A: Applicant details

Your Name	PATRICK COLLINS
Student/Staff Number	1900609
Abertay email address	1900609@abertay.ac.uk
Name Of Programme (if applicable)	Evaluating the Effectiveness of Using a Modifiable Ransomware Simulation Tool
Module code	CMP400
School	School of Design and Informatics (SDI) Required
Is this a revised re-submission?	Yes Required, feedback is available in the 'View Notes' section
Supervisor email address	s.rathore@abertay.ac.uk

A2: Resubmission details

Revision details	Instead of using the Hacklab network, Virtual Machines(VMs) will be used for developing and testing features of the ransomware simulation tool such as the replication. These Virtual Machines will also be used for evaluating the effectiveness of all ransomware simulation tools (The Project Artefact and currently existing ransomware simulation tools).

B: Project details

Project title	Evaluating the Effectiveness of Using a Modifiable Ransomware Simulation Tool
Main aim of project	It's the main aim of this project to develop a ransomware simulator that successfully combines all of ransomware's features into one tool. If the simulation tool effectively covers all aspects of ransomware, then a user can be confident it will be an accurate measurement of their network/host security against a ransomware attack. Furthermore, this project plans to enable the user to modify certain features of the ransomware simulation. Such as the encryption algorithm and file extension used for each simulation scenario. By doing so we can better simulate zero-day ransomware attacks and improve detection and security against them
Proposed start date	07/11/2022 Required
Proposed end date	09/05/2023 Required
Site of research	Abertay University
What is the nature of this research?	○ Reviewing existing non-ethically sensitive literature ○ Reviewing existing literature which may be considered ethically sensitive ○ Non-ethically sensitive practical research ◉ Ethically sensitive practical research Required Ethically sensitive research: anything involving humans, including surveys, interviews and samples; collection of data deemed 'sensitive' according to GDPR rules; animal subjects requiring Home Office license; genetic modification; computer "hacking" on anything other than your own systems or those provided specifically for that purpose (such as Hacklab systems). Practical research: all research involving observations and measurements, including practical work, experiments, surveys, fieldwork, interviews, etc. NB any research project that is not

based exclusively on analyzing previously published data is defined as a 'practical' project.

C: External projects (if applicable)

Name of external body

Status of external application

- ○ Not yet applied for
- ○ Approved
- ○ Pending
- ○ Declined
- ○ External ethical approval not required

External ethics application reference

Date approved (if applicable)

D: Studies involving animals or biological samples, human participants

Special issues with biological samples

- ☐ D1. Research involving animals of a type requiring a Home Office licence
- ☐ D2. Research involving genetic modification (GM)
- ☐ D3. Research involving stored human samples, for example organs, tissues, cells (excluding established cell lines)

Does the project involve human participants in any way, including surveys

No

Required

E: Studies with human participants

Tick all statements that apply

- ☐ E1. You will describe the main experimental procedures to participants in advance, so that they are informed about what to expect
- ☐ E2. You will inform participants that their participation is voluntary
- ☐ E3. You will obtain explicit informed consent for participation
- ☐ E4. If the research is observational, you will ask participants for their consent to being observed
- ☐ E5. You will tell participants that they may withdraw from the research at any time and for any reason
- ☐ E6. With questionnaires you will give participants the option of omitting questions they do not want to answer
- ☐ E7. You will tell participants their data will be treated with full confidentiality and that, if published, it will not be identifiable as theirs unless they explicitly consent to be identified.
- ☐ E8. You will comply with all GDPR requirements outlined in the Universities policy document
- ☐ E9. You will debrief participants at the end of their participation (i.e. give them a brief explanation of the study)
- ☐ E10. You will NOT deliberately mislead participants in any way
- ☐ E11. Your study will NOT involve a significant risk of participants or researchers experiencing either physical or psychological distress or discomfort

If any statement is NOT ticked, you must ensure that the reasons for this are made explicit in Section G

E12. Will the project involve members of any special groups listed below, or another vulnerable group?

- ☐ Children (under 16 years of age)
- ☐ Schoolchildren of all ages
- ☐ Any person who may have difficulty understanding information provided to them
- ☐ Patients
- ☐ People in custody
- ☐ People engaged in illegal activities (e.g. drug taking)

If another vulnerable group not listed here is involved, please enter that in the "other" box

F: Studies not involving human or animal participants or samples

Please describe briefly how you would plan to execute your project, giving details of your proposed methodology	The project's effectiveness will be evaluated using a quantitative approach against other ransomware simulation tools using the detection tool Snort. Rules will be created in Snort to detect ransomware behaviour on the network and system. The ransomware simulation tool created in this project and other existing tools will then be tested against these rules to gain data on the detection rate. The data of the detection rate will be compared to get the effectiveness of each tool. Statistical graphs will display this data and the findings of each tool.

G: Details of proposed research (if applicable)

G1. Aims of study and rationale	Many of the existing ransomware simulators aren't actually simulating how ransomware behaves effectively. It's important to carry out this project to know the current state and direction we are going in with ransomware simulators. If we are going in the wrong direction, then any individual who decides to deploy these simulation scenarios to test their security will be given a false security assessment and critical flaws in the network security will be overlooked leading to more ransomware attacks to occur. If successful, this project will provide a guide for future developers on how to effectively design and implement a ransomware simulation tool. Hopefully improving upon the one developed in this project. The project will also identify if the idea of a ransomware simulation tool itself is flawed and should not be used or continued to be developed in the

	future.
G2. External Partners	N/A
G3. Expertise	N/A
G4. Participants	N/A
G5. Materials and/or apparatus	N/A
G6. Procedure	Literature Review The project will begin with literature research and review on ransomware simulation tools and ransomware features to aid in the Project Development and further understanding of the project area. Project Development The ransomware simulation tool will be coded in the programming language C++ following the project plan outlined in the Gantt chart in the feasibility demonstration. Ransomware Detection For the detection of the ransomware simulation tools, the network intrusion detection tool Snort will be used. Evaluation The project's effectiveness will be evaluated using a quantitative approach against other ransomware simulation tools using Snort. Rules will be created to detect ransomware behaviour on the network and system. The ransomware simulation tool created in this project and other existing tools will then be tested against these rules to gain data on the detection rate. The data of the detection rate will be compared to get the effectiveness of each tool. Statistical graphs will display this data and the findings of each tool.

H: Ethical issues

What ethical issues (if any) does your project raise? How will you mitigate against these ethical issues?	Personal data on the computer system will be temporarily encrypted using an encryption algorithm when the user runs the encryption feature of the ransomware simulation tool. The user will be able to select which data they wish to encrypt and only the selected data will be encrypted. The selected encrypted data can be decrypted at any time by the user running the decryption feature of the ransomware simulation tool. Also, a countdown timer is planned to be implemented to automatically decrypt the data without the user having to run the decryption process. Each ransomware feature implemented will be split up and have to be run individually. The decision for doing this is to avoid the sample becoming a live sample that may harm the system. Virtual Machines(VMs) will be used for developing and testing features of the ransomware simulation tool such as the replication. These Virtual Machines will also be used for evaluating the effectiveness of all ransomware simulation tools (The Project Artefact and currently existing ransomware simulation tools).

I: Confirmation/declaration

I confirm that

- ☑ I am aware I need to submit a Risk Assessment and will do so before commencing the proposed study. Note, all studies except Literature Reviews must complete an appropriate risk assessment prior to commencing the study. (Note: you must follow whatever procedures your School has in place for the review and approval of risk assessment. Students should seek advice from their supervisor).
- ☑ I have read and understood Abertay University's policy on research ethics (see document 'Research Ethics at Abertay' on the Research Ethics intranet webpage), the Abertay University Health and Safety Policy, and any equivalent School Policy.

- ☑ For each working location (including university facilities and my home), I will identify what to do and who to contact in case of emergency, and will make myself aware of any existing safety, First Aid or emergency procedures.
- ☑ Any data collected from experiments will be stored securely within a week in Abertay University facilities following the guidance set out in the University's Data Storage Policy.
- ☑ I understand that it is my responsibility to ensure compliance with any relevant regulatory or legal requirements (such as data protection legislation, stored tissue regulations, animal experimentation licensing, etc).
- ☑ The proposed study will not discriminate against participants on the grounds of race, sex, religion or belief, sexual orientation, disability, pregnancy and maternity, gender reassignment, marriage and civil partnership, and/or age.
- ☑ I have completed all sections of this form fully and accurately
- ☑ I understand that should I receive an Approval with Specific Conditions, I will need to comply with the Conditions set out in the Decision email
- ☑ I understand that should my application not be Approved, I will not be permitted to conduct any work on my proposed project. (In such circumstances a revised or alternative application should be submitted.)
- ☑ I understand that should I subsequently amend my study after approval has been given I will inform the ethics committee of the change, and that changes that materially affect the study may require a further submission for ethical approval.

Please also confirm that either

- ◉ 1: Your supervisor will approve any materials that you provide to human participants before use (e.g. consent forms, questionnaires, interview questions). The supervisor will be sent a copy of this form to approve before further processing.
- ○ 2: This is a staff project, no supervisor involved

Have you included (if applicable to your project)?

- ☐ PIS/Consent form (see GDPR-compliant template on internet)
- ☐ debriefing form (or equivalent description of verbal debrief)
- ☐ proof of external permissions

- ☐ letters to parents/children/head teachers etc. Full interview/focus group schedule
- ☐ confirmation of PVG approval (written – please do not attach PVG)
- ☐ adverts/flyers for participants