NECCDC

2017

Northeast Collegiate Cyber Defense Competition Team Packet

March 17-19, 2017

Rochester Institute of Technology

Table of Contents

Platinum

U.S. DEPARTMENT OF HOMELAND SECURITY

NATIONAL SECURITY AGENCY
★ UNITED STATES OF AMERICA ★

amazon
web services

Gold

AIR FORCE
CIVILIAN
SERVICE

paloalto
NETWORKS®

SIG
SUSQUEHANNA

VERACODE
SECURING THE SOFTWARE THAT POWERS YOUR WORLD.

Silver

Bronze

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

SecureWorks®
INTELLIGENCE-DRIVEN INFORMATION SECURITY SOLUTIONS

Welcome Letter

Dear Competitors,

On behalf of the B. Thomas College of Computing and Information Science of Rochester Institute of Technology, I would like to welcome you to the tenth Annual Northeast Collegiate Cyber Defense Competition (NECCDC). Cybersecurity is becoming an ever more important part of our national security efforts and this competition is one of most important events in training our future cybersecurity experts.

We are very grateful to all of our sponsors as well as to the University of Texas at San Antonio (UTSA) for their guidance, event templates and materials. Our staff, volunteers, and sponsors have worked hard to make this an interesting, exciting, and challenging competition. One of the exciting aspects of this competition is that the winner of this contest will receive travel expenses to compete at the National Collegiate Cyber Defense Competition to be held in April 2017 in San Antonio, Texas.

We encourage you to spend some time with members of the other teams to enhance your learning experience. We wish the very best of luck to each of you and your teams! Many thanks to you for participating in this competition.

Dr. Bo Yuan
Department of Computing Security
Rochester Institute of Technology

Schedule

Friday – March 17, 2017

10:00 AM -11:00 AM Team Registration (Golisano Atrium)

11:00 AM – 11:30 PM Opening Announcements / Orientation (Louise Slaughter Hall SLA-2220-2240)

11:30 AM – 12:30 PM Lunch (SLA-2220- 2240) / **White Team** Orientation (Golisano Auditorium GOL-1400)

01:00 PM – 06:00 PM **Competition Day 1** – (Golisano Building Rooms Assigned)

02:00 PM – 04:00 PM Northeast Regional **Coaches Meeting** (Golisano Auditorium GOL-1400)

07:00 PM - 09:00 PM Dinner for Sponsors, Red, Black and White Teams (SLA-2220- 2240)

Saturday – March 18, 2017

08:00 AM – 08:45 AM Breakfast & Announcements (SLA-2220- 2240)

09:00 AM – 06:00 PM **Competition Day 2** - (Golisano Building Rooms Assigned)

09:00 AM – 12:00 PM **Symposium on Cybersecurity** (Golisano Auditorium GOL-1400, audiences: sponsors, guests, coaches, volunteers, alternates, etc)

12:00 PM – 01:00 PM Boxed Lunches Available (no break in competition) (GOL-2400)

06:00 PM – 08:00 PM Sponsors Meet & Greet (SLA-2220- 2240)

Sunday – March 19, 2017

08:00 AM – 08:45 AM Breakfast & Announcements (SLA-2220- 2240)

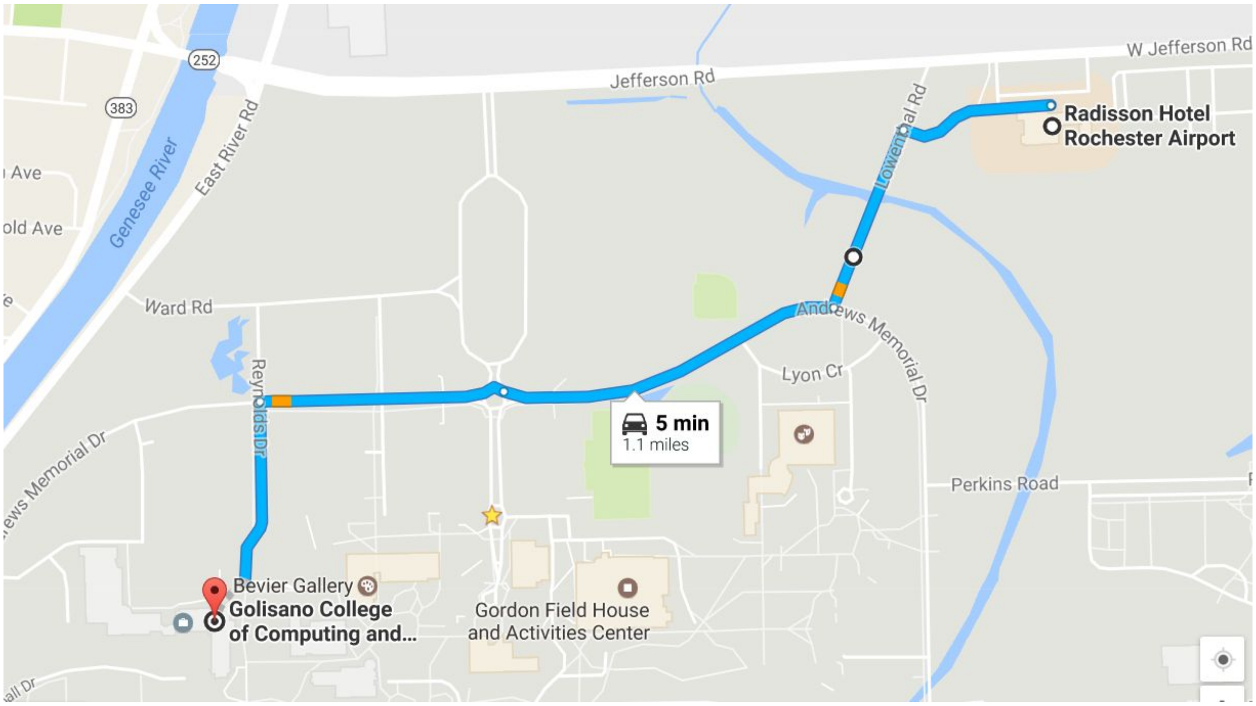
09:00 AM – 12:00 PM **Competition Day 3** - (Golisano Building Rooms Assigned)

12:00 PM – 01:00 PM Clean Up and Feedback Session (Stay in Rooms)

01:00 PM – 03:00 PM Luncheon and Awards Ceremony (SLA-2220- 2240)

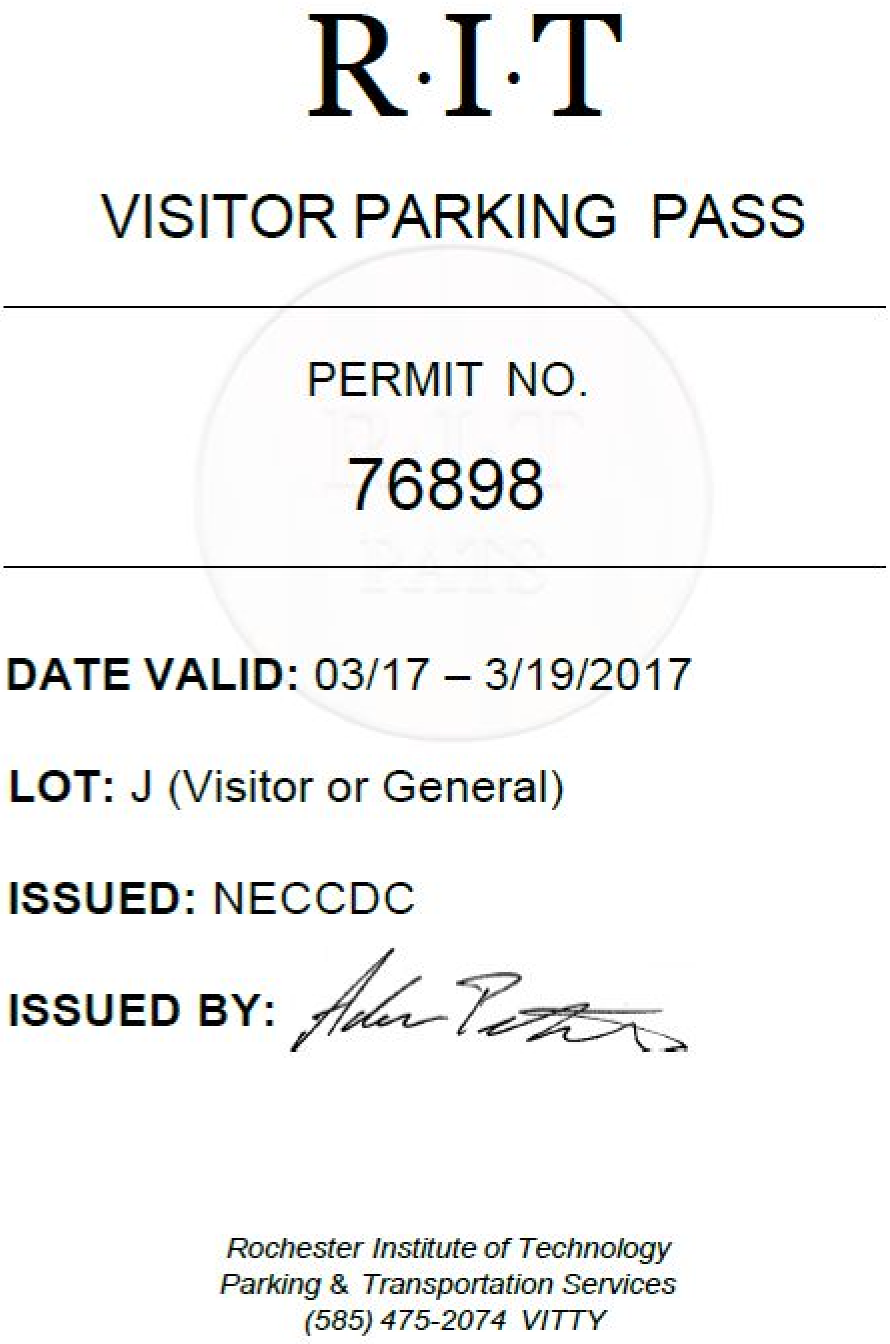
Driving Directions

The competition is being held in **Golisano Hall**, B Thomas Golisano College of Computing and Information Sciences at RIT. Parking is available in the J lot. (see next page for a campus map). It takes about 5 minutes from the Radisson Hotel to **Golisano Hall**.



Parking Pass

Please print out the parking permit on the next page and put it on the dashboard of your car.



R·I·T

VISITOR PARKING PASS

PERMIT NO.

76898

DATE VALID: 03/17 – 3/19/2017

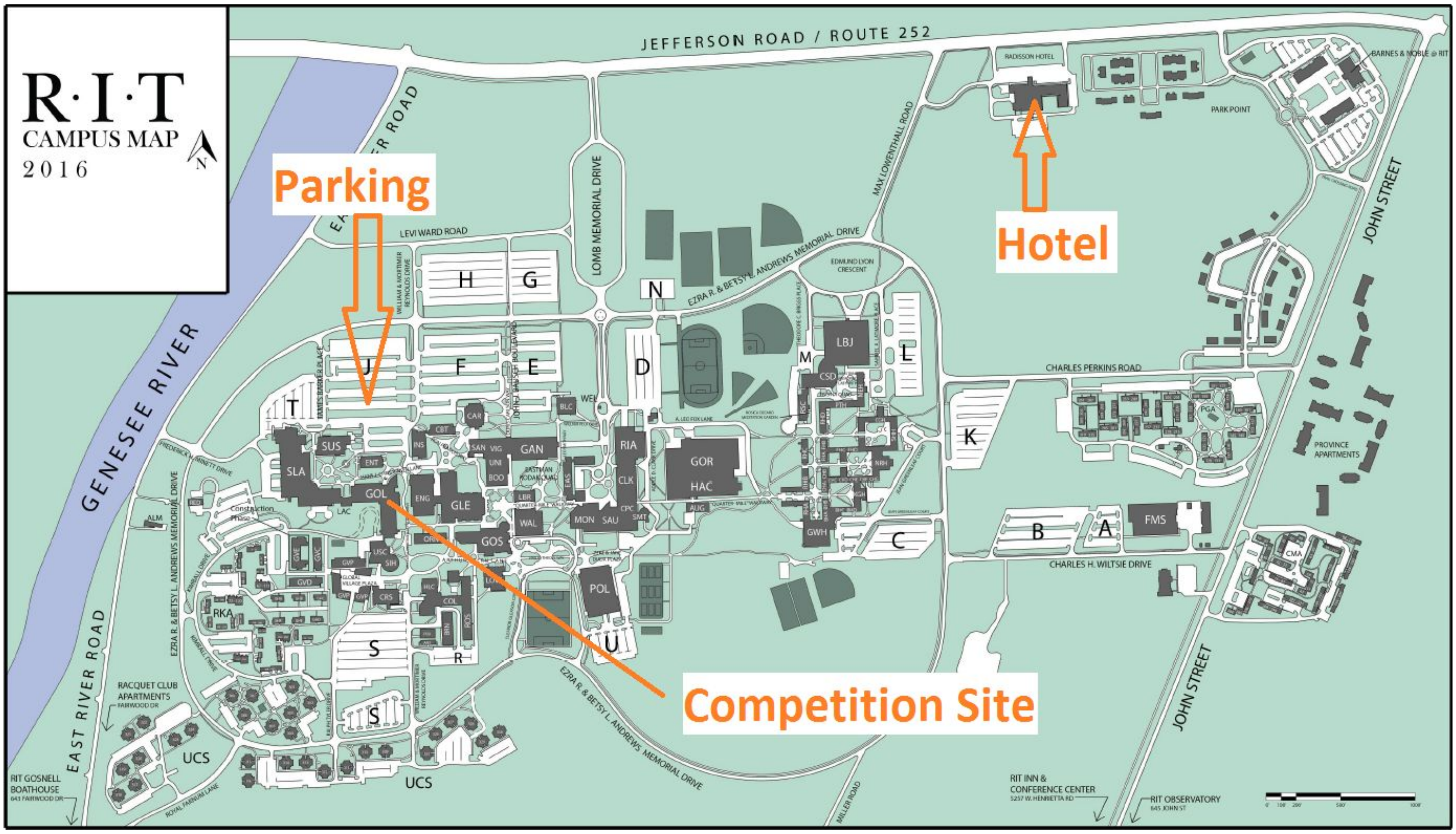
LOT: J (Visitor or General)

ISSUED: NECCDC

ISSUED BY:

Rochester Institute of Technology
Parking & Transportation Services
(585) 475-2074 VITTY

RIT Campus Map



Hotel Information

Radisson Inn
175 Jefferson Rd, Rochester, NY 14623
(585) 475-1910

It is right in front of RIT and the closest accommodations to campus. We have blocked rooms for teams until February 17th at the rate of $103 per night.

Competition Overview

The Northeast Collegiate Cyber-Defense Competition (NECCDC) is the regional qualifier for the national Collegiate Cyber-Defense Competition (CCDC). The northeast region represents institutions in the states of New York, Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, and Connecticut.

The NECCDC will select one winner and one alternate to represent the region in the CCDC for 2017. This year's CCDC is being held in San Antonio, Texas, on **April 13-15, 2017**.

More information on the CCDC can be found at the CCDC website:

http://www.nationalccdc.org/

The CCDC represents a collection of defense-only competitions in cyber-security. The competition is designed to test each student team's ability to secure a networked computer system while maintaining standard business functionality. The teams are expected to manage the computer network, keep it operational, and prevent unauthorized access. Each team will be expected to maintain and provide public services per company policy and mission. Each team will start the competition with a set of identically configured systems.

The objective of the competition is to measure a team's ability to maintain secure computer network operations in a simulated business environment. This is not just a technical competition, but also one built upon the foundation of business operations, policy, and procedures. A technical success that adversely impacts the business operation will result in a lower score as will a business success which results in security weaknesses.

Student teams will be scored on the basis of their ability to detect and respond to outside threats, including cyber-attacks, while maintaining availability of existing network services such as mail servers and web servers, respond to business requests such as the addition or removal of additional services, and balance security against varying business needs.

Team Identification

Blue Team

Student team representing a specific academic institution competing in this competition; each team consists of up to 12 competitors. Each competition team may consist of up to eight (8) members chosen from the submitted roster. The remainder of the roster is for substitution in the event a member of the active competition team cannot compete. Substitution in the competition team requires approval from the head judge present at the competition.

Red Team

Professional network penetration testers from the security industry. This team actively fills the role of the "attacker". Specifically, the Red Team:

- Scans and maps the network of each Blue Team
- Attempts to penetrate the defensive capabilities of each Blue Team network and modify any acquired environment
- Assesses the security of each Blue Team network
- Attempts to capture specific files on targeted devices of each Blue Team network

White Team

Professionals and representatives from industry who serve as competition judges, room monitors, and security enforcement personnel in the various competition rooms. Judges will assess the competition team's ability to maintain their network and service availability based upon a business inject and a scoring instrument, delivering inject scenarios, scoring of injects, creating log entries, securing log files, issuing or controlling the timing of injects, etc. Each competing Blue Team will have at least one White Team member present in their room who will assist in the judging process by observing the team, confirming proper inject completion, as well as reporting issues (if any).

Black Team

In addition to the Red, White, and Blue teams, there is also a Black Team which is tasked with the technical operations of the competition environment. This team is comprised of industry professionals and faculty, is tasked with the preparation, deployment, and support of event infrastructure. This team does not interact directly with the Blue Team and is effectively merged with the White Team for the NECCDC.

Competition Scenario

Your team has been hired as the new system administrators/security operations experts for a new startup named F-Sports Baseball. F-Sports is developing an innovative fantasy baseball platform that will revolutionize the world. F-Sports’ founder and CEO Jessica Goldsmith started the company in her dorm room and after her first series,a fundraising is finally able to hire full time staff for administration and security. Having grown out of a dorm room, F-Sports infrastructure has just started to become more complex. While there is some documentation available, due to the agile nature of the F-Sports platform it is unlikely that all the documentation provided is up to date.

Company Profile

F-Sports Baseball, LLC.

www.fsports.co

“F-Sports Baseball, LLC. is a startup dedicated to providing online daily fantasy sports competitions for alternative prize points based on the outcomes of real major league games. The company was founded in 2016 and is based in Mountain View, California.

F-Sports provides an interactive web 3.0 company focused on meeting the fantasy sports needs for a new generation, with a focus on simplicity and user experience. F-Sports makes playing fantasy sports fun and exciting for the whole family.

In order to meet this demand F-Sports is built upon a robust, heterogeneous architecture featuring the newest technology. It is this reliance on new age development methodologies and technology that allows F-Sports to offer its service to customers at a fraction of the cost.”

Letter from the Owner

From: Jessica Goldsmith
To: New Technology Personnel

Dear Team,

We are pleased to welcome you to F-Sports! We here at F-Sports focus on making a product that the whole family can enjoy. As many of you have already noticed, all of you are new additions to the F-Sports team. Previously, as a small organization, we didn't have a major need for a dedicated IT/Security/Reliability expertise. For this reason we expect you to be able to learn about our environment as we grow and do your absolute best to make F-Sports the success I know it can be.

The developers and I have been managing our infrastructure up until now, however we're way too busy now as business is starting to pick up. I will provide you the documentation we have made and I will send you the username and passwords for the systems shortly.

Our team isn't really made up of administrators, we've just set things up to the best of our abilities thus far. Based on your reputations, I'm confident that we've built the right team to take over responsibilities of the company's infrastructure, and I'm sure that we'll get through this and come out as a much better company on the other side.

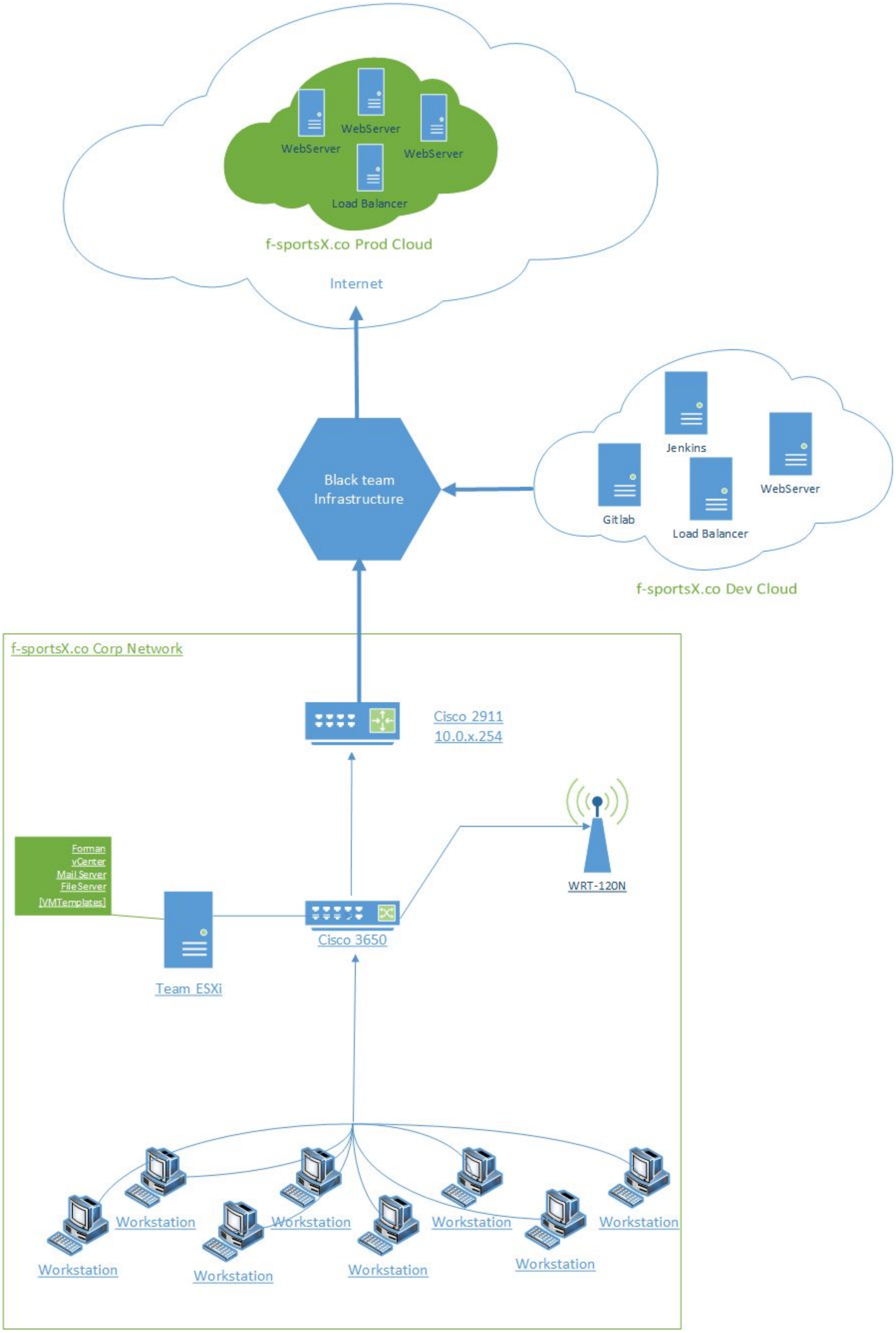
Most importantly, I want you to know that I'm always open to how we can improve things and have an open-door policy.

Thanks,

Jess

P.S. I know this is bad timing, but I'll be unavailable for the next week as I'll be on vacation in Baltimore, and am not sure what Internet access is like out there.

Network Topology



Network Description

The F-Sports Baseball, LLC. network is comprised of a local corporate network, a development network, and a production network. Each network is currently allocated a set of 254 addresses. The username for any hosts should be either **administrator**, **admin**, **user**, or **root** with a password of **Netsys123$**.

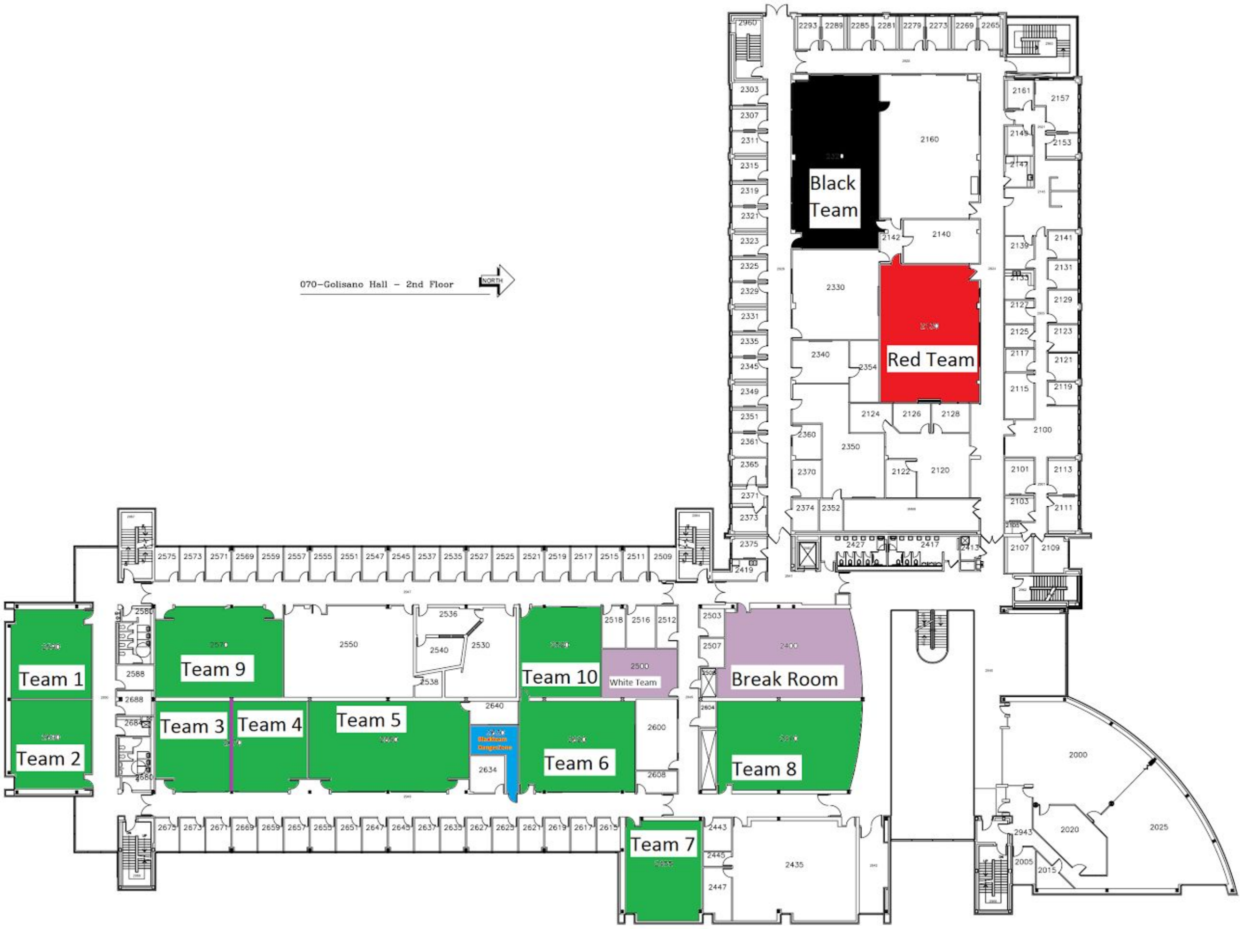
The details on your IP network prefix, domain name, and other team-specific configuration will be provided to you in your designated competition room.

Inventory of systems listed in the topology document:

System	Location	IP	OS	Scored Services
Router	Corp	.254	Cisco	--
Switch	Corp	.1	Cisco	--
Wireless AP	Corp	.9	Cisco	--
Caterpie	Corp	.40	Windows	DNS, LDAP
Weedle	Corp	.2	Linux	--
Pidgy	Corp	.3	Linux	--
Rattata	Corp	.8	Linux	--
Spearow	Corp	.4	Windows	--
Magikarp	Corp	.12	Windows	SMB
Voltorb	Corp	.22	Linux	FTP
Ekans	Corp	.5	Windows	--
Sandshrew	Corp	.6	Windows	--
Clefairy	Corp	.7	Linux	
Zubat	Corp	.30	Linux	VCenter
Machop	Corp	.37	Linux	Foreman, Web
Bellsprout	Corp	.20	Linux	Mail
Vulpix	Dev	--	Linux	F-Scores Inc
Venonat	Dev	--	Linux	
Diglett	Dev	.21	Linux	Web1, Web2, SSH
Meowth	Dev	.2	Linux	SSH, Web, Database
Psyduck	Dev	.19	Linux	Web
Abra	Prod	--	Linux	SSH, Web
Mankey	Prod	--	Linux	SSH, Database
Growlithe	Prod	--	Linux	SSH
Poliwag	Prod	--	Linux	SSH

Note that client systems must remain end-user systems and cannot be re-provisioned as server systems.

Team Rooms Layout



CCDC National Competition Rules

1. **Competitor Eligibility**
    a. Competitors in CCDC events must be full-time students of the institution they are representing:
        i. Team members must qualify as full-time students as defined by the institution they are attending.
        ii. Individual competitors may participate in CCDC events for a maximum of five seasons. A CCDC season is defined as the period of time between the start of the first state event and the completion of the National CCDC event. Participation on a team in any CCDC event during a given season counts as participation for that entire season.
        iii. A competitor in their final semester prior to graduation is exempt from the full-time student requirement and may compete in CCDC events as a part-time student provided the competitor has a demonstrated record of full-time attendance for the previous semester or quarter.
        iv. If a team member competes in a qualifying, state, or regional CCDC event and graduates before the next CCDC event in the same season, that team member will be allowed to continue to compete at CCDC events during the same season should their team win and advance to the next round of competition.
    b. Competitors may only be a member of one team per CCDC season.

2. **Team Composition**
    a. Each team must submit a roster of up to 12 competitors to the competition director of the first CCDC event they participate in during a given CCDC competition season. Rosters must be submitted at least two weeks prior to the start of that event. All competitors on the roster must meet all stated eligibility requirements. No changes to the team roster will be permitted after the team competes in their first CCDC event. The competition team must be chosen from the submitted roster. A competition team is defined as the group of individuals competing in a CCDC event.
    b. Each competition team may consist of up to eight (8) members chosen from the submitted roster.
    c. Each competition team may have no more than two (2) graduate students as team members.
    d. If the member of a competition team advancing to a qualifying, state, regional, or national competition is unable to attend that competition, that team may substitute another student from the roster in their place prior to the start of that competition.
    e. Once a CCDC event has begun, substitutions or additions of team members are

prohibited. A team must complete the competition with the team that started the competition.

f. Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and the teams before and during the competition. In the event of the Team Captain's absence, teams must have an identified team liaison serving as the captain in the competition space at all times during competition hours.

g. An institution is only allowed to compete one team in any CCDC event or season.

3. Team Representatives

a. Each team must have at least one representative present at every CCDC event. The representative must be a faculty or staff member of the institution the team is representing.

b. Once a CCDC event has started, representatives may not coach, assist, or advise their team until the completion of that event (including overnight hours for multi-day competitions).

c. Representatives may not enter their team's competition space during any CCDC event.

d. Representatives must not interfere with any other competing team.

e. Except in the event of an emergency, a representative must avoid contact with their team during CCDC competition hours and must not attempt to influence their team's performance in any way.

4. Competition Conduct

a. Throughout the competition, Operations and White Team members will occasionally need access to a team's system(s) for scoring, troubleshooting, etc. Teams must immediately allow Operations and White Team members' access when requested.

b. Teams must not connect any devices or peripherals to the competition network unless specifically authorized to do so by Operations or White Team members.

c. Teams may not modify the hardware configurations of competition systems. Teams must not open the case of any server, printer, PC, monitor, KVM, router, switch, firewall, or any other piece of equipment used during the competition. All hardware related questions and issues should be referred to the White Team.

d. Teams may not remove any item from the competition area unless specifically authorized to do so by Operations or White Team members including items brought into the team areas at the start of the competition.

e. Team members are forbidden from entering or attempting to enter another team's competition workspace or room during CCDC events.

f. Teams must compete without "outside assistance" from non-team members including team representatives from the start of the competition to the end of the competition (including overnight hours for multi-day events). All private communications (calls, emails, chat, texting, directed emails, forum postings, conversations, requests for assistance, etc.) with non-team members including team representatives that would help the team gain an unfair advantage are not allowed and are grounds for disqualification and/or a penalty assigned to the appropriate team.

g. No memory sticks, flash drives, removable drives, CDROMs, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.

h. All cellular calls, texts, smartphone usage, and so on must be made and received/viewed outside of the team's competition space and must not be used to receive outside assistance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.

i. Teams may not bring any computer, laptop, tablets, PDA, or wireless device into the competition area unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.

j. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.

k. Team sponsors and observers are not competitors and are prohibited from directly assisting any competitor through direct advice, "suggestions", or hands-on assistance. Any team sponsor or observers found assisting a team will be asked to leave the competition area for the duration of the competition and/or a penalty will be assigned to the appropriate team.

l. Team members will not initiate any contact with members of the Red Team during the hours of live competition. Team members are free to talk to Red Team members during official competition events such as breakfasts, dinners, mixers, and receptions that occur outside of live competition hours.

m. Teams are free to examine their own systems but no offensive activity against other teams, the Operations Team, the White Team, or the Red Team will be tolerated. This includes port scans, unauthorized connection attempts, vulnerability scans, etc. Any team performing offensive activity against other teams, the Operations Team, the White Team, the Red Team, or any global asset will be immediately disqualified from the competition. If there are any questions or concerns during the competition about whether or not specific actions can be considered offensive in nature contact the Operations Team before performing those actions.

n. Teams are allowed to use active response mechanisms such as TCP resets when responding to suspicious/malicious activity. Any active mechanisms that interfere with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams. Any firewall rule, IDS, IPS, or defensive action that interferes with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams.

o. All team members will wear badges identifying team affiliation at all times during competition hours.

p. Only Operations Team/White Team members will be allowed in competition areas outside of competition hours.

5. Internet Usage

a. Internet resources such as FAQ's, how-to's, existing forums and responses, and company websites, are completely valid for competition use provided there is no fee required to access those resources and access to those resources has not been granted based on a previous membership, purchase, or fee. Only resources that could reasonably be available to all teams are permitted. For example, accessing Cisco resources through a CCO account would not be permitted but searching a public Cisco support forum would be permitted. Public sites such as Security Focus or Packetstorm are acceptable. Only public resources that every team could access if they chose to are permitted.

b. Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. Teams are not allowed to access private Internet-accessible libraries, FTP sites, web sites, network storage, or shared drives during the competition. All Internet resources used during the competition must be freely available to all other teams. Accessing private staging areas is grounds for disqualification and/or a penalty assigned to the appropriate team.

c. No peer to peer or distributed file sharing clients or servers are permitted on competition networks unless specifically authorized by the competition officials.

d. Internet activity, where allowed, will be monitored and any team member caught viewing inappropriate or unauthorized content will be subject to disqualification and/or a penalty assigned to the appropriate team. This includes direct contact with outside sources through AIM/chat/email or any other public or nonpublic services including sites such as Facebook. For the purposes of this competition inappropriate content includes pornography or explicit materials, pirated media files, sites containing key generators and pirated software, etc. If there are any questions or concerns during the competition about whether or not specific materials are unauthorized contact the White Team immediately.

e. All network activity that takes place on the competition network may be logged and subject to release. Competition officials are not responsible for the security of any information, including login credentials, which competitors place on the competition network.

6. Permitted Materials

a. No memory sticks, flash drives, removable drives, CDROMs, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.
b. Teams may not bring any type of computer, laptop, tablet, PDA, cell phone, smart phone, or wireless device into the competition area unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.
c. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition as specified by the competition officials.

7. Professional Conduct

a. All participants, including competitors, coaches, White Team, Red Team, Operations Team, and Gold Team members, are expected to behave professionally at all times during all CCDC events including preparation meetings, receptions, mixers, banquets, competitions and so on.
b. In addition to published CCDC rules, Host Site policies and rules apply throughout the competition and must be respected by all CCDC participants.
c. All CCDC events are alcohol free events. No drinking is permitted at any time during competition hours.
d. Activities such as swearing, consumption of alcohol or illegal drugs, disrespectful or unruly behavior, sexual harassment, improper physical contact, becoming argumentative, willful violence, or willful physical damage have no place at the competition and will not be tolerated.
e. Violations of the rules can be deemed unprofessional conduct if determined to be intentional or malicious by competition officials.
f. Competitors behaving in an unprofessional manner may receive a warning from the White Team, Gold Team, or Operations Team for their first offense. For egregious actions or for subsequent violations following a warning, competitors may have a penalty assessed against their team, be disqualified, and/or expelled from the competition site. Competitors expelled for unprofessional conduct will be banned from future CCDC competitions for a period of no less than 12 months from the date of their expulsion.
g. Individual(s), other than competitors, behaving in an unprofessional manner may be warned against such behavior by the White Team or asked to leave the competition entirely by the Competition Director, the Operations Team, or Gold Team.

8. **Questions and Disputes, Disclosure**
    a. PRIOR TO THE COMPETITION: Team captains are encouraged to work with the Competition Director and their staff to resolve any questions regarding the rules of the competition or scoring methods before the competition begins.
    b. DURING THE COMPETITION: Protests by any team must be presented in writing by the Team Captain to the White Team as soon as possible. The competition officials will be the final arbitrators for any protests or questions arising before, during, or after the competition. Rulings by the competition officials are final. All competition results are official and final as of the Closing Ceremony
    c. In the event of an individual disqualification, that team member must leave the competition area immediately upon notification of disqualification and must not re-enter the competition area at any time. Disqualified individuals are also ineligible for individual or team awards.
    d. In the event of a team disqualification, the entire team must leave the competition area immediately upon notice of disqualification and is ineligible for any individual or team award.
    e. All competition materials including injects, scoring sheets, and team-generated reports and documents must remain in the competition area. Only materials brought into the competition area by the student teams may be removed after the competition concludes.

9. **Scoring**
    a. Scoring will be based on keeping required services up, controlling/preventing un-authorized access, and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing injects and maintaining services. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by the Red Team.
    b. Scores will be maintained by the competition officials and may be shared at the end of the competition. There will be no running totals provided during the competition. Team rankings may be provided at the beginning of each competition day.
    c. Any team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score. Should any question arise about scoring, the scoring engine, or how they function, the Team Captain should immediately contact the competition officials to address the issue.
    d. Teams are strongly encouraged to provide incident reports for each Red Team incident they detect. Incident reports can be completed as needed throughout the competition and presented to the White Team for collection. Incident reports must contain a description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, access obtained, damage done, etc.), a discussion of what was affected, and a remediation plan. A

thorough incident report that correctly identifies a successful Red Team attack may reduce the Red Team penalty for that event by up to 50 percent – no partial points will be given for incomplete or vague incident reports.

NECCDC Regional Competition Rules

In an effort to properly prepare winning teams for the national CCDC, the NECCDC makes use of national CCDC competition rules with the following clarifications:

1. **Software Use**
    a. EULA violations are considered a serious offense and may result in disqualification:
        i. No personal-only use or non-commercial trial software is allowed.
        ii. Commercial trials or free use software (e.g. Apache License, GPL) are allowed.
2. **Service Level Agreement**
    a. Physically disconnecting or powering-off of team network infrastructure is seen as a serious offense and will result in a point penalty roughly equivalent to 4 hours of downtime.
        i. Reloading of network infrastructure requires notification and approval prior to service disruption.
        ii. This policy extends to physical network connections for individual server systems.
3. **NECCDC Substitution Rule**
    a. Roster limited to 12 of the initially named students.
    b. At the beginning of each day of the regional competition up to 8 of students on the roster are named as competitors.
    c. Up to 2 graduate students are allowed during all time
    d. No substitutions are allowed during the day.
4. **Lab usage restrictions**
    a. Do not use other workstations or desktops in labs other than specifically assigned to the team.
    b. Do not set BIOS passwords on workstations
    c. No hardware level manipulations on workstations

NECCDC Scoring Methodology

Final scores will be awarded using the following point distribution:

Table 1. Final Score Weights

40%	Functional service uptimes and SLA violations as measured by the scoring engine.
40%	Successful completion of inject scenarios
20%	Incident Response and Red Team Activity

System restoration is not provided by the Black team and should be accounted for by the students themselves. In the case of hardware failure the Black team will endeavor to restore the hardware to the previous state, if possible. Any penalties that are incurred as a result of hardware failure will be removed.