Mid-Atlantic Collegiate Cyber Defense Competition

Presented by National CyberWatch Center

2015 Team Packet

Information contained in this document is subject to change

Table of Contents

COMPETITION SCHEDULE

Wednesday, March 25	
9:00 AM - 5:00 PM	Competition Setup (Closed to public)
Thursday, March 26	
7:00 AM to 11:00 PM	Competition Setup
7:30 AM to 8:45 AM	Blue Team Registration (Kossiakoff Center Lobby)
7:30 AM to 11:30 AM	Sponsor Setup
9:00 AM to 10:00 AM	Opening Briefing (Kossiakoff Center Auditorium) *Keynote Speaker – Admiral Patrick M. Walsh, USN, Ret.* *Senior Vice President, iSIGHT Partners*
10:15 AM to 11:15 AM	Blue teams pre-competition prep (Blue Team Competition Area)
11:15 AM to 12:30 PM	Lunch (On your own)
12:30 PM to 1:30 PM	Sponsors' Career Presentations (Kossiakoff Center Auditorium)
1:30 PM to 3:30 PM	Job Fair (Kossiakoff Center Mezzanine)
4:00 PM to 5:30 PM	Northrop Grumman Cyber Security Operations Center Tour *Sign up at the Northrop Grumman booth during the job fair*
Friday, March 27	
7:00 AM to 7:30 AM	Volunteer check-in & briefing (Kossiakoff Center Lobby)
7:30 AM to 8:15 AM	Blue Team check-in (Kossiakoff Center Lobby)
8:30 AM to 8:50 AM	Morning briefing (Kossiakoff Center Auditorium)
9:00 AM to 5:00 PM	Competition day-one (Kossiakoff Center)
12:00 PM - 1:00 PM	Lunch (on your own)
5:15 PM to 5:30 PM	Day-one debrief (Kossiakoff Center Auditorium)
Saturday, March 28	
7:00 AM to 7:30 AM	Volunteer check-in & briefing (Kossiakoff Center Lobby)
7:30 AM to 8:15 AM	Blue Team check-in (Kossiakoff Center Lobby)
8:30 AM to 8:50 AM	Morning briefing (Kossiakoff Center Auditorium)
9:00 AM to 3:00 PM	Competition day-two (Kossiakoff Center)
9:00 AM to 9:30	K-12 Cybersecurity Fair and Expo registration (Kossiakoff Center Lobby)
9:30 AM to 1:00 PM	K-12 Cybersecurity Fair and Expo (Kossiakoff Center)
12:00 PM to 1:00 PM	Lunch (On your own)
3:15 PM to 4:30 PM	Competition breakdown (Kossiakoff Center)
5:30 PM to 7:30 PM	Awards ceremony and debrief (Kossiakoff Center Auditorium)

Information contained in this document is subject to change

CCDC MISSION

"The goal of a Cyber Defense Competition is to provide hands-on application of information assurance skills; as such, they enhance students' understanding of both theory and practice. They provide students a laboratory in which to experiment, just as in other fields of science. They fulfill the same role as capstone projects in a traditional engineering program (i.e., projects that allow students to synthesize and integrate knowledge acquired through course work and other learning experiences into a project usually conducted in a workplace). The competition combines legal, ethical, forensics, and technical components while emphasizing a team approach. Such experiential education increases the knowledge and expertise of future professionals who may be in a position to contribute to the secure design and operation of critical information and its supporting infrastructure" (from *Exploring a National Cyber Security Exercise for Colleges and Universities*, Ron Dodge, Lance J. Hoffman, Daniel Ragsdale, and Tim Rosenberg, 2004).

COMPETITION OBJECTIVES

- Build a meaningful mechanism by which institutions of higher education may evaluate their programs;
- Provide an educational venue in which students are able to apply the theory and skills they have learned in their course work;
- Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams; and
- Open a dialog and awareness among participating institutions and students.

TERMINOLOGY

Throughout this document, the following terms are used:

- **Operations Team/Gold 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 host institution responsible for serving as a liaison between competition officials and the Blue Team's institution.

COMPETITION RULES

1. **Competitor Eligibility**
    a. Competitors in CCDC events must be full-time students of the institution they are representing.
        i. Team members must qualify as full-time students as defined by the institution they are attending.
        ii. Individual competitors may participate in CCDC events for a maximum of five seasons. A CCDC season is defined as the period of time between the start of the first state event and the completion of the National CCDC event. Participation on a team in any CCDC event during a given season counts as participation for that entire season.
        iii. A competitor in their final semester prior to graduation is exempt from the full-time student requirement and may compete in CCDC events as a part-time student provided the competitor has a demonstrated record of full-time attendance for the previous semester or quarter.
        iv. If a team member competes in a qualifying, state, or regional CCDC event and graduates before the next CCDC event in the same season, that team member will be allowed to continue to compete at CCDC events during the same season should their team win and advance to the next round of competition.
    b. Competitors may only be a member of one team per CCDC season.
    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 at all times 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 other teams, the Operations Team, the White Team, or the Red Team will be tolerated. This includes port scans, unauthorized connection attempts, vulnerability scans, etc. Any team performing offensive activity against other teams, the Operations Team, the White Team, the Red Team, or any global asset will be immediately **disqualified** from the competition. If there are any questions or concerns during the competition about whether or not specific actions can be considered offensive in nature contact the Operations Team before performing those actions.
k. Teams are allowed to use active response mechanisms such as TCP resets when responding to suspicious/malicious activity. Any active mechanisms that interfere with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams. Any firewall rule, IDS, IPS, or defensive action that interferes with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams.
l. All team members will wear badges identifying team affiliation at all times 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 or not specific materials are unauthorized contact the White Team immediately.
e. All network activity that takes place on the competition network may be logged and subject to release. Competition officials are not responsible for the security of any information, including login credentials, which competitors place on the competition network.

6. **Permitted Materials**
   a. No memory sticks, flash drives, removable drives, CDROMs, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.
   b. Teams may not bring any type of computer, laptop, tablet, PDA, cell phone, smart phone, or wireless device into the competition area unless specifically authorized by the Operations or White Team in advance. Any violation of these rules will result in disqualification of the team member and/or a penalty assigned to the appropriate team.

c. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition as specified by the competition officials.

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

8. **Questions, 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. Should any question arise about scoring, the scoring engine, or how they function, the Team Captain should immediately contact the competition officials to address the issue.
    d. Teams are strongly encouraged to provide incident reports for each Red Team incident they detect. Incident reports can be completed as needed throughout the competition and presented to the White Team for collection. Incident reports must contain a description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, access obtained, damage done, etc.), a discussion of what was affected, and a remediation plan. A thorough incident report that correctly identifies 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. With the advent of viable remote access technologies and virtualization, teams will have the ability to participate in CCDC events from their respective institutions. This section addresses policy for proper engagement in CCDC events for remote teams.
    b. Remote teams are required to compete from a location with controlled access, i.e., a separate room or a portion of a room that is dedicated for use during the CCDC event. Workstations and internet access must comply with published requirements.
    c. One or more Remote Site Judge(s) must be assigned to the team site. At least one Remote Site Judge must be present at the remote site for the duration of the event in order to facilitate the execution of the CCDC. The qualifications of Remote Site Judge are the same as Event Judge. Subject to the specifications of the remote competition, the responsibilities of the Remote Site Judge may include the following:
        i. Be present with the participating team to assure compliance with all event rules
        ii. Provide direction and clarification to the team as to rules and requirements
        iii. Establish communication with all Event Judges and provide status when requested

iv. Provide technical assistance to remote teams regarding use of the remote system
v. Review all equipment to be used during the remote competition for compliance with all event rules
vi. Assure that the Team Captain has communicated to the Event Judges approval of initial system integrity and remote system functionality
vii. Assist Event Judges in the resolution of grievances and disciplinary action, including possible disqualification, where needed
viii. Report excessive misconduct to local security or police
ix. Assess completion of various Injects based on timeliness and quality when requested by Event Judges
x. Act as a liaison to site personnel responsible for core networking and internet connectivity
xi. Provide direct technical assistance to teams when requested by Event Judges
xii. Provide feedback to students subsequent to the completion of the CCDC event

d. A recommendation for Remote Site Judge(s) is expected to be given from a Team representative of the participating institution to the CCDC Event Manager. Remote Site Judge(s) must not be currently employed, a student of, or otherwise affiliated with the participating institution, other than membership on an advisory board. CCDC Event Managers should also be apprised of a contact from the participating institution responsible for core networking and internet connectivity that will be available during the CCDC event.

11. **Local Competition Rules**

Unless otherwise stated below the rules of the National Collegiate Cyber Defense Competition will serve as the rules of the official rules of the Mid-Atlantic Collegiate Cyber Defense Competition all-inclusive and unaltered.

12. **Red Team Attack Rules**

a. Confine attack activity to the official target list located on the ScoreBot player page.
b. No physical attacks without prior approval.
c. No physical contact with any blue team player.
d. If contact is necessary with a white team, black team, or a competition staff member, red team members must identify themselves as a member of the red team.
e. No Distributed Denial of Service (DDoS) attacks.

2015 SCENARIO

The 10th MACCDC scenario involves support the information systems and defending against cyber-attacks within a mass transportation IT operation. The ten teams advancing to the regional finals will inherit a commuter rail system's IT infrastructure and be responsible for defending and maintaining the system for the duration of the competition.

The Hackistan Army of Liberation (HAL) is directing their aggression against the state of Maryland for both supporting the 2013 election in Hackistan (MACCDC 2013) and for their inability to cause disruption during the 2014 March Blizzard (MACCDC 2014). HAL has posted public information threatening US citizens, vowing digital and physical revenge unless their demand is met for no further US support and interference with their country's affairs.

HAL possesses highly-effective cyber-attack capabilities and there is highly confident intelligence that HAL is targeting regional commuter rail control networks and information systems. Intelligence indicates that HAL is planning on using their cyber-attack as a means of making the statement that the U.S. governmental organizations are ineffective and cannot be trusted. Blue teams will be deployed to regional commuter rail network operation centers to defend against HAL and to provide operational services throughout the threat timeframe.

RED CELL GOALS

- Obtain execute privilege on the defenders' systems
- Acquire flags
- Steal Data
- Corrupt data
- Prevent Data Transmission
- Disable services

SCORING

General Information
All Blue Teams start with 0 points. Blue Teams are ranked against each other in order of highest (best) to lowest score.

Defending Teams will be scored across the following domains:

1. **Services**: All scored services must remain up, available, and with a high degree of integrity. All services are given a predefined point value and will be checked periodically in Service Rounds. For each service that passes the necessary check the team will receive the appropriate number of points for that service. Partial points may be award if services are online, but not fully functionally or with a compromise to integrity. Red Team activity can adversely affect service scores. **The more service points a team receives, the better.**
2. **Injects**: During the course of the event, teams may receive any number of Injects. An Inject is any assigned task to be completed in the appropriate amount of time. Sample Injects include creating policy documents, making technical changes and attending meetings. If the Inject is completed on time and to the standard required, the team will receive the

appropriate number of points. Unless indicated otherwise, the Team Captains may assign Injects to specific team members for completion. Partial points may be award for Injects that are not fully completed but have some completed elements. Red Team activity can adversely affect Inject scores. **The more Inject points a team receives, the better.**

3. **Flags**: The Blue Team will have flags to locate inside their *own* environment. The flags will come in two varieties: one will be informative and scenario-based; the other will be used to verify information integrity. A flag consists of two pieces of information. You'll be provided with one piece (typically in the format of a question) and must respond with the correct corresponding piece in order to get credit for locating the flag. Additionally, there will be flags located within the team's environment that the Red Team will be attempting to capture. It will be the team's job to defend these flags against theft from the Red Team, if a flag is captured from the team's environment by the Red Team the team will be penalized. The more flag points a team receives, the better.
4. **Red Team Activity:** While defending against Red Team activity is not a direct scoring category, the activities performed by the Red Cell may have an impact on one or all of the given scoring categories. It is imperative teams work to prevent Red Team activities: The Red Team (attackers) will have specific goals during this event. Sample goals include compromising a server, stealing data, or modifying records. Each Red Team goal is assigned a point value. If the goal is accomplished, the Red Team team/member is awarded the points and the Blue Team has a corresponding amount of points deducted from their score. For example; A Red Team player has the goal of obtaining a specific file off a Blue Team's mail server. The goal is worth 250 points. If the Red Team player acquires the file, they will receive 250 points and the victim Blue Team will have 250 points deducted from their score.

Raw scores are used for these scoring metrics. However, at the end of each day's competition, Blue Teams are ranked using an ordinal scale, which is a measurement scale that assigns values to objects based on their ranking with respect to one another. For example, a first place finish at the end of day one in the Service Functionality scoring metric warrants an ordinal score of 1; a second place finish warrants an ordinal score of 2; up to an eighth place finish warranting an ordinal score of 8. This process is repeated for the Injects and Flags scoring metrics.

The ordinal scores from the three (3) scoring metrics are then totaled for each Blue Team, yielding a combined ordinal score for each day of competition, which is used to rank the Blue Teams from first through eighth place. The winning Blue Team will be based on the lowest combined ordinal score obtained during the competition time.

Tie Breakers

In the event of a tie for first place, the team with the highest raw combined Inject and service score will win.

Service Rounds

The services are scored in Rounds. For each round, a Blue Team will be scored on:

1. Service Availability (Are critical services available with a high degree of integrity?)
2. Data Confidentiality (Has key data been stolen?)
3. System Compromises (Have any systems been compromised by the Red Team?)

TCP is scored at three levels:

1. **Level 1** is the TCP three-way handshake. If the port is not open, or does not complete the three-way handshake, then the team is award zero points for that service out of the total possible score listed in the Server/Services table (see above).
2. **Level 2** is the service request. If Level 1 is passed (the port is open and the three-way handshake is completed), then the scoring engine makes a service request (e.g., HTTP GET request). If the request fails, then the Blue Team is award one-half of the available points for that service.
3. **Level 3** is the integrity check. If Levels 1 and 2 are passed, then checks will be performed on the various response data to ensure their integrity has not changed since the start of the exercise. If the flag fails the integrity check, then the Blue Team is award one fourth the number of available points.

UDP is scored at two levels:

1. **Level 1** checks to see if the port is open by issuing a service request to that port. If the port is unresponsive, then the Blue Team zero of the available points for that service as listed in the Server/Services table (see above).
2. **Level 2** is the integrity check. If Level 1 is passed, then checks will be performed on the various flags to ensure their integrity has not changed since the start of the exercise. If the flag fails the integrity check, then the Blue Team is awarded one half the number of Level 1 points.

Dependent Services

The services that are being scored represent critical services. The scored services may rely on NON-SCORED services. If a service is NOT being scored it does NOT mean that it is NOT necessary for a scored service to run. Shutting down a dependent service may result in your team's losing service score.

Non-Service Scored Assets

There may be non-service scored assets within each Blue Team network. A non-service scored asset is one that is on the official Services List and NAT'd to the outside.

As the name of these assets implies, these assets are not checked for ICMP or any network services. Any service outage or lack of network connectivity on these assets will NOT impact the service portion of a team's score.

Service Data Confidentiality

The Scoring Engine will be checking for stolen flags. A flag could be a file in a file system or an entry in a database table, or even a username/password combination. If a flag is successfully stolen from a Blue Team and submitted for scoring, points will be deducted to the Blue Team score.

Red Team

- The Red Team will be attempting to find and exploit weaknesses in each Blue Team's environment. All systems reachable by the Red Team within the Blue Team's internal and external IP address space are valid targets. This includes systems that are not being scored.

- The Red Team will be using Phone Home scripts to prove execute privileges on a scored asset. The Phone Home script connects to the Scoring Server across the game network. Any attempts to block the Phone Home script by using source or destination IP addressing is forbidden, unless the Operations Team gives permission (permission would be given after a successful Incident Response report is filed and reviewed by the attending Law Enforcement representative – see the Scoring: Law Enforcement section below).
- Any Phone Home from a hidden asset does NOT impact the Blue Team's score. A Phone Home from a hidden asset DOES count towards the score of a Red Team member. As a result, the total number of Red Team Phone Homes may be more than the combined number of Phone Homes from all Blue Teams.
- Since each Blue Team has access to their assets through the vSphere client, any Phone Home from a non-service scored asset DOES impact the Blue Team's overall score, with the value of the Phone Home being deducted from the Blue Team's score.
- Blue Teams have points deducted from their score in the event of a successful Phone Home, per round. Teams may obtain a portion of their points back based on conducting an investigation. If the law enforcement official running the investigation thinks they have enough evidence to obtain a search warrant, points may be returned to the Blue Team. If the law enforcement official running the investigation thinks they have enough evidence to obtain an arrest warrant, additional points will be returned to the Blue Team.

Injects

Throughout the competition, the Blue Team will be presented with Injects. The type of Injects will vary in nature and be weighted based upon the difficulty and time sensitivity of the tasking. Tasks may contain multiple parts. Some examples: setting up an Intranet web server; performing a zone transfer between a secondary DNS server and the primary DNS server.

Injects can be delivered through any number of methods and will include the point values and time restrictions associated with the task. Upon completion of the Injects, the performance of the Blue Team will be noted and scores adjusted.

There are two special injects that will be required of every team; Supervisory Reporting and Incident Reporting.

Supervisor Reporting

Each Team Captain will meet face-to-face with the Chief Executive (CE) of the commuter rail system.

During the initial meeting (five minutes, timed), the CE will expect to be briefed on the current status of the organizations information systems, number of users impacted by downed systems, as well other items the Team Captain will consider relevant for the CE to know. At this initial meeting, each Team Captain will be given action items to complete and a fixed time. Items may include a written status report, a high-level remediation plan, a resources inventory, a request for prioritized additional resources subject to budget constraints and other similar management factors.

During the second session (ten minutes, timed), each Team Captain will meet with the CE and will have a chance to present written and verbal responses from the first meeting and provide updates on any changes that transpired.

Each team will be scored using the following metrics:

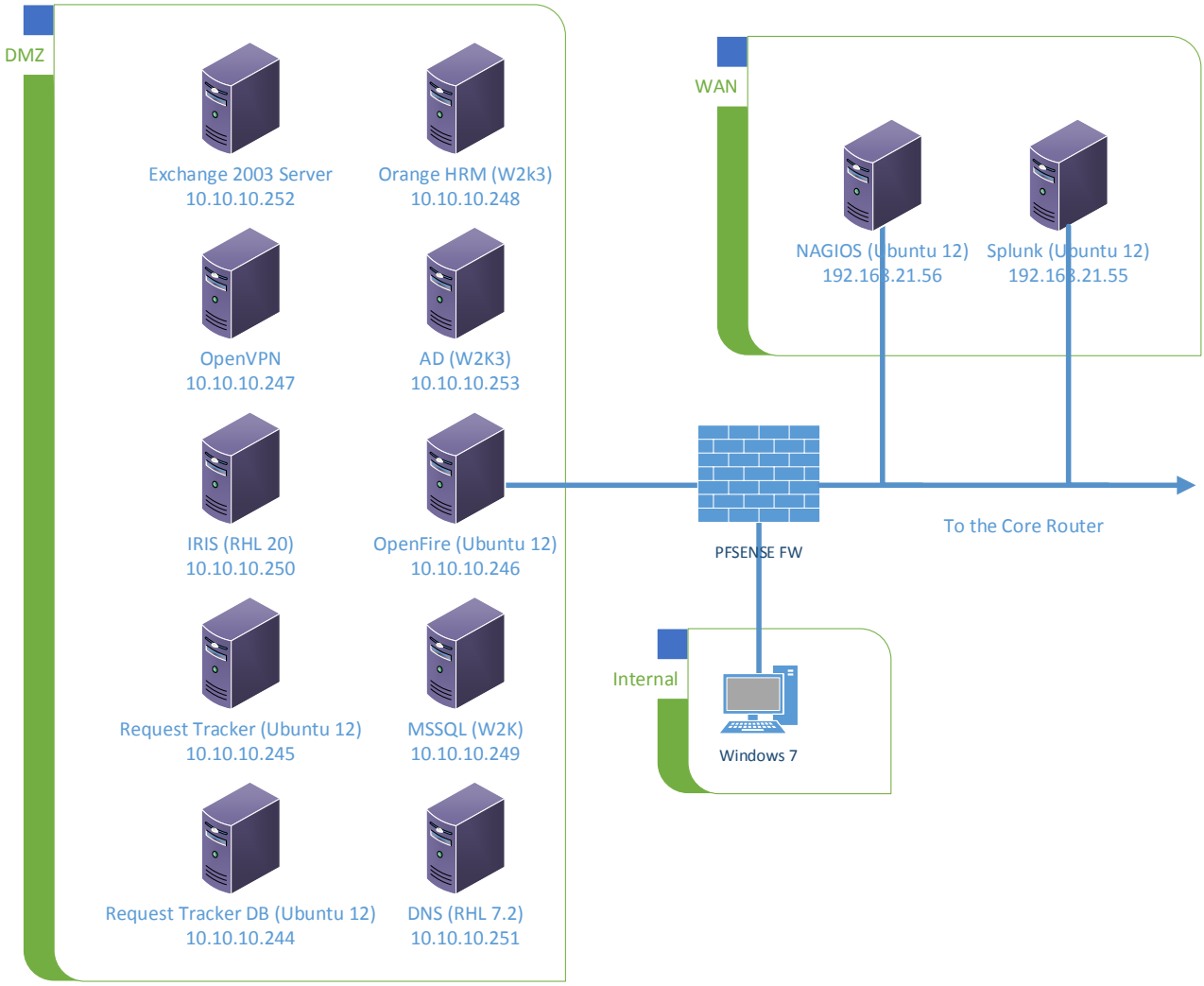
- Oral presentation skills
- Writing skills
- Clarity of communicating the situation
- Ability to rise above techno-babble
- Creativity in reacting to new information

Incident Reporting

All Blue Teams must complete at least two Incident Response forms and open two cases with the law enforcement officials in attendance. Incident Response forms will be provided. Instruction for submitting incident response forms will be provided during team briefing.

DEFENDER'S NETWORK

Each Blue Team will be responsible for defending the following assets:



IP ADDRESS TABLE

All teams have the same internal IP address space of 10.10.10.x

Team	External IP Space
Anne Arundel Community College	192.168.21.X
Capitol Technology University	192.168.22.X
County College of Morris	192.168.23.X
East Carolina University	192.168.24.X
James Madison University	192.168.25.X
Liberty University	192.168.26.X
Towson University	192.168.27.X
University of MD Baltimore County	192.168.28.X
University of MD College Park	192.168.29.X
Wilmington University	192.168.30.X
MDDF	192.168.31.X

SYSTEM INFORMATION

Assets

- **Microsoft Active Directory (AD) Server** - Windows Server 2003: This is your primary domain controller and is responsible for managing user and system information across the enterprise. There are several hundred users. The AD server is also your primary DNS server. As your primary DNS server, it must allow zone transfers and other inbound DNS requests. Failure to resolve DNS lookups from outside your network could result in service problems/penalties.
- **DNS2** – Red Hat 7.2: Secondary DNS server
- **Microsoft Exchange Server** – Windows Server 2003: This server provides all email communication for the team. This includes all necessary email services such as IMAP, SMTP, POP3 and Outlook Web mail. This server also functions as your team's secondary Active Directory Server.
- **Windows 7**: Desktop
- **OrangeHRM –** Windows 2003 Server. OHRM Open Source is a free HR management system that offers a wealth of modules to suit the needs of your business. This widely-used system is feature-rich, intuitive and provides an essential HR management platform along with free documentation and access to a broad community of users.
- **OpenVPN** – Ubuntu 12.04: OpenVPN is a full-featured open source SSL VPN solution that accommodates a wide range of configurations, including remote access, site-to-site VPNs, Wi-Fi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls. Starting with the fundamental premise that complexity is the enemy of security, OpenVPN offers a cost-effective, lightweight alternative to other VPN technologies that is well-targeted for the SME and enterprise markets.

- **IRIS –** RHL 20: IRIS is an open source advanced traffic management system. It provides an integrated platform for transportation agencies to manage traffic monitoring and control devices. The software is written in Java and licensed for anyone to use under the GPL. In addition, all dependencies required to install and operate an IRIS system are available as free software. IRIS stands for Intelligent Roadway Information System.
- **Openfire –** Ubuntu 12.04: OpenFire is a real time collaboration (RTC) server licensed under the Open Source Apache License. It uses the only widely adopted open protocol for instant messaging, XMPP (also called Jabber). Openfire is incredibly easy to setup and administer, but offers rock-solid security and performance.
- **Request Tracker** – Ubuntu 12.04: RT is a *battle-tested* issue tracking system which thousands of organizations use for *bug tracking*, *help desk ticketing*, *customer service*, *workflow processes*, *change management*, *network operations*, *youth counselling* and even more. Organizations around the world have been *running smoothly thanks to RT* for over 10 years.
- **Request Tracker DB** – Ubuntu 12.04: This is the database server for RT
- **MSSQL 2000** - Windows 2000 server offering up enterprise database services.
- **Splunk -** Ubuntu 12.04: Splunk Enterprise makes it simple to collect, analyze and act upon the untapped value of the big data generated by your technology infrastructure, security systems and business applications—giving you the insights to drive operational performance and business results.
- **Nagios** – Ubuntu 12.04: Network service monitoring system. This server is NOT configured
- **pfSense** – Your network's forward facing firewall. It has three interfaces.