(a few)

Notes on lab exercise

Dr. Luca Allodi
Security Group, WIN, TU/e

Cyber Attacks and Defenses
Q2 2020

Overview of lab session on the 15th Dec.

- The exercise will be held during the class of the **15th of December**.
  - Please reserve 15’ extra at the end of the class timeslot to accommodate for possible delays due to the online setup

- All students will work in **groups of two people**
  - You will need a laptop, one per group.

- Prize: + half a point at the exam IF at least one actor identified correctly
  - BONUS: or all attacker actions identified correctly

- The class will be held online on MS Teams
Timeline TO the 15th

- Group forming
- Survey
- Exercise

30 Nov  
7 Dec
14 Dec
15 Dec

Information on groups

- Group formation open until 7th of December
- After deadline group switching/forming will be closed
  - We will randomly assign remaining students to groups
  - Up to you to get in touch with your teammate and organize yourself for the 15th
- **Group members get the same bonus at the exam**
  - Either NONE or +0.5 pnts
Information on survey

- Mandatory to fill in

- NEITHER graded NOR of any influence on your final grade

- Self assessment + technical questions
  - We only use it to have a better idea of the class composition and background for the exercise

Timeline OF the 15th

- Start of class 13:30
- Crash course on incident investigation + demo + 30 mins
- Warm-up exercise + 20 mins
- Pause + 10 mins
- Exercise + 50 mins
- Questionnaire + 15 mins + 15' buf
Overview of exercise

You

BOTH: Alert investigation
ONE: Taking notes

Us

Alert investigation

TU/e SOC

Rest of TU/e network

Final questionnaire (survey monkey)

Alert generation

Inject "normal" traffic

Inject "attack" traffic

Alert generation

Report findings

Fetch results

You

ONE: Taking notes

Rest of TU/e network

Some suggestions

• Suggested group configuration:
  • One student operates the interface
  • The other takes notes on the provided handouts
    • More on this in the video explaining the interface, will be up soon!

• You will still have access to the SOC when answering the final questionnaire
  • Will still be able to reconstruct some information...
  • PROVIDED you have enough details in the notes to know what to look for!
Taking notes will save the day

<table>
<thead>
<tr>
<th>IP ADDRESS (e.g. 192.168.0.0, etc.)</th>
<th>ROLE (e.g. Attacker, Victim, C&amp;C, etc.)</th>
<th>ACTION (e.g. SSH attack, Port Scan, Sensitive data upload, etc.)</th>
<th>ADDITIONAL COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

⚠️ Handout you will receive before the exercise (present in your MS Teams channel)!

Use it to keep note of interesting incidents/activities you observe

Will be vital to answer the final questionnaire!

Preview of final questionnaire (1)

GENERAL INFORMATION

1. Insert your student ID *
   - Student ID 1
   - Student ID 2

2. Which was your SOC name? *
   - svsco01-augustus.win.tue.nl
   - svsco02-nemo.win.tue.nl

<- Both of your IDs
(we use them to uniquely identify the group)
(make sure they are correct)
IF you're alone, just fill in yours (once)

<- This corresponds to the URL you visited
when accessing the SOC
Preview of final questionnaire (2)

Insert the IP address(es) of the attacker, one per line. If no IP address is known, write "NA".
- What is the confidence you have on the attacker's IP(s)? *

Low  | Medium | High
---   | ---    | ---
   |   |   

Insert the IP address(es) of the victim, one per line. If no IP address is known, write "NA".
- What is the confidence you have on the victim's IP(s)? *

Low  | Medium | High
---   | ---    | ---
   |   |   

5. Did you observed any of the following reconnaissance activities?

6. Which vulnerability did the attacker exploit?

7. Which of the following actions did you observe? (check at most 2 boxes)
   For each option selected insert the IP address of the receiver of such activities
   (i.e. HTTP requests -> web server's IP; enumerating SMB shares -> SMB server's IP; …)

---

Make sure your notes will be useful to reconstruct this information when you need it!