**Prospectus Report**
**Due Friday January 23, 2026**
**Group Information and Resources**

## Team Description

### Summary of Technical Strengths

Paige Brasfield - Paige is a cybersecurity major who currently works as a digital consultant at the GVSU libraries. She has experience in threat and network analysis, user security, virtualization software, cloud-based environments, and imaging and configuring laptops. She has received lots of hands-on experience through her internship this past summer and is hoping to land a position as a cybersecurity or network analyst. Her greatest technical strength is intrusion detection.

Logan Jacobs - Logan is a cybersecurity and computer science student. He was previously a computer science and statistics student so he has more experience in programming but has worked on a few cybersecurity related projects including password repositories and network/software security related labs. He has experience with using linux and packet analyzers which should prove useful for this project. He is familiar with many cybersecurity frameworks and topics, including how they work through lectures and academic work. His interests focus on network defense and digital forensics.

Dylan Stellman - Dylan is a cybersecurity major. He is an active member in the hacking club and works at GVSU IT. He hopes to pursue something in the IT field, working in the SOC or networking out of school. He had an internship working in a SOC alongside other professionals. Here he gained various skills in endpoint detections, network security, and phishing detections. He also has skills in SIEM tools, coding languages, and network analyzers.

Fernando Bresso - Fernando is a cybersecurity major. He takes part in the Hackers Analyzing Threats club at Grand Valley State University, participating in the NCCDC competition. He hopes to continue working at his internship, Tesa Tape Inc., after he graduates, shifting to a role in cybersecurity within the same company. His strengths include basic frontend and backend development, Python programming and scripting, and basic networking fundamentals

Selim Harzallah - Selim is a cybersecurity student with experience in Linux systems, virtual machines, and network analysis. He has worked on defensive security projects involving packet analysis, intrusion detection, phishing analysis, and log review. He is comfortable using Python for scripting and automation and has experience working with virtualized and cloud-based environments. His interests focus on network defense and realistic simulation of network traffic.

### Anticipation of Growth Areas

Paige Brasfield - Paige has a background in network analysis but is looking to get more hands-on experience with the creation of network tools and environments.

Logan Jacobs - Logan has little experience in networking and is looking to learn more about creating networks and using tools to test them for security. He is also looking to see how criminal information used in digital forensics bypasses some of these securities.

Dylan Stellman - Dylan has some background in networking but would like to learn more about how to set up and emulate network conditions.

Fernando Bresso - Fernando has experience working on frontend and backend programming and working with Python. But he is hoping to grow each of these skills by applying it to a polished networking project for simulating network infrastructure and security

Selim Harzallah - Selim has experience with network analysis and defensive security tools but is looking to further develop his skills in network emulation and traffic simulation, particularly in building realistic and controlled network scenarios.

## **Project Description**

### Background

This project will involve the design, development, and validation of a comprehensive network simulation platform tailored for simulating a diverse set of network protocols. This platform will build upon established network simulation technologies (such as Mininet). Network parameters such as latency, jitter, packet loss, and bandwidth constraints should be adjustable in real-time through scripting or directly through the user interface. This will enable controlled testing of network protocol performance under varying conditions, including conditions representative of rural or bandwidth-limited environments. The platform will support the injection of malicious traffic to simulate denial-of-service and other cyberattack scenarios and other traffic to simulate interactions with other realistic traffic flows on a network. Given sufficient time, the system may also support traffic generation from external devices. The user interface will allow for the configuration of latency, jitter, and loss independently for network flows in either direction. Users will be able to select standardized sets of network conditions (for example, reflecting rural networks, wireless networks, urban fiber optic networks, etc.) rather than needing to configure all parameters separately. It will also allow for the specification of other traffic to be running on the virtualized network at the same time as described above.

### Description of Intended Features/Backlog

- Emulate a network environment using virtual hosts
- Allow for custom adjustments to
    - Latency

    - Jitter
    - Packet loss
    - Bandwidth
- UI which is user-friendly so users can select which network topology, network conditions, and attacks they want to simulate
- Inject malicious traffic to simulate attack scenarios
- Multiple sets of network conditions like enterprise, rural, LAN, WLAN, WAN, etc.
- Keep track of network data on chart in real-time
- Generate report based on network simulation

Anticipated Platform/Tooling

- Jira Project Management Software
- Mininet or NS3
- Proxmox
- Python
- Flask or Django

Relevant Ethical Principles

ACM Code Of Ethics

1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.

1.6 Respect privacy.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.

2.9 Design and implement systems that are robustly and usably secure.

3.4 Articulate, apply, and support policies and processes that reflect the principles of the Code.

3.5 Create opportunities for members of the organization or group to grow as professionals.

**Meeting Times**

Meeting 1
Tuesday 20 Jan - (1:34 - 2:11) ⇒ finishing the prospectus report and discussing the growth of the project.


Today
Total: 00:37:00
Prospectus report - meeting 1
Network Testbed
1:34PM - 2:11PM
00:37:00

## Meeting 2