



# HackTrack

---

Dec1703 for Dr. Daniels

# Team

- **Nick Lewis**
  - Communications Co-Leader
- **Davis Batten**
  - Key Concept Holder
- **Anh Nguyen**
  - Webmaster
- **Vitale Cernetchi**
  - Communications Co-Leader
- **Dan Doyle**
  - Team Leader



# Agenda

- Introduction
- Design
- Implementation
- Project Management
- Demo
- Conclusions
- Questions

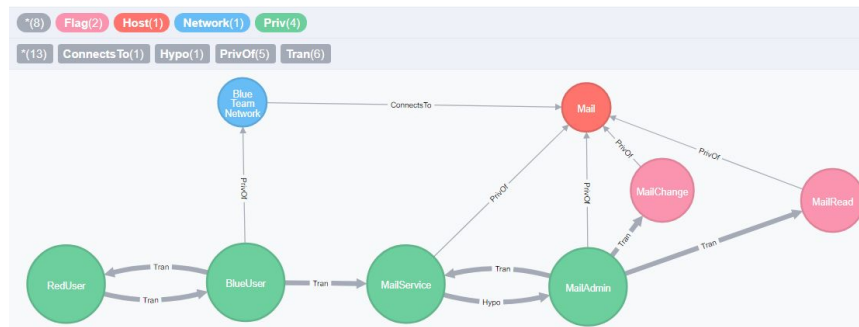


# Introduction

---

# CDC/Attack Graphs

- Cyber Defense Competition
  - One **Red team** hacking into many **Blue team** networks
  - Difficulty in picking next attack
  - Repeated work/effort
- Attack Graphs
  - Visual representation of a network
  - Nodes are privileges
  - Edges are transitions between privileges
  - Usually produced by “hand”

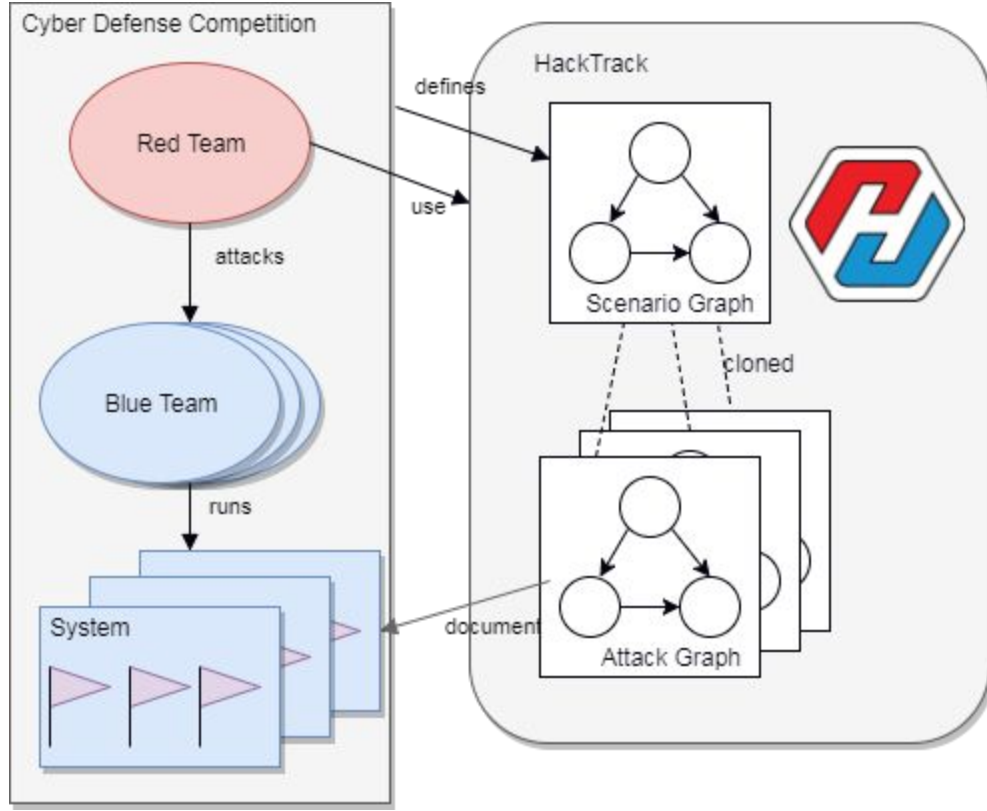


# Project Overview

## Attack Graph-based Web Application

- **Red team vs Blue team**
  - **Red team** consists of the participants testing security
  - **Blue teams** manage the systems which are attacked by the **Red team**
- **Real-time visualization of the competition**
  - Constantly changing graph showing **Red team's** progress
  - Allows **Red team** members to re-strategize their attacks quickly based on another member's work
- **Organized records of the data found**
  - Efficient record-keeping for other **Red team** members to use in their attacks





# Deliverables

- Source code for the application
- Documentation for the app
- Virtual machine image implementing the project





Design

---

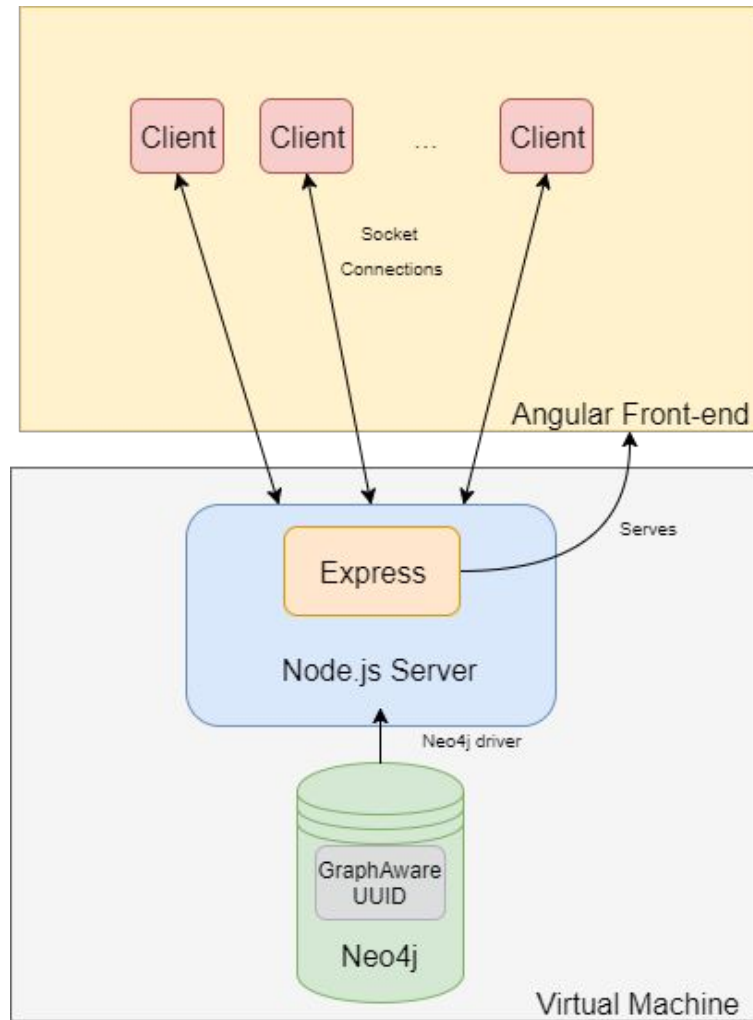
# Requirements & Standards

- Users can view all data about blue teams
- Users can edit a blue team attack graph
- Hypothesis edges created from found edges
- Server checks for path to flag
- Task list should be maintained for each user
- Support for Chrome & Firefox



# Architecture

- Back-end (Virtual Machine)
  - Neo4j Graph Database
    - GraphAware
  - Node.js Server
    - Express
    - Neo4j Driver
- Front-end
  - Angular



# Components - Node.js and Express

## Node

- Server-side Javascript environment
- All code is written in Javascript
- Node Package Manager

## Express

- Web application framework for Node.js
- Exposes REST API



express



# Components - Angular 4

- Front-end web application platform
- Written in Typescript and HTML
- Component-based UI development
- Dynamic data-binding



# Components - Neo4j and GraphAware

## Neo4j

- Graph database
- Easier to represent attack graphs
- Allows graph traversal algorithms to be used on application data



## GraphAware

- Add-ons for Neo4j
- UUID's for specific database items



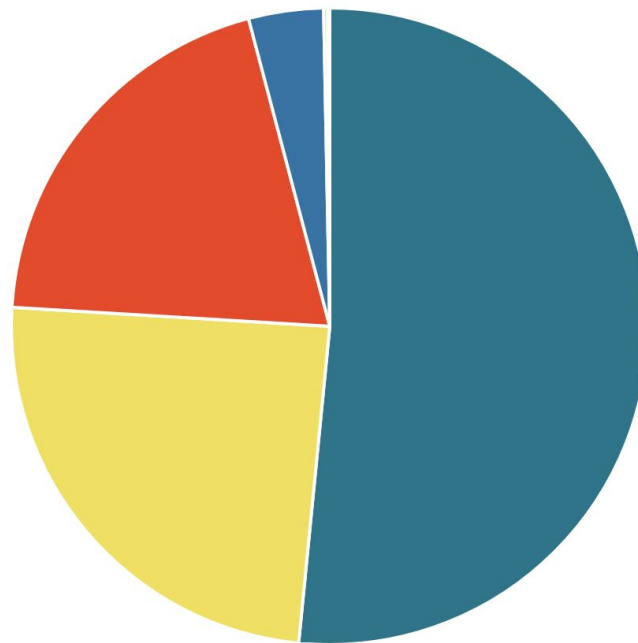
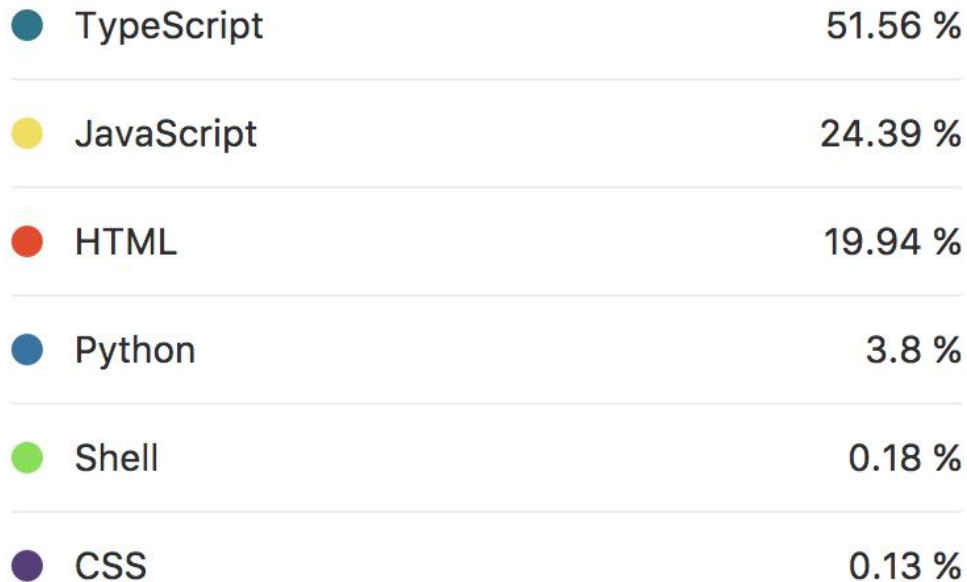
GraphAware<sup>®</sup>



# Implementation

---

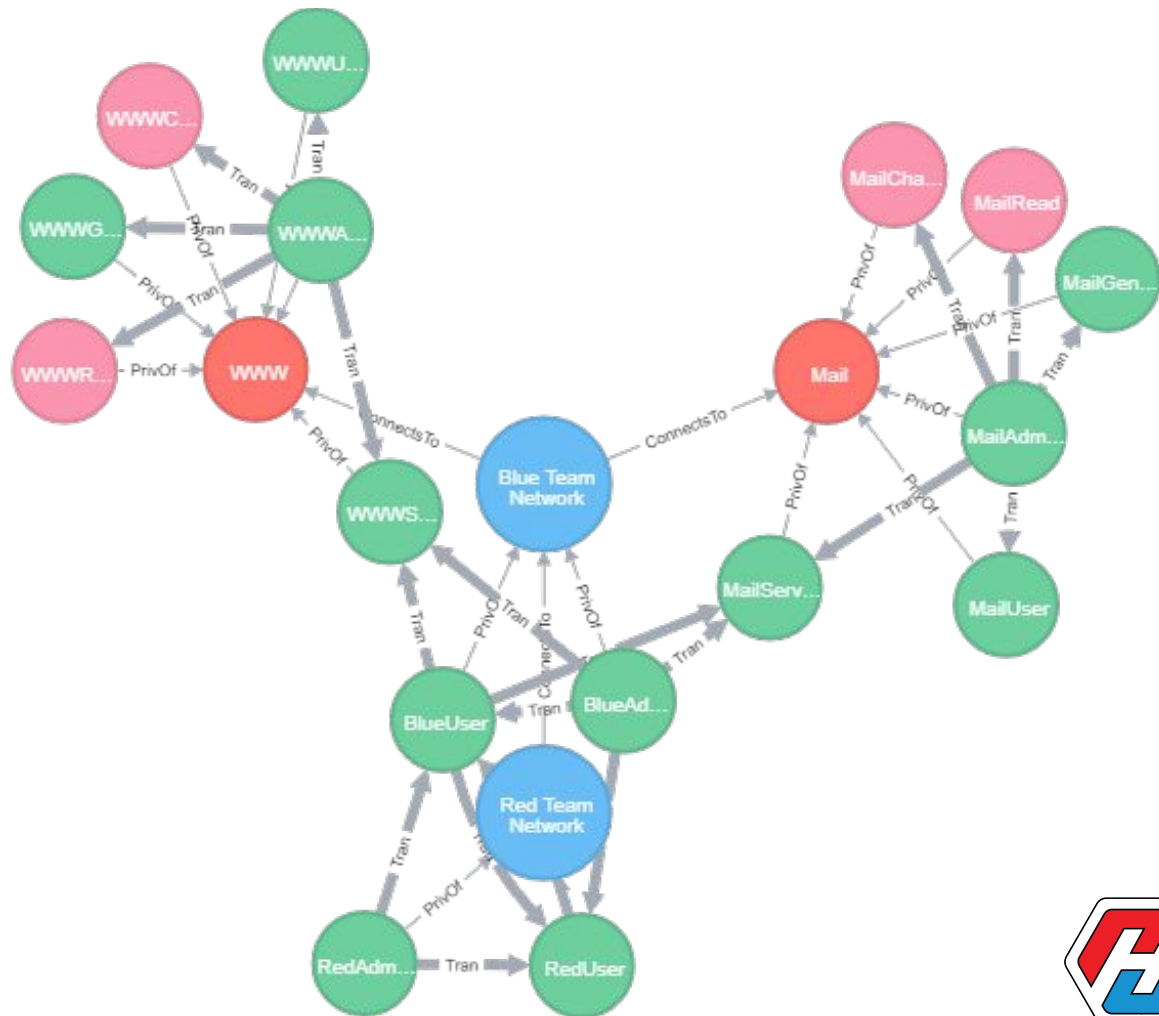
# Programming Languages Used





# Schema

- Nodes
  - Networks
  - Hosts
  - Privileges
  - Flags
- Relationships
  - Connects To
  - Privilege Of
  - Transition
  - Hypothesis



# Challenges

- Discovered issues in implementation late in the semester
- Versioning issues with Neo4j
- Deprecation of our initial Neo4j driver
- Multiple forms on a page (Angular issue)
- Learning curve of new technologies
- Graduate student left project



# Project Management

---

# Collaboration

- GitLab for version control
  - Issues board
  - Developer branches
  - Merge requests
- Team dynamic
  - 2 team meetings / week
  - 1 client meeting / week
  - Google Docs
    - Documentation
    - Reports
      - 1st semester - weekly
      - 2nd semester - biweekly
  - Code Jams



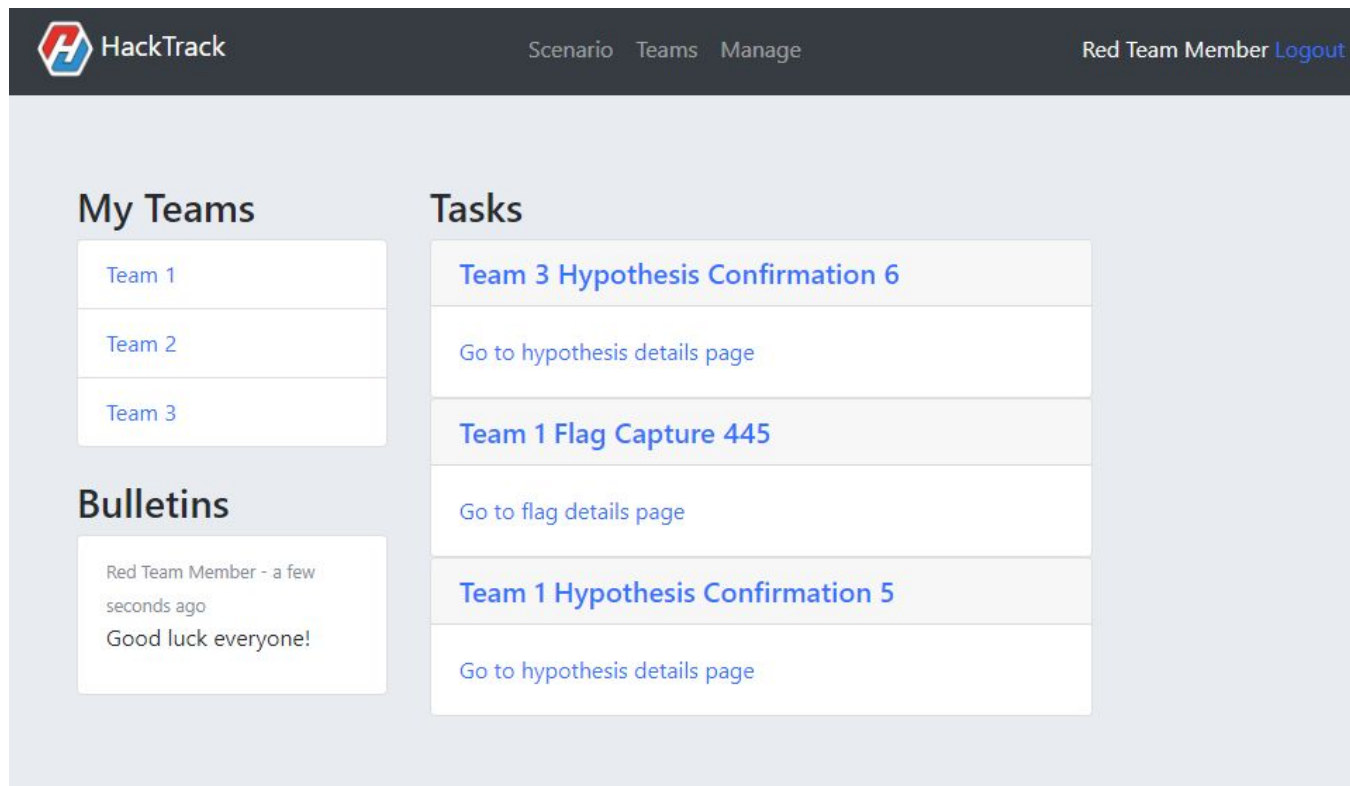
# Testing

- Testing Environment
  - Karma
  - Jasmine
- Types of Testing
  - API Testing
  - View Testing
  - E2E Testing



Demo

# Home page



The screenshot shows the HackTrack home page. At the top, there is a dark navigation bar with the HackTrack logo on the left, the text "Scenario Teams Manage" in the center, and "Red Team Member Logout" on the right. Below the navigation bar, the page is divided into three main sections: "My Teams", "Tasks", and "Bulletins".

**My Teams**

- Team 1
- Team 2
- Team 3

**Tasks**

- Team 3 Hypothesis Confirmation 6**  
Go to hypothesis details page
- Team 1 Flag Capture 445**  
Go to flag details page
- Team 1 Hypothesis Confirmation 5**  
Go to hypothesis details page

**Bulletins**

- Red Team Member - a few seconds ago  
Good luck everyone!



# Show/Confirm Hypothesis

## Hypothesis

**From**

WWWUser

**To**

WWWAdmin

**Team**

2

**Description**

Their password is "AdminPassword123"

**Instructions**

Found their team password on the table.

Confirm

Deny





# Create/Show Transition

## New Transition

Team

Team 1

To

WWWAdmin

From

WWWUser


Description

Their password is "AdminPassword123"

How was it gained?

Found their team password on the table.

Submit



HackTrack

## Transition

**From**  
WWWUser

**To**  
WWWAdmin

**Description**  
Their password is "AdminPassword123"

**Instructions**  
Found their team password on the table.

**Found By**  
test



# Team page

## Team 1

Unsubscribe

1/4

## Networks

Blue Team Network

New Network

## Flags

MailRead

MailChange

WWWRead (Claimed)

WWWChange



# Privilege View

[Home](#) / [Teams](#) / [Team](#) / [Network](#) / [Host](#) / [Privilege](#)

## MailService

### In

#529 -> MailAdmin

#520 -> BlueUser

#518 -> BlueAdmin

### Out

#14 -> MailAdmin

#5 -> *MailAdmin* [Hypothesis]

New Transition



# Conclusion

---

Questions?