

KEA Competence Penetration Testing

hand-in assignments

Henrik Kramselund Jereminsen
hlk@zencurity.com

October 28, 2021



Hand-in 1: Pentest a network and deliver pentest report

Assignment:

Pentest a network - with at least some results. Select one which you are allowed to port scan and one which is not highly critical for you.

I recommend using Nmap with scripts.

Create a report, use the report template for inspiration.

The report should include the following sections at least:

- Title, Table of contents, formal report thanks
- Confidentiality agreement – Write "Confidential" on each page
- Executive summary – big companies always want this
- Information about the scan done, what was it
- Scope and targets
- Review of all targets – detailed information and recommendations
- Conclusion – may be more technical
- Appendices – various information, Whois info about subnets and prefixes

You are very much welcome to run multiple tools! If you find web servers run Nikto, if you think there are network devices, try SNMP walk.

Must be handed in as PDF on Fronter and latest on November 16, 2021 23:59 . Teams up to two are allowed. Make sure to list team members in the report.

Expect PDF as A4, portrait mode up to 5-10 pages with illustrations as needed. Double if team.

Recommend to use a report template with table of contents, front matter, page numbers etc.

Help:

Think about what you would like to receive if you were responsible for security in the network examined.