EDINBURGH NAPIER UNIVERSITY

SCHOOL OF COMPUTING

PROJECT DIARY

Student: Andrew Rocke **Supervisor: Petros Karadimas**

Date: 16/11/2024 **Last diary date: 08/10/2024**

Objectives:

Initial Report – consists of above 2000 word literature review, that consists of 3 paragraphs: ICS, IDS & ML. Gannt Chart

Progress:

Researched the Machine Learning topic, lots of good papers on machine learning. Found the excellent paper identifying pitfalls

@inproceedings{arp2022and,
title={Dos and don'ts of machine learning in computer security},
author={Arp, Daniel and Quiring, Erwin and Pendlebury, Feargus and Warnecke, Alexander and Pierazzi, Fabio and Wressnegger, Christian and Cavallaro, Lorenzo and Rieck, Konrad},
booktitle={31st USENIX Security Symposium (USENIX Security 22)},
pages={3971--3988},
year={2022}
}

Identified Random Forests for Binary Classification and decided to base experiment on this

Manages to run Snort on a PCAP using community Rules

Supervisor's Comments: