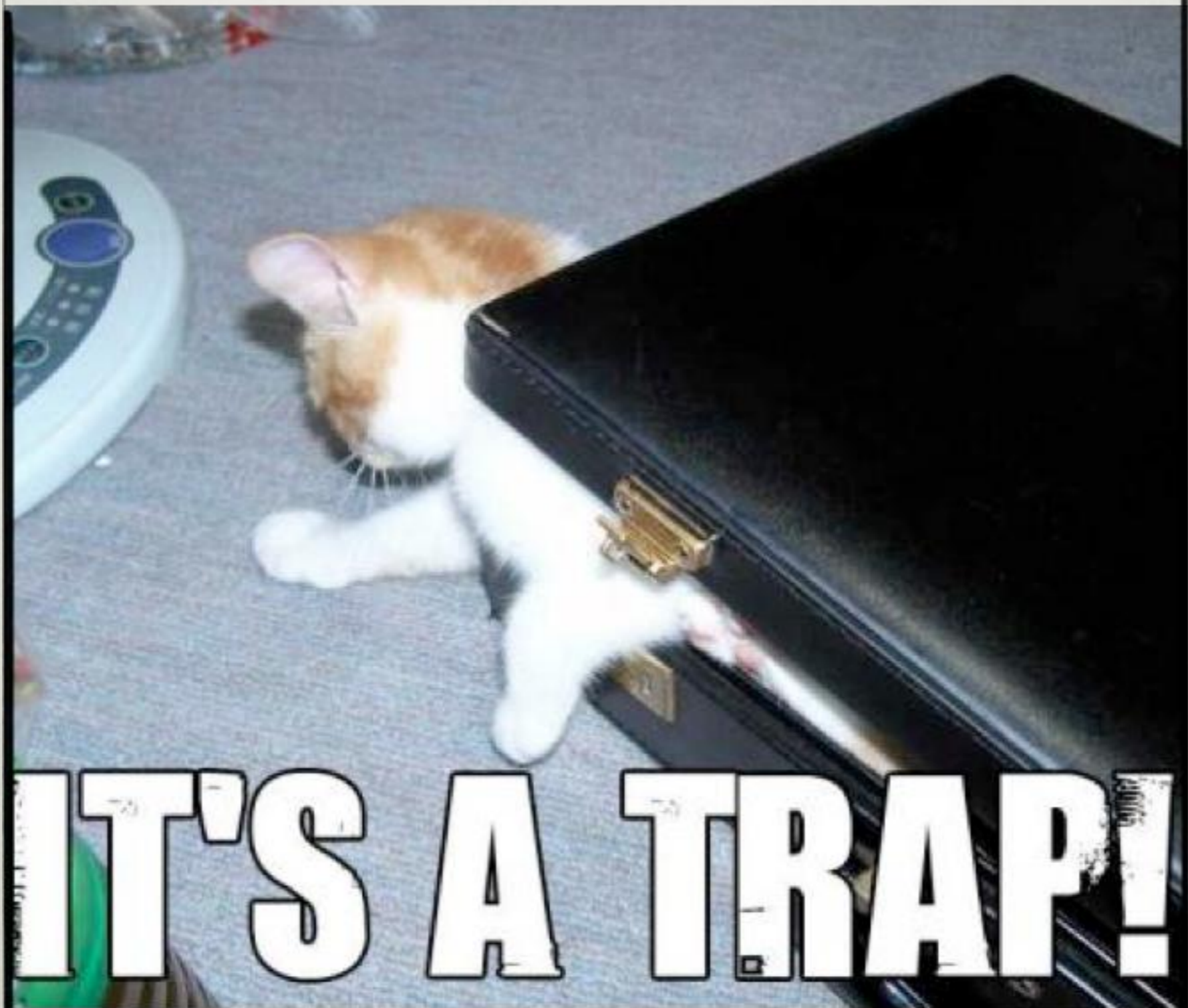


# Medus Įsilaužėliams (honeypots)

@lfx

liudas.sodonis.eu



# WTF?

---

- Tai spąstai.
- Tai resursas - kurio tikslas yra būti užpultam, įlaužtam, kompromituotam.

# Koceptas

---

- Viskas labai paprasta.
- Sistema netur jokios produkcinė naudos.
- Bet koks aktyvumas honeypote reiškia kad, kažkas kas neturėtų ten būti ten yra.
- Tai įrankiai, kurie leidžia pažinti priešą.

# Tipai

---

- Produkcijos
- Tyrimo

# Tipai

---

- Serveriai:
  - Mažo interaktyvumo
    - Servisai  
(sshd,ftpd,smptd,httpd,etcd.)
  - Didelio interaktyvumo (pilna OS)

# Tipai

---

- Klientai
  - Mažo interaktyvumo (browsers)
  - Didelio interaktyvumo (&OS)

Servisai

# Mažo interaktyvumo

---

- Imituoja viena servisą (sshd,ftpd,smtp).
- Mažiau galimybių.
- Lengva pastebėti netikrą sistemą.
- Ne visos komandos.
- Lengva paleisti ir prižiūrėti.

# Kippo

---

- Py.
- Lengvas.
- Greitas.
- Logai.

---

**Demo**

# Didelio interaktyvumo

---

- Pilnavertė OS. Papildomi alertai, loginimas, firewall'ai ir pan.
- Sudėtinga prižiūrėti ir paruošti.
- Daug kartu vertingesnis.
- Mažai arba jokių limitų.

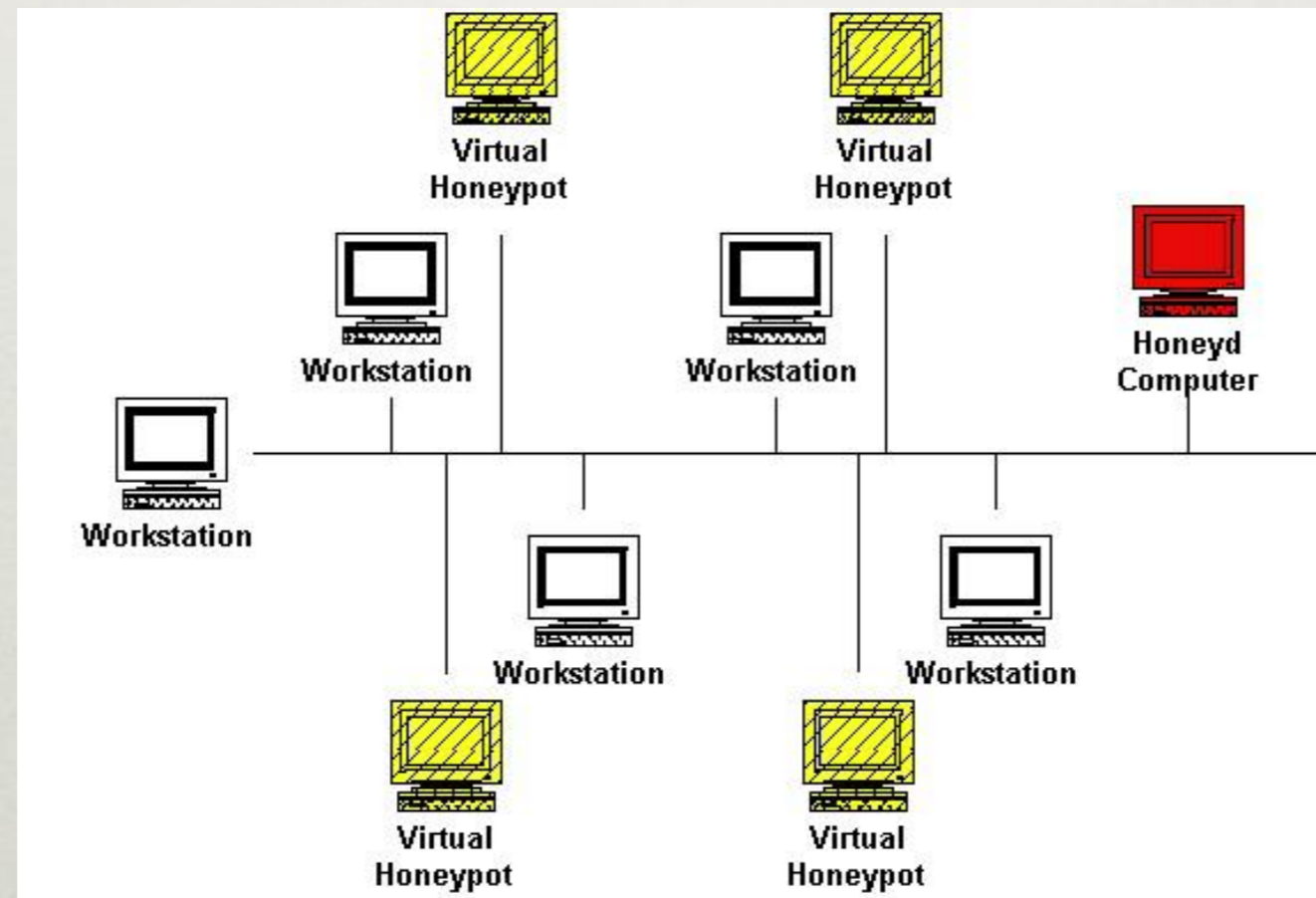
# Honeyd

---

- Emuluoja OS ir servigus.
- Produkcinis.
- Stebi nenaudojamus IP. Kai užtinka kreipimasį į juos atsako pats.
- Gali vienu metu emuliuoti bet kiek tikrų mašinų.

# Honeyd

---



# Honeyd Logas

- Feb 12 23:06:33 Connection to closed port: udp (210.35.128.1:1978 - 172.16.85.101:1978)
- Feb 12 23:23:40 Connection request: tcp (66.136.92.78:3269 - 172.16.85.102:25)
- Feb 12 23:23:40 Connection established: tcp (66.136.92.78:3269 - 172.16.85.102:25) <-> sh scripts/smtp.sh
- Feb 12 23:24:14 Connection dropped with reset: tcp (66.136.92.78:3269 - 172.16.85.102:25)
- Feb 12 23:34:53 Killing attempted connection: tcp (216.237.78.227:3297 - 172.16.85.102:80)
- Feb 12 23:39:14 Connection: udp (10.5.5.71:1026 - 172.16.85.101:137)
- Feb 12 23:39:14 Connection established: udp (10.5.5.71:1026 - 172.16.85.101:137)
  
- Wed Feb 12 23:23:40 UTC 2003: SMTP started from Port
- EHLO relay.verizon.net
- MAIL From:

Klientai

# Dalys

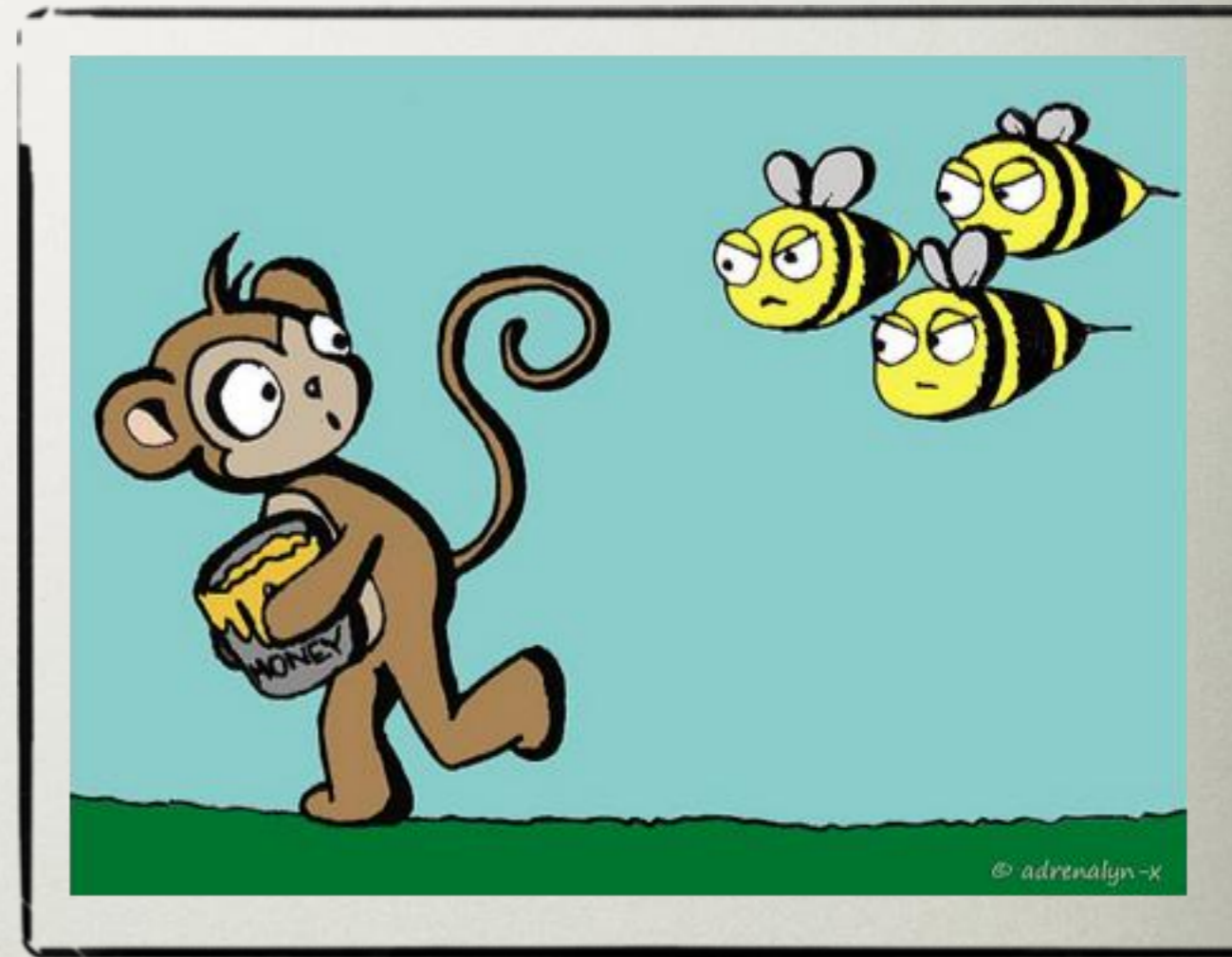
---

- Sąrašas.
- Klientas.
- Analizatorius.

# HoneyMonkey

---

- Sukurtas MS.
- Skirtas testuoti IE ir pačia OS.
- Aplanko potencialiai blogą saitą.  
Analizatorius tikrina pakitimus IE ir OS.  
Ir t.t.



# Capture-HPC

---

- Panašiai veikia kaip ir HoneyMokey, bet turi daugiau galimybiu.
- Tokių kaip paleisti ne tik IE.
- Frameworkas

# SpyBye

---

- Veikia kaip proxy.
- Skanuoja linkus su ClamAV.
- Pasako linka geras, pavojingas ar nežinomas.

Kiti

# Tarpit

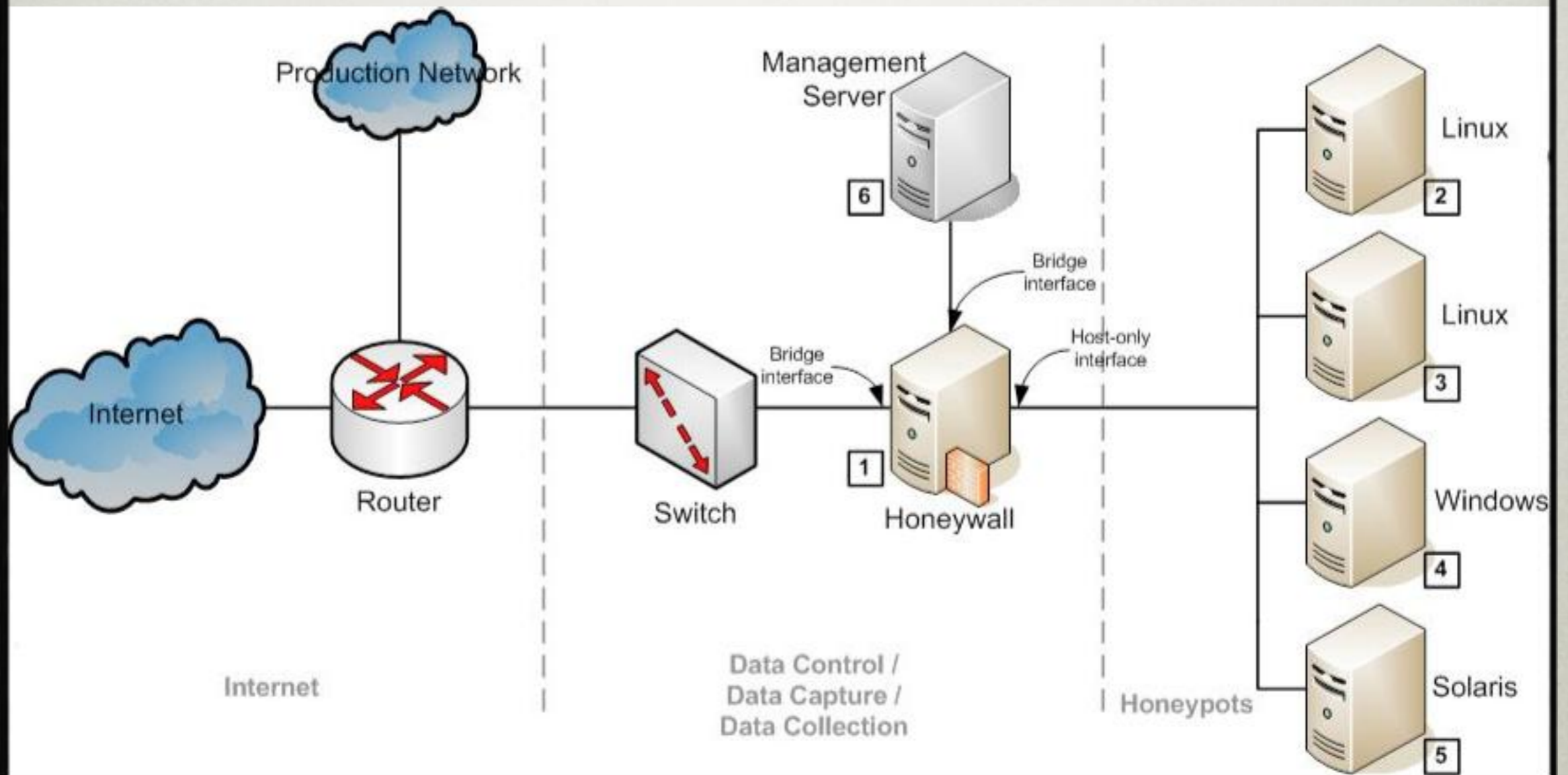
---

- arba dar sticky honeypots.
- Skirti lėtinti arba visai sustabdyti įsialužėlį arba kirminą.
- SMPT
- LaBrea

# HoneyNets

---

- Ištisi tinklai prijungtų honeypot'ų.
- Visas tinklas skirtas tam, kad būtų įsilaužta.



# Privalumai

---

- Leidžia surinkti mažus gabalus, bet labai vertingos informacijos.
- Naudoja mažai resursų.
- Padeda prigauti ir/ar sustabdyti įsilaužėlius.

# Trūkumai

---

- Rizika prikausomai nuo tipo.
- Gali būti mažai pažinties info, priklusomas nuo tipo.
- Kartais logų peržiūrėjimas užtrunka labai labai ilgai.
- Fingerprinting

End