KV6003 Individual Computing Project - Terms of Reference

Carl Slatter

16th November 2020

1 Background

The modern technological landscape demands much from innovation. We must find new ways of solving existing and new problems in the world. This is amazing for convenience, and quality of life, but does pose a problem for security. There is Hypponen's law in IOT that states, the more you add in terms of functionality, the more that must be secured. A concrete cube may be secure, but is not overly functional. I am incredibly interested in the duality between attack and defence. It seems to be a constant cat and mouse game of which defence is paramount. I hope that by looking at both sides with a purple team perspective, I can gain a deep understanding of the landscape we have currently and moving forwards.

Cyber-Security is really "Managed insecurity", I intend to discover where cyber attacks are at, and how they have innovated over the years. Cyber threats are growing, how can be detect them? How can we proactively block them? These are questions that must be answered in order to get a good overview. I must be able to show my understanding in a theoretical and practical way to be able to potentially apply it to a real life scenario. I will have to develop my understanding of infrastructure, networking, semi low-level programming and penetration testing.

Developing realistic solutions for smaller businesses is really important. They are arguably more at risk, with less resources for security. The is a culture of security snake-oil and scare-ware, and supposed all-in-one solutions rather than defence-in-depth. This is evident in the numerous adverts that claim much and deliver little. With the detection work, I hope to show the importance of the human element to security, how it can be the weakest link, or the strongest asset. I must look at current solutions with a critical eye with care to be realistic about defence.

Malware has evolved over time, what was once an exercise of freedom and curiosity, is now a platform for theft and crime. Defences catch up over time, it will be eye-opening to see the different methods historically that the two sides try to out-smart each other. Malware analysis is something I haven't really touched on before, though I have be interested for a long while now. It will benefit my defence greatly.

2 Proposed Work

I aim to create documentation in the form of my dissertation to describe the Cyber-Security landscape in regards to infrastructure. This will involve talking about infrastructure directly, it's use, implementation and potential pitfalls, but more importantly, how it can be secured. On the other side, I will be looking at the common ways that infrastructure is compromised, in a network setting. I do think that a good comparison is important for this.

I will be investigating how threats have evolved as a whole, whether that be malware, obfuscation and clever exfiltration. I believe it is important to at least touch on how this was done in the past, to understand how the future may follow similar foundations. Naturally an investigation into threats would be pointless without a practical defence, I hope to compare both endpoint and infrastructure defences in relation to both a sample of threats, and to one another. I will then analyse this data and draw sensible conclusions based upon it.

I also hope to create a rudimentary intrusion detection system written in C. This will be a proof of concept to show my understanding, rather than a product. My hopes are that by developing network defence myself, I can gain an even deeper understanding.

3 Aims and Objectives

3.1 Aims

To understand the theory behind defence in relation to common threat vectors. To develop attack and defence to aid the theory, in a practical manner.

3.2 Objectives

1. **Analysis of historic threats and malware**
2. **Analyse modern attack:defence landscape**
3. **Explanation of entry vectors and profiling**
4. **Explanation of exploitation**
5. **Explanation of obfuscation**
6. **Explanation of exfiltration**
7. **Investigate IDS/IPS systems w/ comparison**
8. **Illustrate proof of concept IDS**
9. **Investigate antivirus systems w/ comparison**
10. **Discussion of meaningful defence (defence-in-depth, social engineering resilience)**

3.3 PoC IDS Objectives (It must..)

1. **Detect network interfaces**
2. **Bind to a network interface**
3. **Capture data and output to a file/standard output**
4. **Flag up unusual activity from a few notable attack types**
5. **Control via command switches**
6. **Be well written and meaningful to the idioms of the language**
7. **Have testing/design documentation**

4 Skills

- Programming in C (KF5006)
- Networking Technology 3 (KF6005)
- Advanced Operating Systems II (KF6003)
- Cyber-Security Awareness
- Reverse-Engineering
- Data Analysis

5 Resources

5.1 Hardware

- Dedicated high RAM machine - Already bought
- Lab Machines for possible testing

5.2 Software

- CIS Lab Equipment - Routers, Switches, Virtualised Hardware etc.. - Covid contingencies may mean I have to downscale for my own setup
- VMware Workstation - To host vulnerable and attacker infrastructure
- VScodium - IDE for IDS development
- Packet Libraries - unsure about specifics at the time of writing, likely scapy and libpcap
- Various Antivirus Licences - Prefer free or monthly subscription
- IDS/IPS/SIEMs Licences - Will have to prefer free or cheap ones (as a small company would)
- Malware Samples - Sourced from Github collections
- Operating System Distributions - Obtained online

6 Structure and Contents of the Report

6.1 Report Structure

Introduction - This chapter sets out the basis of the project, the motivations behind it and what I am looking Investigate. It will summarise the whole project.

Analyse historic & modern defence - This chapter is a broad overview of the cat and mouse game, with a focus on how both sides evolve over time, and how to tip the scales in the defences favour. Analysis of IDS/IPS & AV technologies, in sub sections.

This chapter then covers cases of past incidents, how they happened, why they were effective and what we can learn from them for modern day. I will cover, emotet, loverletter, heartbleed, wannacry among others.

Does this need to be split?

Explanation of entry vectors and profiling - This chapter covers the idea of what a vulnerability is at it's core, how they are found and the commonalities among vulnerabilities. It will include the discussion of tools like NMAP, vulnerability scanners like OPENVAS, nikto, wpscan, sqlmap and nessus.

Explanation of malware mechanisms - This chapter covers the common mechanisms of exploitation and stealth that malware makes use of. This includes the use of obfuscation, encryption, exfiltration and the impacts they have. This covers a description of the methods, rather than historic implementation

For the terms of reference it isn't necessary, in the analysis they will want their own sections in the chapter. – Alun

Investigate IDS/IPS systems w/ comparison - This chapter is to lay out my experiment methodology, why I did what I did, what I'd expect vs what I got and an analysis of the results themselves.

Analysis of my PoC IDS - This chapter describes my motivation for creating this, how I went about it and how it operates.

Synthesis of my PoC IDS - I will talk about what can be learned from it, in relation to the scale of commercial products.

Investigate antivirus systems w/ comparison - This chapter is to lay out my experiment methodology, why I did what I did, what I'd expect vs what I got and an analysis of the results themselves.

Discussion of meaningful defence (defence-in-depth, social engineering resilience) - This chapter encompasses what can be done to aid defence to it's maximum. I will focus on defense in depth and diversification of defence mechanisms. Topics include, proper training, access control, security positive culture, adequate funding, regular security testing, development infrastructure and a wide variety of hardware solutions.

6.2 Conclusion

This will summarise all that was found, how it relates to what I set out to discover and what it means for the future of defence.

6.3 List of Appendices

- ToR
- Experiment and PoC Design/Testing
- IDS Source Code
- Experimentation Result Documentation
- Risk Assesment
- Ethics Form

7 Marking Scheme

The marking scheme sets out what criteria we are going to use for the project.

Project Type: General Computing

Project Report

Analysis

- Analyse historic & modern attack/defence landscape - Analysis of liturature
- Explanation of entry vectors and profiling
- Explanation of malware mechanisms
- Analyse PoC systems & technology used

Synthesis

- Illustrate proof of concept IDS & implementation
- Investigate IDS/IPS systems w/ comparison
- Investigate antivirus systems w/ comparison

Evaluation

- Discussion of meaningful defence
- Conclusion

Product

- Dissertation Paper
- Experiment and PoC Design/Testing
- IDS Source Code
- Experimentation Result Documentation w/ Metric Justification

Fitness for Purpose

- There must be analysis of both sides
- There must be comparison of feasible solutions
- The program must be functional to a proof of concept level

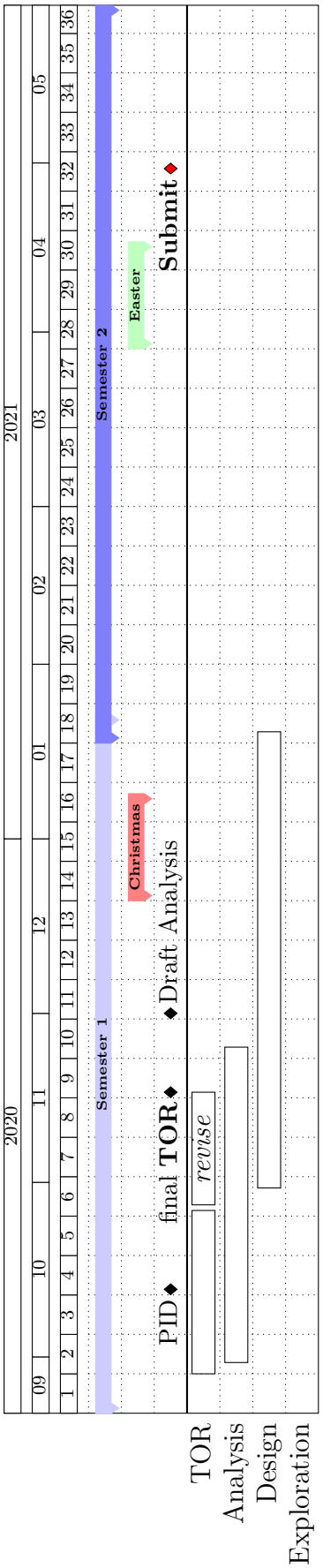
Build Quality

- Experiment design quality
- Code quality & testing
- Quality of analysis & synthesis
- Quality of meaningful mitigation

slight issues with page gaps - not sure if it matters - carl

Don't worry about page breaks, fixing bad ones is something to do at the very end – Alun

8 Project Plan



9 Ethics Form

Ethical category of project *[Complete after approval]*	
Red	☐
Amber	☐
Green	☐

Department of Computer Science and Digital Technologies

UNDERGRADUATE COMPUTING PROJECTS: ETHICS REGISTRATION AND APPROVAL FORM

Section One: Registration *[To be completed by student]*

Title of research project/dissertation	
Researcher's name	
Programme of study	
Academic Year	
Module code	
Supervisor's name	
Second marker's name	
Start Date of Project	

Brief outline of research topic:

Short description of proposed research methods including identification of participants:

Ethical considerations in the research project	YES	NO
1. Does your research involve an external organisation or partner?	☐	☐
2. Does your research involve human participants?	☐	☐
3. If yes to Q.2, will you inform the participants about the research?	☐	☐
4. Will you obtain their consent using the standard consent form?	☐	☐
5. Is any deception involved?	☐	☐
6. Do any participants constitute a 'vulnerable group'? (refer to definition of Vulnerable People)	☐	☐
7. Will the research involve the following information?		
Commercially sensitive	☐	☐
Personally sensitive	☐	☐
Politically sensitive	☐	☐
Legally sensitive	☐	☐
8. Is the research likely to have any significant environmental impacts?	☐	☐
9. Are there likely to be any risks for the participants in your research?	☐	☐
10. Are there likely to be any risks for you in conducting the research?	☐	☐
11. If yes [to 5, 6, 7, 8, 9 or 10 above] have you identified steps to address the issues and mitigate any risks to participants, yourself or the environment?	☐	☐

Statement to explain how any issues identified above will be addressed and what steps will be taken to mitigate such risks or adverse impacts

Ethical category of research project
Based on the above Ethical Considerations and with reference to the University's Ethical Scrutiny Risk Assessment tool identify the Ethical category of your research project (refer to http://www.northumbria.ac.uk/static/5007/respdf/riskassesmenttool for further guidance):

[Please tick as appropriate]

Red	☐	vulnerable participants; human tissue; sensitive data; risks to participants & researchers etc.
Amber	☐	human participants requiring informed consent; commercially sensitive information etc.
Green	☐	no participants involved; secondary data only; no sensitive data

I have read the University and the Faculty Ethics Policy and Procedures and confirm that the answers I have given above are correct. Where issues arise under items 5, 6, 7, 8, 9 or 10 [above] I have described in writing how I intend to approach these issues in the research.

Researcher's signature .....

Date .....

Section 1 Ethics Registration to be submitted to Principal Supervisor or Module Tutor and allocated to a reviewer as follows:

Green risk - may be approved by Supervisor
Amber risk - to be submitted for approval by one independent reviewer (second marker)
Red risk - to be submitted for approval by two independent members of Faculty Research Ethics Committee

10 Risk Assessment Form

Risk	Mitigation
Malware reaches internet, and spreads into the wild	No direct internet access
Malware breaches hypervisor	Dedicated ESXI machine or live cd with disconnected drives (if at home). Modern and up to date hypervisor that is ring 3. Disabling of VMware tools. Defense in depth
Malware reaches local network	Use of virtualized custom network (no bridged!)
Malware persists on VM	Reverting to earlier snapshot / Scrubbing drive
Malware spreads in transit	Encrypted zips with password
Malware reaches router	No connected network cables or WIFI, static addressing
Malware spreads to shared folders	Avoid use of shared folders, have samples encrypted on snapshot, no downloads needed.
Malware detects VM, does not run	Install common apps, artificially use pc, increase RAM, remove additions/VMware tools, fake internet server (steps needed to bypass average VM checks)
Attacks act on the wrong target	All attacks will be done inside the virtualized network, that cannot reach the outside, this includes potential Kali/parrotOS. I will have a defined addressing scheme as part of the experiment