# Assumed Breach Model

# From Zero to DA

[ AFK.conf ]

# ls env:

- Red Team @ Morphus
- ~5 years xp offensive security
- Twitter / Github: @g0ttfrid
- Linkedin: in/yurimaia

# Agenda

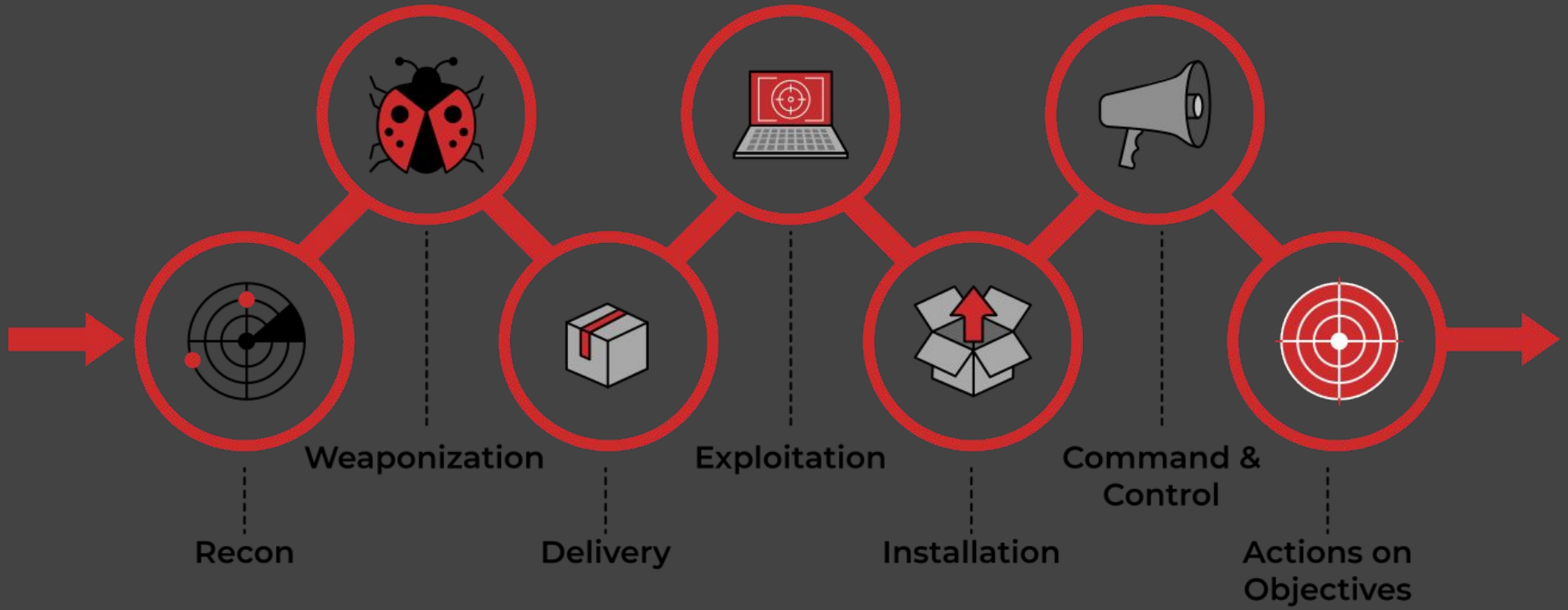
- Red Team
- Attack Lifecycle
- Engagement Planning
- Engagement Execution

# Red Team

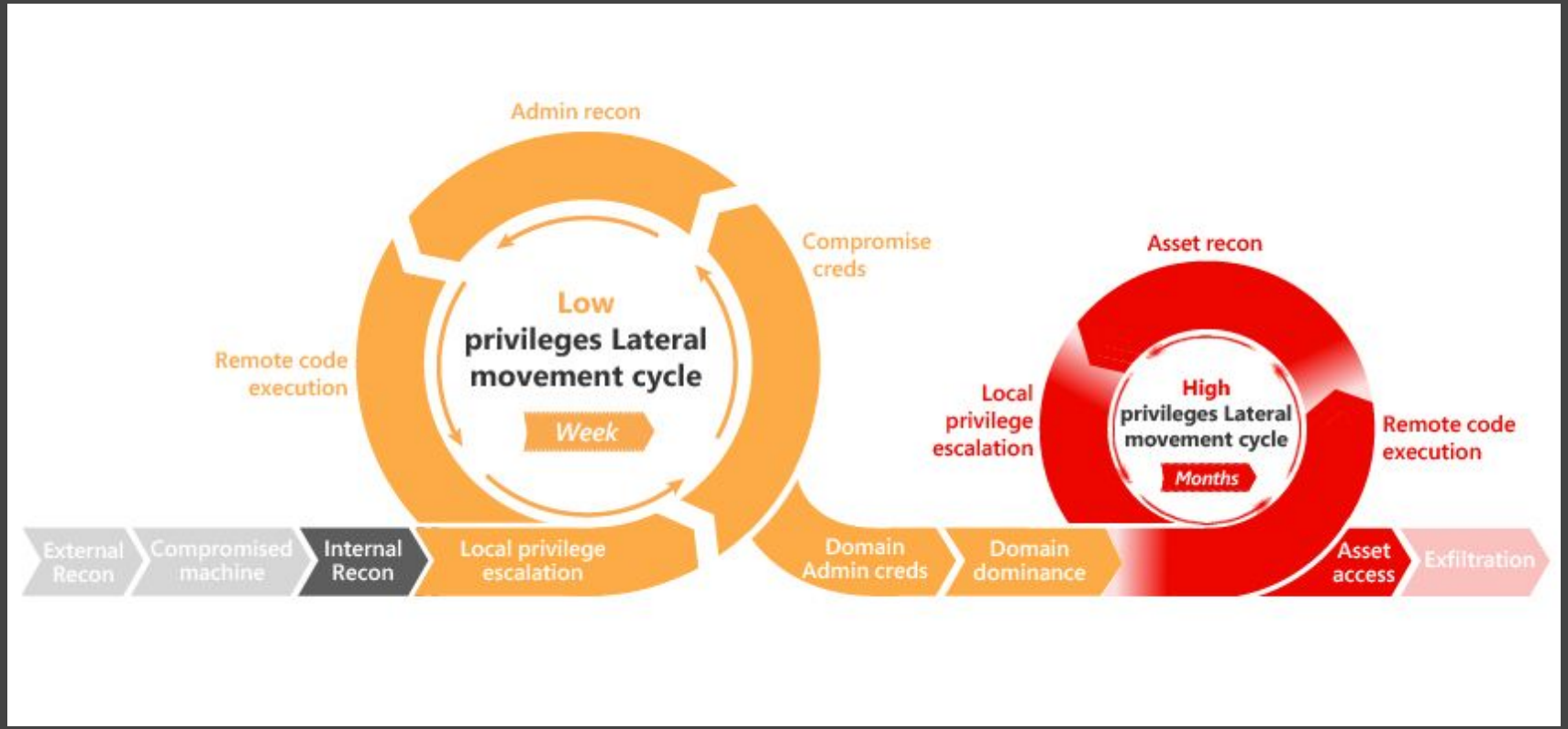
Red Teaming is the process of using tactics, techniques and procedures (TTPs) to emulate a real-world threat, with the goal of measuring the effectiveness of the people, processes and technologies used to defend an environment.

http://redteam.guide/

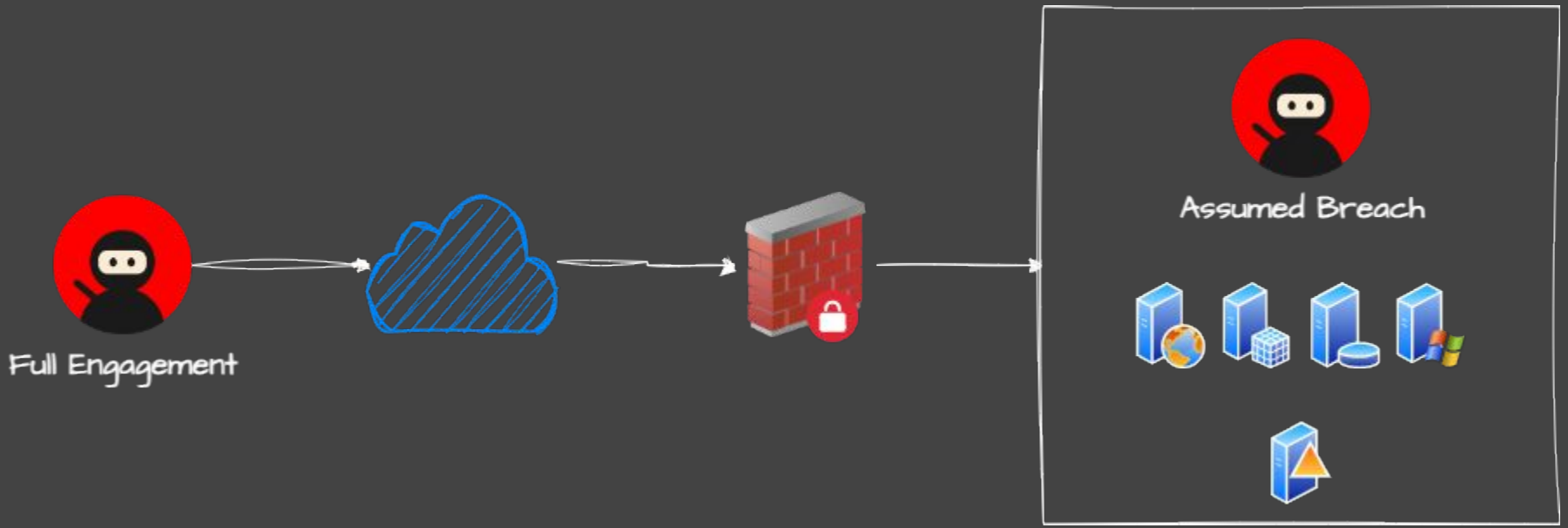
# Attack Lifecycle by Lockheed Martin



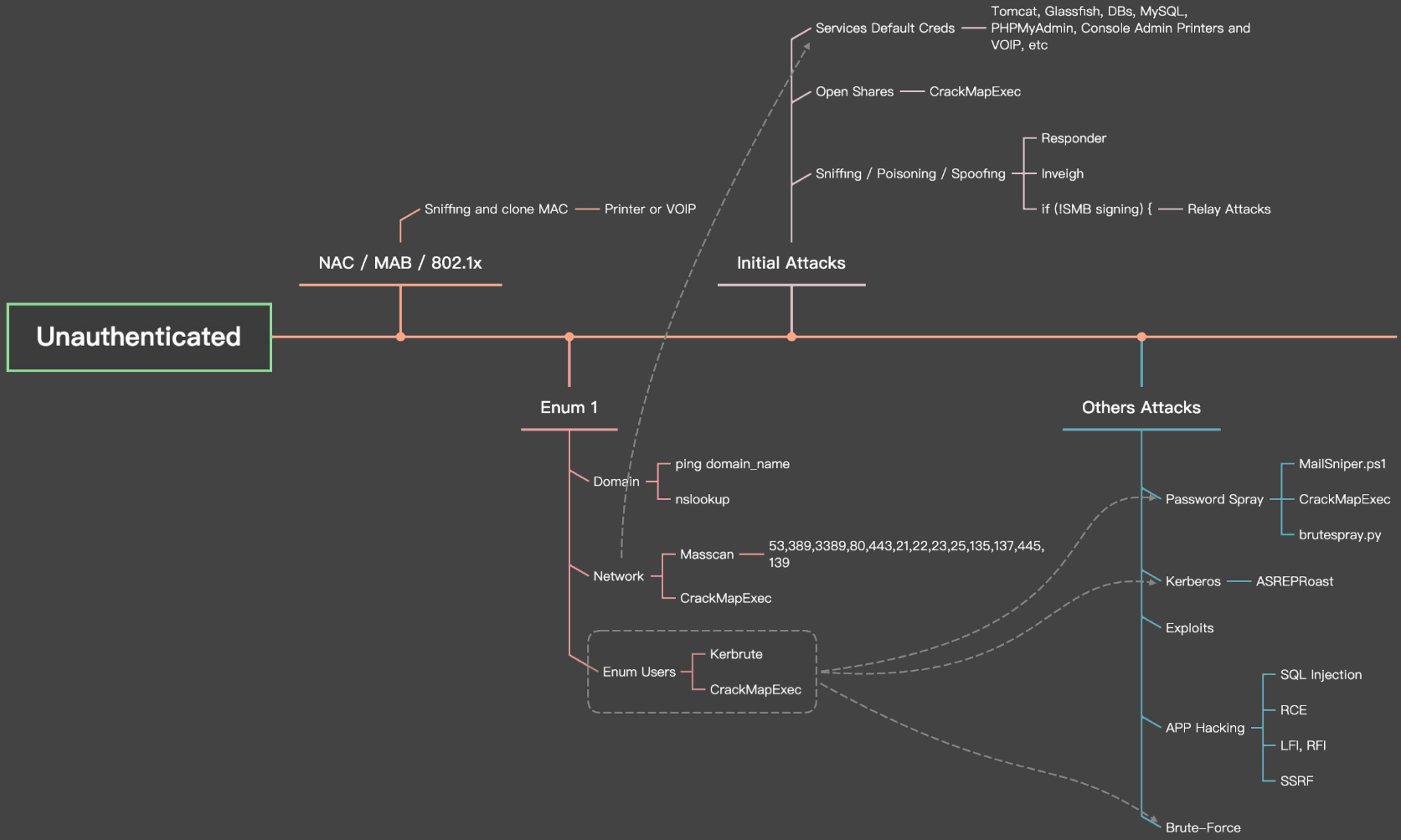
# Attack Lifecycle by Microsoft

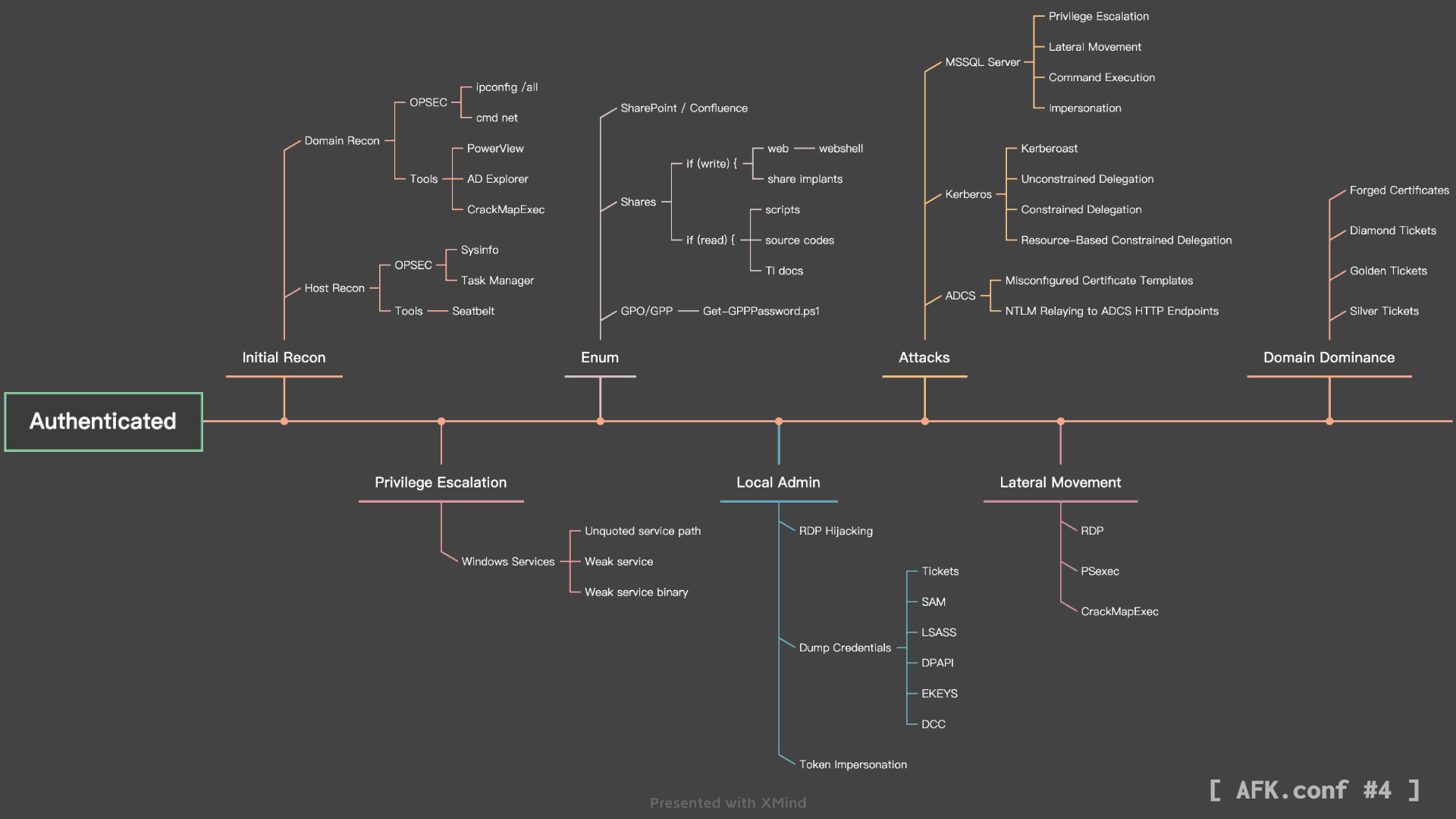


# Engagement Planning



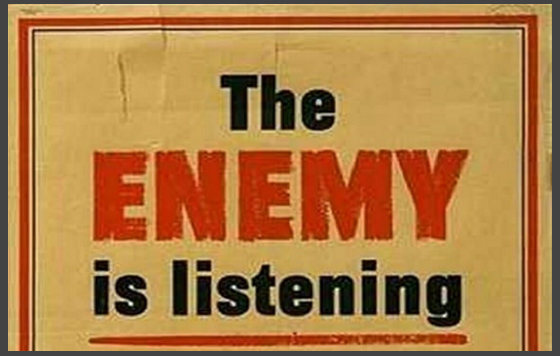
# Execution

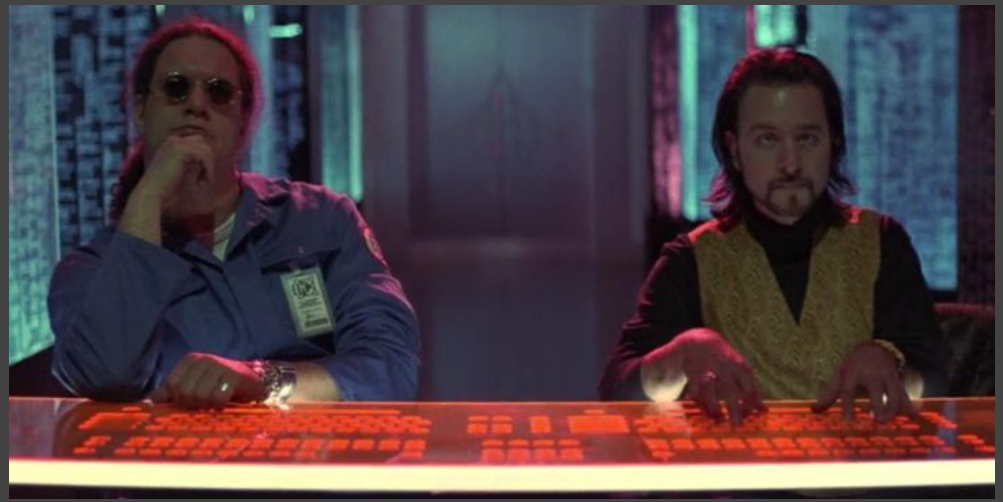




# OPSEC

- Protect your infra
- Set the username/hostname/domain
- Use system resources to your advantage
- Use compromised hosts to pivot on the network



# Thanks!