Mid-Atlantic Collegiate
CYBER DEFENSE COMPETITION

presented by

National CyberWatch Center

March 15 – 17, 2018

Johns Hopkins University Applied Physics Laboratory

2018 Team Packet

NATIONAL CYBERWATCH CENTER

NSF

APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY

2018 SPONSORS & SUPPORTERS

Information contained in this document is subject to change

Contents

Competition Schedule

Tuesday, March 13	**(Closed to the Public)**
9:00 AM to 5:00 PM	Competition Setup
Wednesday, March 14	**(Closed to the Public)**
9:00 AM to 5:00 PM	Competition Setup
Thursday, March 15	**(By Invitation Only / Closed to the Public)**
7:00 AM to 11:00 PM	Competition Setup
9:00 AM to 10:00 AM	Blue Team Registration (Kossiakoff Center Lobby)
9:00 AM to 11:00 AM	Sponsor Registration
9:00 AM to 11:00 AM	Job Fair Setup
10:00 AM to 11:00 AM	Opening Briefing (Kossiakoff Center Auditorium)
11:00 AM to 12:00 PM	Blue teams' pre-competition prep (Cyber Stadium)
12:00 PM to 1:00 PM	Lunch Break
1:00 PM to 2:00 PM	Sponsors' Briefings (Kossiakoff Center Auditorium)
2:00 PM to 4:00 PM	Job Fair (Kossiakoff Center Mezzanine)
4:15 PM to 5:30 PM	Special Event (TBA)
Friday, March 16	**(Open to the Public)**
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 (Cyber Stadium)
12:00 PM to 1:00 PM	Lunch Break
1:00 PM to 3:00 PM	CEO Meetings (Kossiakoff Center Auditorium)
5:10 PM to 5:30 PM	Day-one debrief (Kossiakoff Center Auditorium)
Saturday, March 17	**(Open to the Public)**
7:00 AM to 7:30 AM	Volunteer check-in & briefing (Kossiakoff Center Lobby)
7:30 AM to 8:30 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 (Cyber Stadium)
9:00 AM to 11:00 AM	CEO Meetings (Kossiakoff Center Auditorium)
11:00 AM to 12:00 PM	Lunch Break
3:00 PM	Competition Ends
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)

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 team;
- 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 and provide administrative support to the competition.
- **Orange Team**: competition officials that serve as end users of Blue Team systems and evaluate availability of services.
- **Blue Team/Competition Team**: the college and university 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 representatives**: a faculty or staff representative of the Blue Team host college or university 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.

    a. 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 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 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.

Local Competition Rules

11. **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 during the competition.
    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.
    f. No attacks that are not recoverable by blue team action or recoverable only through a virtual machine revert to snapshot or rebuild performed by the operations team.

12. **Questions, Disputes, and Disclosures**
    a. At no time may a team question, dispute, or protest the actions of another team. All disputes and/or protests must be in regard to an incident occurring with the presenting team. Any dispute or protest filed by a team alleging actions of another team will not be accepted.

Scenario

Breaking News

A major online news service, The SWoRN Chronicle, has recently been the target of a group of Hackistanian hackers that appear to want to disrupt the reliable and credible reporting that sets the Chronicle apart from other news organizations. These insurgents have been well documented to generate fake news in order to sway public opinion. They use a variety of methods and are currently exploiting and infiltrating SWoRN Chronicle systems. Evidence has included the insertion of malware, bogus news stories, and complete hijacking of systems.

The SWoRN Chronicle executive team has enlisted the assistance of eight qualified teams to shut down the insurgent's activities on the internal systems that are geographically distributed throughout the cybersphere. The teams will inherit the existing systems and be expected to defend them from further attack, detect and eliminate current exploits, and perform the day-to-day tasks necessary to maintain the systems.

The eight teams will be responsible for supporting field reporters as they deliver new content in the form of written articles and multimedia posts. They will also be responsible for guaranteeing availability of factual news to end users around the world.

Red Team

The Red Team will be attempting to locate and exploit weaknesses in each Blue Team's environment. Not all systems accessible by the Red Team within the Blue Team's internal and external IP address space are valid targets. However, all Blue Team systems may be used by the Red Team to exploit vulnerabilities in systems that are in play. This includes systems that are not being scored. The goals of the Red Team are to:

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

Scoring

General Information

All Blue Teams start with 0 points. Blue Team are ranked against each other in order from lowest (best) to highest final ordinal score.

Blue 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 using Service Round Checks. The actual number of service rounds is not disclosed prior to or during the competition. For each service that passes the necessary check the team will receive the appropriate number of points for that service. The scoring engine will use IPv4 and IPv6 to

conduct service checks. Red Team activity can adversely affect service scores. **The more service points a team receives, the better.**

2. **Injects**: Throughout the competition, the Blue Team will be presented with Injects. An Inject is any assigned task to be completed in the assigned amount of time. Inject type will vary and be weighted based upon the difficulty and time sensitivity of the tasking. Tasks may contain multiple parts. Sample Injects include creating policy documents, making technical changes and attending meetings. Injects can be delivered through any number of methods including electronically, on paper, and orally. Injects will scored by a White Team member. 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. Red Team activity can adversely affect a team's ability to complete injects. It is the Blue Teams' responsibility to keep their systems available. No extra time or point credit will be given for injects not completed due to inability to access a system. **The more Inject points a team receives, the better.**

3. **Red Team Activity:** The activities performed by the Red Team have an impact on many of the scoring categories. It is imperative Blue Teams work to prevent Red Team activities. The Red Team will have specific goals during this event. Sample goals include compromising a server, stealing data, or modifying injects. All Red Team activities are meant to disrupt or misinform and are not directly scored.

4. **CEO Reporting:** Each Team Captain will meet face-to-face with the Chief Executive (CE) of the SWoRN Chronicle. During the initial meeting (ten minutes, timed), the CE will expect to be briefed on the current status of the organization's 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 within a fixed time. Items may include a written status report, a high-level remediation plan, a resource 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

5. **Incident Response:** All Blue Teams must submit at least four 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 the initial team briefing. Incident response forms will be scored based on coherence and technical accuracy/depth.

6. **Malware Reports**: Malware has been inserted into the Blue Team systems prior to the start of the competition. The location and type of malware inserted has been documented by competition officials. All Blue Teams will search for and report malware discovered on their systems using the form provided. The report must include the location where the malware was found, the type of malware found, and the method of remediation used to remove the malware. Only the reports that correctly identify the malware inserted prior to the start of the competition will be scored. Malware Report forms will be provided.

7. **Orange Team Checks**: Each Blue Team will have an Orange Team member assigned to them to perform end user service availability throughout the duration of the competition. These checks will be performed at random intervals during each hour of competition. A ticket will be entered into the Blue Teams' Jira system that will inform the team of the results of each check. If the Jira system is unavailable the Orange Team will have no way to enter the ticket. The Orange Team checks will still be graded if access to Jira isn't available, these updates are simply for the team's knowledge of what the Orange team is seeing and grading on. The Orange Team will be using the Team's WIFI so if that is not accessible, all other checks for that hour will fail.

8. **Field Reporter:** This year one of each Blue Team's competing team members will be required to be in the "Briefing Room" writing up stories for the news site. This is not a writing competition so the articles can be brief but must include the main details of the story provided. Their responsibilities will be to update the blog/news site with the latest news stories each hour, and also to help remotely with the competition in any way, shape, or form. One of the Orange Team's checks will be to ensure that a new story is posted each hour. Think of this person as an onsite reporter and as a remote working for the team. Teams can swap out field reporters during lunch or day breaks only. Team Captains are the only team members allowed to physically go to the Briefing room to speak with the field reporter.

Raw scores are used for these scoring metrics. 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 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 all of the scoring metrics.

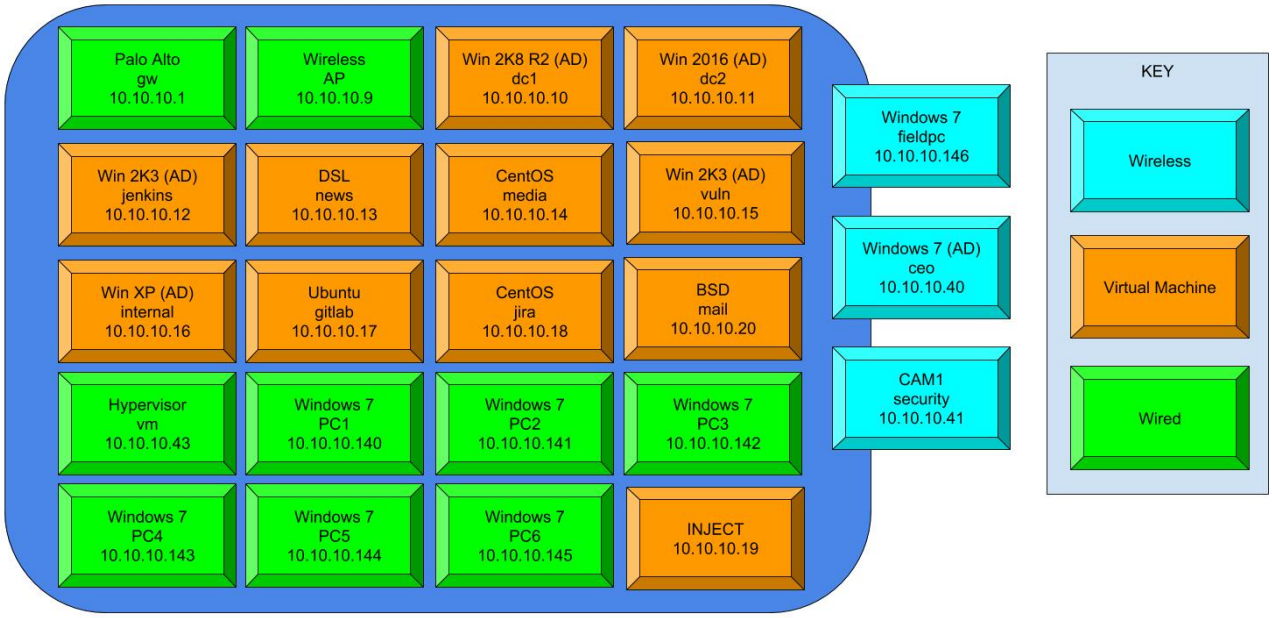
The ordinal scores from all of the scoring metrics are then totaled for each Blue Team, yielding a combined ordinal score, which is used to rank the Blue Teams from first through eighth-place. The winning Blue Team will be based on the lowest combined ordinal score obtained during the competition time.

Tie Breakers

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

Blue Team Range

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



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

IP Address Table

Team Number	Team	External IPv4 Space	IPv6 Global Unicast
1	Liberty University	192.168.21.0/24	2001:db8:ccdc:1:10:10:10:X/64
2	Millersville University	192.168.22.0/24	2001:db8:ccdc:2:10:10:10:X/64
3	Radford University	192.168.23.0/24	2001:db8:ccdc:3:10:10:10:X/64
4	University of Maryland, Baltimore County	192.168.24.0/24	2001:db8:ccdc:4:10:10:10:X/64
5	University of Maryland, College Park	192.168.25.0/24	2001:db8:ccdc:5:10:10:10:X/64
6	University of Virginia	192.168.26.0/24	2001:db8:ccdc:6:10:10:10:X/64
7	Virginia Commonwealth University	192.168.27.0/24	2001:db8:ccdc:7:10:10:10:X/64
8	Wilmington University	192.168.28.0/24	2001:db8:ccdc:8:10:10:10:X/64

Wireless

This year we are bringing back wireless. The Red Team will not be allowed to attack it in any way but will certainly be able to use it just like Orange team, the CEO, and the team's wireless security camera and field reporter will be able to use it to access the Blue Team's internal network. It will not be scored for services but will be scored as part of the CEO and Orange team's hourly activities.

Security Camera

10.10.10.41/192.168.2x.41 will be a Wireless camera. The Blue Teams are not allowed to modify or apply changes to the physical device. The Orange Team will be acting as the security guards for the team's area. Ability to access the camera will be an Orange Team check and is also scored as a service.

Mission Critical Systems & Services

The term Mission Critical is an activity, device, service or system whose failure or disruption will cause a failure in business operations. **All devices are considered mission critical.** The following services are considered mission critical and will be scored based on the metrics found in the Scoring section above:

Server	Internal IP	External IP	Scored Services
Primary DC	10.10.10.10	192.168.2X.10	SYSVOL/NETLOGON, LDAP, DNS
Backup DC	10.10.10.11	192.168.2X.11	SYSVOL/NETLOGON, LDAP, DNS
Jenkins	10.10.10.12	192.168.2X.12	RDP, HTTP
News Web Server	10.10.10.13	192.168.2X.13	SSH, HTTP, MYSQL
Media Server	10.10.10.14	192.168.2X.14	SSH, HTTP
Vulnerability Scanner	10.10.10.15	192.168.2X.15	RDP, HTTP, ElasticSearch
Wiki	10.10.10.16	192.168.2X.16	SMB, HTTP, FTP
GitLab	10.10.10.17	192.168.2X.17	SSH, HTTP, VNC
Ticketing System (Jira)	10.10.10.18	192.168.2X.18	SSH, HTTP
???? (Inject)	10.10.10.19	192.168.2X.19	??????? ???????? ???????
OpenBSD	10.10.10.20	192.168.2X.20	SMTP, IMAP, SSH
Security Camera	10.10.10.41	192.168.2X.41	HTTP

System information

- **Palo Alto Firewall** - This is the Blue Team's firewall. There are many like it but this one belongs to the Blue Team (for 2 days).
- **WAP** - Wireless Access Point
- **Primary DC -** Windows Domain Controller that handles DNS and authentication for all of the Windows machines as well as the email server. The required services are the SYSVOL/NETLOGON shares for Domain GPO distribution, LDAP for authentication and DNS.
- **Backup DC** - Backup Domain Controller that supports all of the same services as the primary Domain Controller.
- **Windows 2003/Jenkins -** This is the build server for the news page. It needs to be able to pull the current distribution of WordPress from the Gitlab server automatically, and be able to stand it up, verify its functionality, and push it to the News server.
- **News Web Server -** A small Linux distribution designed for the sole purpose of hosting the WordPress news site for the team. This site is scored in multiple ways not just services
- **Content Distribution System / Media Server -** Content Distribution / Media Server that hosts recordings and videos for the News team to use. The News page pulls media from this resource.
- **Vulnerability Scanner -** This is here for the vulnerability assessment team (Orange team) to use. Their login via RDP and HTTP must stay available to them at all times for them to do their job. Scheduled scans should not be interrupted without critical business cause.

- **Internal Corporate Wiki -** This site is used for internal information and requires authentication. Information should be stored here and updated as needed. Orange team will be using some of the information on this site to access the team network.
- **Gitlab Server** - This server hosts the WordPress files for the news site. Any updates for the WordPress install should be done through here.
- **Ticketing System / Chat Server** - This site is where Orange team will submit their checks in tickets to the Blue Team as a status update. There will also be a chat service on this machine so that Orange, Field Reporters, and the CEO can communicate if they wish.
- **10.10.10.19** - THIS IS RESERVED FOR A INJECT AND WILL NOT BE ACCESSIBLE UNTIL THE INJECT IS RECEIVED.
- **BSD** - The Team's mail service. This will be used to send and exchange mail with the CEO, orange team, as well as where injects will be coming in. Alternative method copies must be requested if email is nonfunctional for each hour and the teams must supply a method of delivery to the white cell accessible from the White network.