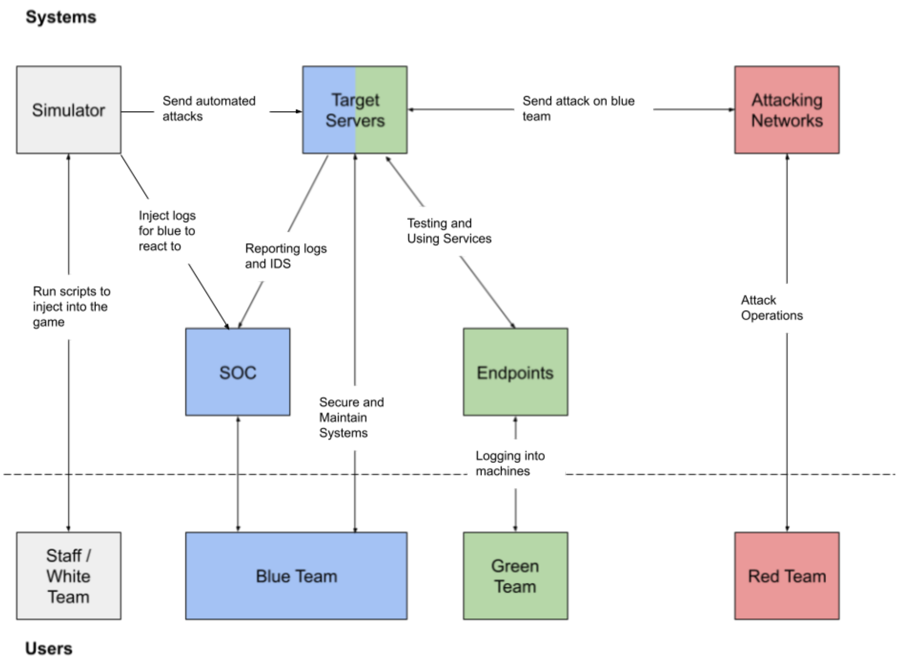
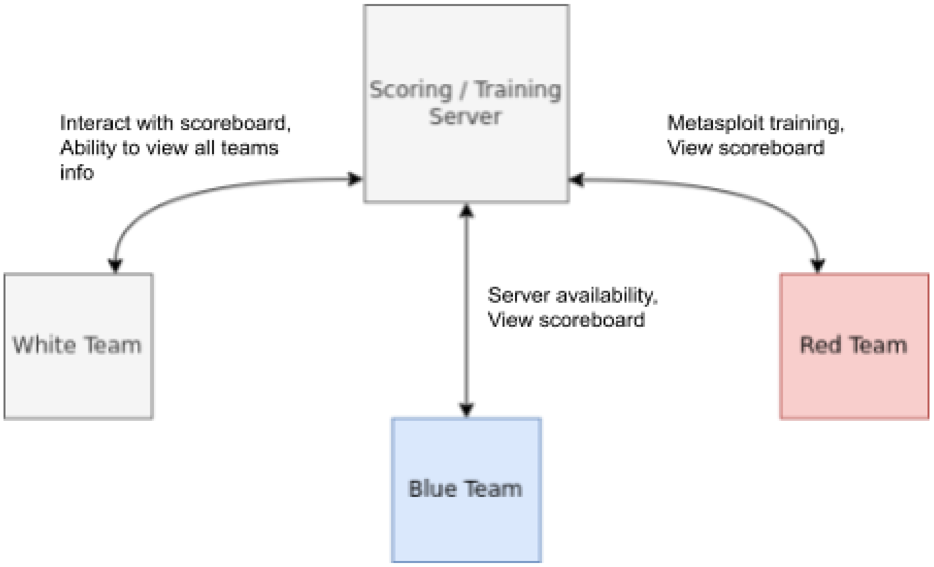
4.3 Proposed Design

4.3.1 Overview

CySim Design With User Interaction:



CySim Scoring Web Server User Interactions:


Scoring / Training Server
Interact with scoreboard, Ability to view all teams info
Metasploit training, View scoreboard
Server availability, View scoreboard
White Team
Red Team
Blue Team

Describe key components or subsystems and how they contribute to the overall design.

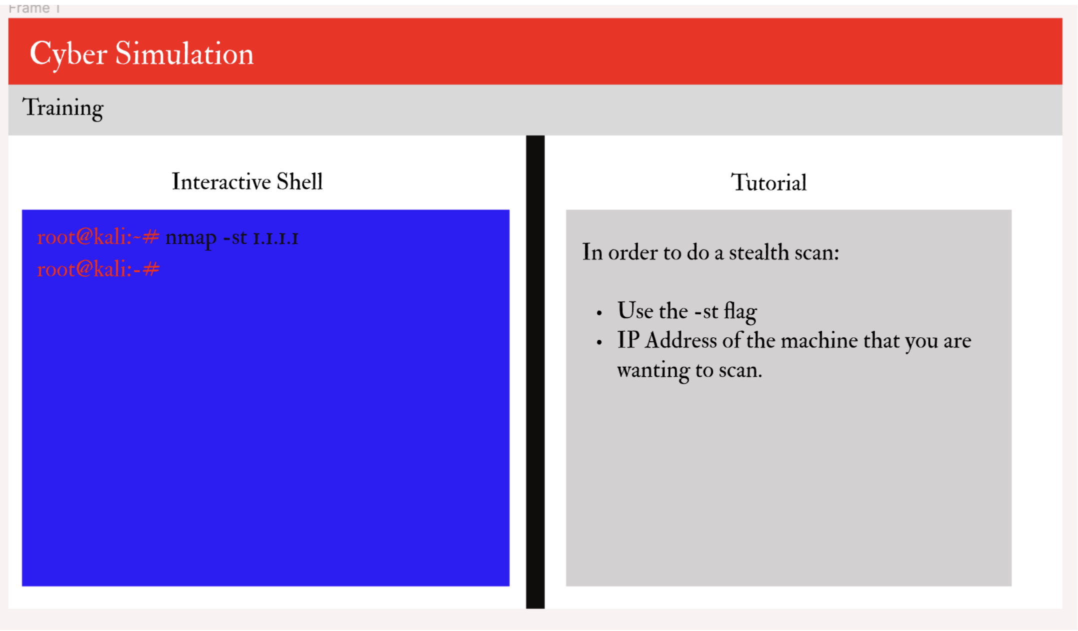
Our current design for CySim as a whole is a mock blue/green team enterprise network and red team attack network for teams to utilize for the games. For our implementatable design at this early stage of CySim, we are designing a web server that all teams in the game can interact with. This server will show the current score of the scenario, be used by teams for training in how to utilize the systems given to them, and allow for submissions to impact team scores. This facilitates the operations of game scenarios and allows for interactive teaching as teams are able to see how their actions impact their score.

4.3.2 Detailed Design and Visual(s)

Provide a detailed, technical description of your design, aided by visualizations. This description should be understandable to peer engineers. In other words, it should be clearly written and sufficiently detailed such that another senior design team can look through it and implement it.

The description should include a high-level overview written for peer engineers. This should list all sub-systems or components, their role in the whole system, and how they will be integrated or interconnected. A visual should accompany this description. Typically, a detailed block diagram will suffice, but other visual forms can be acceptable.

The description should also include more specific descriptions of subsystems and components (e.g., their internal operations). Once again, a good rule of thumb is: could another engineer with similar expertise build the component/sub-system based on your description? Use visualizations to support your descriptions. Different visual types may be relevant to different types of projects, components, or subsystems. You may include, but are not limited to: block diagrams, circuit diagrams, sketches/pictures of physical components and their operation, wireframes, etc.

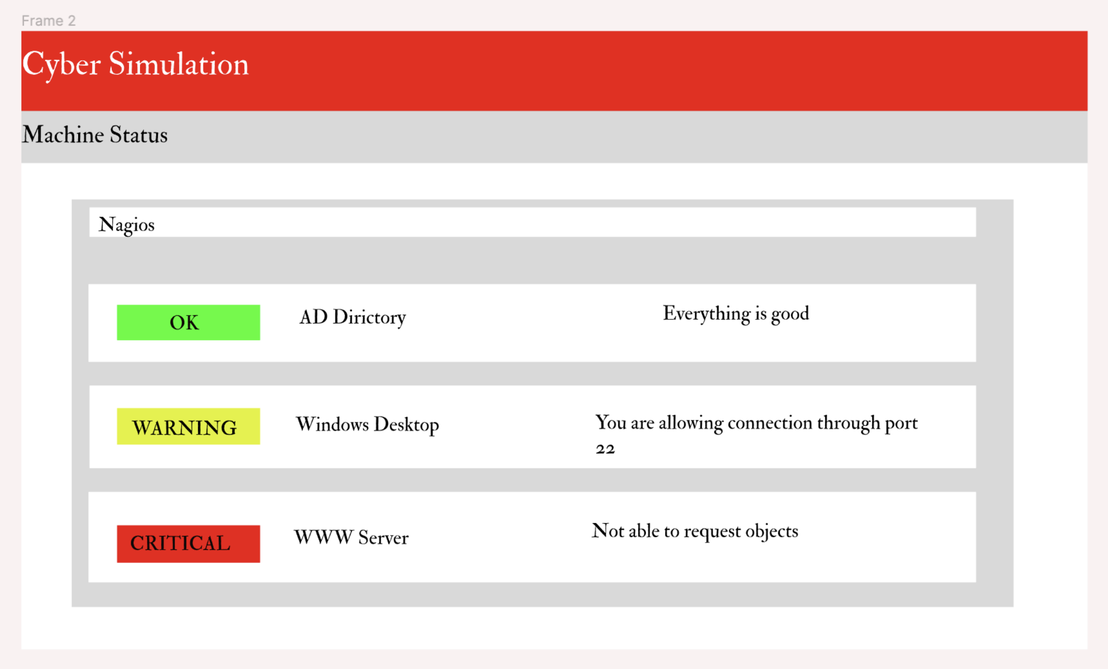


```
root@kali:~# nmap -st 1.1.1.1
root@kali:-#
```

In order to do a stealth scan:

- Use the -st flag
- IP Address of the machine that you are wanting to scan.

- There will be a training module so that users can use CySim as a practice environment. You will be able to learn both offensive and defensive security practices in this module.



Frame 2

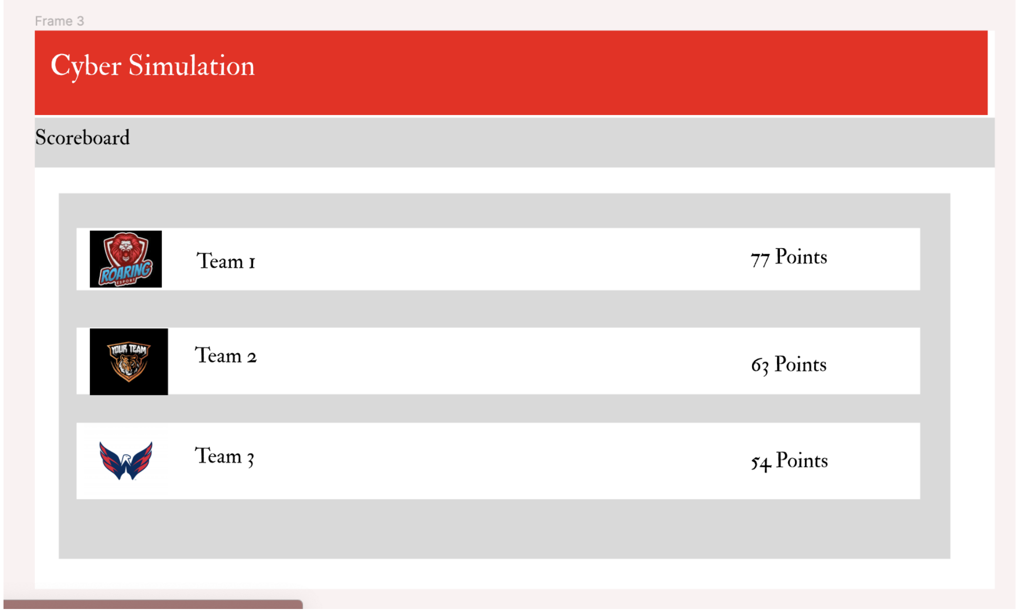
Cyber Simulation

Machine Status

Nagios

OK	AD Dirictory	Everything is good
WARNING	Windows Desktop	You are allowing connection through port 22
CRITICAL	WWW Server	Not able to request objects

- There will also be a status page to be able to see the status of the blue teams machines in one central location. The blue team will use this to know that their services are up and running and the red team will use it to know which of the blue teams machines are remaining. Status scans will happen every ~15 mins.



Frame 3

Cyber Simulation

Scoreboard

	Team 1	77 Points
	Team 2	63 Points
	Team 3	54 Points

- This is the leader board for all of the teams that are competing in the competition. The teams will be able to come to this module to see where they are standing in the competition.

4.3.3 Functionality

Describe how your design is intended to operate in its user and/or real-world context. What would a user do? How would the device/system/etc. respond? This description can be supplemented by a visual, such as a timeline, storyboard, or sketch.

CySim was created for a variety of purposes, these are shown below:

Provide mock real world experience for students, this means that students will have the ability to use CySim to get thrown into real world situations, from there these students will be able to learn how to prepare, respond and all around adapt based on the circumstances at hand.

Provide companies with the opportunity to train their employees, this means that if a bank is having an issue with accounts and data being stolen, they can send their employees to cysim and practice encountering these issues in a hypothetical experience. This allows these employees to better understand how to react and prevent these potential threats from occuring in the first place. All in all this can be a big advantage and bonus to companies that utilize CySim.

CySim will function as an arena for cybersecurity competitions as well. This can vary from "Red, Blue, Green" to other situations, inside there will be spectators, a scoreboard displaying information and live results, as well as a press room.

4.3.4 Areas of Concern and Development

How well does/will the current design satisfy requirements and meet user needs?

Currently, our design for CySim meets the needs of our users because we have thought of the needs of all of the user types which includes Blue Team, Red Team-, Red Team+, and Staff. If a user logs in as the blue team member then they will be presented with everything they need. Like all of the machines' status, score, and availability.

If they were to login as the Red Team- these are the attackers that are using CySim as a training platform and they will have a desktop with a kali linux to be able to access a terminal in metasploit. Their machine will be placed somewhere on the network to be able to run scans to find all the available machines that they have to attack and start their process at the reconnaissance stage.

The Red Team+ are the organization user's that can pass their scripted events. These types of attacks will not be man'd by a terminal. When a user is logging in as this they will be able to see the scoreboard, blue team machine status page, and all of the scripted events that they have available.

Based on your current design, what are your primary concerns for delivering a product/system that addresses requirements and meets user and client needs?

At this stage in the design process, we're most concerned with ensuring the stability of the services we implement so that as we build more modular game types on top of our foundation, we are able to grow CySim without having to start over from scratch any time a change comes down the line. This design will also have to be modular enough to support design changes over the next couple years before CySim is launched.

What are your immediate plans for developing the solution to address those concerns? What questions do you have for clients, TAs, and faculty advisers?

To address these concerns, we are building the most basic components first and starting with what we know must absolutely be included. Infrastructure to support the VMs and hypervisor machines is an example of one of these critical components, and the work we achieve on the control server/central web server will pave the way for every game type and user interaction to come.

4.4 Technology Considerations

Describe the distinct technologies you are using in your design. Highlight the strengths, weaknesses, and trade-offs made in technology available. Discuss possible solutions and design alternatives.

As part of CySims development we have decided or been required to use the following technologies:

- **Splunk:** Splunk will be used as another form of network monitoring in order to train participants on real-world network management practices during the exercises. Since it's an industry standard tool, it will be an effective inclusion in CySim.
- **pfSense:** pfSense is considered a universal, basic firewall tool that comes built-in with many Linux distributions. It will be used in CySim to train participants on the basic concepts surrounding firewalls, while more advanced groups might use a different firewall system.
- **Nagios:** Nagios is a system monitoring software which can be used to monitor system status during an event.
- **Windows 10:** The biggest strength is Windows 10 being one of the largest and most popular OS's with a wide range of compatibility with many different softwares. It is also free to use the basic version, cutting down costs. Some weaknesses include lack of customization and advanced features that other OS's include. Some alternatives include Mac OS as well as Linux distributions such as Ubuntu, Kali, or Mint.
- **Ubuntu Linux:** Some strengths of Ubuntu is that it is the largest distribution of Linux. This means that it has good compatibility with a wide range of software as well as the great customization features which are a hallmark of the Linux operating system. It is also free, allowing for costs to be cut down. Some weaknesses include the lack of advanced tools built into the OS that a distribution like Kali or Parrot OS would have. Some alternatives of course would be Kali, Parrot, or Mint distributions of Linux.
- **.NET Core:** Some strengths of .NET is that it is fast, diverse, scalable, and has a lot of documentation. Some weaknesses include library constraints and overall lack of experience with the technology in our team. Some alternatives are Mono and Ceylon but these are not as popular and less likely to be supported outside of this project.
- **Server:** The main server that we're given will be multi-purpose: It will host the web application that the red and blue teams interface with to participate in the game, as well as any other number of necessary services to drive the gameplay and provision the CySim field.

4.5 Design Analysis

Discuss what you have done so far, i.e., what have you built, implemented, or tested? Did your proposed design from 4.3 work? Why or why not? Based on what has worked or not worked (e.g., what you have or haven't been able to build, what functioned as expected or not), what plans do you have for future design and implementation work? For example, are there implications for the overall feasibility of your design or have you just experienced build issues?

At the moment, our design in 4.3 has been approved by our client, and we are moving forward with the web app development as soon as our client's server is provisioned to us. We're feeling confident that our web app design is up to our client's specifications, and will be expanding our design when it's up and running.