Project Proposal for CSCD 350 Spring 2024

ScanMasterX

V 1.0

Team #10: UwUltimate Stardust Crusaders

Submitted By

Lewis Thomas	lthomas32@ewu.edu
William Reese	wreese1@ewu.edu
Eric Leachman	eleachman04@ewu.edu
Dennis Vinnikov	dvinnikov@ewu.edu
Alexa Darrington	adarrington@ewu.edu

Instructor: Sanmeet Kaur

GSA: Harley Davis, Dominic MacIsaac

Lab Section: Rm 219 – Section 2

Date: 04/15/2024

GitHub Repository: https://github.com/Sanmeet-EWU/github-teams-project-bid-uwultimate-stardust-crusaders/tree/main

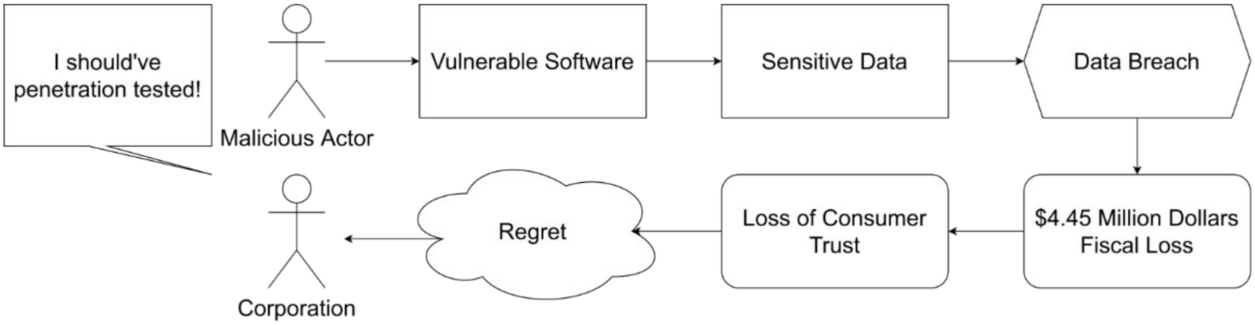
Motivation

The constant threat of cyber-attacks and the rising cost of cyber security breaches poses a huge problem for every company, big or small. Many attacks are carried out through vulnerable systems and code, where hackers demand ransom and often get it, resulting in millions of fiscal losses for businesses. Forbes estimated there will be 10 trillion in damages caused by cybercrime by 2025 [1]. Sometimes this problem is handled after the attack is already carried out, with little remediation and ransoms paid secretly. Our solution is to catch these problems before they even happen and lessen the possibility of any threats/attacks carried out. We want to educate and bring awareness to businesses that it is very important to secure their data and network and create a tool they can use.

Our intended users are businesses and developers in general as this tool can be used by almost every sector to tell them vulnerabilities in their network and take better steps to secure their systems and data. More specifically, people who aren't well versed in cyber security practices and who are non-specialists in the field could benefit greatly from ScanMaster X. This tool can be used by many different organizations/businesses including healthcare, financial institutions, educational institutions, and any business seeking to secure their system.

These organizations with limited IT resources and knowledge face difficulties in securing their systems due to many reasons. This could be lack of expertise, resource constraints, and lack of education and proper understanding of the intricacies of securing machines and networks. Many businesses also don't prioritize the importance of doing this, and how devastating it can be when something goes wrong.

Our solution would benefits users in many ways and their businesses (and their piece of mind). Our tool would provide ease of use for developers and people with limited cyber security knowledge to use and understand vulnerabilities they can fix and be aware of. This would provide a cost-effective solution where businesses wouldn't have to hire dedicated staff or outsource to expensive security firms. This saves time as well which in turns also saves money for businesses wanting to test networks without the technical know how. Additionally, our efforts will better educate the users and lessen threats in the cyber world, hopefully reducing future attacks and creating awareness. Our solution would improve software quality and decrease costs, providing a useful tool and a benefit to these users.



Approach

Our solution is a software designed to simplify network and machine testing. It aims to make testing accessible to users with limited cyber security knowledge. While there are existing programs for dynamic testing, they often require a deep understanding of networking and vulnerabilities to use effectively.

The core of our solution lies in a GUI (Graphical User Interface) designed to abstract the intricacies of network testing and computer security. This interface serves as the gateway for users to interact with the program seamlessly. By incorporating user-friendly elements such as drop-down menus and comprehensive prompts, we aim to make the testing process intuitive and accessible.

The initial phase of the flow involves utilizing established frameworks like nmap to map out the network topology. This step is crucial in understanding the network structure and identifying potential entry points for attackers. The GUI facilitates this mapping process, providing visual representations of the network layout in a graph format for easier comprehension.

Once the network topology is established, our solution delves into comprehensive network assessment. We will employ techniques to identify open ports and conduct fingerprinting to gather detailed information about these ports. Leveraging the NIST (National Institute of Standards and Technology) database, we will correlate port vulnerabilities and overlay heat maps on the network topology. This visualization aids in highlighting vulnerable areas and prioritizing security measures.

Furthermore, our plan is to integrate the data with the MITRE framework to contextualize vulnerabilities and map them to potential stages in an attack. This analysis should provide actionable insights into the likelihood and severity of potential breaches, allowing organization and developers to harden their systems and proactively prevent cyber threats.

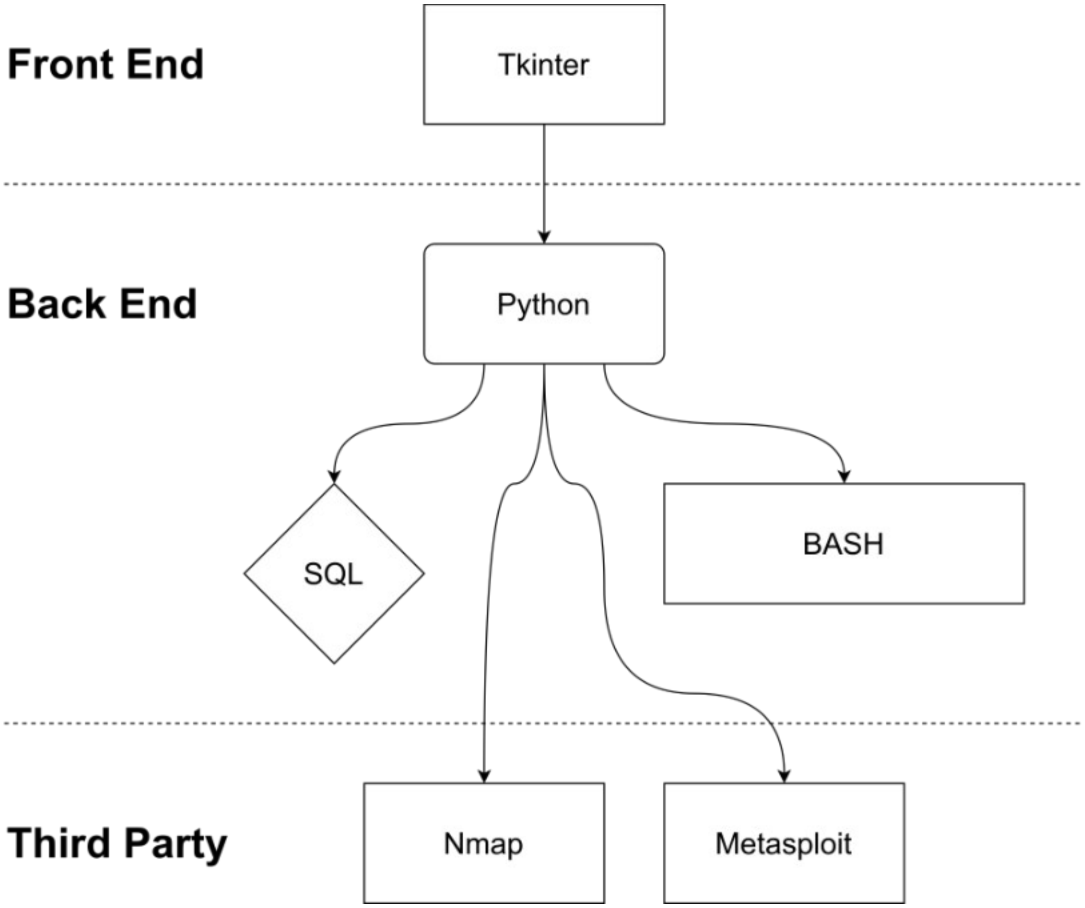
Moving beyond assessment, our plan is to use exploitation frameworks such as Metasploit to actively test the system. We will use the previous reconnaissance methodologies to identify predefined vulnerabilities and match them based on a curated list. This last step will emphasize how vulnerable their system is.

In addition, our plan is to include robust password cracking capabilities. We will offer interfaces for dictionary attacks and hybrid attacks, enabling organizations to test the strength of their passwords. By measuring the cracking speeds, we can provide detailed reports. These reports will spotlight weaknesses caused by developers and users accessing their systems.

Our solution simplifies network and machine testing, but it's important to acknowledge its limitations. Like other dynamic testing programs, ours requires time and expertise to execute effectively, affecting the speed of vulnerability exploitation. We face similar challenges regarding speed and the range of vulnerabilities we can cover in a limited time-frame.

The nature of our solution is that of a standalone program, designed to be run locally for efficient network access and testing. The software components encompass various virtual machines to create proof-of-concept topologies and possibly a database for storing critical information. While the database plays a supporting role, the primary focus remains on the functionality and features that enhance security assessment and testing capabilities.

On the hardware front, each team member requires a laptop equipped with an x86 chip to run virtual machines effectively. Alternatively, cloud-based virtual machines can be leveraged, with interaction facilitated through Command Line Interface (CLI) for seamless integration and testing. As a lot of the software and vulnerable machines we will be testing are only able to be ran on an x86 chip.



Challenges and Risks

Communication is likely to be the biggest obstacle this group will face in regard to finishing this project in a timely manner. Each member of this team has their own individual sets of limitations and challenges due to school. As students, we have our own classes to attend, homework to do, work to attend, and lives to live. We also have our own individual strengths and specialties which could potentially lead to differing opinions. Additionally, our work ethics likely vary, which could lead to misunderstanding and frustration. This will potentially lead to issues if we fail to get ahead of this before any serious amount of technical work starts.

To combat these issues, communication will be key. Communication should occur on a few different levels. Our team should commit itself to having team meetings at regular intervals. These meetings will allow us to check in with each other and get a macro view of the individual work we have been putting in and how it relates to the project as a whole. This will allow members to be aware of the location and pace of other members. Meeting notes should be taken and published so that they can be referenced by all users. Information of note for these notes might include lists of responsibilities, roles, timelines, and due dates.

We should strive to make a space where group members can go to get a current snapshot of the project. This might look like a Kanban, Trello, or Miro board. This centralized space might include easy to digest representations of workloads, diagrams, notes, and ideas. This space should also include a space for any meeting notes that are taken.

Individual group members should strive to be transparent about their progress and needs. This project is designed to challenge our abilities to work together, and our group should make it a goal to attend to the needs of the other group members. This is more easily done if we are open and transparent about any difficulties we face.

REFERENCES

[1] https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/

Glossary

IT – Information Technology

GUI – Graphical User Interface

NIST **–** National Institute of Standards and Technology

CLI – Command Line Interface