WESTERN REGIONAL COLLEGIATE CYBER DEFENSE COMPETITION

Western Regional Collegiate Cyber Defense Competition

OFFICIAL PROGRAM

Stacy
Booth

TABLE OF CONTENTS

WELCOME!

On behalf of CyberWatch West and the Cal Poly Pomona Center for Information Assurance (CIA), I would like to welcome you to the Western Regional Collegiate Cyber Defense Competition (WRCCDC). We hope that you will find this regional competition a challenging experience. The winning team from this regional competition will advance to the National Collegiate Cyber Defense Competition (NCCDC) hosted by the University of Texas at San Antonio (UTSA).

We are excited to be able to host this event. We are also very thankful for our industry and professional association sponsors. Our staff, volunteers, and sponsors have tried to make this an interesting, exciting, and challenging competition. The competition is receiving increased attention from government and industry and we expect this attention to continue to grow. Western Regional CCDC held its first event in 2008. Since then we've grown to where virtual invitational events and a virtual qualifier are held to accommodate demand.

We encourage you to provide comments and feedback to help us improve future events. We wish the best of luck to each of the teams!

Daniel Manson, Ph.D.
Professor/Chair
Computer Information Systems
Cal Poly Pomona
WRCCDC Organizer

© 2016 California State Polytechnic University, Pomona

WELCOME 2016 COMPETITORS!

CAL POLY POMONA

California State University DOMINGUEZ HILLS

CSUN | CALIFORNIA STATE UNIVERSITY NORTHRIDGE

RCC RIVERSIDE CITY COLLEGE

Stanford University

Berkeley UNIVERSITY OF CALIFORNIA

UC RIVERSIDE UNIVERSITY OF CALIFORNIA

UAT University of Advancing Technology Learn. Experience. Innovate.

© 2016 California State Polytechnic University, Pomona

THANK YOU TO OUR SPONSORS!

Raytheon

workday.

facebook.

Bank of America

FireEye™

Homeland Security

cyberwatch west

UNIVERSITY of WASHINGTON | BOTHELL
CYBER SECURITY ENGINEERING

paloalto NETWORKS

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

ISACA®
Trust in, and value from, information systems
Los Angeles Chapter

LogicSecurity

SPAWAR

ISE
independent security evaluators

2016 COMPETITION SCHEDULE

All competition activities to be in the Sheraton Fairplex Conference Center.

Thursday – March 17

7:00 PM	Registration	California Room
8:30 PM	Orientation - Competition Instructions and Brief-In	California Room

Friday – March 18

9:00 AM	Competition Begins	Exposition Hall
11:30 AM	Grab & Go Lunch – no break in competition	Prefunction Area
5:30 PM	Grab & Go Dinner – no break in competition	Prefunction Area
9:00 PM	Competition Ends for the Day	

Saturday – March 19

9:00 AM	Competition Resumes	Exposition Hall
11:30 AM	Grab & Go Lunch – no break in competition	Prefunction Area
6:00 PM	WRCCDC 2016 Competition Ends	
7:00 PM	Recruiting Mixer	California Room
9:00 PM	Recruiting Mixer Ends	

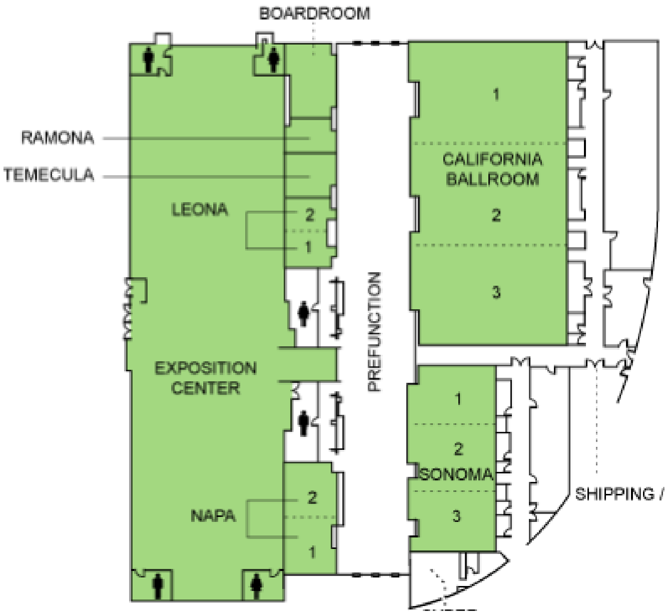
Sunday – March 20

9:00 AM in California Room

Hot Breakfast, Keynote Speakers, Debriefs & Awards

12:00 Noon – End

See you next year!



WRCCDC GOAL

The overall goal of the competition is to test the skills and knowledge of competing teams. This is done by providing a fair and equal playing field for all Blue Teams and exposing them to new challenges. The following measures have been instituted to provide the same opportunity for all Blue Teams:

1. Blue Teams are assigned their own pods with identical sets of hardware and software.
2. A dedicated internal network connects to a competition network allowing equal bandwidth and access for scoring and operations.
3. Identical business injects (tasks) are issued at the same time to all Blue Teams.
4. During the entire competition access to Blue Team pods are restricted to the members of the certified student team, White Team or Black Team members and others designated by WRCCDC coordinators.

It is assumed that all participants have read and will abide by the rules governing this event. WRCCDC has adopted National CCDC rules with the exception of a few local rules. Anything not covered by either set is at the WRCCDC judges' discretion to be determined via committee or vote, however deemed appropriate. Any decision made by WRCCDC judges is final.

COMPETITION SCORING

As the IT team, your job is managing and maintaining your systems while fulfilling management's requests. If vulnerabilities are discovered in your systems you must correct it. If your environment is exploited it must be reported. When Management makes demands you must attend to their desires in a timely fashion. Here are the ways your IT team might gain or lose favor with Management.

Teams gain points by:

- Keeping required public services and applications available and fully functional.
- Completing business tasks (injects) in a timely manner.
- Completing accurate Business Incident Reports when necessary.

Teams lose points by:

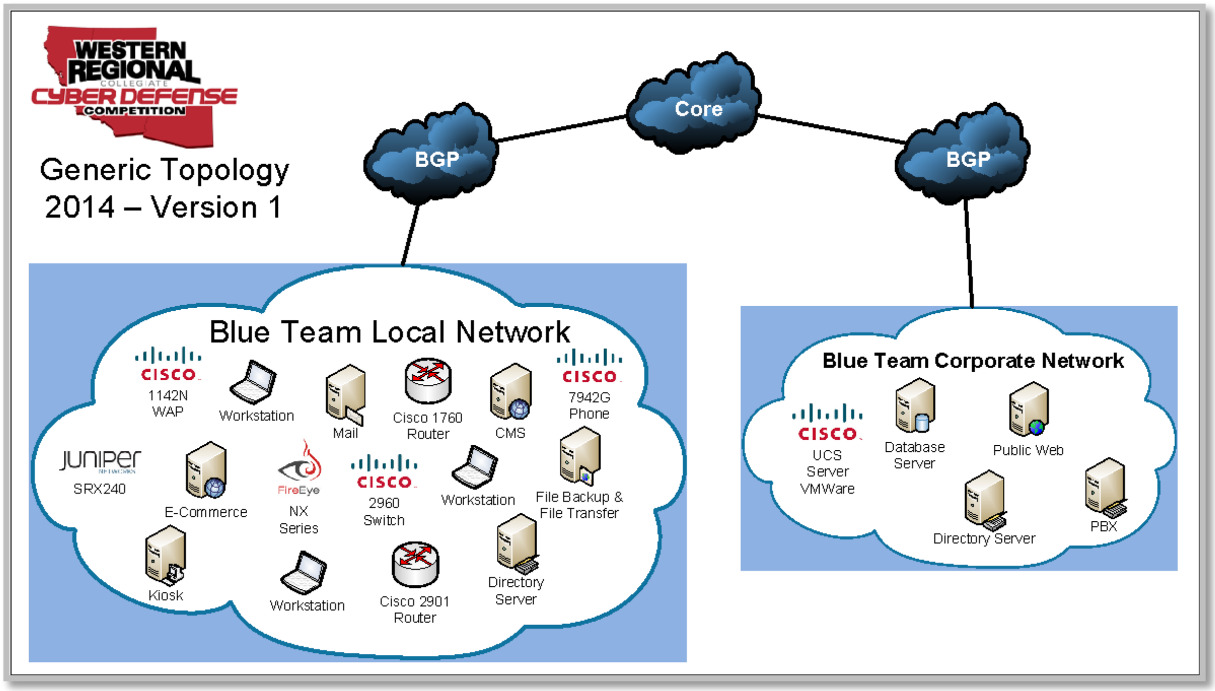
- Violating service level agreements.
- Usage of recovery services provided by the Black Team.

© 2016 California State Polytechnic University, Pomona

- Successful penetrations by the Red Team.
- Failing to pass Orange Team service checks

Some injects will be tasks focused on systems management. Other injects will mandate a presentation to The Board. Assume that The Board has the power to allocate money to IT projects or reduce budgets according to the information given them.

NETWORK & GENERIC TOPOLOGY



Above is the generic topology for this year's competition. A more definitive topology will be handed out the first day of the competition.

Each pod will be considered a standalone network with one or more connections to the central competition core network through which regulated Internet access is provided. All networks will be connected to a central router that will be maintained by the BLACK Team.

Internet access will be directed through a neutral web proxy with no filtering. A log of all sites and actions will be logged and may be reviewed at any time during the competition. Access to resources specifically banned by the competition rules can result in immediate disqualification. Judgement as to whether a site meets the criteria for qualification will be a joint decision made by the WHITE and BLACK team representatives.

Only connections using HTTP (tcp/80), HTTPS (tcp/443), and FTP (tcp/20, tcp/21) using passive mode will be permitted. Requests for other exceptions can be made by BLUE teams to the BLACK team in writing with adequate justification; however, these requests can be denied and/or rescinded by the BLACK team for any reason at any time.

All teams will be provided with access to a central read-only file repository where common operating system installation files, patches, and other files related to the competition will be made available.

POTENTIAL OPERATING SYSTEMS

The following is a list of potential operating systems that may be encountered as part of the competition; however, this list is not exhaustive. Note that both the 32Bit and 64Bit versions of the operating system may be used, along with any variants or derivatives (i.e. Standard, Enterprise, etc.):

FreeBSD
Debian Linux
Ubuntu Linux
Mint Linux
Arch Linux
CentOS Linux
Gentoo Linux
Fedora Linux
Cisco IOS
JunOS
PAN-OS
MS Windows 7
MS Windows 8
MS Windows XP
MS Windows Vista
MS Windows Server 2012
MS Windows Server 2003
MS Windows Server 2008

FUNCTIONAL SERVICES

Certain services are expected to be operational at all times or as specified throughout the competition because points will be awarded for operational services. In addition to being up and accepting connections, the services must be fully functional and serve the intended business purpose. At random intervals, certain services will be tested for function and content where appropriate.

Your job is to restore, support, monitor, maintain secure and report suspicious activity as the authoritative administrators for all devices and services. You will need to keep internal systems and operational systems maintained as best as possible. You will have traffic going into and out of your environment but you must keep a vigilant watch because your customer is under continuous attack. Finally, you will need to try and find the perpetrators via forensic means. Services may be added and/or removed at any point throughout the Protocols allowed into your network include but are not limited to:

FTP – One or more files made available via an FTP server will be downloaded and checked for content and validity. Note that this service may be dependent on user accounts with known passwords, or may be accessed anonymously. Details regarding connection specifics will be included with the scenario description or through injects. File names and contents must remain intact unless otherwise instructed. Each successful service check consists of a login, file download, and content integrity validation, and will be awarded points.

HTTP - Web services accessed via the HTTP protocol will be checked. Each successful connection, page download, and content integrity validation will be awarded points.

HTTPS - Similar to the HTTP check. Connecting via the HTTPS protocol, each successful connection, page download, and content integrity validation will be awarded points.

SMTP - Email will be sent to a valid email account via SMTP. This will simulate customers sending messages. Each successful delivery of email to one or more accounts will be awarded points.

POP3 - Email accounts will be checked via POP3. This check will simulate other employees checking their Inbox via the POP3 protocol. Note that this service is dependent on user accounts with known passwords. Each successful access of a users' mailbox will be awarded points. Note that both the insecure (POP3) and secure (POP3S) variants may be used.

SSH - An SSH session will be initiated to simulate a vendor or end-user account logging in on a regular basis to check error logs or perform other duties. Note that this service is dependent on user accounts with known passwords. Each successful login and command execution will be awarded points.

DNS - DNS queries will be performed against the DNS server. Known DNS records hosted by each team for public services will be queried. A query for a domain name will be sent to the server, a response with the correct IP will be awarded points.

© 2016 California State Polytechnic University, Pomona

COMPETITION SCENARIO

Welcome to Elsinore Beer!

Brief History:

Elsinore Beer is a 114-year-old Canadian beer and ale brewery started by Johan "Hans" Helsingør in 1902. Originally named Helsingor Ale Company, ownership of the brewery passed to Johan's son, Johannes, and eventually his grandson, John Elsinore, who took over as owner in 1975. The family-owned brewery operated under several names during history before officially incorporating as Elsinore Beer in 1976 with John Elsinore as CEO and Board Chairman.

John Elsinore grew Elsinore Beer from a small family business to a Canadian regional favorite but was never able to fulfill his dream of moving into the North American market. His failing health required him to step down as CEO in 2008 and allow Claude Elsinore, John's nephew and then VP of Operations and Finance, to take over as acting President and Interim CEO.

Claude Elsinore was appointed President and CEO with John Elsinore's death on October 31, 2010. John's Will and Trust stipulated his majority ownership stake in Elsinore Beer would be held by the Trust until Pamela Elsinore, his daughter, turned 40 years old.

North American Expansion:

On January 17, 2016, the day she turned 40, Pamela Elsinore inherited her father's majority stake and immediately took the title of CEO relegating her uncle, Claude Elsinore, to president. The newly minted CEO announced she and Henry Green had been secretly working since mid-2015 to bring to life her father's wish of moving into North America. That very day, under Pam's direction, Elsinore Beer purchased *Brewski Bottle and Crown, LLC* of California. The Brewski acquisition included a corporate building, local distribution network, brew facility, and warehouse.

That January Pamela and Henry put together a North American launch team and began operations. The relaunched brewery relied on Elsinore Beer facilities in Canada to brew and bottle most products using existing recipes and production lines. The California facilities would be devoted to logistical support and brewing small batches of specialty craft product expected to become popular and profitable in the local market.

© 2016 California State Polytechnic University, Pomona

Current Events:

The Brewski relaunch is still in its infancy and facing a number of challenges. Brewski Bottle and Crown had been in decline for a number of years and officially shuttered in late 2015. While Pam and Henry Green were able to quickly get product to market by importing and distributing Elsinore Beer under the Brewski branding, they need the California corporate office, housed in the previous Brewski HQ, to immediately begin operations.

Information technology for Brewski has been contracted through a local provider who has promised to deliver an experienced team of IT specialists. The current network and servers consist of a scraped together environment -mixing salvaged Brewski hardware and surplus Elsinore Beer technology. A functioning infrastructure and corporate network currently exists but it likely suffers from a number of issues related to the haste it was created. This new IT Team is expected to immediately:

- Take over Network Operations of the California Brewski location
- Find and address existing configuration and setup issues
- Begin providing IT Support and Help Desk functions for staff

The IT team will also be tasked with implementing the technical changes required to support the Brewski name change to Elsinore; advise, recommend, and provide technical expertise for the senior management team; develop and maintain appropriate IT policy, procedures and controls, etc.

Special Considerations:

1. It is common knowledge Claude and Pamela are currently battling one another and tensions run high. While Pamela maintains controlling interest and voting rights, Claude is far more popular with the balance of the board and investors. The North American expansion is a high stakes gamble. Pamela is convinced both Claude and Elsinore Beer Brewmaster, Max Smith, are working behind the scenes to sabotage the expansion and topple her control.

© 2016 California State Polytechnic University, Pomona

2. There have been a number of strange occurrences with the Elsinore Beer technology since John Elsinore passed away Halloween night 2010. Issues include a number of unexpected system crashes, unexplained faults in the physical security system, erratic workstation behavior reported by users, etc. More superstitious staff are convinced John Elsinore's ghost is haunting the company's computers. While this is certainly not the case, a rational explanation for the glitches has not been found and it's unknown if these problems will be seen at Brewski.

ORANGE TEAM – "TRAFFIC GENERATORS"

The Orange Team, also known as "traffic generators", is another method of service checks but is geared towards end-user experience – remote and internal employees, customers or clients. These users attempt to utilize Blue Team services. Some Orange Team activities include:

- Use of email systems, help desk tickets, Sharepoint, etc.
- Place phone calls (remote users, customers, clients, etc.)

Orange Team adds the human touch to the competition environment.

THE PRESENTATION ROOM

The Presentation Room provides competitors the opportunity to polish their communication skills through the composing and presenting of succinct reports on a variety of topics. Presenters should assume that the people they'll address are powerful decision makers who require the Blue Team's input but they should not assume these people have a very deep level of technical knowledge or skill.

Presentation Rules:

- Presentations are to be 5 minutes long. No penalty for going over.
- No penalty for presenting without a slide show or handouts.
- No penalty for presenter's attire.
- Optional: Ask all presenters one question, the same question, per session
- No less than 3 Judges should be present when judging presentations.

- 25% scoring penalty on Presenters who arrive late.
- Presenters leaving early will receive a zero score on their presentation.
- Presenters are not allowed to contact with their team while in a session.

LEAD VOLUNTEERS

Dr. Dan Manson
Founder and Gold Team lead, Dan guides and develops WRCCDC in recruiting, funding and sponsors.

Joe Luna
Red Team lead & original member of WRCCDC, Joe recruits and manages Red Team

James Schneider
Another original member, James is the Black Team lead, systems developer and tech support for events

Michelle Behne
WRCCDC event manager and lead White Team judge, organizes and coordinates WRCCDC activities.

Gary Black
Leads in developing injects, collaborates on systems and scenario development, and maintains the event pacing.

Phil Lucas
Competition communications, inject coordination and scoring

Anna Carlin
Career Builder Boot Camp coordinator and facilitator, and providing event support

Justin Townsend
White Team Liaison to Red Team, scenario and inject development

Glen Shiery & Karoline Bednarski
Volunteer Coordinators

Tim Krugh
Orange Team Lead

© 2016 California State Polytechnic University, Pomona

VOLUNTEER INVOLVEMENT

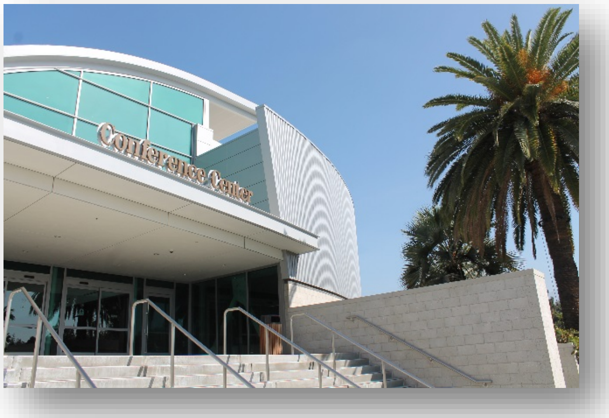
Without a large number of volunteers the competition would not exist. Volunteer efforts start months before the first invitational with a core group of individuals and the number swells so that the regional event has more volunteers than competitors. Some of those volunteers are:

- Students - our future WRCCDC competitors
- WRCCDC Alumni
- Industry professionals
- Sponsors

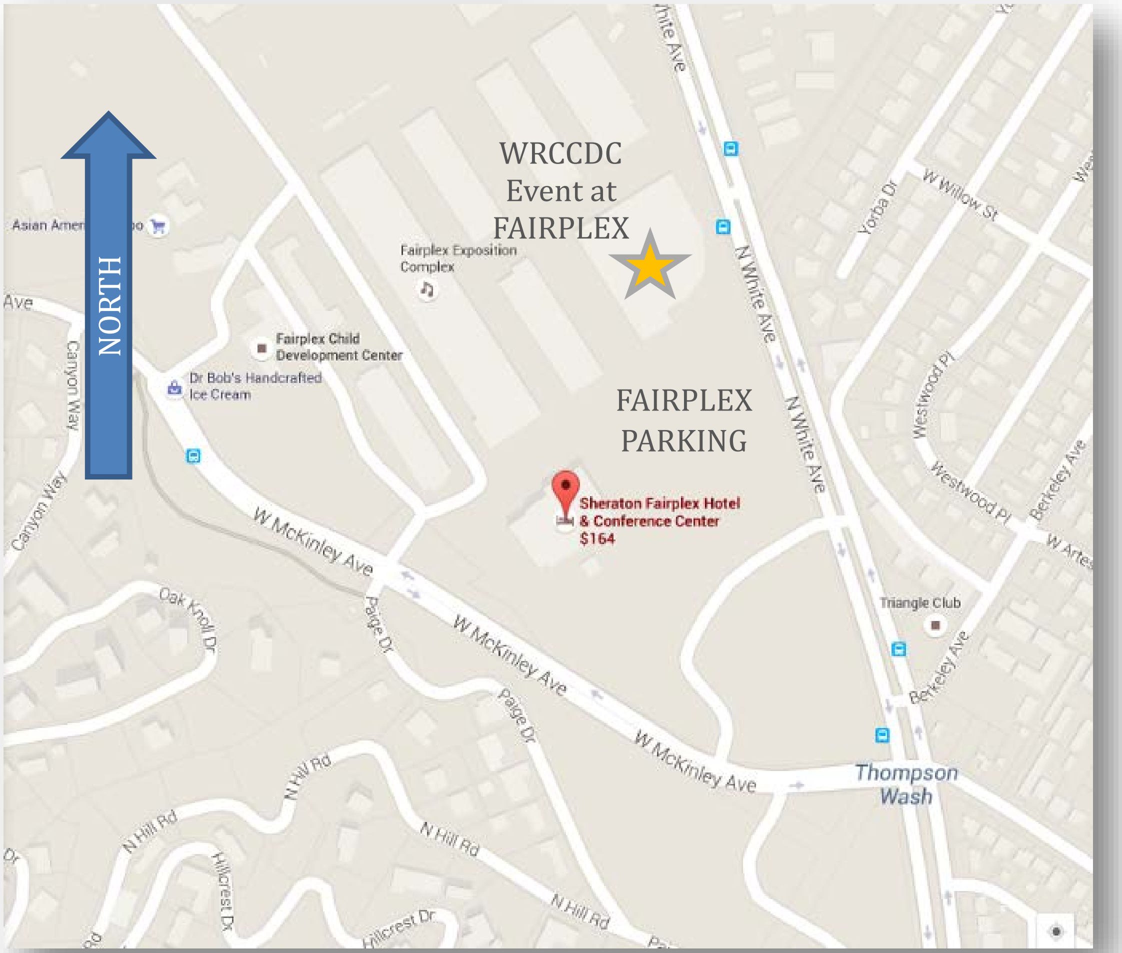
It is with gratitude for all the efforts, all the resources, the goodwill and sponsors who make the WRCCDC a reality so future cyber security professionals can experience a taste of reality during one intensely stressful and fun weekend.

LOCATION & LODGING

This year WRCCDC is held at the Sheraton Fairplex Hotel & Conference Center.



Sheraton Fairplex Hotel
& Conference Center
601 W. McKinley Ave., Pomona, CA 91768
909-622-2220
Directions: http://bit.ly/1PTwNTg



2016 NATIONAL CCDC RULES

The following are the approved national rules for the 2016 CCDC season. Please refer to the official rules for your specific CCDC event for any local variations.

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 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.

 a. Competitors may only be a member of one team per CCDC season.

 b. 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.

 c. 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.

0. **Team Composition**

 . 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.

a. Each competition team may consist of up to eight (8) members chosen from the submitted roster.
b. Each competition team may have no more than two (2) graduate students as team members.
c. 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.
d. 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.
e. 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.
f. Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and the teams before and during the competition. In the event of the Team Captain's absence, teams must have an identified team liaison serving as the captain in the competition space at all times during competition hours.
g. An institution is only allowed to compete one team in any CCDC event or season.

1. **Team Representatives**
   . 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.
   a. 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).
   b. Representatives may not enter their team's competition space during any CCDC event.
   c. Representatives must not interfere with any other competing team.
   d. 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.

0. **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.

0. 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.

0. **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.

0. **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.

0. **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.

0. 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, in order 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.

1. Remote/ Team Site Judging and Compliance

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.

a. 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

© 2016 California State Polytechnic University, Pomona

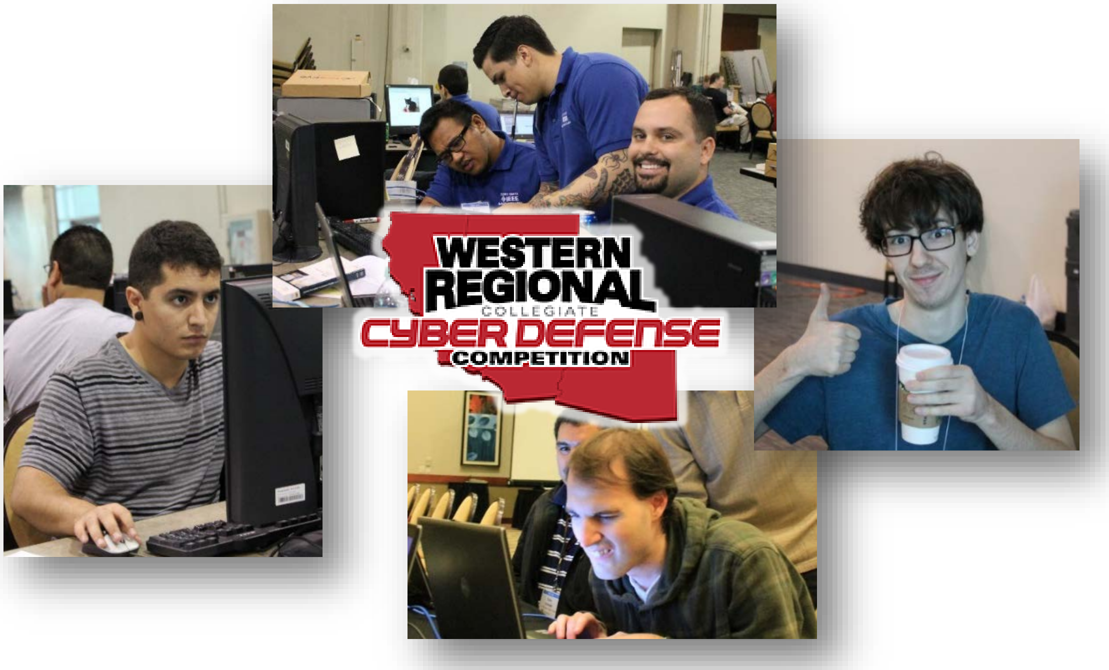
- vi. Assure that the Team Captain has communicated to the Event Judges approval of initial system integrity and remote system functionality
- vii. Assist Event Judges in the resolution of grievances and disciplinary action, including possible disqualification, where needed
- viii. Report excessive misconduct 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

b. 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. 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.

Local Competition Rules

The local competition rules section is unique to each specific CCDC competition. Please refer to the official rules for your CCDC event for more information.

GOOD LUCK, TEAMS!



Crowe Horwath.

Crowe Cybersecurity Services

Have You Seen the Headlines Lately?

Given the recent numerous newsworthy security breaches, companies are asking important questions about their current cybersecurity capabilities, gaps, and requirements. The Crowe Horwath LLP team helps organizations incorporate a proactive program to mitigate cybersecurity risks in an effort to strengthen the confidentiality, integrity, and availability of organizational assets. Our services include:

- Penetration testing and security awareness
- Application security
- Data privacy
- IT compliance and attestation
- Cybersecurity assessments
- Security implementations
- Incident response
- Third-Party risk management

To learn more about fulltime or internship opportunities, please visit www.gocrowe.com or contact campus.recruiting@crowehorwath.com for more information.

Visit our blog to stay updated at www.crowehorwath.com/cybersecurity-watch.

Audit | Tax | Advisory | Risk | Performance

The Unique Alternative to the Big Four®

In accordance with applicable professional standards, some firm services may not be available to attest clients.

© 2016 Crowe Horwath LLP, an independent member of Crowe Horwath International crowehorwath.com/disclosure