Western Regional
Collegiate Cyber Defense Competition

OFFICIAL COMPETITION GUIDE

TABLE OF CONTENTS

Contact: Dr. Dan Manson at dmanson@csupomona.edu

Based on work from University of Texas at San Antonio and Rochester Institute of Technology

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. This is the seventh Western Regional CCDC and this is the first year we held a virtual qualifier. We encourage you to provide comments and feedback to help us improve future events. We wish the best of luck to each of you and your teams!

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

Contact: Dr. Dan Manson at dmanson@csupomona.edu

THANK YOU TO OUR SPONSORS!

Raytheon

CWW cyberwatch west

Homeland Security

facebook

workday.

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

FireEye

LogicSecurity

CYLANCE

CISCO

Contact: Dr. Dan Manson at dmanson@csupomona.edu

Based on work from University of Texas at San Antonio and Rochester Institute of Technology

2015 COMPETITION SCHEDULE

Thursday – March 26

7:00 PM	Registration	Ursa Minor
8:30 PM	Competition Instructions and Brief-In	Ursa Minor

Friday – March 27

9:00 AM	Competition Begins	Ursa Major
11:30 AM	Grab & Go Lunch – no break in competition	Ursa Major
6:00 PM	Competition Ends for the Day Dinner	Ursa Minor
7:00 PM	Game Room	Game Room, Lower Level

Saturday – March 28

9:00 AM	Competition Begins	Ursa Major
11:30 AM	Grab & Go Lunch – no break in competition	Ursa Major
6:00 PM	WRCCDC 2015 Competition Ends Clean up, Prep for Recruiting Mixer	
7:00 PM	Recruiting Mixer	Ursa Minor
7:00 PM	Game Room	Game Room, Lower Level
9:00 PM	Q&A with Red, Black & White Teams	Andromeda Rooms A, B, C

Sunday – March 29

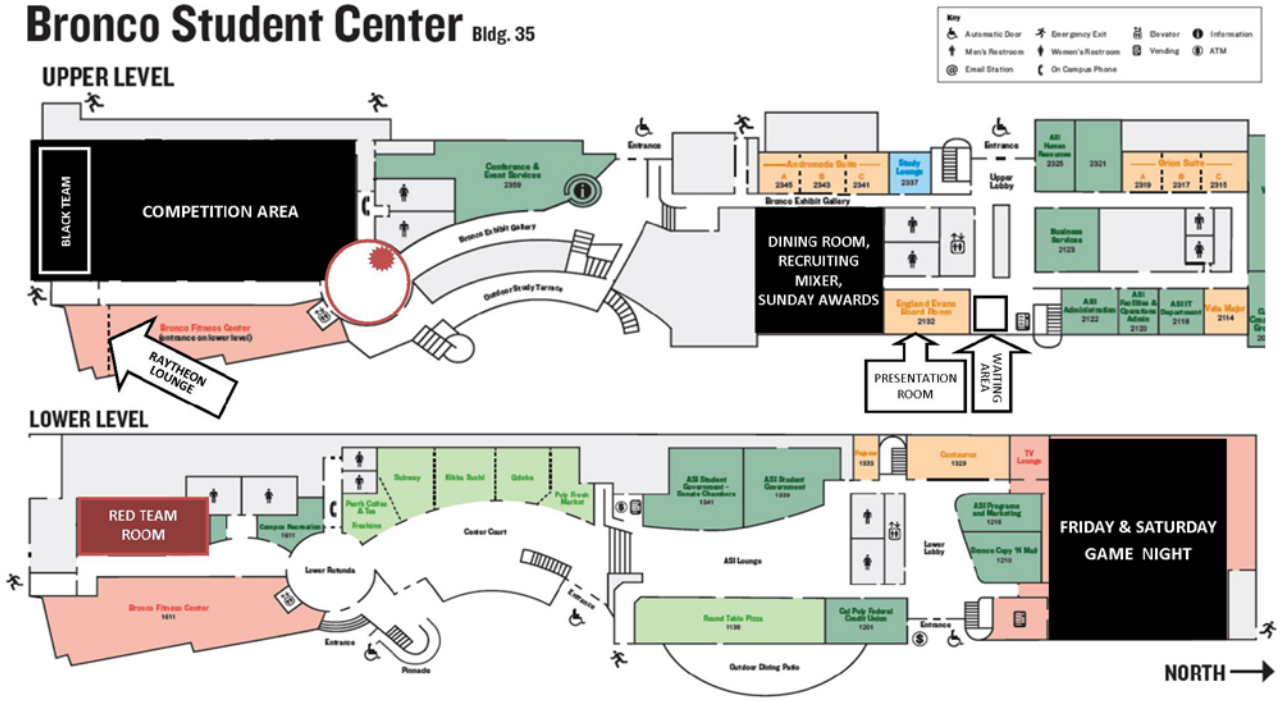
9:00 AM	Keynote Speakers & Debriefs	Ursa Minor
11:30 AM	Lunch	Ursa Minor
12:30 PM	Award Ceremony	Ursa Minor

Contact: Dr. Dan Manson at dmanson@csupomona.edu

LOCATION & LODGING

This year WRCCDC will hold the event in Cal Poly Pomona's Bronco Center. A parking pass is required for both the competition and the hotel. Lodging will be provided at Kellogg West a hotel facility on the Cal Poly Pomona campus. Address is:

Kellogg West
3801 W. Temple Ave., Pomona, Ca
909-869-4146
http://www.kelloggwest.org/kw-directions.aspx



The floor plan of the Cal Poly Bronco Student Center shows where the many WRCCDC activities will occur.

Contact: Dr. Dan Manson at dmanson@csupomona.edu

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. The rules are located on the WRCCDC website: http://www.wrccdc.org. WRCCDC rules override NCCDC rules in the event of a conflict. 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 the 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:

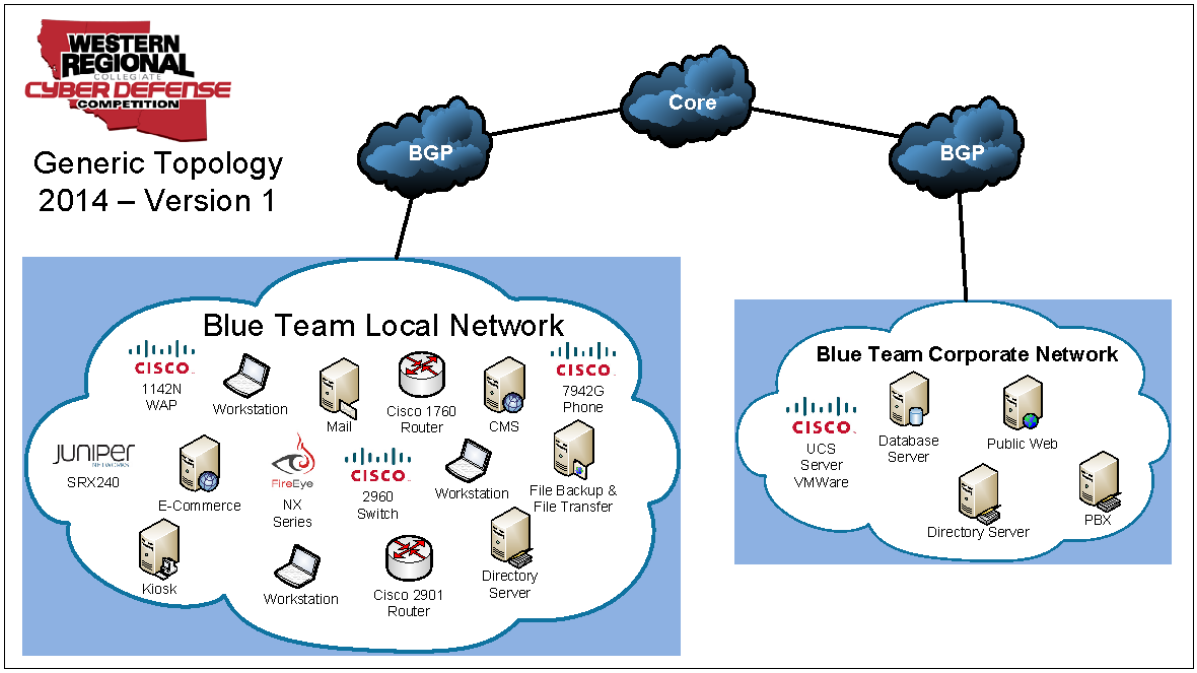
- Violating service level agreements.
- Usage of recovery services provided by the Black Team.
- Successful penetrations by the Red Team.

Contact: Dr. Dan Manson at dmanson@csupomona.edu

- 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 restricted to a "blind" list of URLs. This list allows access to necessary support sites for all the applications used in the competition. Each team may request 10 additional sites prior to the competition. Approved URLs will be added to the list of available URLs. During the WRCCDC teams may request additional sites but must have good justification for the request. There will be no penalty for any reasonable URL requested.

Contact: Dr. Dan Manson at dmanson@csupomona.edu

Connections sourced from the pod networks will be filtered. 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; however, these requests can be denied and/or rescinded by the black team for any reason at any time.

Each team will be provided with access to a central read-only file repository where common operating system installation files, patches, and other files 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 i.e. Standard, Enterprise, etc.):

Debian Linux	Fedora Linux	MS Windows Vista	MS Windows Server 2008
Ubuntu Linux	Cisco IOS 15	MS Windows Server 2012	
Mint Linux	Cisco IOS 12.4	MS Windows Server 2003	
Arch Linux	MS Windows 7		
CentOS Linux	MS Windows 8		
Gentoo Linux	MS Windows XP		

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

Contact: Dr. Dan Manson at dmanson@csupomona.edu

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 connection, login, file download,

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

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

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

DNS - DNS lookups 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.

COMPETITION SCENARIO - *GOOD KARMA'S WEST COAST EXPANSION*

Backstory

Good Karma was founded as Karma Networks in the 1990's as a corporate ISDN provider located on the East Coast by Greg Goodman. Karma quickly found success by providing reasonably priced technical expertise and unmatched customer service. Over the past 10 years, Karma has gradually moved from providing simple broadband access and now offers an array hosted email and web services.

Karma Networks renamed itself to ***Good Karma*** eighteen months ago and now solely operates as a web services and hosting provider. Good Karma has been building an ever increasing clientele with this new business model.

Contact: Dr. Dan Manson at dmanson@csupomona.edu

Several of Good Karma's larger clients have been pressing Mr. Goodman to expand his operations to the west coast. These clients want to expand themselves and prefer to host their west coast services with Karma rather than negotiate separate contracts with existing west coast providers.

Greg Goodman has decided it was time for this expansion and acquired a small, failing hosting company named Virtual Pizza Servers in Southern California from Steve Scumbaugh. Steve created Virtual Pizza Servers to celebrate his twin passions of eating pizza and letting everyone else do the work while he surfed the Internet.

The purchase agreement stipulated that Virtual Pizza Servers will be renamed to West Coast Karma and all existing contracts and SLA's will be respected. The agreement also requires West Coast Karma keep Mr. Scumbaugh as President and Chief Operation Officer for no less than 3 years.

Steve blamed the failure of Virtual Pizza Servers on his previous IT and engineering staff. Both teams were dismissed Thursday evening. West Coast Karma has hired a small team of contractors to take over IT operations for West Coast Karma/Virtual Pizza Servers on very short notice.

The Mission

Your Team immediately assumes all current IT operations.

1) Support existing hosted services and provide support to clients until additional staff can be hired and trained.
2) Ensure there are no violations to existing service level agreements and contracts.
3) Provide IT support functions and helpdesk operations for administrative staff until additional staff can be hired and trained.
4) Bring up new hosted environments and services as new clients are needed.
5) Be ready to assist current Good Karma clients who wish to migrate from the current east coast data center.
6) Take charge of rebranding Virtual Pizza Servers to West Coast Karma (web pages, email, all public facing documents, etc.).

Good Luck……... You are going to need it.

Contact: Dr. Dan Manson at dmanson@csupomona.edu

Based on work from University of Texas at San Antonio and Rochester Institute of Technology

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 – both remote users and end users as in customers or clients. These are only some Orange Team activities:

- 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 the opportunity for competitors to polish their communication skills through the composing and presenting of succinct reports on current topics. Presenters should assume that the people they'll address in the presentation room are powerful decision makers who require the Blue Team's input. Therefore, presentations should not assume these people have a very deep level of technical knowledge or skill.

Here are this year's rules for the Presentation Room:

- Optional: Ask all presenters one question, the same question, per session
- All presentations should be 5 minutes long. No penalty for going over the 5 minutes.
- No penalty for presenting without a slide show or handouts.
- No penalty for presenter's attire.
- 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.
- A team can have more than 1 presenter but must identify the lead presenter.
- A lead presenter must handle 70% of the presentation.
- Presenters are not allowed to contact with their team while in a presentation session.

Contact: Dr. Dan Manson at dmanson@csupomona.edu

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 looking forward to competing in future WRCCDC events
- 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 intense and stressful weekend.

GOOD LUCK, TEAMS!

Contact: Dr. Dan Manson at dmanson@csupomona.edu

Based on work from University of Texas at San Antonio and Rochester Institute of Technology