

# **WELCOME TO THE 2019**



# **NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION**



*Presented by*

**Raytheon**

**2019 National Championship**

**April 23 – 25, 2019**

**Orlando, FL**

**Team Packet**

Conducted by the Center for Infrastructure Assurance and Security



## **Table of Contents**

|   |    |
|---|----|
| Welcome Letter from Dr. Gregory White ..... | 4  |
| Sponsors.....                               | 5  |
| Competition Schedule.....                   | 6  |
| Competition Rules.....                      | 7  |
| Scoring .....                               | 16 |
| Password Changes .....                      | 18 |
| Competition Network Information .....       | 19 |
| Team Network Diagram.....                   | 20 |
| Letter from Cryovine.....                   | 21 |
| Network Information.....                    | 2  |



# Raytheon

On behalf of the Institute for Cyber Security's Center for Infrastructure Assurance and Security (CIAS) and The University of Texas at San Antonio (UTSA), I'd like to welcome each of you to the National Collegiate Cyber Defense Competition. You have already won your regional competition and have demonstrated your operational skills and information security capabilities. We hope you will find this national competition a challenging learning experience which enhances and expands your skill set.

The CIAS and UTSA are excited to host the NCCDC, and we are very thankful to Raytheon, our sponsors, and our industry partners. Our staff, volunteers, and sponsors work hard to make this an interesting, exciting, and challenging competition. As most of you know, this three-day event has grown from modest beginnings to a significant positive impact on security programs around the nation. The competition is receiving increased attention from government and industry, and we expect this attention to continue to grow. As competitors, your input is valuable - the entire CCDC program has been shaped and refined based on feedback from past competitors. Please provide comments and feedback to help us improve the NCCDC and other future events. While this is a competition, we encourage you to take a few minutes to meet your competitors, talk to the vendors and sponsors, and enjoy yourselves. We wish you and your team the very best of luck!

Gregory White, Ph.D.  
Director  
Center for Infrastructure Assurance and Security

# 2019



NATIONAL  
COLLEGIATE  
CYBER  
DEFENSE  
COMPETITION

Presented By

# Raytheon

## PLATINUM



AIR FORCE  
RESERVE

Uber

InfoSec



REliaquest

## PROGRAM



NSA  
WHERE INTELLIGENCE GOES TO WORK  
[IntelligenceCareers.gov/NSA](http://IntelligenceCareers.gov/NSA)

Naval Information  
Warfare Center  
ATLANTIC



FIRE EYE™

## GOLD

Southwest.

information security

splunk>

BOEING

## SILVER

FORCEPOINT  
Powered by Raytheon

SAIC.  
Redefining Ingenuity

PROFI TAP

## SPONSORS

Carnegie  
Mellon  
University

Information  
Networking  
Institute

COBALT STRIKE  
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

G-C PARTNERS

Randori

W  
UNIVERSITY of WASHINGTON | BOTHELL  
MASTER OF SCIENCE IN CYBER SECURITY ENGINEERING



# Raytheon

## Competition Schedule

Please note that due to the nature of the competition, schedule changes may occur.

### Tuesday, April 23<sup>rd</sup>

|                 |                                |
|-----------------|--------------------------------|
| 8:00 – 8:45 AM  | Registration                   |
| 9:00 – 10:00 AM | Opening Remarks – Salon 3/4    |
| 12:00 – 1:00 PM | Lunch (brought to team rooms)  |
| 3:00 PM         | Afternoon Break – Salon 3/4    |
| 6:15 PM         | Competition Stop               |
| 7:00 – 10:00 PM | Kickoff Dinner – Signature 2** |

### Wednesday, April 24<sup>th</sup>

|                   |                                      |
|-------------------|--------------------------------------|
| 9:00 – 9:45 AM    | Opening Remarks – Salon 3/4          |
| 12:00 – 1:00 PM   | Lunch (brought to team rooms)        |
| 3:00 PM           | Afternoon Break – Salon 3/4          |
| 6:15 PM           | Competition Stop                     |
| 7:00 PM – 9:00 PM | Networking Reception – Executive H** |

### Thursday, April 25<sup>th</sup>

|                     |  |
|---------------------|--|
| 9:00 – 11:00 AM     | Panoply – Salon 9/10                           |
| 11:00 AM – 12:00 PM | Lunch for competitors and coaches – Salon 9/10 |
| 12:00 – 2:00 PM     | Awards Ceremony – Salon 3/4                    |

**\*\* - These events are for competitors, coaches, sponsors, Red Team members, and invited guests only.**



# Raytheon

## Competition Rules

### Overview

The competition is designed to test each team's ability to secure and administer networked computer systems while maintaining standard business functionality. The scenario involves team members simulating a group of new employees brought in to manage and protect the IT infrastructure at a small aerospace and defense Contractor. The teams are expected to manage the computer network, keep it operational, and control/prevent any unauthorized access. Each team will be expected to maintain and provide public services: a website, an email server, a database server, an application server, and workstations used by simulated sales, marketing, and research staff. Each team will start the competition with a set of identically configured systems.

The objective of the competition is to measure each 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. A technical success that impacts the business operation will result in a lower score, as will a business success which results in security weaknesses.

Throughout these rules, the following terms are used:

- Gold Team/Operations Team - competition officials that organize, run, and manage the competition.
- White Team - competition officials that observe team performance in their competition area and evaluate team performance and rule compliance.
- Red Team - penetration testing professionals simulating external hackers attempting to gain unauthorized access to competition teams' systems.
- Black Team - competition support members that provide technical support, pick-up and deliver communications, and provide overall administrative support to the competition.
- Blue Team/Competition Team - the institution competitive teams consisting of students competing in a CCDC event.
- Team Captain - a student member of the Blue Team identified as the primary liaison between the Blue Team and the White Team.
- Team Co-Captain - a student member of the Blue Team identified as the secondary or backup liaison between the Blue Team and the White Team, should the Team Captain be unavailable (i.e. not in the competition room).
- Team representatives - a faculty or staff representative of the Blue Team's host institution responsible for serving as a liaison between competition officials and the Blue Team's institution.



# Raytheon

## 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 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.
- c. A team member may not participate in any role at CCDC events held outside the region in which their team competes during the same CCDC season.
- d. Individuals who have participated in previous CCDC events in any role other than as a competitor must obtain eligibility approval from the director of the region in which their team competes prior to being added to the team roster. Once a candidate's eligibility has been approved, they will remain eligible for all CCDC events during the same 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.



# Raytheon

- 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, a team must complete the competition with the team that started the competition. Substitutions, additions, or removals of team members are prohibited except for extreme circumstances.
  - i. Team Representatives must petition the Competition Director in writing for the right to perform a change to the competition team.
  - ii. The Competition Director must approve any substitutions or additions prior to those actions occurring.
- f. Teams or team members arriving after an event's official start time, for reasons beyond their control, may be allowed to join the competition provided a substitution has not already been made. Event coordinators will review the reason for tardiness and make the final determination.
- g. 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 during competition hours.
- h. An institution is only allowed to compete one team in any CCDC event or season.
- i. A CCDC team may only compete in one region during any given CCDC season.
- j. Exhibition teams are not eligible to win any CCDC event and will not be considered for placement rankings in any CCDC event.

### 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. The representative, or any non-team member, must not discuss any aspect of the competition event, specifically event injections, configurations, operations, team performance or red team functions, 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. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
- h. Team representatives, 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.
- i. 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.

- j. Teams are free to examine their own systems but no offensive activity against any system outside the team's assigned network(s), including those of other CCDC teams, will be tolerated. Any team performing offensive activity against any system outside the team's assigned network(s) will be immediately disqualified from the competition. If there are any questions or concerns during the competition about whether specific actions can be considered offensive in nature contact the Operations Team before performing those actions.
- k. Teams can 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.
- l. All team members will wear badges identifying team affiliation during competition hours.
- m. Only Operations Team/White Team members will be allowed in competition areas outside of competition hours.

## 5. Internet Usage

- a. Internet resources such as FAQs, 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, email accounts, or shared drives during the competition. All Internet resources used during the competition must be freely available to all other teams. The use of external collaboration and storage environments such as Google Docs/Drive is prohibited unless the environment was provided by and is administered by competition officials. Accessing private staging areas or email accounts 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 non-public 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 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, Ops Team, and Gold Team members, are expected to behave professionally 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, Disputes, and Disclosures

- 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.



# Raytheon

- 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. Any team member that modifies a competition system or system component, with or without intent, to mislead the scoring engine into assessing a system or service as operational, when in fact it is not, may be disqualified and/or the team assessed penalties. Should any question arise about scoring, the scoring engine, or how scoring functions, 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 and addresses a successful Red Team attack may reduce the Red Team penalty for that event – no partial points will be given for incomplete or vague incident reports.

## 10. Remote/ Team Site Judging and Compliance

- a. This section does not apply at the 2019 National CCDC

## 11. Local Competition Rules

- a. MP3 players may be brought into competition rooms and are permitted with headphone use only.
- b. Incident reports must be complete to receive any consideration for points. You may create your own form, but all incident reports must have team number, date, source IP, destination IP, date/time of activity, description of activity, and remediation/mitigation plans. Only incident reports that correspond to actual Red Team activity where your team lost points will be considered for point recovery. “I got port scanned” is not a valid incident response report.
- c. No unapproved operating system or application changes are permitted (servers or workstations). You may patch, apply service packs, and update but you must defend what you are given unless otherwise stated.
- d. You may not migrate any critical services, operating systems, or systems from a hardware platform to a virtualized platform (or vice versa) without authorization.
- e. You may not containerize any platform or service without authorization.
- f. You may not migrate or replicate any critical services to a different platform or system without authorization.
- g. You may setup a DMZ or NAT critical services provided the critical service is always reachable on the “public” IP address and fully qualified domain name it was initially assigned.



# Raytheon

- h. You must configure all SMTP servers (physical and virtual) to allow the scoring engine to connect to and send mail from a valid user at your organization to another valid user at the same organization. For example the scoring engine must be able to connect as [bob@cryovine.com](mailto:bob@cryovine.com) and send email to [tina@cryovine.com](mailto:tina@cryovine.com).
- i. Food and drinks may be brought into team rooms but **MUST** be placed on tables away from competition equipment. No eating or drinking at the keyboard!
- j. Teams must not intentionally disconnect competition systems from the network unless you are moving cables from one system to another. All systems must remain connected to the network, be powered up, and be operational in their assigned role. This includes user workstations and virtual systems.
- k. All inject responses and deliverables must be typed and delivered electronically where possible either via upload or USB key.
- l. You must maintain both the functionality and content of all critical services. For example, a website that serves dynamic content must continue to serve up dynamic content. An FTP service that allows anonymous access must continue to allow anonymous access.
- m. Teams must respond to customer requests from the Orange Team. These activities are monitored and do factor into your overall score.
- n. You must use the email address provided to you by the NCCDC staff to register for any freeware/shareware you use during the competition. If registration for an account requires clicking an activation link, please inform the Operations staff. You will not have access to the email account – it is only to be used for account registrations or activations.
- o. Password changes to user accounts for critical services must be provided to the Operations team in electronic format.
- p. If you configure SPOP, you must inform the Operations Team prior to making the change and you must run SPOP on TCP port 995.
- q. Proxy addition requests must be made in writing and submitted to the Operations Team.
- r. GitHub projects written by team members or affiliates must have existed and have been publicly available for at least 6 months prior to the NCCDC, must not be competition specific, and must have relevance and use to the security/IT community at large. All requests for access to GitHub or other Internet resources will be reviewed and may be denied if deemed inappropriate for competition use.

## Scoring

The winner will be determined by the highest cumulative score at the end of the competition. Accumulated point values are broken down as follows (some variance in points may occur due to the timing and randomization of scoring engine checks):

- Critical services account for roughly half the possible points (based on a random polling interval of core services)
- Successful completion of business tasks account for roughly half the possible points (awarded points will vary by task, but will be part of a cumulative total)
- Orange Team actions factor into inject point totals and Orange Team members will be scoring some injects



# Raytheon

Successful Red Team actions will result in point deductions from a team's total score based on the level of access obtained, the sensitivity of information retrieved, critical services affected, and so on. Failure to support Orange Team requests will result in point deductions and penalties.

## Functional Services

Certain services are always expected to be operational or as specified throughout the competition. In addition to being up and accepting connections, the services must be functional and serve the intended business purpose. At semi-random intervals, certain services will be tested for functionality and content where appropriate. Each successfully served request will gain the team the specified number of points. Unresponsive services are always marked as failures.

## HTTP/HTTPS

A request for a specific web page will be made. Once the request is made, the result will be stored in a file and compared to the expected result using an MD5 sum of the returned page and key words/phrases on the page. The returned content must match the expected content for points to be awarded.

## SMTP

Email will be sent and received through a valid email account via SMTP. This will simulate an employee in the field using their email. Each successful test of email functionality will be awarded points. SMTP services must always be able to support unauthenticated sessions. The scoring engine must be able to connect to your SMTP and be able to send mail from one valid user to another valid user. For example, [bob@cryovine](mailto:bob@cryovine) must be able to send mail to [tina@cryovine.com](mailto:tina@cryovine.com).

## POP3

A simulated user connection will be made using a valid userid and password to check for mail. POP services must accept logins as described in the critical service description. POP services must support logins with a simple userid and password (such as "bevans" with a password of "afk\$tmgh"). SPOP, APOP, and plaintext are the only supported authentication methods. Changes in POP3 authentication must be coordinated with the Operations Team prior to implementation.

## SSH

An SSH session will be initiated to the system using a valid user account and password. The user will attempt to execute a specific command within that session. If the login and command are successful, points are awarded.

## DNS

DNS lookups will be performed against the DNS server. Each successfully served request will be awarded points.



# Raytheon

## FTP

Connections will be made to the FTP server (either as anonymous or as a valid user depending on what is detailed in the critical service description) to check for the presence and availability of specific files (both file presence and integrity are checked). Failed logins, missing files, or modified/corrupt files will cause the check to fail.

**Each** of the critical services operates under a Service Level Agreement (SLA) and teams will be assessed penalties for extended critical service outages. If any critical service is continuously down for 6 service checks, the team will be assessed a 20-point penalty. After a service is down for 6 consecutive checks, **each additional 6 consecutive checks** where the service is down will result in an additional 20-point penalty.

**NOTE:** If you modify the configuration of any critical service, such as adding a userid/password where none existed before, modifying a user level password, or changing authentication methods you MUST coordinate with the Operations Team desk prior to making that change.

## Business Tasks (Injects)

Each team will be presented with identical business tasks at various points during the competition. Points will be awarded based upon successful completion of each business tasking or part of a tasking. Tasks will vary in nature and points and will be weighted based upon the difficulty, importance, and time sensitivity of the tasking. Tasks may contain multiple parts with point values assigned to each specific part of the tasking.

Some examples:

- Opening an FTP service for 2 hours given a specific user name and password: 200 points
- Closing the FTP after the 2 hours is up: 50 points
- Creating/enabling new user accounts: 100 points
- Installing new software package on CEO's desktop within 30 minutes: 100 points

Every team must try to complete each task. Failure to attempt completion of any tasking will result in a team penalty and can result in a "firing" of team members. You MUST provide a response to ALL injects that require a written deliverable or report (even if your "deliverable" just says you didn't complete the inject).

## Red Team Actions

Successful Red Team actions will result in penalties that reduce the affected team's score. Red Team actions include the following (penalties may be different than listed below):

- Obtaining root/administrator level access to a team system: -100 points
- Obtaining user level access to a team system (shell access or equivalent): -25 points
- Recovery of userids and passwords from a team system (encrypted or unencrypted): -50 points
- Recovery of one or more sensitive files or pieces of information from a team system (configuration files, corporate data, etc.): -25 points



- Recovery of customer credit card numbers: -50 points
- Recovery of personally identifiable customer information (name, address, and credit card number): -200 points
- Recovery of encrypted customer data or an encrypted database: -25 points

Red Team actions are cumulative. For example, a successful attack that yields root level access and allows the downloading of userids and passwords will result in a -150-point penalty. Red Team actions are scored on a **per system** and **per method** basis – a buffer overflow attack that allows the Red Team to penetrate a team's system will only be scored once for that system; however, a different attack that allows the Red Team to penetrate the same system will also be scored. Only the highest level of account access will be scored per attack – for example, if the Red Team compromises a single user account and obtains root access in the same attack the penalty will be -100 points for root level access and not -125 points for root and user level access. Please note the point values described above are examples – actual penalty points may be adjusted to match competition environment.

Red Teams can also execute additional malicious action based on their access. Attacks such as defacing websites, disabling or stopping services, adding/removing users, and removing or modifying files are permitted and may occur.

## Password Changes

If your team changes user level passwords for **scored** services that require a password (such as SSH, POP3, and FTP) you must provide a comma separated text file containing your password changes to the Operations Team (in electronic format). The file should contain comma separated values with one user per line like this:

```
user, password  
user2, password2
```

The only information inside the file should be the users and passwords – **do not** include headers or any other additional information inside the file. You must provide 1 file for EACH service that requires password changes – **do not** include multiple services in the same file. Name the file “TeamXX\_SERVICE\_PWD” and replace XX with your team number and SERVICE with the critical service these password changes apply to. For example, a password file for the REM\_SSH service must be named “TeamXX\_Rem\_SSH\_PWD”. An improperly named file will be rejected. Accepted files will be loaded into the scoring engine as is. You must allow 10 to 15 minutes for password changes to take effect. **You DO NOT need to provide us with password changes to “root” or “administrator” accounts – only user accounts.** You must bring password change files to the Operations Team via the provided USB key. Passwords can be up to 24 characters long and may consist of any combination of upper case letters, lower case letters, numbers, and the following special characters: . @ # \$ % & ! ? : \* ^ \_ - + = < > ~



# Raytheon

## Competition Network Information

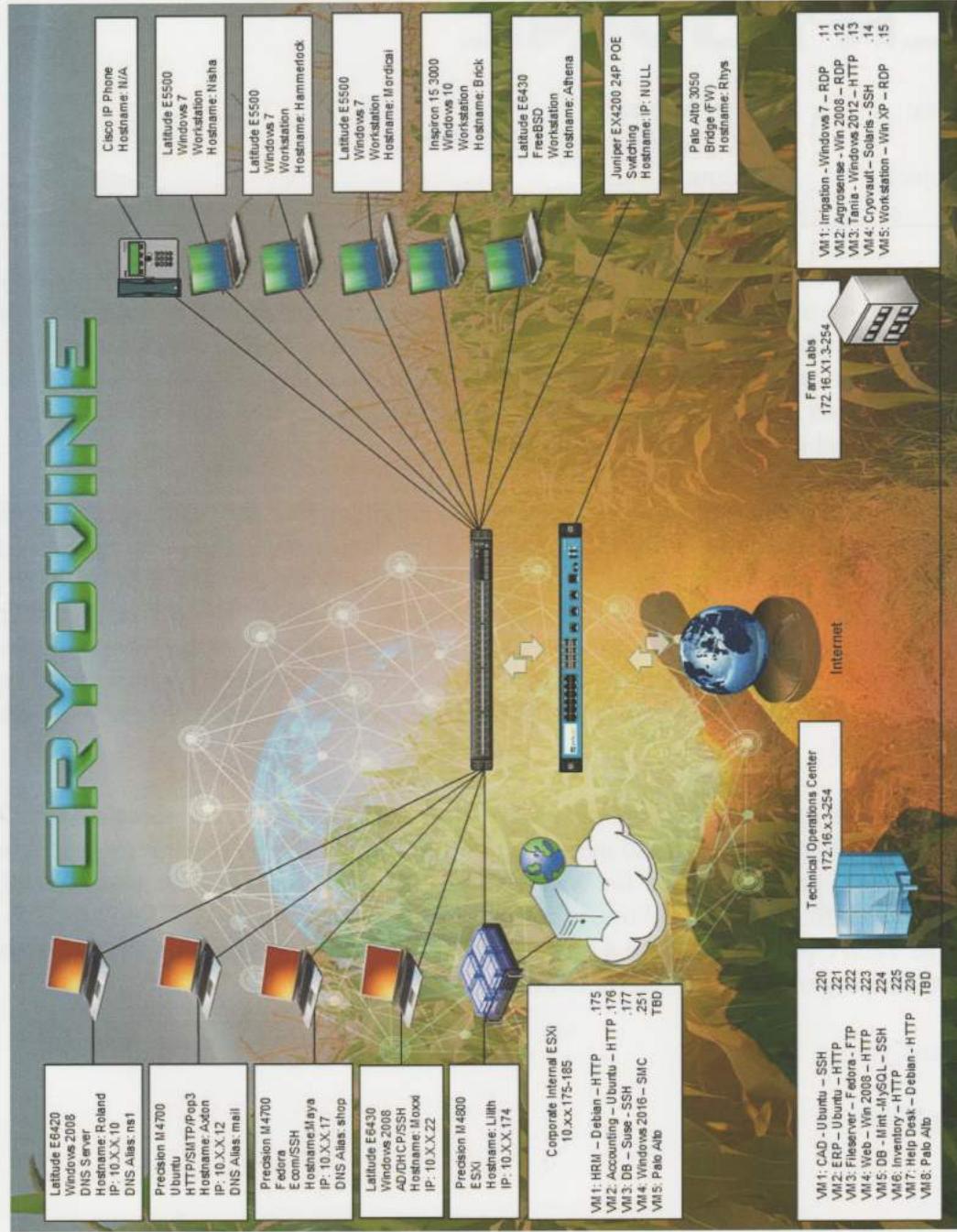
Here are some network addresses you will want to take note of:

- 10.120.0.9 – Software/patch server
- 10.120.0.10 – NTP server for official competition time
- 10.120.0.20 – Team inject portal
- 10.120.0.100 – Core VoIP server (your VoIP phone must be able to communicate with this IP)
- 10.120.0.53 – Primary External DNS (use your team's DNS server first, and this as the secondary)
- 10.X.X.1 – Default route for your team's core network
- 172.16.X.1 – Default route for your team's Tech Ops network
- 172.16.X.2 – IP address for your team's Tech Ops vSphere server (use an HTML 5 compliant browser to access it on TCP port 443)
- 172.16.X1.1 – Default route for your team's Farm Lab systems
- 192.168.7.X – IP address of your team's Splunk instance (where X is the same as your core network, Team 1 = 10, Team 2 = 20, ...)
  
- 10.111.1.200 – Printer #1 (HP Laserjet – use HP universal printer driver from software portal)
- 10.111.1.201 – Printer #2 (HP Laserjet – use HP universal printer driver from software portal)



# Raytheon

Team Network Diagram





# Raytheon

## Letter from the CEO

### CRYOVINE

From: Michael Mamaril  
To: New Cyber Security and IT Gurus  
Subject: Welcome

---

Welcome to Cryovine! We are thrilled to have you on board. As you know from your hiring briefings, we are an agriculture firm specializing in cryogenic seed storage, plant development, and farm to table initiatives. Our previous administrative staff is no longer with us. The network and services seem to be “working”, but I would not take anything for granted. I have my suspicions our network was hacked into recently and I’m sure the previous admins would not have detected it.

You are now responsible for managing and maintaining this network. Patch and repair as you see fit, but before making any big changes like replacing applications or operating systems come see me or our CIO for approval. We’re not making any big changes right away so plan on fixing what’s here first and then we’ll talk about changes. Be careful when you upgrade/patch, as some of the systems are precisely configured to support current operations. Some of these applications might be sensitive to changes in patch level, passwords, and registry settings. Make sure you can quickly roll back any changes that affect critical services. And make sure you backup our critical data!

Our network has three major sections. The headquarters office, our remote Tech Ops office, and our remote Farm Lab research network. You should be able to reach remote systems using RDP or SSH as appropriate (RDP for Windows systems, SSH for non-Windows typically). You are responsible for securing and operating both network environments. The Farm Lab is connected to the Tech Ops network with a direct link, but it should be accessible from any system in our core network or our Tech Ops network.

Thank you,

Big Mike



# Raytheon

## Network Information from the Director of IT

The outline below details what little documentation was provided by the former administrative team on the inner workings of our infrastructure. While the executive staff recognizes this information is spotty at best, it should provide your team with enough details to get you started.

### Overall Network Architecture:

#### Network Details:

Teams are assigned IP blocks as listed below (Corporate – 10.X.X.X, Tech Ops – 172.16.X.X, Farm – 172.16.X1.X):

Team 1 10.10.10.0, 172.16.10.0, and 172.16.11.0  
Team 2 10.20.20.0, 172.16.20.0, and 172.16.21.0  
Team 3 10.30.30.0, 172.16.30.0, and 172.16.31.0  
Team 4 10.40.40.0, 172.16.40.0, and 172.16.41.0  
Team 5 10.50.50.0, 172.16.50.0, and 172.16.51.0  
Team 6 10.60.60.0, 172.16.60.0, and 172.16.61.0  
Team 7 10.70.70.0, 172.16.70.0, and 172.16.71.0  
Team 8 10.80.80.0, 172.16.80.0, and 172.16.81.0  
Team 9 10.90.90.0, 172.16.90.0, and 172.16.91.0  
Team 10 10.100.100.0, 172.16.100.0, and 172.16.101.0

Subnet mask: 255.255.255.0

Default gateway: Always the .1 address of the network.

**NOTE:** The .1 addresses on the above subnets belong to the operations network and are your default gateways for these networks. Do not attempt to use the .1 address inside your team network. Do not scan, ping, probe, or interfere with .1.

The Tech Ops systems are cloud-based and running on an ESXi platform outside your team room. You are responsible for the security of those systems and the ESXi server they run on. The Tech Ops systems reside on the 172.16.X.0 network assigned to your team (see above). Tech Ops systems must remain accessible on their assigned “public” 172.16.X.X IP address assigned to your team. Authorized corporate users (including external users), our researchers, and service providers should be able to access Tech Ops systems from any source IP address via RDP for Windows systems and SSH for non-Windows systems.

The systems in your Farm Lab network are running in a cloud service – you will not have access to the server hosting them. Your Farm Lab systems should only be accessible to subnets belonging to your team. From within your 10.X.X.0 and 172.16.X.0 networks, you should be



# Raytheon

able to connect to the Farm Lab systems on HTTP, RDP, or SSH services as appropriate. Farm Lab systems will need outbound access (HTTP/HTTPS, DNS, ICMP, and so on) at all times.

*Networks available for internal NAT:*

You may use any 10.X.X.0 network for internal NAT where the second octet matches your team network's second octet. For example, Team 1 could use 10.10.11.0, Team 2 could use 10.20.22.0, Team 3 could use 10.30.33.0, and so on. If you choose to NAT your systems you must still provide "public" access to all critical services on the specified IP addresses.

*Users:*

Valid user accounts must remain active on all systems where they appear. You may not delete or disable valid user accounts. Accounts identified as administrators must have direct access to all critical services (RDP, SSH, FTP, SMB, and so on) and the ability to login to those services using their own accounts. For example, a user with administrative level permissions should be able to SSH to any of the scored SSH services and RDP/SSH to any remote system in the R&D networks using their own account.

*Company Directory:*

A company directory is available in our corporate HRM system.

*Passwords:*

A password sheet with known administrator/root passwords will be in your team rooms.

*Internet Proxy:*

All Internet bound traffic will pass through a transparent proxy. Connection attempts to sites not allowed in the proxy will be denied. You may submit written requests to add sites to the proxy. Sites will be reviewed and may or may not be added at the discretion of competition officials.

SSL Certificates for the proxy can be found on the software portal in a directory called "Proxy Certificates". Installing these certificates on your systems will help address any issues you might have with certificate errors. Please install the certificate as a "Trusted Root Certification Authority" and not as a personal certificate.

*DHCP:*

Your corporate network must maintain a DHCP service with an address pool from 10.X.X.101 to 10.X.X.150 (where X is your team network, Team 1=10, Team 2=20, and so on).



# Raytheon

### Critical Services:

For our business to function properly, the following services must always be available and open to any external IP address (except the SMB services as described below). Please note the names of the critical services – these are the names you must use when submitting password changes (ie use POP3 as the service name). The critical service must remain accessible on the IP address specified and must provide the content and functionality from its original configuration (unless you are directed to or required to make modifications by an inject). For example, an FTP service that supports anonymous read access must always support anonymous read access and a static website must provide all the original content throughout the competition.

- ECOM: You must maintain the HTTP service on 10.X.X.17
- HRM: You must maintain the HTTP service on 10.X.X.175
- DNS: You must maintain the DNS service on 10.X.X.10
- FTP: You must maintain the FTP service on 172.16.X.222
- POP3: You must maintain the POP3 service on 10.X.X.12
- SMTP: You must maintain the SMTP service on 10.X.X.12
- HELP\_DESK: You must maintain the HTTP service on 172.16.X.230
- WWW: You must maintain the HTTP service on 172.16.X.223
- SSH1: You must maintain the SSH service on 10.X.X.176
- SSH2: You must maintain the SSH service on 172.16.X.224
- ERP: You must maintain the HTTP service on 172.16.X.221

**NOTE:** All critical services operate under an SLA agreement. A penalty will be assessed every time an SLA violation occurs. An SLA violation is defined as the failure of 6 consecutive checks.



# Raytheon

### **Farm Lab Services:**

The following services must be accessible at all times from any system in your team's subnets (10.X.X.0 and 172.16.X.0):

- RDP on 172.16.X1.11
- RDP on 172.16.X1.12
- RDP and HTTP/port 8080 on 172.16.X1.13
- SSH on 172.16.X1.14
- RDP on 172.16.X1.15

### **Additional network services:**

In addition to the critical services you are scored on, your team must also abide by the following directives concerning network traffic.

ICMP – You must always allow ICMP traffic from 10.120.0.0/16, 10.111.0.0/16, and 192.168.251.0/24 to reach **all** systems in your core and Tech Ops networks. Your systems must respond to ICMP traffic from the subnets listed above.

VoIP - Inside your network is a Cisco VoIP phone with an IP address of 10.X.X.252. You must allow it to communicate with the 10.120.0.X network for your voice service to work. If you restrict the traffic to/from this phone you must determine the ports required for VoIP communications and allow those in and out of your network.

Internally you will also need to maintain:

- File Servers
- Client Workstations
- Active Directory
- Access to critical services
- Network Printing to competition printers
- Internet Access for workstations

### **Outbound Services:**

Your user base will need outbound access to common protocols such as HTTP, HTTPS, SSH, FTP, SFTP, POP3, DNS, and update services. Internet bound traffic should be passing through a transparent proxy. All systems should be configured to use your team's DNS server first (10.X.X.10) and 10.120.0.53 second. DNS queries to any other name server will be rejected.

**As our business needs change, so might the preceding list of critical and outbound services shown above.** The list provided is merely a snapshot in time of current critical services. Failure



# Raytheon

to provide any of these services for a prolonged amount time costs our company money and may ultimately cost you your job.

Please note that systems identified as a “Workstation” must remain user workstations and cannot be re-tasked, reloaded, or otherwise altered unless you receive an inject instructing you to do so.

**CCS Service:**

On many of your team systems you may notice a service called “CCSClient”. This is a scoring process used by competition officials. You must leave this process in place and running on any Windows, Debian, Fedora, or Ubuntu system inside your corporate and R&D network. You must allow this process to communicate with the 10.120.0.0/16 network on port 80 at all times. Do not modify any files in C:\CCS on Windows systems or /opt/CCS on Linux systems. The CCSClient is already installed on any backup images provided to you, but if you perform a clean install of any Windows, Debian, or Ubuntu system you must place the CCSClient onto that system after the installation. Installation files for the CCS Client are available on the software portal.