ET4397IN Network Security

- 16 Lectures covering vulnerabilities and security practices of every OSI layer.
  - **Physical layer:** intercepting traffic on copper cables, fiber optics, wireless systems, satellite, microwave, building resilient topologies
  - **Link Layer:** Traffic hijacking, ARP, VLANs, MPLS, WiFi, telecom networks, port-based network access control (802.1X)
  - **Network Layer:** best practices security network design, switch design/attacks, threat intelligence, IP security, DNS/DNSSec, secure/covert tunnels, firewalls/diodes, routing attacks, intradomain security
  - **Transport Layer:** TCP attacks, TLS/SSL ecosystem, side-channels
  - **Application Layer:** NG-Firewalls, honeypots, botnets, real-time communication security
  - **System security:** meta-data analysis, anonymizing proxies

TU Delft

ET4397IN Network Security

- 16 Lectures with demos covering every OSI layer.
  - **Physical layer:** tapping into a copper cable, wireless systems interception
  - **Link Layer:** MITM, malicious GSM network
  - **Network Layer:** protocol specification attacks, poisoning attacks
  - **Transport Layer:** session hijacking, retrieving keys by side-channels
  - **Application Layer:** botnets, threat intel using TUDelft's telescope
  - **System security:** identify people through meta data, build a backdoor into a PRNG to decode SSL in real-time

ET4397IN Network Security

- Focus on concepts, no programming knowledge required
- Grading: 50% homework (conceptual questions)
  50% final exam

  OR

  50% homework (conceptual questions)
  50% mini project (software/hardware)

More information, list of content, tentative schedule on
www.networksecuritycourse.nl

TU Delft