Hack IT 2018 Case: *No trace left behind?*

Thomas Kobber Panum
Ph.D. Student
Network Security Group
Electronic Systems, Aalborg University

AALBORG UNIVERSITET

Introduction

Thomas Kobber Panum

(newly) Ph.D. Student at Network Security Group

Formerly Data Scientist (~3 years in industry)

- Applied Machine Learning to various areas: *medical, insurance, and logistics*
- Made a tool for bypassing an implementation of Google's RECAPTCHA

M.Sc. in Software Engineering (Machine Intelligence), Aalborg University

Currently: Writing my 2-month PhD Plan within the field of network security and machine learning

Twitter: @tpanum, GitHub: @tpanum

The Case: No trace left behind?

Designed as *treasure hunt*

You will have to go through a series of steps in order to solve the exercise

Each step will unlock points, which will be used for the final scoring

You will need to perform:

- Fingerprinting
- Binary Inspection
- Network Traffic Analysis
- Clever investigation :-)

Written and designed by: Jens Myrup Pedersen

The Case: No trace left behind?

For years, the police has been working towards infiltrating a group of cynical criminals, working throughout all the major Danish cities: The group is assumed to control large parts of the underground economy, including trafficking, money laundering, drug trade, and assassinations. During a cold and stormy evening, a large number of specially trained policemen are ready for the big raid towards the supposed head quarters on an abandoned farm in a desolated area of Northern Jutland. However, except for a party going on at the neighboring farm, they found that the criminals already left the buildings.

There is nothing to be found – until a policeman stumbles upon an old computer. He is able to boot it, and reaches a Windows XP login screen. There is only one user (username: LisbethSalander), but due to the password protection he is unable to login.

Maybe the computer carries the secrets the police are looking for?

All information available at GitHub here.

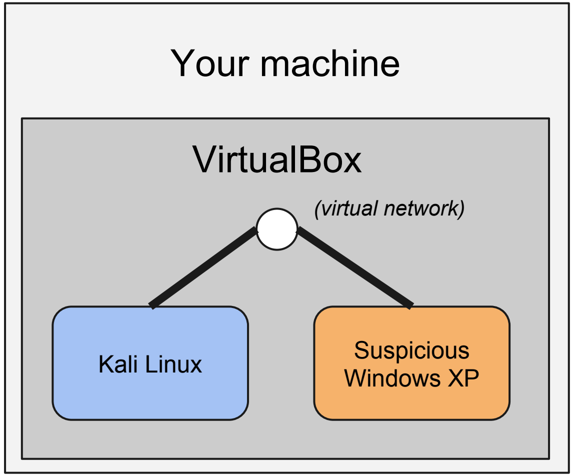
The Case: No trace left behind?

You will be provided with two VirtualBox images:

- **Kali Linux** (attacker), contains all the tools you need in order to solve the exercise
- **Suspicious Windows XP** (target), contains all the answers

In order to start working on the exercises the two virtual machines need network access to each other.

This can be done in multiple ways, but there is a guide on how to setup and connect the machines to a virtual network in VirtualBox is available on GitHub here.



The Case: No trace left behind?

The end goal is:

...the names and titles of the steering group of the network.

Do not forget to write down intermediate steps and solutions!

They count towards the scoring in the end

Solving parts of the puzzle still yield points!

Being the first team to complete the exercise yields additional points

The Case: No trace left behind?

During breakfast there will be handed out a paper describing the expected steps and hints in order to fulfill them

But not solutions will not be uncovered!

All solutions needs to be sent by email to Thomas (tkp@es.aau.dk)

github.com/aau-network-security/hackit-2018-case

The Case: No trace left behind?

Information can be found here:

github.com/aau-network-security/hackit-2018-case