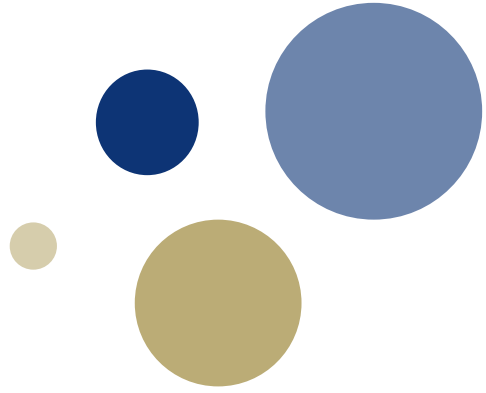
NTNU

Norwegian University of
Science and Technology



IMT4116 REM Oral Exam

Overview and self-assessment

Matthías Ragnarsson

June 13, 2017

Basic laboratory setup

— My laboratory was an Archlinux machine on Tigger, using Virtualbox.

— In Virtualbox I had 2 analysis machines

- Remnux for internet traffic interceptor/emulator.
- Archlinux with Blackarch pentesting repository for various static analyses and browsing.

and 1 victim machine

- Windows 7 as provided in the course with other necessary installs.

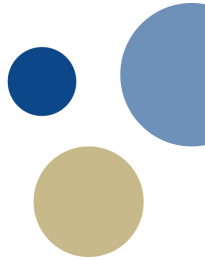
Basic Static Analysis

- Tools: strings, peframe, rabin2
- Procedure: Ran them and collected usual suspect data and according to gut feeling.
- The good
  - Seemed alright results before other analysis steps (not sure what else would've helped with later steps)
- Could've
  - Given a better account of the tools I was using and screenshots.
  - Included hashes, file names etc. as IoCs.
  - Maybe given a more wordy account of the hypotheses.

Basic Dynamic Analysis

- Tools: Procmon, CaptureBAT, Process Hacker 2, Wireshark/Tshark, Inetsim, fakedns, set default gateway to Remnux.
- Procedure: For each sample I turned on the tools, waited 1-2 minutes, killed sample process in Procmon, turned off tools.
- The good
  - Minimal answers, not sure if there was more.
- Could've
  - Looked at the logs more thoroughly? But not sure if there was more. I didn't seem to get much data.
  - Done a more wordy account of hypothesis.

Advanced Analysis (1)



— Tools: IDA Pro free, radare2, x64dbg, tools from previous sections as appropriate and other CLI tools.

— Procedure: Mostly just basic and advanced static analysis.

— The good

- Clear and concise mostly.

— Could've

- Done some screen shots in the **a** section. Didn't think about it at that time.
- Done some better dynamic analysis in **b iii** to determine loop count.
- Done some network analysis in **e** to confirm IP address, protocol and commands. Static analysis only could be following a diversion. This was done before I added a network analysis setup.

Advanced Analysis (2)

— Could've

- in **f ii**, figured out one Window check function.
- in **g ii**, figured out mutex name. Process Hacker wouldn't show handles (there's some trick to it). Decided not to waste time doing this manually.
- in **g v**, figured out system parameter for name. Wasn't sure, skipped and never got back to it.

Combined Analysis

- Tools: Same as in the previous sections.
- Procedure: Straight forward answering each question with appropriate tools.
- The good
  - Went ok, but think I missed something about the latter traffic analysis towards the end.
- Could've
  - Documented more in the static analysis, hash etc.
  - Interacted more with the traffic in **e** in order to know more about the nature of the traffic. Could've written more in **h** summary if so.

Open Source

- Tools: Duckduckgo.
- Procedure: Searched on duckduckgo and found promising results.
- The good
  - Basic information given and link to a good source.
- Could've
  - Made a more thorough documentation. I figured out that I mistook technical audience to be general non-technical audience in the beginning. At that point I was too tired to revise and just linked to appropriate sources.

Questions?