

A person in a dark jacket is operating a boat's winch. The winch is a large, black, cylindrical device with a white rope wrapped around it. The person's hands are visible, gripping the winch handle. The background shows the blue ocean and a white boat structure. The image is overlaid with a dark semi-transparent rectangle containing the title and authors' names.

# Vulnerability Analysis

Panico | Greminger

# Testing

- Sicherheitslücken finden
  - Konfigurationsfehler
  - Anwendungsdesign
- Zwei Arten von Testing
  - Active
  - Passive

# Active

- Direkte Interaktion mit einer Komponente
- Automatisiert
  - Geringerer Aufwand
  - Port- und Servicescans
- Manuell
  - Tiefere Analyse nötig
  - Beispiel: Schwachstellen in Webanwendungen

# Passive

- Analyse von Metadaten und Datenverkehr, ohne direkte Interaktion
- Metadaten
  - Informationen über Dateien, Dokumente und Anwendungen
- Datenverkehr
  - Schwachstellen im Netzwerk

# Validation

- Überprüfung von Testergebnissen
- Redundante Ergebnisse vermeiden

# Research

- Öffentliche Informationen zu Schwachstellen finden
- Exploit-Datenbanken zur Bestätigung der Schwachstellen

# Beispiel

