Julian Albert
Cameron O’Connor
CS 433

NetVision: Insight into Your Network

Introduction:

Network scanners play a crucial role in cybersecurity by providing organizations with the ability to identify, assess, and manage security risks within their network infrastructure. These tools are essential for maintaining the security and integrity of networks in the face of evolving cyber threats. By scanning network devices, ports, and services, organizations can gain visibility into their network topology and identify potential vulnerabilities that could be exploited by attackers.

Network scanners enable proactive security measures by allowing organizations to conduct regular vulnerability assessments, penetration tests, and security audits. This helps to identify and remediate security weaknesses before they can be exploited by malicious actors. They are widely used by security analysts and professionals in the cybersecurity field. They are an essential component of any comprehensive cybersecurity program and are used extensively across various industries and organizations.

Objectives

The objective of this project is to leverage a set of foundational tools such as Nmap and Scapy to establish a robust scanning functionality. By utilizing these tools, we aim to conduct comprehensive network scans to identify IP addresses, open ports, and other common identification specifications.

Additionally, we intend to develop a web-based application that presents the scan results in a user-friendly interface. This application will leverage modern frontend frameworks and data visualization tools to display the scan findings visually, allowing users to interact with the data effectively. Through this project, we seek to not only develop a powerful network scanning tool but also create a user-friendly platform that enables users to analyze and interpret scan results efficiently.

By the end of the term, our goal is to showcase a fully operational network scanner capable of efficiently identifying live hosts and open ports and an intuitive web app. If we have more time. It would be interesting to include API’s for more data such a geolocation and data visualization tools.

Timeline

	Tasks	**Assignments**
Week 6	-Test code -Fix/Add code -Design user interface	Project midterm report
Week 7	-Continue with code -Make sure it works	
Week 8	-Finish frontend design	

	-Start integration	
Week 9	-Deployment and hosting -Finalize all testing -Prepare presentation	
Week 10	-Publish -Present	Project presentation
Week 11	-Submit the final project	Project final deliverables

Our decision to build a network scanner was driven by our keen interest in cybersecurity and our desire to apply our skills to a practical project. Given our limited prior experience in this field, this endeavor presented an invaluable opportunity for learning and growth. Throughout the project, we encountered various challenges, but it ultimately proved to be a rewarding experience, providing us with a solid foundation in cybersecurity concepts and practices. Furthermore, we both have background knowledge on front-end design, so it would be exciting to integrate the two. Despite our initial lack of expertise, we were able to navigate the complexities of network security and emerge with a deeper understanding of the subject matter.

Related work

- Currently, the project is capable of identifying IPs and ports on an allowed network
- List out the users on the network in a more readable way
- Using Nmap we can target IP addresses (only if we are allowed to) and identify open ports along with associated service information
- Considering geolocation services, possibly integrate with geolocation services or APIs.
- Data Visualization Tools: We are considering using data visualization libraries like D3.js or Chart.js to create interactive charts and graphs for displaying scan results and statistics.

What we have done

- Research and planning; frameworks, architecture, web app design, possible database
- Specify the features and functionalities to be implemented; goals, scope, objectives
- Setup development environment; python, vscode, terminal, Nmap, scrapy
- Version control system; Github, git
- Backend Development; functionality, port scanning script

Lessons learned so far

- Time Expectations: Be prepared for tasks to exceed initial estimates.
- Network Permissions: Network access permissions can lead to unexpected complications.
- Precise Host and Port Identification: Capable of accurately pinpointing active hosts and open ports while minimizing false results.
- Dynamic Network Adaptation: Ability to adjust scanner settings to accommodate rapidly changing network landscapes.
- Compatibility Assurance: Ensuring seamless operation across diverse operating systems and network environments.

Action plan and timeline for the rest of the term

1. Finish Backend development
2. Frontend development; layout and wireframes using HTML, CSS, and JavaScript.
3. Integration and testing; integrate the frontend and backend components
    a. Conduct thorough testing of the application's functionality
    b. Debug and fix any issues or bugs identified
4. Deployment and Hosting; deploy on a web server (or locally?)
5. Present our final project