# Honeypots

Felix Klement
Korbinian Spielvogel

# Agenda

1. What is a honeypot?
2. Usage of a Honeypot
3. Classification & Types of Honeypots
4. **Demo**
5. Researches
6. Advantages & Disadvantages
7. Conclusion
8. References

Got questions?

Ask at https://www.sli.do
with the event code: `HONEY`

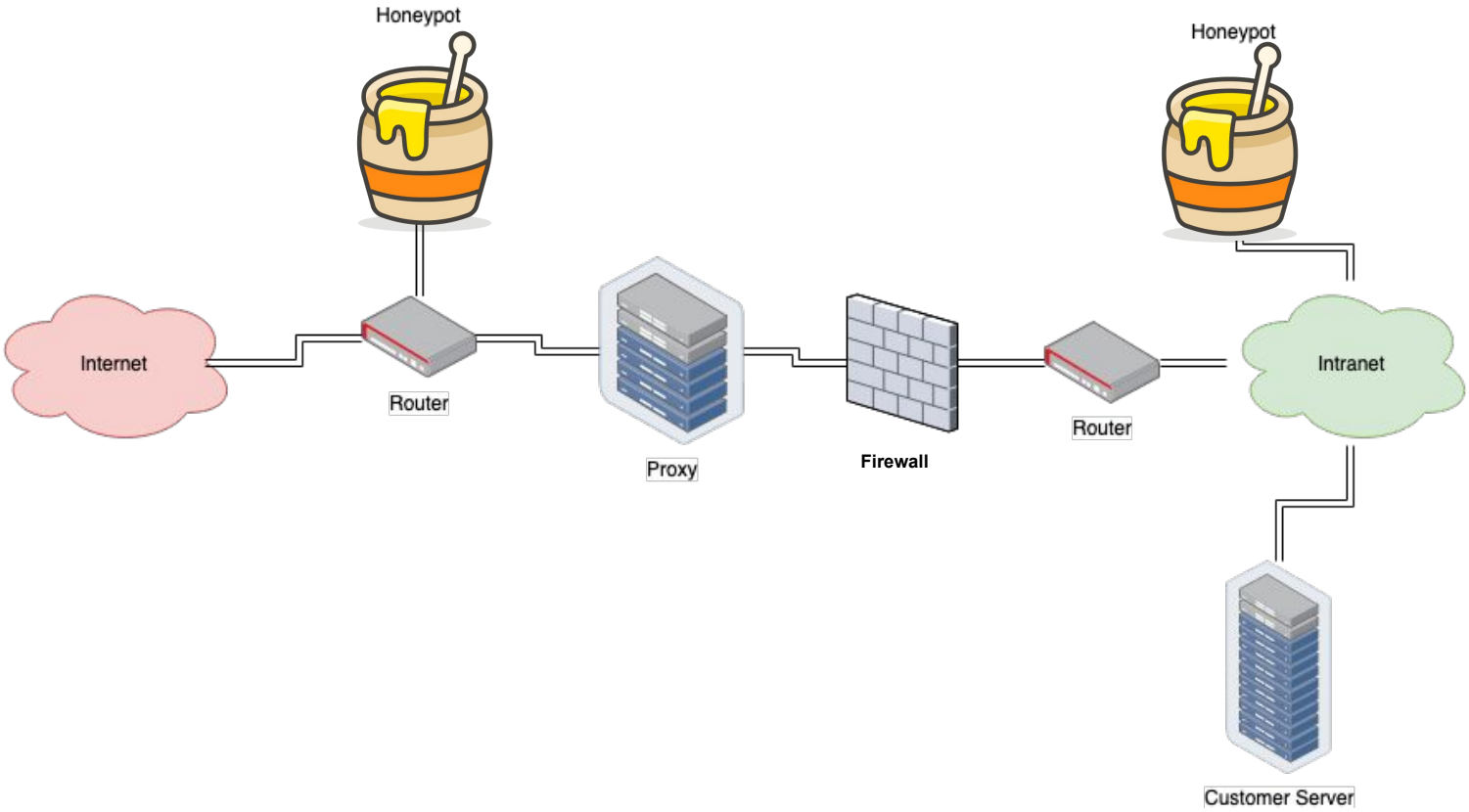
# What is a honeypot?

- System designed to lure attackers
  - Contains data that appears to be legitimate
  - Offers several exploitable vulnerabilities
  - Fakes activity / processes
- Highly monitored (analyze attacks / notify defenders)
- No valid user interacts with it

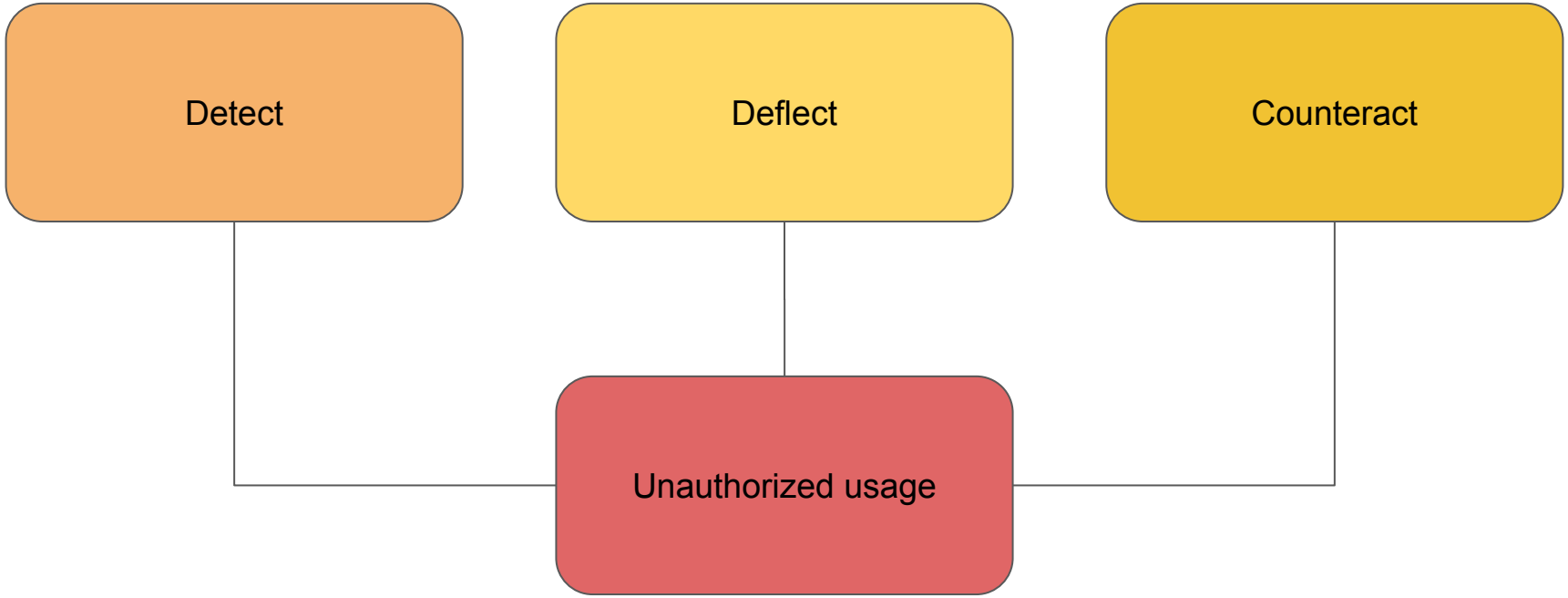
# What is a honeypot?


Source: [4]

# Example network



# General usage of a Honeypot?



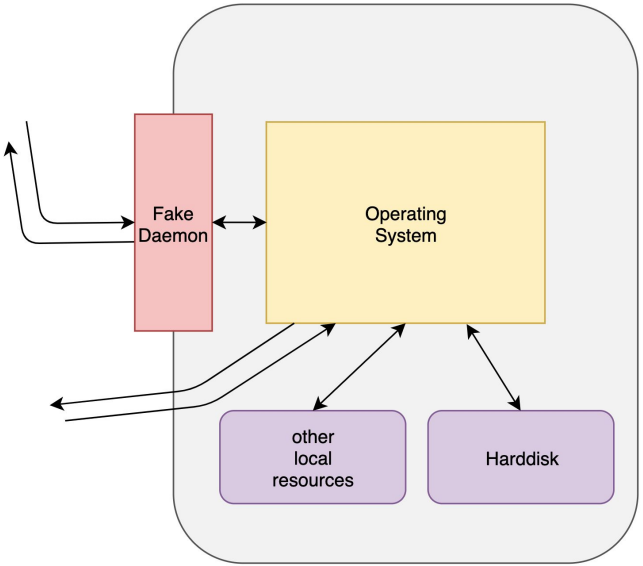
# Classification

Based on level of interaction

Based on the purpose

# Classification - Based on the level of interaction

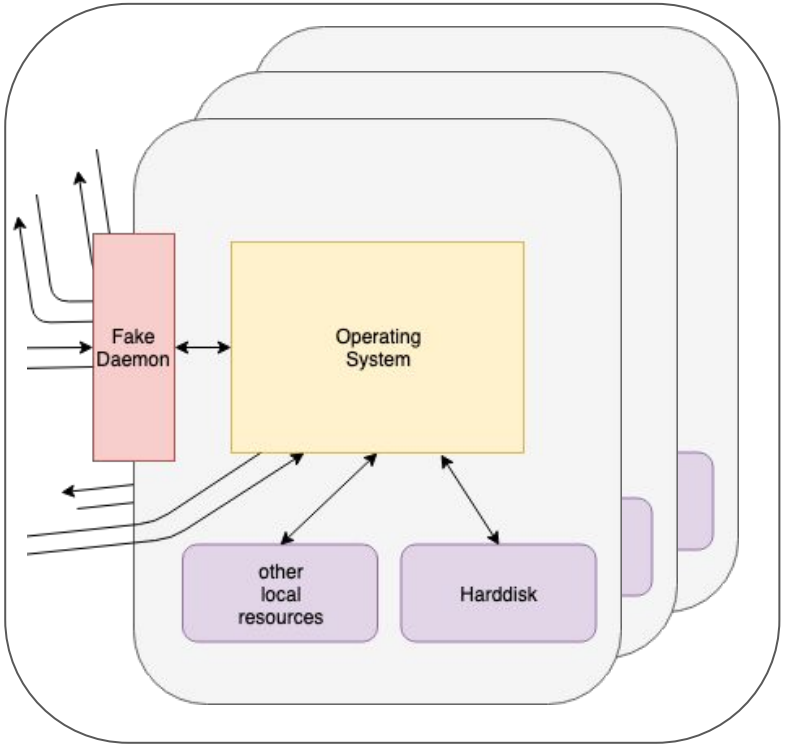
## Pure honeypot:




- Full-fledged production system
- Vulnerable activities are monitored through a bug tap
- Possible risk that attacker could turn tables
- Labor-intensive to configure and manage

# Classification - Based on the level of interaction

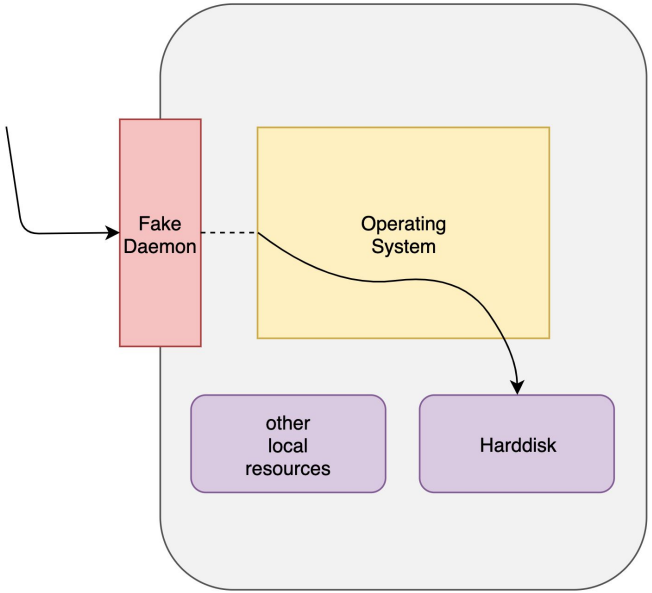
High-interaction honeypot:




- Bare metal machine with multiple VMs
- Real services, application and OS's
- Captures extensive information but has a high risk and a time intensive maintenance
- Complete isolation through use of VM

# Classification - Based on the level of interaction

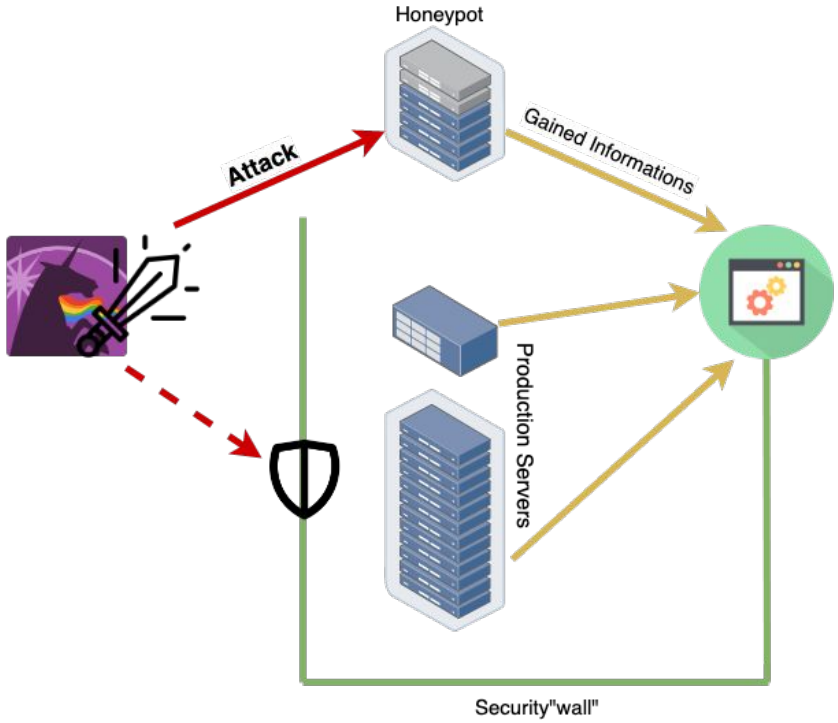
## Low-interaction honeypot:




- Emulates certain services and application
- Greater risk of being discovered by attackers
- Low risk and easy to deploy/maintain
- Preliminary stage to a medium-interaction honeypot

# Classification - Based on the purpose

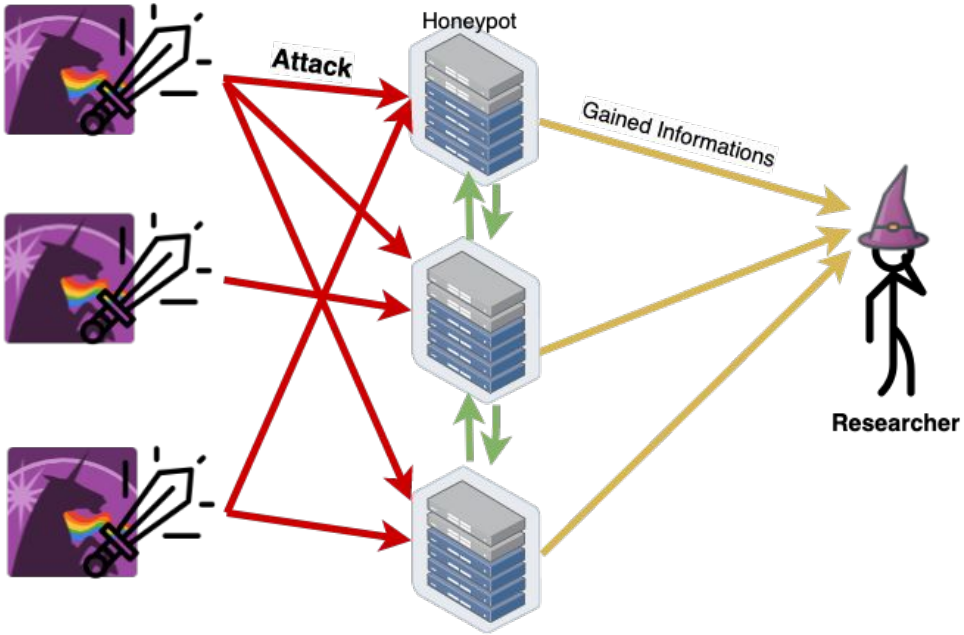
Production honeypot:




- Are deployed inside production systems
- Honeypots play the role of a decoy
- Should attract and occupy hackers to tie up their time and resources

# Classification - Based on the purpose

Research honeypot:




- Perform a more in detail analysis
- Track data across different participants in an attack
- Mostly very complex and hard to understand for non professionals

# DEMO


Source: [5]

Cowrie to analyse attacking patterns

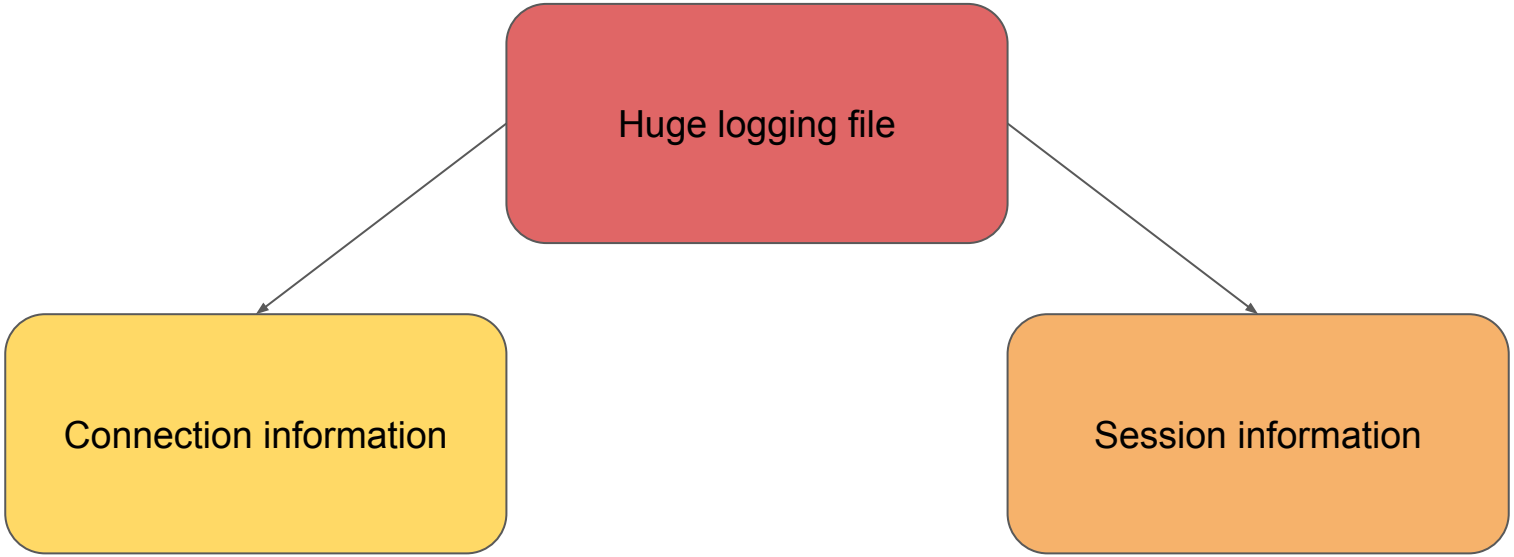
# Demo Setup

SSID: DONAUghty

- `ssh <username>@192.168.0.101 -p 2222`
- try to guess username & password

  (**hint**: *it's pretty common* + *less is sometimes more*)
- once connected, gather information about the server

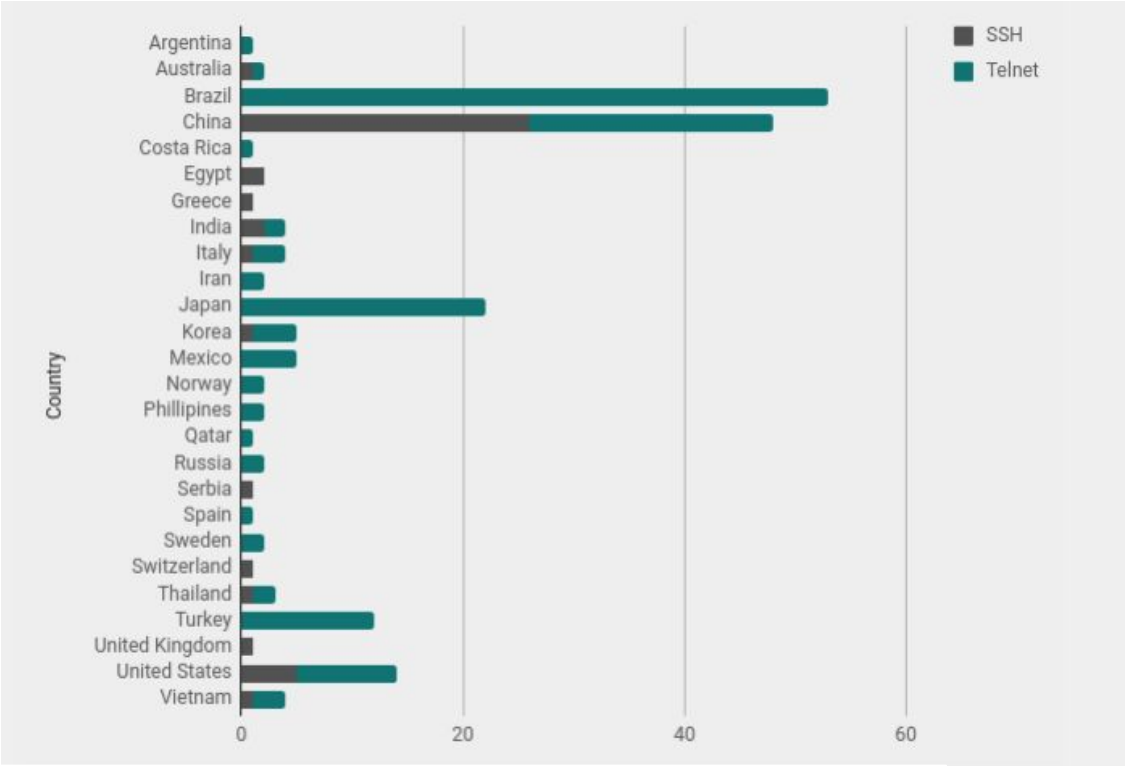
# What did we gain?



# Pew Pew Map

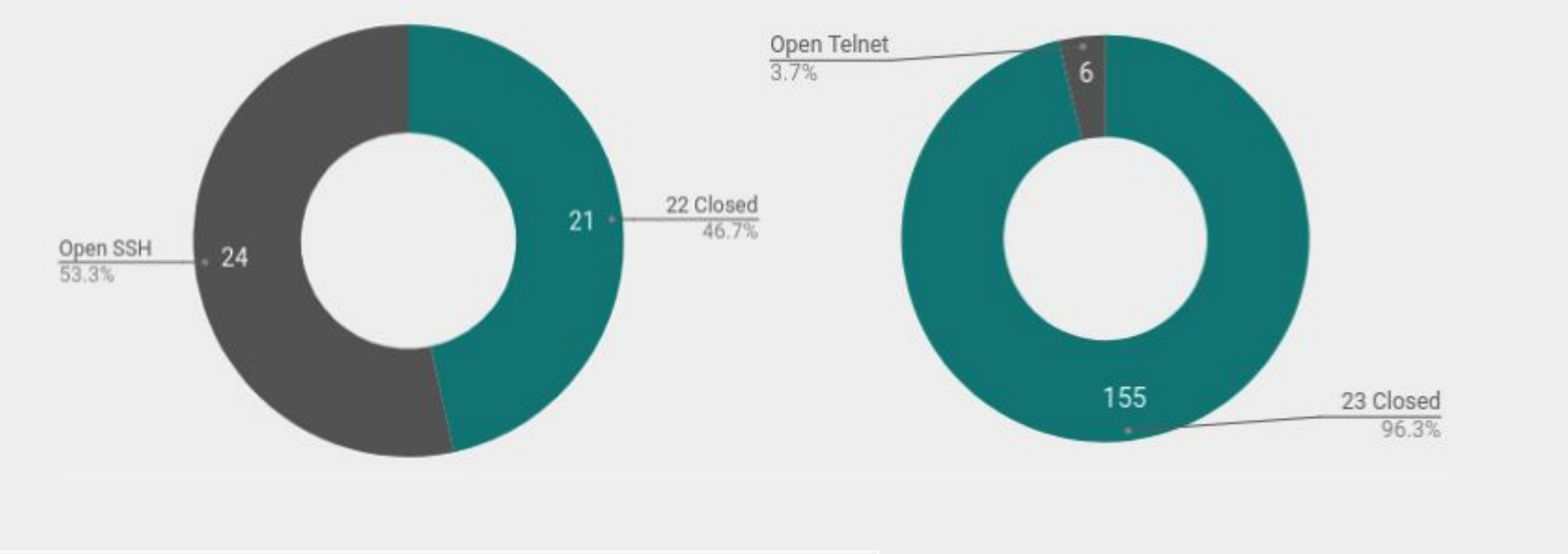

Source: [1]

# Geographic distribution (using maxmind)




Source: [1]

# Bot or not?




Source: [1]

# Disadvantages

**Data irregularity**

No attacks mean there is no data to analyze

**Distinguishable**

Experienced hackers can often differentiate between a honeypot and a real system

# Advantages

Collect real data

Cost-effective

Reduce false positives

Encryption resistant

# Summary & Conclusion

- Effective method to track hacker behavior
- Not always designed to identify hackers
- Often more interested in getting into the minds of hackers
  - Design systems with that knowledge
  - Educate other professionals about the lessons learned
- Heighten the effectiveness of computer security tools

# Q & A

Ask at sli.do with the event code: `HONEY`

# References


[1] https://hackertarget.com/cowrie-honeypot-analysis-24hrs/

[2] https://resources.infosecinstitute.com/what-is-a-honey-pot/#gref

[3] https://www.csoonline.com/article/3384702/what-is-a-honeypot-a-trap-for-catching-hackers-in-the-act.htm

[4] https://i.kym-cdn.com/entries/icons/original/000/000/157/itsatrap.jpgl

[5] https://media.giphy.com/media/o0vwzuFwCGAFO/giphy.gif

[6] https://github.com/paralax/awesome-honeypots

[7] https://media.giphy.com/media/KJ1f5iTl4Oo7u/giphy.gif


T. HANKS