TONI VALDEZ

Cybersecurity Project Portfolio

Master of science Cybersecurity
PhD Student in Cyberpsychology

Threat Detection . Digital Forensics. Incident Response

www.tonidanielle.org

Professional Profile

Professional Summary

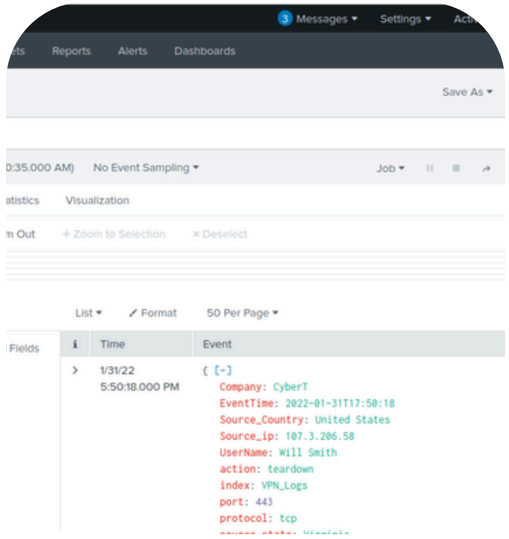
I am a cybersecurity professional with a Master of Science in Cyber security and hands-on experience in threat detection, digital forensics, security monitoring, and incident response through academic projects, technical labs, and independent study, I have developed practical experience using tools such as Splunk, Wireshark, Nmap, Snort, and CrowdStrike.

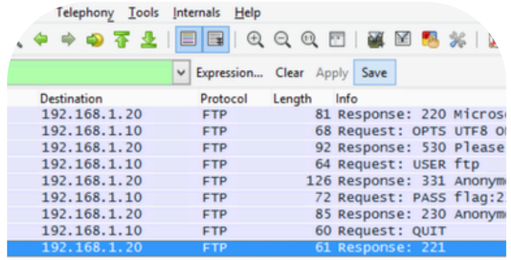
Currently pursuing a PhD in Cyberpsychology, my research interests focus on the relationship between technology, human behavior, and cybersecurity.

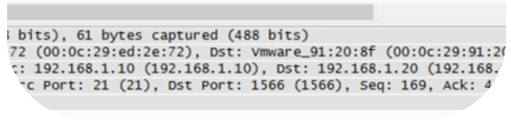
Technical **Skills**

Technical Competencies

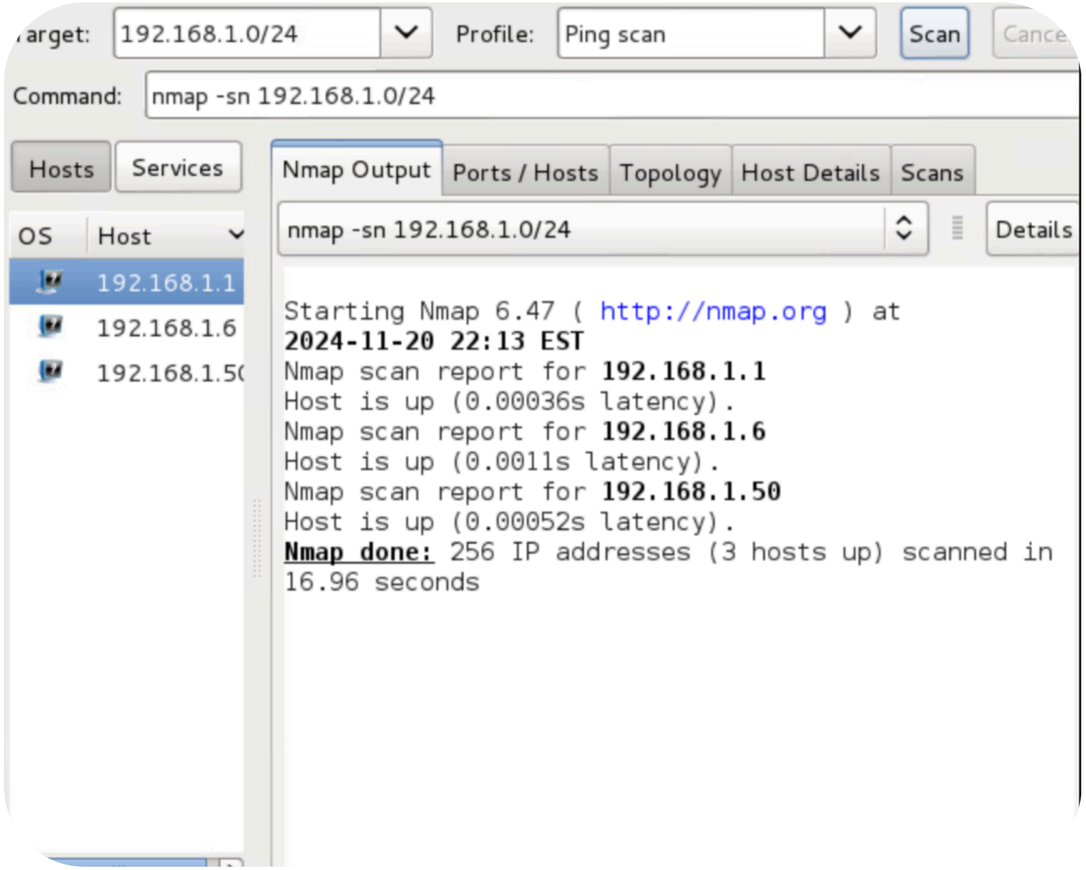
My technical experience includes security monitoring, threat detection, digital forensics, incident response, and network analysis. Through graduate coursework, independent study, hands-on labs, and cybersecurity projects, I have developed practical experience working with industry tools and security frameworks.







Network Enumeration with NMAP



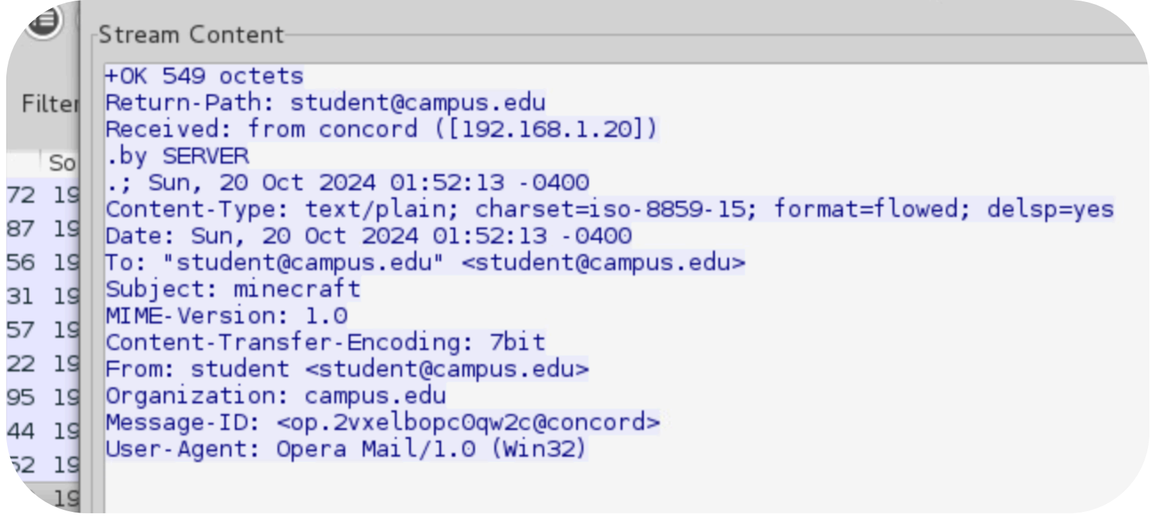
Project Overview

This project involved performing network discovery and host enumeration using Nmap to identify active devices, open ports, and available services. Scan results were analyzed to assess network visibility and identify potential security risks.

Skills Demonstrated:

- Network Enumeration
- Reconnaissance
- Vulnerability Identification
- Network Analysis

Email Traffic Investigation

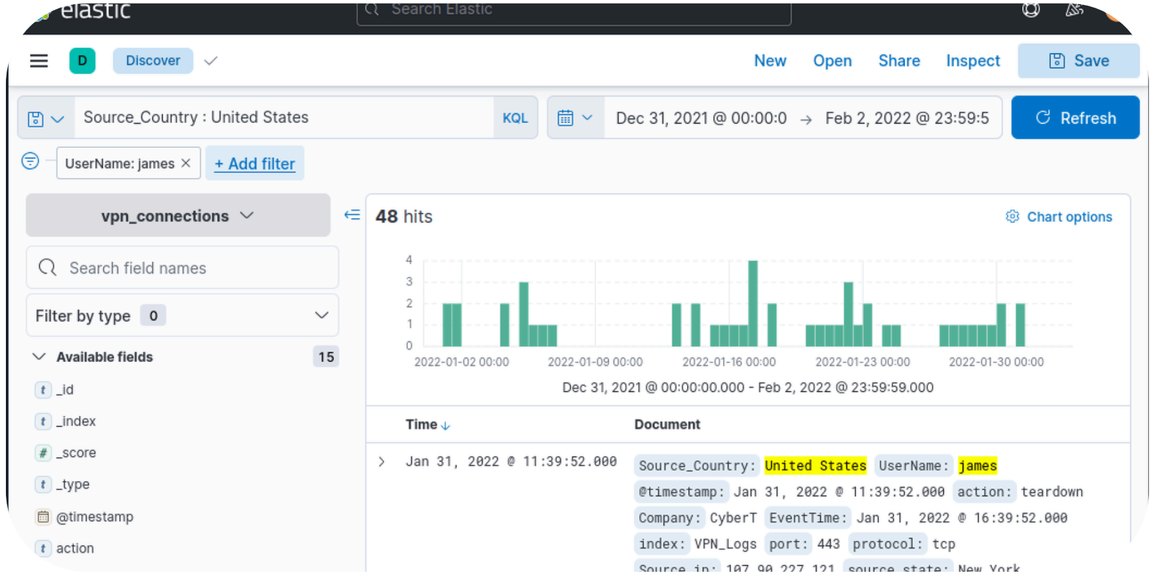


Project Overview

This investigation involved analyzing network communications using Wireshark to reconstruct email traffic and examine packet data. Network streams were reviewed to identify communication patterns and understand transmitted information.

Skills Demonstrated:

- Packet Analysis
- Network Traffic Investigation
- Wireshark Analysis
- Communication Reconstruction



Elastic SIEM Investigation

Investigated VPN logs and security events using Elastic SIEM to identify suspicious activity and analyze event data. Log analysis techniques were used to examine user activity, source locations, and security events.

Key Findings

- Investigated security event logs
- Analyzed VPN activity
- Reviewed user event data
- Identified suspicious activity patterns

Incident Response Plan

Project Overview

Developed a NIST-based incident response plan focused on preparation, identification, containment, eradication, recovery, and lessons learned. The project emphasized documentation, response coordination, and organizational security readiness.

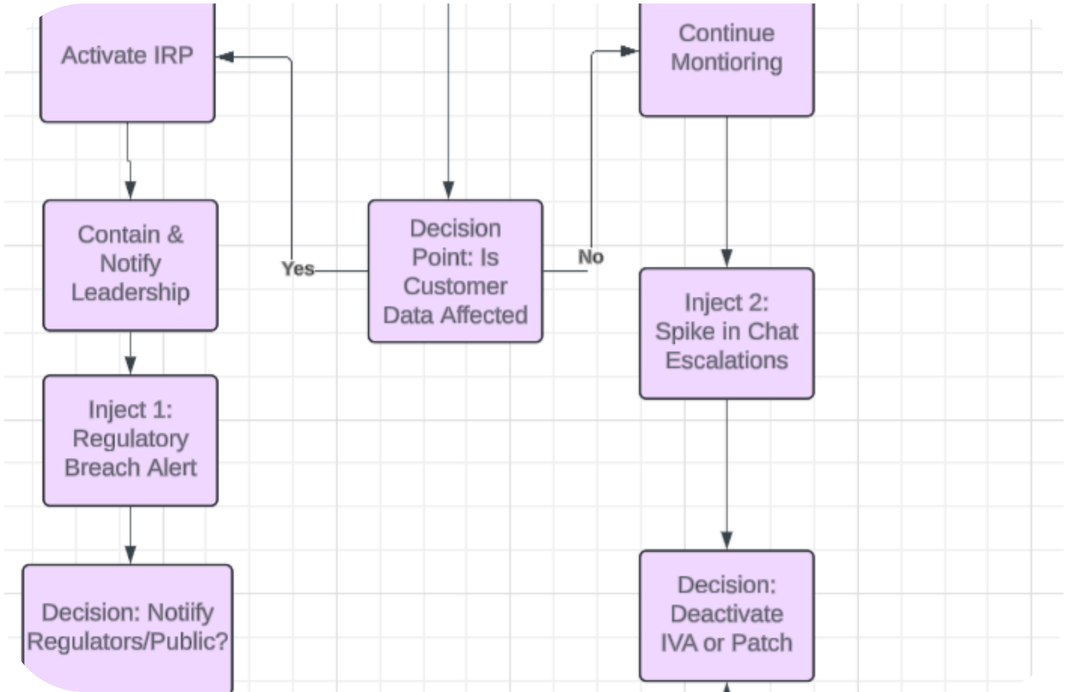
Introduction

Limetree recently experienced a security breach due to the vulnerabilities that exist within the company. These vulnerabilities would impact Limetree's operation in the future. It is imperative that these vulnerabilities are resolved to protect the security of the company. An incident response plan will be produced to help the company, and its stakeholders develop a plan of action to handle security incidents, breaches, and cyber incidents. This plan will mitigate damage, reduce recovery time, and ensure an effective response to security incidents. An assessment is conducted to determine the root cause of the security breach and assess Limetree Inc security environment. The result of the assessment is based on the interview of William Jeffries, a security manager employee by the company. These vulnerabilities are related to the security systems, personnel, administrative security, and physical security.

Examples of what caused the incident

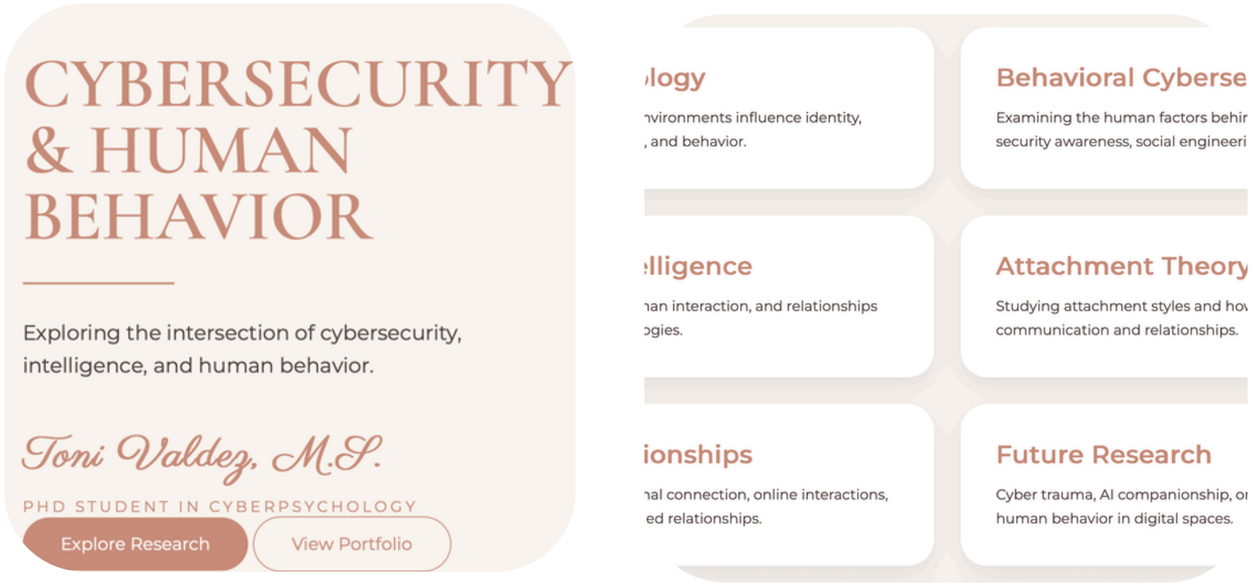
Incident Response Phases

The incident response plan followed the NIST SP 800-61 framework to establish a structured approach for handling security incidents. The process emphasized preparation, identification, containment, eradication, recovery, and lessons learned.



NIST INCIDENT

Response Lifecycle



Research Interests

Current Research Interests

My research interests focus on cyberpsychology, behavioral cybersecurity, attachment theory, artificial intelligence, and the impact of technology on human behavior. As a PhD student in Cyberpsychology, I am particularly interested in how digital environments influence relationships, security behaviors, and online interactions.

EDUCATION & CONTACT

Education

- M.S Cybersecurity, SNHU
- PhD Student, Cyberpsychology, Capitol Tech University
- CompTIA Security + (SY0-701)

Portfolio

Linkedin

Github