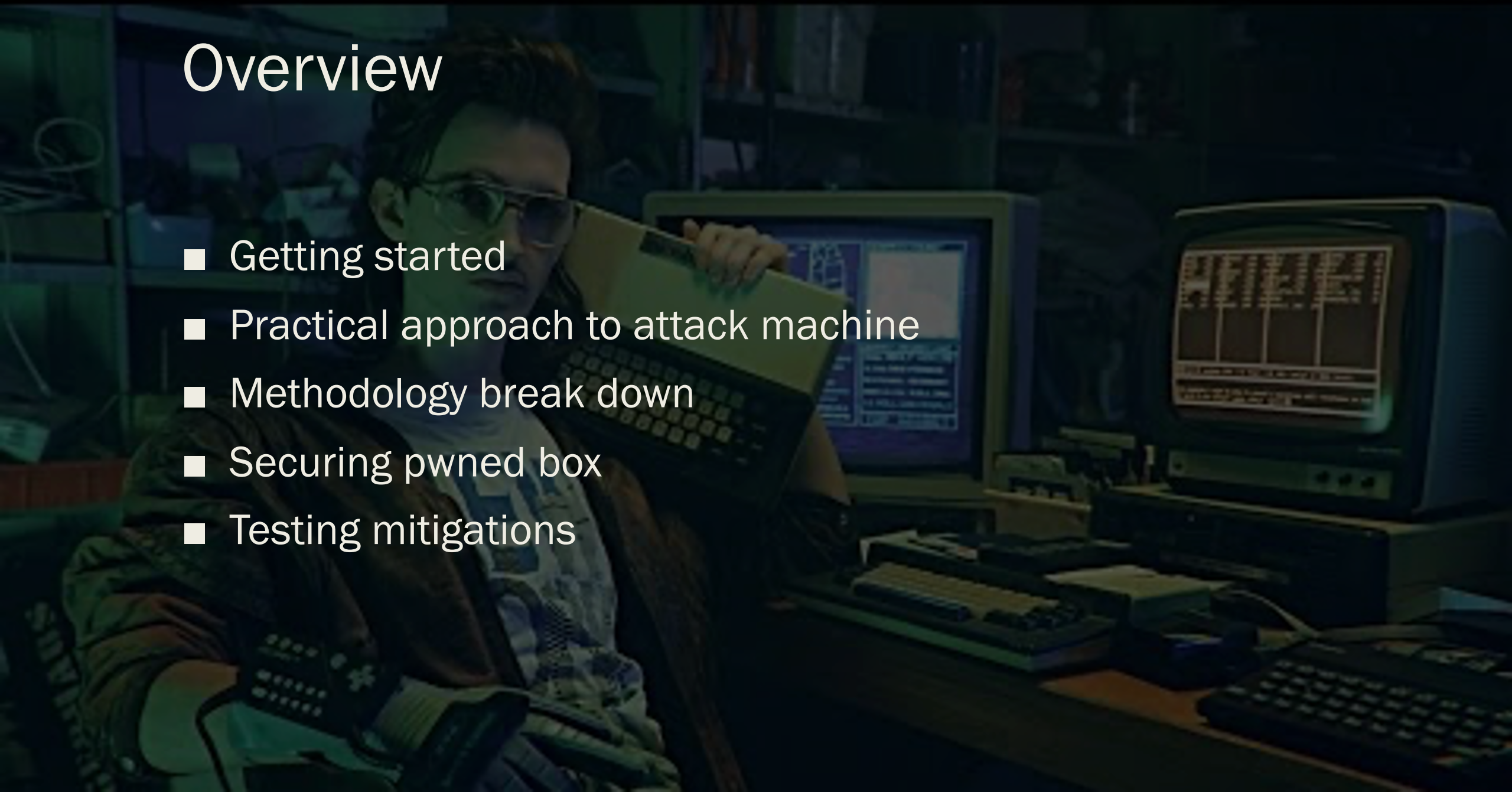
ATTACK AND DEFEND

Overview



- Getting started
- Practical approach to attack machine
- Methodology break down
- Securing pwned box
- Testing mitigations

Attack and Defend

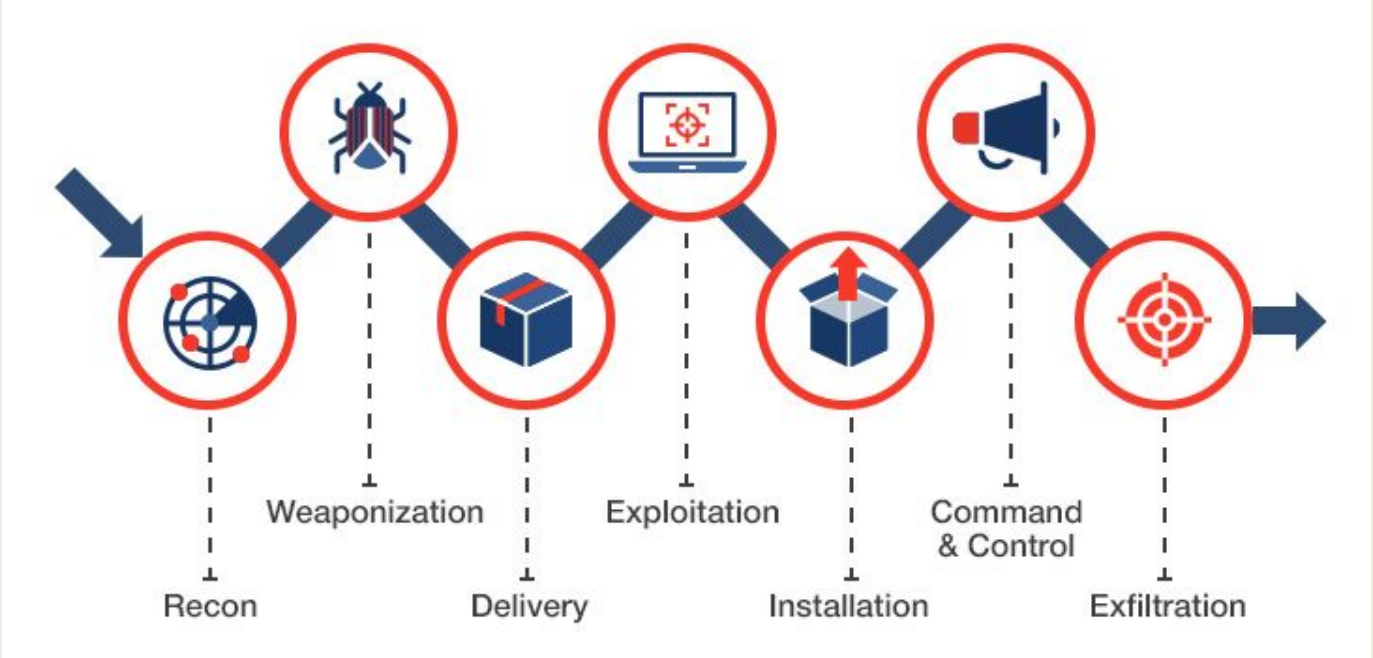
- CTF style of competition
- Everyday life of SOC security engineer
- Exploitation and persistence
- Pentesting and remediation

Ways to Practice

- Requirements
  - *A Computer and will to learn*
- Hack the box
  - *Fun, virtual lab*
- Vulnhub
  - *Self-hosted and configured*
- Competitions

Initial Approach

- https://attack.mitre.org/
- Scanning
  - *What ports are open?*
  - *How can we get in?*
- Enumeration
  - *Anything interesting?*



Hemisphere: Gemini (Vulnhub)

- Vulnhub
  - *Gemini*
  - *ColddBox*
- Easy box
- 2 Flags
  - *User*
  - *Root*