Something Awesome Project

z5205522 Alan Trieu COMP6441

Overview

For my Something Awesome Project, I aimed to challenge myself by learning basic CTF concepts and applying them through various wargames – Natas, Narnia and the extended wargames from COMP6841.

By the end of the project, I have completed Natas0 to Natas26, Narnia0, Narnia1 and all the extended wargames that were released up to the submission date. All of these are in blogs, which detail my thought-process, reflections and what I have learned.

The bulk of COMP6441 is focused on guiding students to think critically and practice analysing everything, but I still really wanted to leave this course with some tangible "hard" skill. In hindsight, the wargames forced me to critically-think and analyse in a practical setting and complemented the fundamental theme of 'thinking like an attacker' introduced in lectures.

Initially, instead of the wargames, I was planning to create a website designed to teach users the basics of cybersecurity through minigames. These minigames would basically be a summary of the concepts Richard taught us throughout the term, including practical activities for cryptography and hashing, along with conceptual activities, like an interactive trust/risk game that you would see on psychometric tests. I realised that there was a lot that could go wrong with this, and it was perhaps too ambitious of a scope to do within only a few weeks. I decided to follow what Josh, my tutor, did, since it would be helpful for COMP6443 and COMP6447 (and perhaps the scripting parts of COMP2041) next term.

Methodology

I began the project by setting weekly learning goals, as detailed in my introduction blog. This went surprisingly smoothly, as I stuck to schedule fairly well. Despite the occasional bumps, I didn't particularly feel rushed at any time during the term. I generally stuck to doing the associated extended wargames about a week after learning the content, excluding reverse engineering, where I completed the activity right after watching the lecture video.

In general, each week consisted of:

1. Watching the COMP6841 lecture videos (+ writing notes)
2. Doing some independent research to cement the introduced concepts (+ writing notes)
3. Attempting the extended wargames
4. Attempting the Natas/Narnia levels
5. Writing blogs for the wargames
6. Writing the weekly reflection blog

The weekly reflection blogs followed the same structure – an overview, achievements/what I learnt, methodology, challenges and plans for next week. The wargame blogs didn't have a particular structure because I wanted to convey only my thought-process and steps trying to complete them. There are a few things I wish I did, which I will cover later.

My notes and wargame thought processes were all first recorded on Google Docs, before being typed up as blog posts. I felt that it would've have been easier to access and to keep track of everything this way, instead of writing them directly as blog posts first. Surprisingly, the Natas doc was fairly wordy – 7599 words!

Something Awesome Project

z5205522 Alan Trieu COMP6441

What I Learned

The bulk of what I learned was actually through the wargames. However, I did find the lecture videos to be very engaging, and honestly would've liked to see more of them (perhaps 2 hours instead of 45-60mins). Despite how intimidating 'hacking' and the surrounding concepts are, they were introduced in a way that was easily digestible and encouraged me to do extra learning.

From my own research, the extended lectures, and extended wargames (more thoroughly covered in each weekly blog), I learned about:

- Types of web exploitation vulnerabilities and how to prevent / defend against them them (SQLi, command injection, directory traversal, XSS and CSRF – generally through filters and proper input sanitisation)
- Two types of binary exploitation and how to defend against them (buffer overflow – proper stack checking via canaries and bounds and format string vulnerability – do not pass strings directly e.g. use %s)
- The inner workings of files (file signatures, file formats and metadata) and how to recover deleted files
- Wireshark
- Relevant commands for forensics (**xxd**, **scalpel**)
- Rootkits, preventions and consequences
- How reverse engineering can be used maliciously and how it can defend against malware
- Cutter and Ghidra
- Dynamic vs static analysis

For the OTW wargames, I learned about / became more familiar with:

- How the DOM is structured
- How cookies are relevant to websites
- Accessing and manipulating cookies (via the browser and via scripting)
- Reading the DOM
- Robots.txt
- Spoofing HTTP referrer
- Reading and understanding source code written by others
- PHP
- Python scripting (via the requests library)
- How URLs are structured (in particular, manipulating directory traversal and parameters)
- URL encoding
- Bash/Shell commands and using them to manipulate
- XOR encryption
- XSS on PHP
- Hex editing
- SQLi
- POST and GET requests
- HTTP headers, request headers
- And last but not least, Googling :)

Web exploitation (SQLi and XSS) were the most enjoyable sections and forensics, reverse engineering and binary exploitation were all pretty much equal second.

As mentioned previously, these wargames encouraged critical-thinking, problem solving and surprisingly, patience. While these aren't exactly tangible, and are hard to measure, I definitely feel like I will leave the course with a different mindset, along with the technical skills gained.

Something Awesome Project

z5205522 Alan Trieu COMP6441

Challenges

The majority of the challenges I faced were definitely in the wargames – both from COMP6841 and OTW. Right from when I began Natas, I had trouble completing the levels by myself, and had to resort to guides. I conveyed this concern to Josh, who reassured me that this was expected. Little did I know that the whole 'resorting to guides' theme would recur throughout the entire project.

Towards the end of the project (essentially up until just now), I have been concerned about not being able to complete Natas. While I was told that this also was expected, I still wanted to push myself to finish Natas34. Unfortunately, I only completed Natas26. While objectively, I think this is decent considering the time frame, but regardless, the project doesn't feel completely satisfying knowing that I still have a few levels left.

My weekly blogs (linked below) and the wargame blogs convey my challenges in more detail. But something I wanted to highlight was my challenges with Narnia. Unlike Natas, where Google searching covers my lack of prerequisite web knowledge, I felt a bit overwhelmed with Narnia. It seemed like binary exploitation relies more heavily on a strong foundation of low-level knowledge. Because of the difficulty I had with Narnia0 and Narnia1, I decided to cut it off short and end it there.

In terms of the Natas levels, what I found most frustrating was my lack of technical skills to competently complete the level fully. I found that I was usually able to correctly identify the correct steps and methods needed to solve them but fell short due to being unable to follow those steps and methods, being blocked by not knowing to do something, even with the help of Google. This left me with no choice but to consult guides. Often, the correct action was something obscure that even with a few more hours of Googling, I would not have been able to do it (e.g. using bash commands or scripting).

While time wasn't a pressing issue, it would have been nice if I had started earlier than the middle of Week 4. This was due to being indecisive about my project (the website minigame idea mentioned earlier).

Also, not a particularly grave concern, but without a proper marking guide at the beginning, I felt like I wasn't doing enough – luckily my tutor gave reassurance.

What I Would Have Done Differently

- Timed all my activities to create a graph of the average time spent, and find the total hours spent on the project
- Start earlier
- Considered using a structure for the wargame blogs
- More clearly shown what I learnt from the wargames in my weekly blogs (they were more focused on the lectures)

Highlights & What I Thought I Did Well

- Time management (wasn't too ambitious with my learning goals – minus trying to complete a giant bulk of OTW initially…)
- Planned well enough to allow myself to comfortably see what I needed to do next, but enough up in the air to flexibly add and remove things without too much of a Domino effect
- Sought a lot of criticism and feedback (at the expense of Josh's time)
- Self-critical and constantly felt the need to improve

Something Awesome Project

z5205522 Alan Trieu COMP6441

Blog Posts

- Something Awesome - Introduction - OpenLearning
- Something Awesome - Week 4 (11/03/2022) - OpenLearning
    - Something Awesome - SQL Injection Wargame - OpenLearning
    - Something Awesome - XSS Wargame - OpenLearning
- Something Awesome - Week 5 - OpenLearning
    - Something Awesome - Natas (Level 0 - Level 3) - OpenLearning
    - Something Awesome - Natas (Level 4 - Level 8) - OpenLearning
    - Something Awesome - Buffer Overflow Wargame - OpenLearning
    - Something Awesome - Format String Vulnerability Wargame - OpenLearning
- Something Awesome - Week 6 - OpenLearning
    - Something Awesome - Natas (Level 9 - Level 12) - OpenLearning
    - Something Awesome - Forensics Wargame - OpenLearning
    - Something Awesome - Narnia (Level 0 - Level 1) - OpenLearning
- Something Awesome - Week 7 - OpenLearning
    - Something Awesome - Natas (Level 13 - Level 17) - OpenLearning
    - Something Awesome - Natas (Level 18 - Level 20) - OpenLearning
- Something Awesome - Week 8 - OpenLearning
    - Something Awesome - Natas (Level 21 - Level 26) - OpenLearning
    - Something Awesome - RE Wargames - OpenLearning

My Natas Documentation

natas - Google Docs

My Video Submission

https://youtu.be/NMZVjS3DD0U