AI CENTER
FEE CTU

Stratosphere
Laboratory

Cyber Security and LLMs

Muris Sladić, Maria Rigaki

www.stratosphereips.org

Cyber Security

Trying to protect computers, networks, and data from unauthorized access, theft, or damage.

How can LLMs help us defend?

Image generated by DALL-E

Strato CyberLab

- To have good defense we need people
- Can LLMs help us get better in Cyber Security?
- Perhaps the hardest part is to start learning
  - How? Where?

- Let’s take a look at Strato CyberLab!

Demo Time!

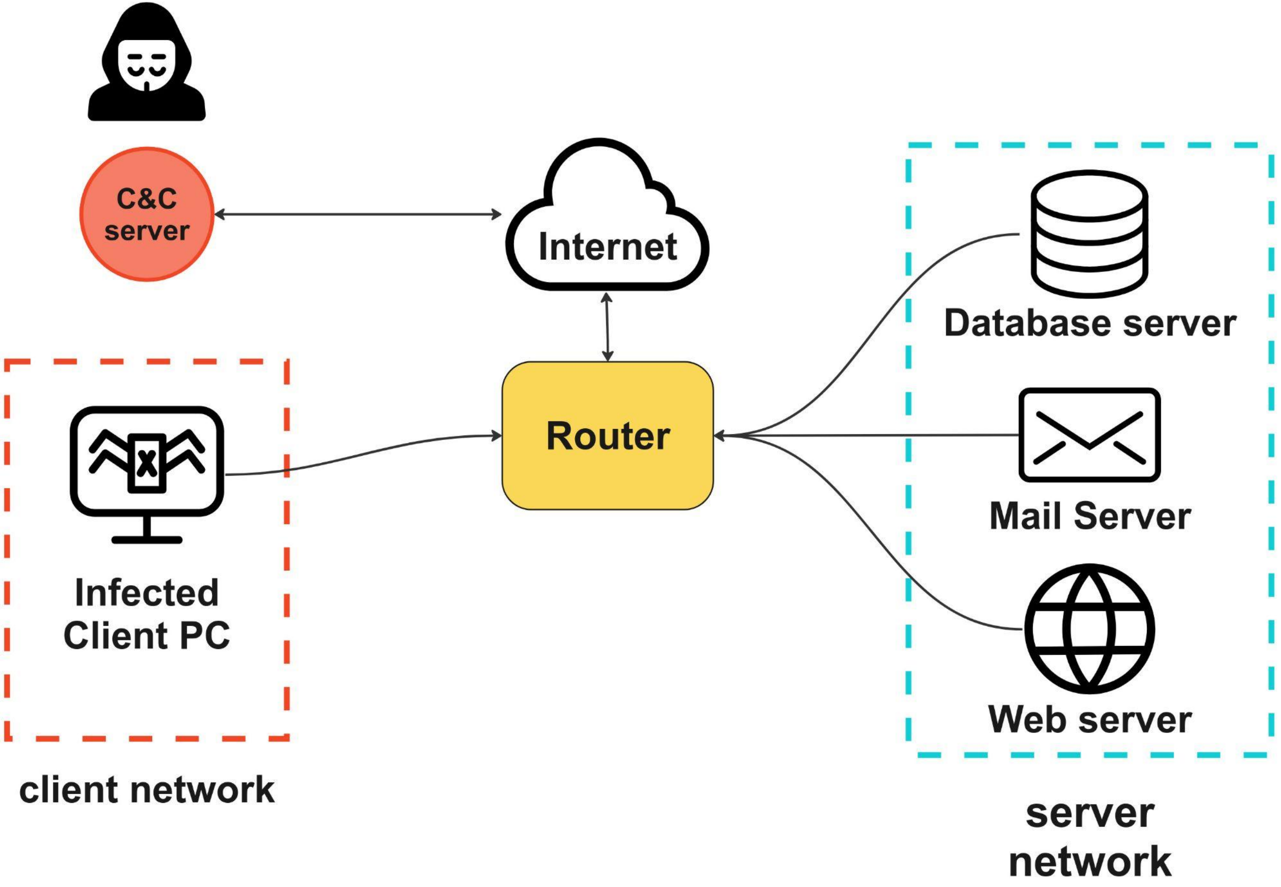
Can LLMs plan and execute network attacks?

Image generated by DALL-E

What are we trying to do?

- Pretend we are hackers
- Find our weak points
- Improve our defense

The NetSecGame Environment



What can the attacker do? (Actions)

- **Scan Networks** to find computers
- **Scan Services** to find what the computers are doing
- **Exploit Services** to gain access
- **Find Data** once they control a new computer
- **Exfiltrate Data** to their Command and Control server

Goal of the Scenario

- Find the email server
- Gain access to it
- Find and exfiltrate the administrator’s emails

Demo Time!

AI CENTER
FEE CTU

Stratosphere
Laboratory

Thank you!