SUMMER RESEARCH 2023/24
PROJECT ABSTRACT

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

PROJECT #30

SUPERVISOR/S:	Marinho Barcellos
PROJECT TITLE:	New Zealand and Australia on the telescope: lessons and opportunities via cybersecurity Internet measurements
FIELD:	Computing Science
DIVISION/SCHOOL:	HECS | School of Computing and Mathematical Sciences
PROJECT LOCATION:	Hamilton
PAPER CODE:	HECSS373-23C (HAM) (TGA)

PROJECT ABSTRACT:

Networks normally expose a set of services (e.g., Web, e-mail) to the rest of the Internet. This is how, for example, the website of the University gets accessed by external users or some e-mail is received from the outside. An organisation's services are supposed to be accessed by the world outside, but on the other hand, they represent an opportunity for miscreants to find vulnerabilities and perform attacks. In this context, it's essential to detect problems early. Internet-wide scanning is a technique that has helped researchers uncover real-world attacks and can help assess the security posture of an organisation's network. One current research thrust explored at the CROW Lab, part of the School of Computing and Mathematical Sciences, is using scanning measurements to perform a census of security practices and the posture of networks in New Zealand. This investigation was initiated via a dissertation in the Masters of Cybersecurity (MCS) and continued via an SRG in 2022-2023.

The proposed project aims to expand the study to include Australia in the current cybersecurity measurement census. By measuring both New Zealand and Australia ("sighting them on the telescope"), we will be able to compare the countries in terms of security practices in their networks and understand better differences and similarities. Since the AU Internet ecosystem is more developed than the one in NZ (around ten times larger), there are lessons to be learned which would benefit Aotearoa's cyberspace. The measurements are underway, so that the student will have the datasets ready to work on from the get-go. The student's tasks consist of sanitising, filtering, structuring, and analysing/correlating the datasets. We will develop with the student a set of scientifically-robust inferences, backed by the evidence collected. The inferences will contribute to a paper to be submitted to a selective conference or indexed journal, of which the student will be invited to co-author. The research does not involve human beings or animals, but Ethical approval has been sought and granted already. The student will have the opportunity to learn many valuable lessons. The lessons include: the specifics of research on Internet scanning; the tools used to process network data obtained from scans; improve analytical skills, which are needed for making sense of the data collected; the scientific process, writing papers, and preparing posters and presentations. The main benefit of this summer research grant will be exposing the student to the research process and motivating them to continue with higher education studies, such as joining the Masters of Cyber Security.

STUDENT SKILLS:

- Knowledge about computer networks and Internet operation
- Knowledge of Linux systems operation
- Programming skills using scripts (Python)
- Responsible attitude towards cybersecurity
- Desirable: ability to read and write efficiently and communicate clearly results

PROJECT TASKS:

- Learn the state of the art on Internet scanning, by studying and discussing the 5-10 most essential papers with the supervisor.
- Hands-on work to learn the operation of the scanning and service enumeration tools used by both researchers and miscreants, with special attention to data collected and limitations.
- Write analytical tools in Python, with libraries such as Pandas, pytricia, and Matplotlib
- Preparation of report
- Preparation of poster

EXPECTED OUTCOMES:

- Student's Research Poster (as per clause 6 of the Scholarship regulations)
- Prepare a student for measurement-based, empirical research on cybersecurity
- Set of analytical tools (scripts) that help implement the methodology to understand and compare security postures of AU and NZ based on scanning data
- Novel findings based on the application of the methodology
- Responsible release of vulnerabilities, communicating them to CERT/NZ