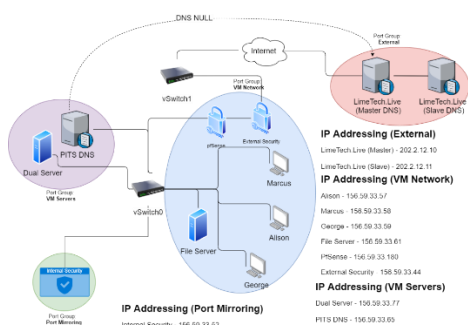


Diamond Zhou *Philip Machado* *Oliver Whitehead* *Thamena Essahaty*
Supervisor: Sandeep Vankadari **Client:** Paul Bryant



509097	3230.125531	156.59.33.156.59.33.	DNS	53	37560
509096	3230.122489	156.59.33.156.59.33.	TCP	33404	514
509095	3230.122379	156.59.33.156.59.33.	RSH	514	33404
509094	3230.122347	156.59.33.156.59.33.	UDP	962	33201
509093	3230.074717	156.59.33.156.59.33.	UDP	962	33201
509092	3228.215211	156.59.33.156.59.55.	ICMP	962	40521
509091	3228.215085	156.59.55.156.59.55.	UDP	962	40528
509089	3228.215044	156.59.55.156.59.33.	UDP	962	13747
509089	3227.953516	156.59.55.156.59.33.	UDP	962	13747
509088	3227.446506	Vhware_2.Vhware_2.	ARP		
509087	3227.446389	Vhware_2.C.Vhware_7.	ARP		
509086	3226.091468	Vhware_2.C.Vhware_7.	ARP		
509085	3226.091741	Vhware_2.C.Vhware_9.	ARP		
509084	3226.518197	156.59.33.156.59.33.	TCP	36742	514
509083	3226.518074	156.59.33.156.59.33.	RSH	514	36742

```
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

Queries
  ✓ vasaandnq.vh1.linetech.live: type MALL, class IN
    Name: vasaandnq.vh1.linetech.live
    [Label Length: 30]
    [Label Count: 4]
    Type: MALL PR (0x0001)
    Class: IN (0x0001)
    [Response IN: 509925]

0000 00 0c 29 7c 44 a5 00 c0 11 bf b9 bc 27 79 08 00 45 00 |J|D...|9;E
0001 24 92 58 0d 00 00 00 00 35 43 02 43 00 01 00 00 00 |A-9.8.8.8
0002 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....E
0003 67 73 04 a5 76 00 c0 00 60 c0 6d 65 74 65 63 00 00 |vsaandnq.vh1.linetec
```

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.