

Logbook for Matthew Lewis Cragg

Student ID 2207432

26th of June

Reading papers, researching, tried rat development 26th of June met carlene, discussed ideas

27th of June

Installed all required software, Metasploit, nmap, kali Linux and windows server in virtual box began experimenting with shell code encryption and binders 28th of June Read and researched more for articles on shell code encryption and binders. Found an article about fileless encryption

29th of June

Spent the day creating the template that will become the structure of the dissertation, and laid the framework of what each section will be

Up until 6th of July

Made the first pass of reverse shell, detection results of 34/70

7th of July

Began in writing the Introduction and Aim

10th of July

Began to explore possibilities of infected dll files, with the hope of replacing a clean dll file with malware.

11th of July

Successfully made a DLL attack, with the detection rate of 9/70

12th of July

Re-ran all attacks to gather screen shots ready for the writing, and to ensure it was all working. Wrote the Objective and Structure section of the dissertation.

13th of July

Started the literature review chapter. Wrote the introduction and two articles. Organised all literature review papers into an excel sheet, sorted in chronological order for use in writing.

17th of July

Read and collected 11 more papers for literature review, refined the section to be ready for writing

19th of July

Wrote the Crypter and Cloud Crypter literature review.

20th and 21st of July

Finished the general cyber sec research, reverse shell, trojan detection, trojan implementation, trojan defence literature review, and other methods of bypassing anti-viruses', finishing the literature review.

24th of July

Proof-read and corrected minor mistakes on literature review, added some new content.

25th of July

Began experimenting with network traffic monitoring to compare

26th of July

Measured, recorded and wrote about the network traffic and packet monitoring, adding it to the paper

31st of July

Explored the idea of bat file being used to stop detecting anti-viruses, and converting it to exe and disguising as legit.

1st of August

Compared programming languages and explained the reasoning for using C, made a table comparing the detection results and survey results.

2nd of August

Wrote out a comparison between coding languages and why I eventually used C.

Re-read and improved upon already written work, and began creating diagrams.

3rd and 4th of August

Began creating the bat file that will copy the dll file and disable Windows Defender.

Began to write the design and implementation section.

7th of August

Remade diagram for method B, the dll injection approach. Recorded a video of both attacks working.

8th of August

Researched and explored various obstruction methods, and how to deliver payloads.

9th of August

Re-recorded on local virtual machines, now showing the icon change and bat to exe conversion. Prepared to write the Design and Implementation

11th of August

Created the diagram for the structure, wrote the design and structure section.

12-18th of August

The week was spent writing the design and implementation section, as well as the testing, network analysis and correcting previous mistakes. Only the conclusion, evaluation and future developments remain.

21st of August

Finished the conclusion, future developments and wrote half of the evaluation

24th of August

Finished the evaluation. Abstract, Research Overview. Research Introduction, Methodology and one other section are left.

25th of August

Wrote the abstract section and parts of the methodology.

26th of August

The research sections were written out.

27th of August up until the 1st of September

Since the majority and bulk of the writing had been finished, the remaining amount of time was spent improving, fixing spelling mistakes, and adding extra content in chapters that looked sparse.

1st of September

Uploaded the first draft to Turnitin.

2nd of September up until the 5th of September

Continued to re-read and fix errors.

9th of September

Sent the draft to Carlene, and fixed errors pointed out by Carlene, and improved the formatting.

10th of September

Created and added the first two cover pages, ready for submission.