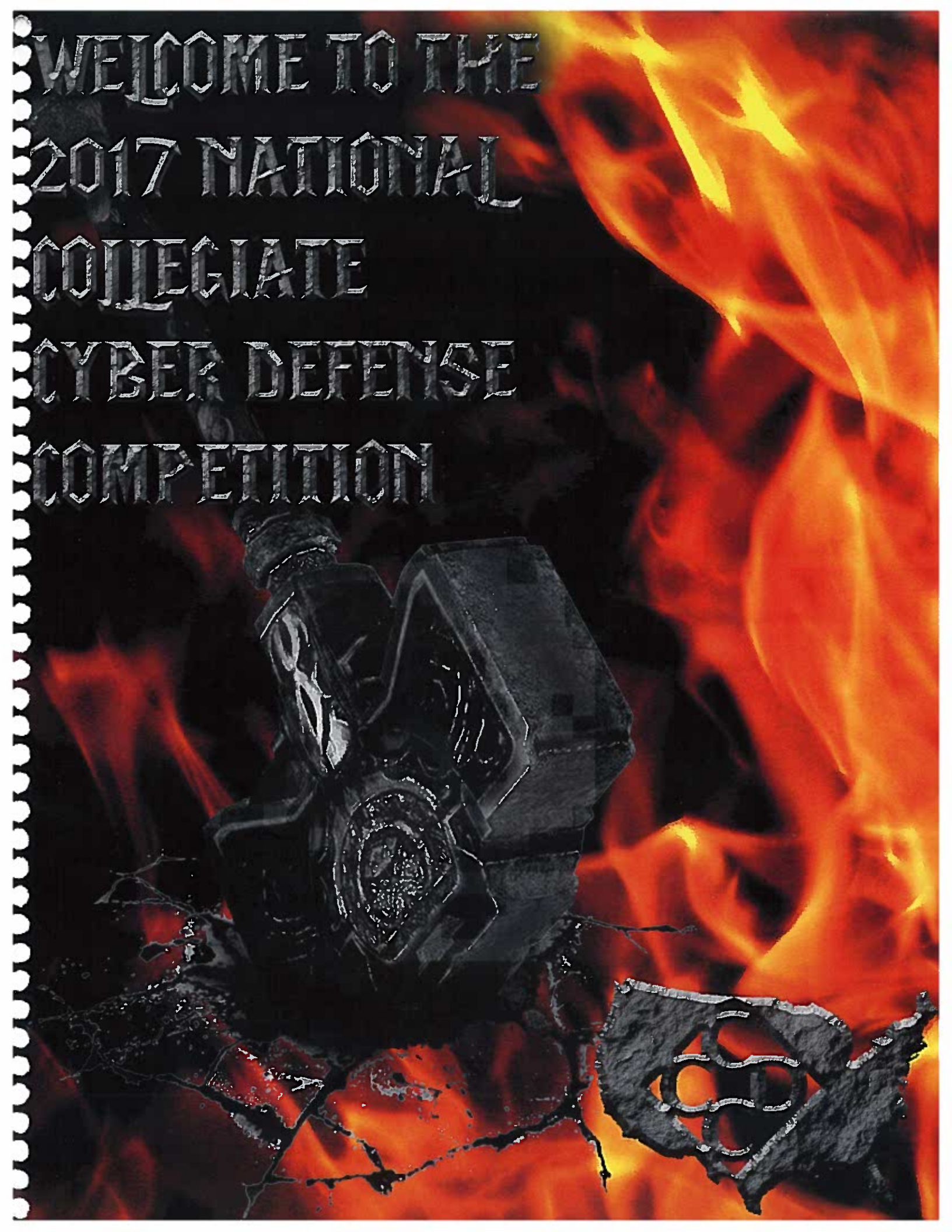
WELCOME TO THE 2017 NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION



Presented by

Raytheon

2017 National Championship

April 13 – 15, 2017

San Antonio, TX

Team Packet

Conducted by the Center for Infrastructure Assurance and Security

Table of Contents

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

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 eleventh 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, industry partners, and the Department of Homeland Security Science and Technology Directorate. 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 explore our wonderful city. We wish you and your team the very best of luck!

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

2017

National Collegiate Cyber Defense Competition

Presented By

Raytheon

Platinum Sponsors

Accenture Security

Walmart Technology

Program Sponsors

Homeland Security Science and Technology

paloalto ACADEMY

IBM Security

Gold Sponsors

amazon security

BOEING

FireEye

splunk>

Trustwave

UBER

Sponsors

AT&T

Carnegie Mellon University Information Networking Institute

DOUBLESTRIKE

HACKER ON RETAINER

LAYER3

shopify

UNIVERSITY of WASHINGTON BOTHELL

Competition Schedule

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

Thursday, April 13th	**All events are at the Henry B. Gonzalez Convention Center**
8:00 – 8:45 AM	Breakfast (Room 214 A&B)**
8:00 – 8:45 AM	Registration (Outside Room 214 A&B)
9:00 – 10:00 AM	Opening Remarks (Room 214 A&B)
12:00 – 1:00 PM	Lunch (brought to team rooms)**
3:30 PM	Afternoon Break (Room 214 A&B)
6:15 PM	Competition Stop
7:00 – 9:00 PM	Presenting Sponsor Dinner (Room 214 A&B)**
Friday, April 14th	
8:00 – 8:45 AM	Breakfast (Room 214 A&B)**
9:00 – 9:30 AM	Opening Remarks (Room 214 A&B)
12:30 – 1:30 PM	Lunch (brought to team rooms)**
3:30 PM	Afternoon Break (Room 214 A&B)
6:15 PM	Competition Stop
7:00 PM – 9:00 PM	Networking Reception (Room 214A&B)**
Saturday, April 15th	
8:00 – 8:50 AM	Breakfast (Room 214 C&D)**
9:00 – 11:30 AM	Panoply (Room 214 C&D)
11:30 – 12:30 PM	Luncheon (Room 214 C&D)**
12:30 – 2:00 PM	Awards Ceremony (214 A&B)

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

Raytheon

Overview

On February 27 and 28, 2004, a group of educators, students, government and industry representatives gathered in San Antonio, Texas, to discuss the feasibility and desirability of establishing regular cyber security exercises with a uniform structure for post-secondary level students. During their discussions, this group suggested the goals of creating a uniform structure for cyber security exercises might include the following:

1. Providing a template from which any educational institution can build a cyber security exercise;
2. Providing enough structure to allow for competition among schools, regardless of size or resources;
3. Motivating more educational institutions to offer students an opportunity to gain practical experience in information assurance.

The group also identified concerns related to limiting participation to post-secondary students, creating a level playing field to eliminate possible advantages due to hardware and bandwidth differences, having a clear set of rules, implementing a fair and impartial scoring system, and addressing possible legal concerns.

To help facilitate the development of a regular, national level cyber security exercise, the Center for Infrastructure Assurance and Security (CIAS) at the University of Texas at San Antonio agreed to host the first Collegiate Cyber Defense Competition (CCDC) for the Southwestern region. While like other cyber defense competitions in many aspects, the CCDC is unique in that it focuses on the operational aspect of managing and protecting an existing network infrastructure. While other exercises examine the abilities of a group of students to design, configure, and protect a network over the course of an entire semester, this competition is focused on the more operational task of assuming administrative and protective duties for an existing "commercial" network. Teams will be scored based on their ability to detect and respond to outside threats, maintain availability of existing services such as mail servers and web servers, respond to business requests such as the addition or removal of services, and balance security needs against business needs. The list of items below will create a fair and even playing field.

- Each team will begin with an identical set of hardware and software: Each team will be given a small, pre-configured, operational network they must secure and maintain. This eliminates any potential advantage for larger schools or organizations that may have better equipment or a larger budget.
- Each team will be located on a dedicated internal network: To remove the variables associated with VPNs and propagation delay, each team's network will be connected to a competition network allowing equal bandwidth and access for scoring and Red Team operations. This also allows tight control over competition traffic.
- Each team will be provided with the same set of business objectives and tasks at the same time during the competition. Only team members, Operations Team members, Gold Team members, Orange Team members, Sponsors, Observers, and White Team members will be allowed inside their competition rooms: Each team will be assigned their own room during the competition and only the members of the team will be allowed inside during the competition. This eliminates the potential influence of coaches or mentors during the competition.
- A non-biased Red Team will be used: A non-biased, volunteer, commercially experienced Red Team will be used during the competition.

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.

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.

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.

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.
   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 2017 National CCDC

11. **Local Competition Rules**

a. MP3 players may be brought into competition rooms and are permitted with headphone use only. Smart phones may not be used as MP3 players.

b. Incident reports must be complete to receive any consideration for points. You may use the provided form or create your own 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 on Day One of the competition. You may patch, apply service packs, and update but you must defend what you are given for the first day.

d. You may not migrate any critical services, operating systems, or systems from a hardware platform to a virtualized platform (or vice versa) without express permission.

e. You may not migrate or replicate any critical services to a different platform or system without prior permission.

f. 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.

g. 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@dwarvenhammer.com and send email to tina@dwarvenhammer.com.

h. 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!
i. 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.
j. All inject responses and deliverables must be typed and delivered electronically where possible either via upload or USB key.
k. 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.
l. Teams must respond to customer requests from the Orange Team. These activities are monitored and do factor into your overall score.
m. 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 be have access to the email account – it is only to be used for account registrations or activations.
n. Password changes to user accounts for critical services must be provided to the Operations team in electronic format. For more details refer to the discussion in your team packet.
o. If you configure SPOP, you must inform the Operations Team prior to making the change and you must run SPOP on TCP port 995.
p. Proxy addition requests must be made in writing to the Operations Team.

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

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 may 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
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.

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.

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.

SQL
An SQL request will be made to the database server. The result will be stored and compared against an expected result. Each successfully served SQL request will be awarded points.

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

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, or modifying a user level password, 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:

- 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.

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 SSH) 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: . @ # $ % & ! ? : * ^ _ - + = < > ~

Competition Network Information

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

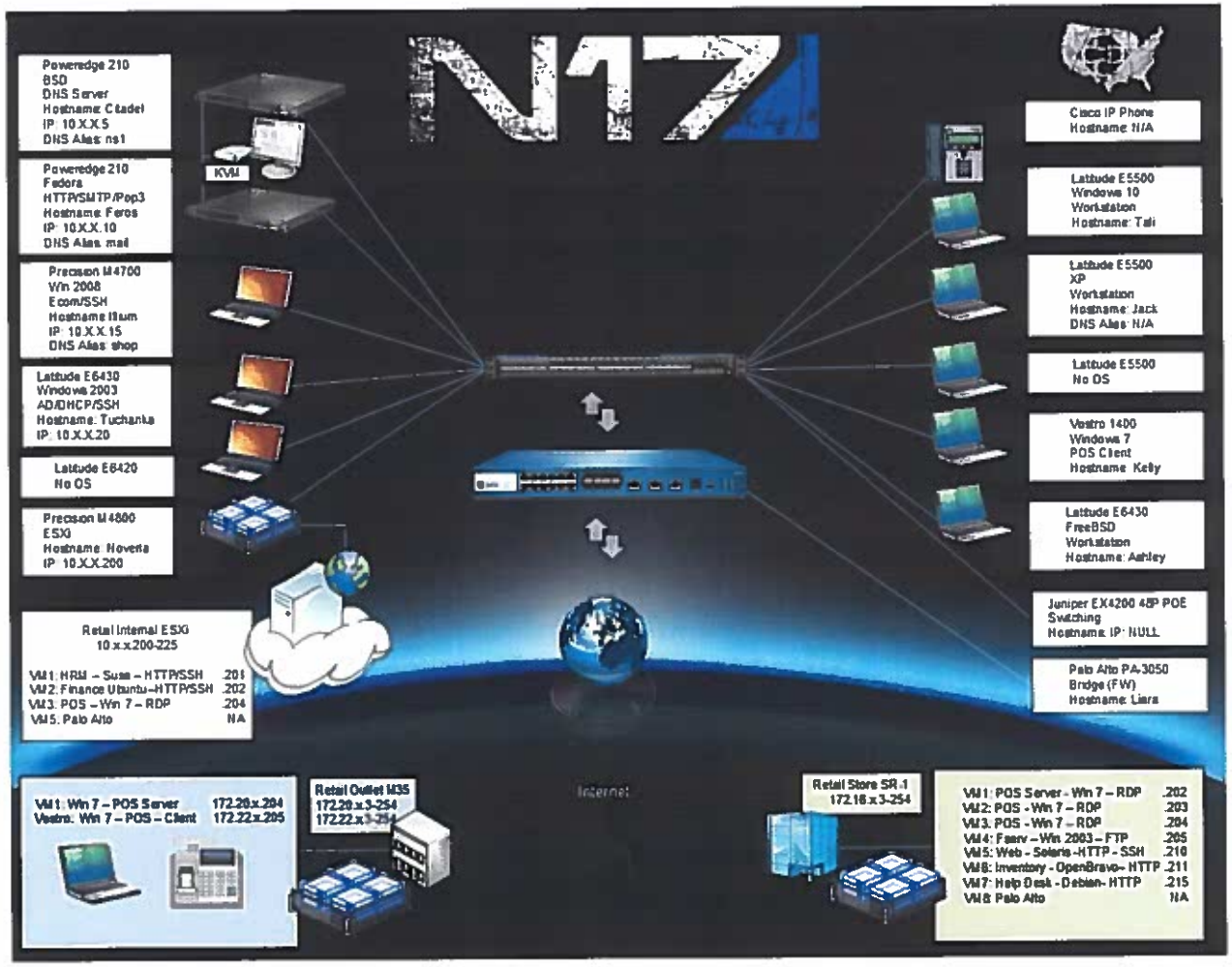
10.120.0.5 – Team portal
10.120.0.9 – Software/patch server
10.120.0.10 – NTP server for official competition time
10.120.0.100 – Core VoIP server
10.120.0.200 – Internet Proxy – TCP port 8080 (you must configure your systems to use this proxy for them to reach the Internet). Remember to bypass local address and local domains in your proxy settings (this includes dwarvenhammer.com).
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 Large Retail Center network
172.23.XX.10 – IP address of your team's Retail Outlet ESXi system (where XX is the same as your core network, Team 1 = 10, Team 2 = 20, …)
172.23.XX.11 – IP address of your team's Large Retail Center ESXi system (where XX 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)

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

Raytheon

Team Network Diagram



NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

Raytheon

Letter from the President

From: Jeff Albertson
To: New Cyber Security and IT Gurus
Subject: Welcome

Welcome to the Dwarven Hammer clan! We are thrilled to have you on board. As you know from your hiring briefings, we are a comic book and collectible retailer with 3 locations and an e-commerce site. 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. We process between 5,000 and 6,000 transactions a month currently, but hope to grow our business in the next 12 months as we scout locations for additional retail locations.

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 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 older and correct software configuration is essential for operation. 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! We are a retail business so make sure the Point of Sale system works at all times – registers and servers. If a register is down we're losing sales.

Our network has three major segments; the main corporate network in our offices here (SR1), our large retail center in Los Angeles (SR2), and our retail outlet in San Antonio (M35). You should be able to reach remote systems using RDP or SSH as appropriate (RDP for Windows systems, SSH for non-Windows typically). Our main Point of Sale system, KeyHut, is DOS based and a little quirky but you'll catch on to it quickly I'm sure. You are responsible for securing and operating all three network environments.

Thank you,

Jeff

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, Large Retail Center – 172.16.X.X, and Remote Outlet):

Team 1 10.10.10.0, 172.16.10.0, 172.20.10.0, and 172.22.10.0
Team 2 10.20.20.0, 172.16.20.0, 172.20.20.0, and 172.22.20.0
Team 3 10.30.30.0, 172.16.30.0, 172.20.30.0, and 172.22.30.0
Team 4 10.40.40.0, 172.16.40.0, 172.20.40.0, and 172.22.40.0
Team 5 10.50.50.0, 172.16.50.0, 172.20.50.0, and 172.22.50.0
Team 6 10.60.60.0, 172.16.60.0, 172.20.60.0, and 172.22.60.0
Team 7 10.70.70.0, 172.16.70.0, 172.20.70.0, and 172.22.70.0
Team 8 10.80.80.0, 172.16.80.0, 172.20.80.0, and 172.22.80.0
Team 9 10.90.90.0, 172.16.90.0, 172.20.90.0, and 172.22.90.0
Team 10 10.100.100.0, 172.16.100.0, 172.20.100.0, and 172.22.100.0

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 Large Retail Center systems are cloud-based and running on an ESXi platform outside your team room. Those systems reside on the 172.16.X.0 network assigned to your team (see above). Large Retail Center 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 consultants, and service providers should be able to access Large Retail Center systems and the Retail Outlet server from any source IP address via RDP for Windows systems and SSH for non-Windows systems. The retail outlet server on 172.20.X.204 is running on an ESXi platform outside your room. Authorized corporate users (including external users), our consultants, and service providers should be able to connect to it using RDP. Point of Sale Clients are linked to specific Point of Sale Servers in their respective locations. Point of Sale Clients **must** be able to communicate at all times with their Point of Sale Servers to function correctly.

Raytheon

The ESXi server in your room uses the default root password for your organization. Your remote ESXi servers are located at 172.23.XX.10 and 172.23.XX.11. These servers have a different root password than your corporate default. You should be able to reach your team's remote ESXi servers using the VSphere clients installed on one of your workstations inside your team room. The VSphere client software is available from the software portal at 10.120.0.9 should you wish to install it on additional workstations.

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 Large Retail Center/Retail Outlet 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.

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.

- WWW: You must maintain the HTTP service on 172.16.X.210
- HRM: You must maintain the HTTP service on 10.X.X.201
- DNS: You must maintain the DNS service on 10.X.X.5
- FTP: You must maintain the FTP service on 172.16.X.205
- POP3: You must maintain the POP3 service on 10.X.X.10
- SMTP: You must maintain the SMTP service on 10.X.X.10
- HELP_DESK: You must maintain the HTTP service on 172.16.X.215
- ECOM: You must maintain the HTTP service on 10.X.X.15
- SSH1: You must maintain the SSH service on 10.X.X.20
- SSH2: You must maintain the SSH service on 10.X.X.201
- SSH3: You must maintain the SSH service on 10.X.X.202
- SSH4: You must maintain the SSH service on 172.16.X.210
- SR1-SMB on 10.X.X.204, SR2-SMB on 172.16.X.202, and M35-SMB on 172.20.X.204: You must allow access to these SMB services from the 10.160.169.0/24, 10.160.201.0/24 and the 10.150.0.1/16 networks. The scoring system and Orange teams will be using these networks to score these three SMB services. They do not need to be accessible to any external IP address like the other services do.

Raytheon

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 each of your 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.

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.

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 other update services. Remember all Internet-bound FTP/HTTP/HTTPS traffic should be going through the proxy located at 10.120.0.200 port 8080. If one of your systems is not configured to use the proxy, then you will need to configure it to use the proxy. All systems should be configured to use your team's DNS server first (10.X.X.5) 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 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. There will be two blank laptops in your environment – you may use them for any purpose you choose (so long as it doesn't violate the rules) and may install any OS on them that you like.