KEA Kompetence Communication and Network Security

hand-in assignments

Henrik Kramselund
hlk@zencurity.com

May 2, 2022

Hand-in 2: Parse network traffic automatically – with Zeek

Assignment:
Parse network traffic using a dedicated program.

Using Zeek as an example you will take some traffic, either an interesting packet dump you have found on the internet, or one you have captured yourself.

The main goal is to show that you can setup a system to parse network traffic.

I recommend looking at the exercises below and use them for the technical part:

- Zeek DNS capturing domain names
- Zeek TLS capturing certificates

Find a device that can sniff traffic, or sniff on a local system and produce network traffic using a mix of programs.

Hints for generating traffic from a Debian server:

- Run `apt update` and `apt upgrade`
- Run the browser and visit a couple of sites

Capture the traffic using either using tcpdump, wireshark or directly using Zeek as live traffic. Hint: using tcpdump or wireshark might be the easiest. You can also use Nitroba pcap as listed in the exercises and found in many places on the internet.

Then run this packet dump through zeek until you have at least the following traffic:

- UDP and TCP
- DNS and HTTP
- TLS certificates

Important: Zeek can generate text output in native format or JSON output You decide which you want to work with.

Demonstrate in the report how this process went, from start to having the output. Create a report about how the network traffic is parsed and what data is saved by Zeek.

Include screenshots and example output from Zeek, interesting packet information that you have found.

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, what is the source
- Show the setup – doing live capture, sniffing from local interface or mirror port
- Show example output in the categories listed above, TCP, UDP, DNS, HTTP, TLS
- Conclusion – may be more technical, list a few benefits from using Zeek, and if there are things which you find bad about the tool or process
- 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 Fronter and latest on June 10, 2022 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.

Expected time usage, 10-20 hours at most.

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

