TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

institute of telecommunications

Exercise 2: Live Capturing

Network Security - Advanced Topics (VU 389.160), Winter Semester 2018/2019

Communication Networks Group at the Institute of Telecommunications

2 A second transmission...

When reporting your findings to your superiors, they inform you that new traffic has arrived at the suspicious laptop while you were focused on decoding the hidden message. Seems like your task of detecting covert channels online is not over yet . . . Quickly, you start capturing traffic again and pay attention to the new traces. Is there indeed another hidden message!?

Important: Before capturing traffic for exercise 2 for the first time, tell the tutors!

Repeat the steps carried out in exercise 1 for capturing, filtering, analyzing, and decoding the previous covert channel. Answer the following questions in the report:

Rep:2.a – Filters

Give a detailed (yet brief) explanation of the steps you carried out to filter irrelevant data (either Wireshark or Rapidminer). Do also specify the keywords and operators required.

Rep:2.b – Univariate analysis

Which features are not viable to mask a covert channel and could be removed from the analysis? List the rejected features and provide short but meaningful reasons for rejection.

Rep:2.c – Bivariate analysis

From the remaining features, which ones are not viable to mask a covert channel and could be removed from the analysis? List the newly rejected features and provide short but meaningful reasons for rejection.

Rep:2.d

What is the IP address of the machine presumably leaking information?

Rep:2.e – Covert channel discovery

Do you think that you have found the covert channel? Give a detailed description of where the covert channel is occurring (`feature_value:covert_symbol` relationship) and provide a capture of the plot where the abnormal behavior of the suspicious feature is isolated and clearly visible.

Rep:2.f – Decoding the message

Write in the report the decoded message. Explain clearly how you carried out the decoding task (step by step in a numbered list).

Rep:2.g – Additional comments

Report briefly any additional comment or observation related to the exercise solving to be considered during the review of your exercise.