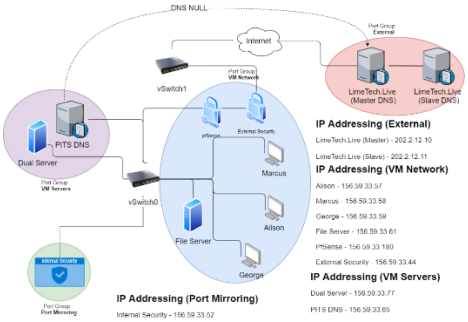
Linux Threat Analysis: Digital Corpora

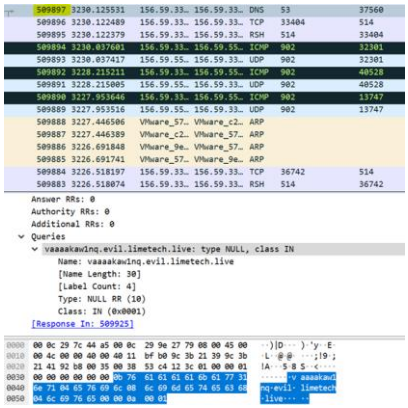
Diamond Zhou *Philip Machado* *Oliver Whitehead* *Thamena Essahaty*

Supervisor: Sandeep Vankadari **Client:** Paul Bryant



Scenario Environment Topology

Project Team Logo



A Produced Packet Capture

INTRODUCTION

The Linux Threat Analysis project was undertaken to address a shortage of scenarios available to teach about the analysis of digital artifacts left on UNIX systems following security incidents. It was initiated as an effort to provide WelTec courses with educational material that could be used in refining and assessing the forensic skills of cybersecurity students. The project also had the potential to contribute to Digital Corpora, a global repository of datasets used in computer forensics education research.

The project team's aim was to design a realistic, computer-based crime, set up a virtual environment for that crime to take place in, and simulate that crime - capturing traces left by attacker and victim alike in evidence files that students could learn to examine with tools and techniques of their choice.

DEVELOPMENT

Once our bid was approved, we explored the purpose and possibilities of the project in a system proposal. This proposal set many key decisions in stone, including our technical methodology, Scrumban – an iterative approach that divided development into sprints.

Our first sprint concerned research, analysis, and design. It was here that we drilled down our crime – the theft of confidential company data by a malicious insider. We hashed out the details of involved devices, fictional personas, digital artifacts, and exploits. Our main sprint objective was to have a conclusive event timeline that told about the who, what, when, where, and how of our scenario.

After delivering our design, we then brought it into reality, pulling through following almost four weeks and one benevolent milestone extension. The implementation involved configuring Kali, CentOS, Ubuntu, and SecOnion virtual machines hosted on vSphere and VMWare.

Our topology was ambitious, forcing us to put our heads down and overcome new and unforeseen challenges. At the sprint's end, we had various workstations, two functional DNS servers, a file server hosting remotely mountable shares, caching proxy server, network monitoring box listening on a mirror port, domain blacklist, firewall, IDS, and dual-purpose central logging/mail server.

In our final iteration, we then simulated our scenario over multiple days and captured traces of our actions in memory, over the network, and on disk. Investigative questions for students and supplementary material for instructors were then developed to accompany our evidence files, altogether comprising the major anticipated products of our project.

CONCLUSION

The Linux Threat Analysis project has reached all planned milestones thus far and is in the final stretch leading up to closure. In spite of all we have recently learnt about the unreliability of plans and expectations, we still anticipate the achievement and delivery of major project outcomes to our Client by then.