Tech Talk

CERT-MZ

HoneyPot.mz

André Tenreiro

andre@cert.mz

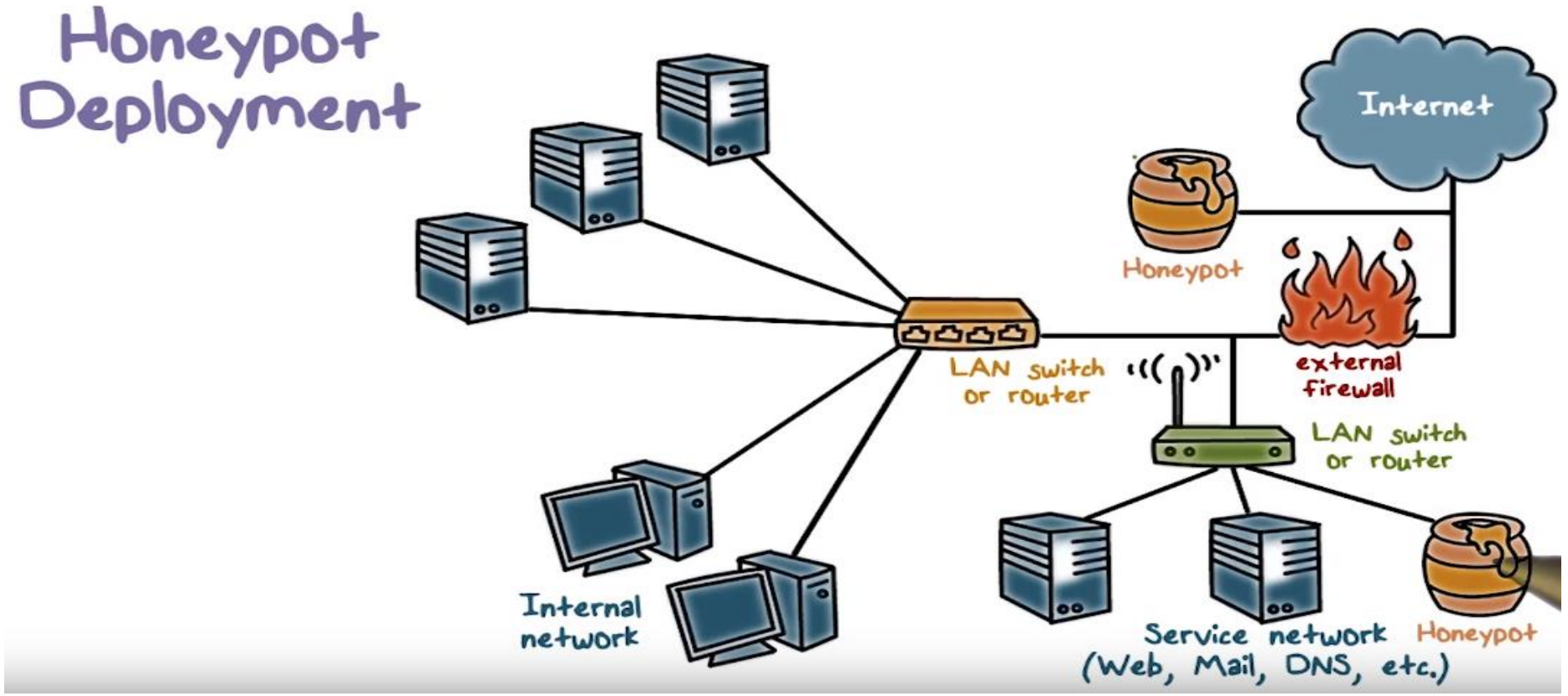
O que é um HoneyPot?

*"**HoneyPot** (tradução livre para o português, Pote de Mel) é uma ferramenta que tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre o invasor.*

É um espécie de armadilha para invasores. O HoneyPot não oferece nenhum tipo de proteção."

In Wikipedia, https://pt.wikipedia.org/wiki/Honeypot

Onde Colocar um HoneyPot?



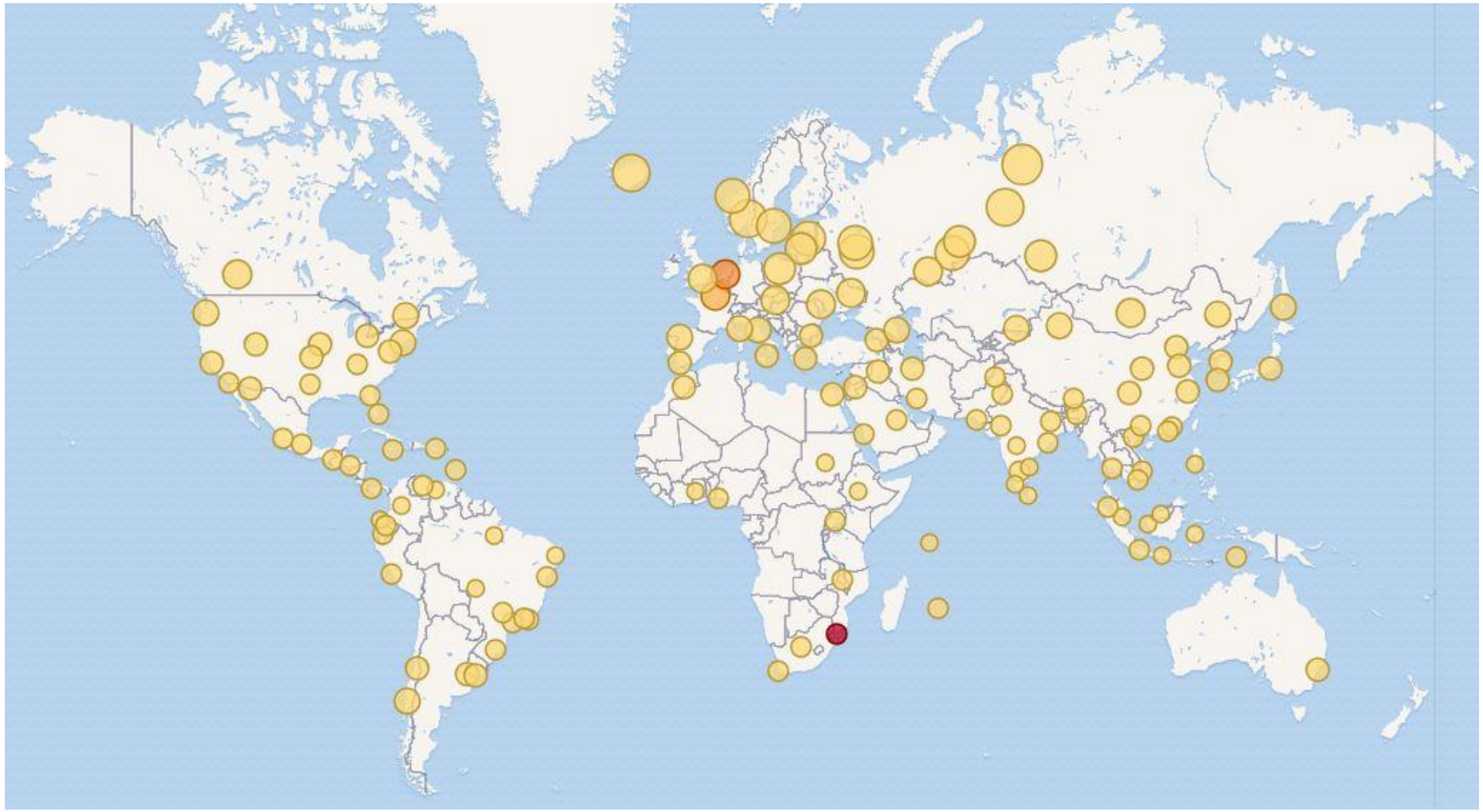
https://youtu.be/FBnTeryebzc (Honeypot Deployment)

HoneyPot do CERT-MZ

- Honeypot essencialmente de pesquisa a correr
- Baseados exclusivamente em tecnologias Opensource
- Simulamos alguns serviços populares tais como:
  - SSH
  - Web
  - RDP
  - VNC
  - VoIP
  - MySQL
  - SMTP
  - Etc.

Para este estudo analisamos mais de 200 mil eventos de segurança

De onde vem os ataques?

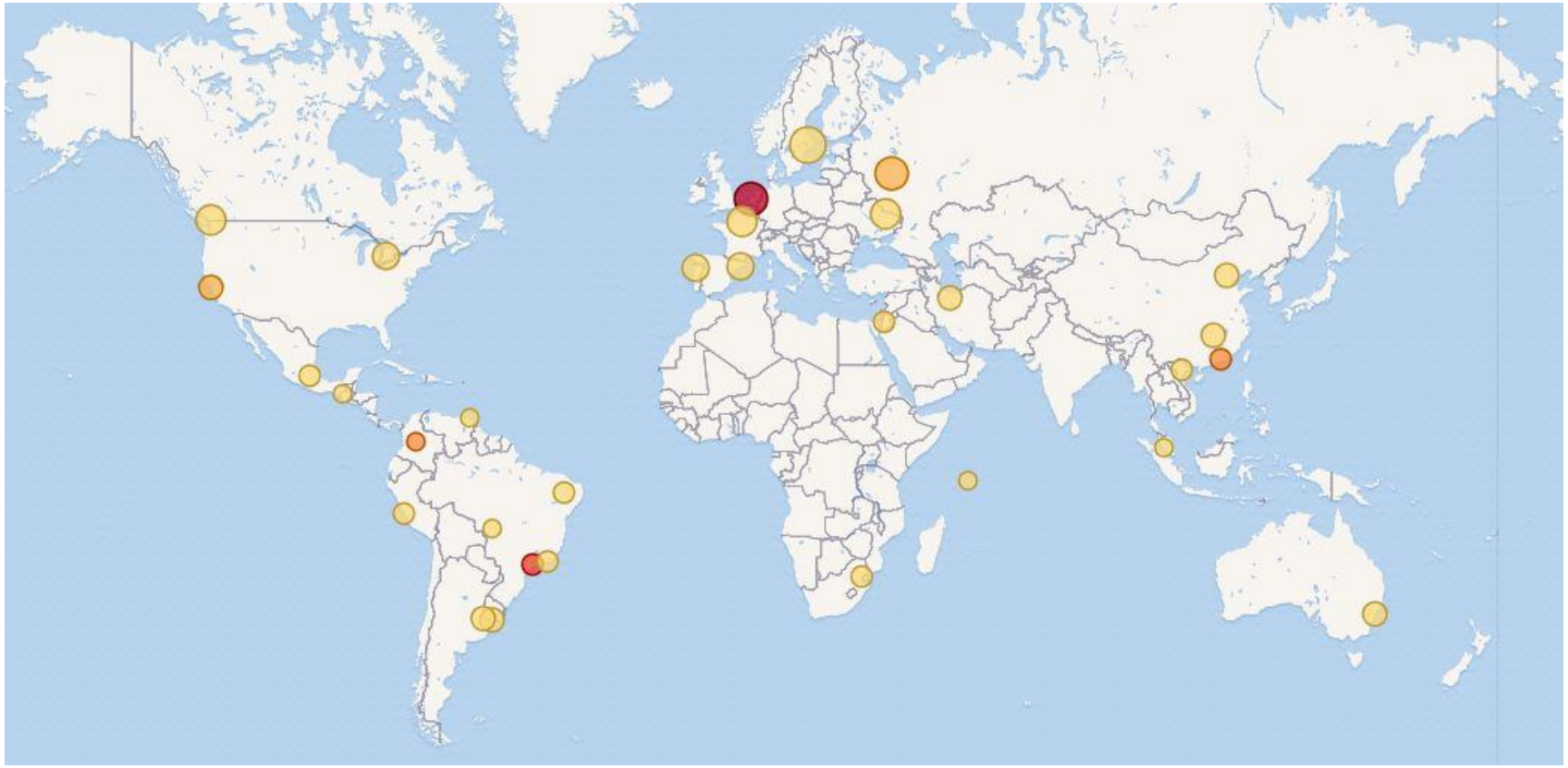


Confidencialidade: Publico

Quais os Protocolos mais explorados?

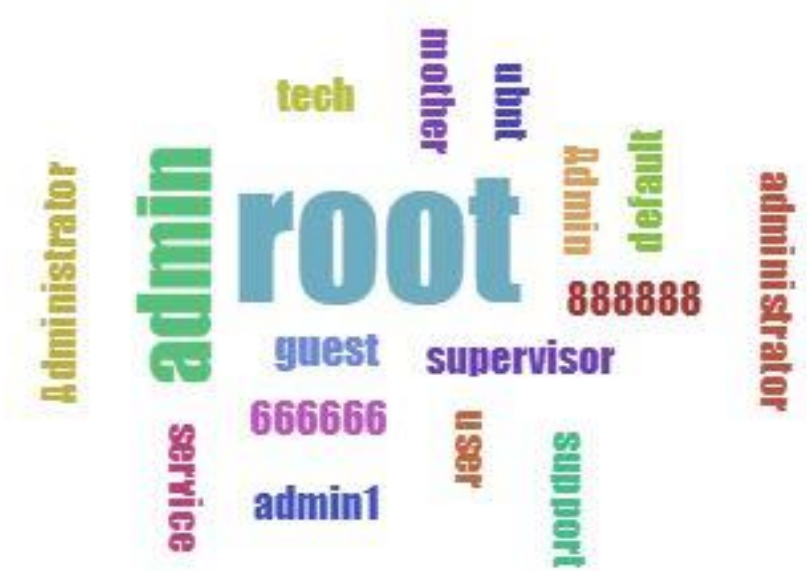
# Rank	Protocolo	Porto
1	SIP	5090
2	SMB	445
3	Asterisk/VoIP	5038
4	SSH	22
5	Web	80

Spammers



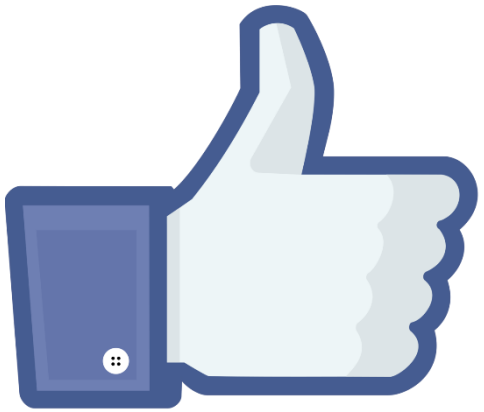
SSH: Bute Force

Usernames



Passwords

Questões ?



Segue-nos!

www.cert.mz

www.facebook.com/CERTMZ

www.linkedin.com/company/certmz