

KEA Competence Communication and Network Security

hand-in assignments

Henrik Kramselund Jereminsen
hlk@zencurity.com

May 24, 2021



Hand-in 1: Dump a HTTP connection with password

Assignment:

Find a device that provides a web administration interface over HTTP - not HTTPS.

Preferably one with a simple username and password admin/admin.

Capture a HTTP session, hint: using tcpdump or wireshark might be the easiest.

Create a report about how the password is sent, in clear text, or perhaps as base 64 and why this is insecure.

Include screenshot.

Create a report, inspiration for report template below.

I suggest the report should include the following sections at least:

- Title, Table of contents, formal report template thanks
- Executive summary – big companies always want this
- Information about the network dump done, what was it
- Review of password security when running HTTP
- Argue why HTTPS would be better, and if you like show similar dump with HTTPS
- Conclusion – may be more technical
- Appendices – various information, Whois info about subnets and prefixes

You are very much welcome to run multiple tools!

Must be handed in as PDF by email to hkj@zencurity.com and latest on June 8, 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.

Help:

Think about what you would like to receive if you were management about to approve a security policy disallowing HTTP based logins.