Week 6 and Week 7 activities

Activity Instructions

Purpose

The purpose of the activity is to:

- expose students to core network forensics tools for analysing pcap and netflows
- conduct a basic network forensic analysis
- use data visualisation tools to explain technical concept to a lay decision maker

Our focus is on analysis and interpretation. It is assumed that basic data collection capabilities (e.g. network sniffing) have been introduced in other modules.

Training Material

The activity is based on a training module provided by the European Union Agency for Network and Information Security (ENISA). It comprises of:

- A Student Manual – this is available on WebCMS (also included in Week 6 optional reading material);
- Virtual machines:
  - An ENISA virtual machine pre-configured with tools and artefacts;
  - Kali Linux virtual machine pre-configured with tools and artefacts.

Students are not to use other materials/tools during the group work but may do so when working individually to complete the assessable outcomes.

Group and take-home working

The activity is across two tutorial sessions. We will be completing two selected exercises from the Student Manual and extending them slightly for the assessment. Students are encouraged to work in groups of 3-4 people for the tutorial and may also take the work to complete at home.

Assessment

The assessment activities are to be completed individually. The following activities will be assessed:

1. A dot point report of your group's examination/analysis for scenario 1 (assessment for Week 6 to be submitted at the end of Week 7);
2. A short 10 question quiz consisting of multiple choice and short answer questions (assessment for Week 7 to be submitted at the end of Week 8).

For (1) you will be assessed on your approach and the clarity and persuasiveness of your report/explanations. You will not be assessed on the correctness of your analysis compared to the ENISA-provided solution (in the Teacher's Manual).

Scenario 1 (Week 6 activity)

Scenario 1 is based on Task 2 of the ENISA training (starting on page 11 of the ENISA document for students). Scenario 1 is being assessed via a dot point case report and an extended explanation of a process.

The scenario is based on a real case, although the technical details have been changed to reflect a publicly available PCAP file.

Scenario

You are the expert engaged by the Taxation Clerk of the Victorian District Court[1] and are provided with the following brief:

Background

The case involves:

- Grand Insurance Co (**Grand**): who have provided a cyber insurance policy to Victim Pty Ltd;
- FEH Software (**FEH**): who manufacture the security software used by Victim Pty Ltd at the time of the infection;
- Victim Pty Ltd (**Victim**): are not a party to the current case. Victim's computers use the IP addresses in the 90.237.150.xxx range. Victim has since ceased trading and their former staff are not available for this case.

In June of 2008, Victim suffered a cyber attacked which resulted in their computer(s) being infected by a computer virus. Eleven months later, and just within the allowed one year timeframe, Victim lodged a claim with their insurer claiming $180,000 damage which was calculated on the basis of $20,000 per infected computer. Grand paid out the claim and is subsequently suing FEH to recoup the monies.

After an extended Court supervised mediation, the parties have agreed to the basis of calculation i.e. $20,000 per infected computer and that infected computers were infected with the Dabber virus. They disagree on the number of computers infected. FEH's expert, a well-known anti-virus researcher, says that only 4 computers were infected so the compensation should be $90,000 i.e. $80,000 plus a little extra to cover overheads relating to Victim's incident response.

You are asked to provide an expert's report answering the following questions:

a) *How many computers were infected*?
b) Is $10,000 the appropriate amount to cover overhead's relating to Victim's incident response?

You are to prepare your report on the basis of the provided material:

- An explanation of the Dabber report by an independent company (see handout from Sophos);

[1] For the purpose of your tutorial don't worry about the nuances regarding different rules in NSW and Victorian Courts

- A PCAP file created by Victim's IT staff at the time of the attack (i.e. the DABBER.PCAP file from the ENISA training[2]).

Instructions

1. Follow the instructions given in the ENISA document for students;
2. Double-check your answer by doing it a different way - swap over to Kali Linux;
3. Don't forget basic forensic procedures, such as hashing the evidence;
4. Use tcpflow to convert the dabber.pcap PCAP file to a netflow
5. Search for PACKAGE.EXE

Assessment - Dot point case report

Prepare a dot point report that explains your examination and finding(s).

Scenario 2 (Week 7 Activity)

Scenario 2 is based on Task 5 ENISA training (starting on page 19 of the ENISA document for students). This scenario is being assessed by the quiz only.

[2] This has also been provided on the course Kali Linux and Win10 images