WESTERN REGIONAL COLLEGIATE CYBER DEFENSE COMPETITION

Western Regional
Collegiate Cyber Defense Competition

2017 COMPETITION PROGRAM

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

TABLE OF CONTENTS

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

WELCOME 2017 COMPETITORS!

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

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

THANK YOU TO OUR SPONSORS!

Raytheon

workday.

IBM

The Los Angeles Coalition
A COALITION FOR THE ECONOMY & JOBS IN LOS ANGELES

UNIVERSITY of WASHINGTON | BOTHELL
CYBER SECURITY ENGINEERING

FURTIM

AIR FORCE CIVILIAN SERVICE

RAPID7

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

paloalto NETWORKS

Bank of America

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

SPAWAR

CWW
cyberwatch west

FireEye

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

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

2017 COMPETITION SCHEDULE

All competition activities to be in the Cal Poly Bronco Center.

Friday – March 24

8:00 AM	Registration	Ursa Minor
9:00 AM	Orientation	Ursa Minor
10:00 AM	Competition Begins	Ursa Major
Noon	Grab & Go Lunch – no break in competition	Ursa Major – Side Room
5:30 PM	Grab & Go Dinner—no break in competition	Ursa Major – Side Room
9:00 PM	Competition Ends for the Day	

Saturday – March 25

9:00 AM	Competition Resumes	Ursa Major
Noon	Grab & Go Lunch – no break in competition	Ursa Major – Side Room
5:00 PM	WRCCDC 2017 Competition Ends	
6:00 PM	WRCCDC Alumni Panel – Interviews with past competitors	England Evans
7:00 PM	Recruiting Mixer & Dinner	Ursa Minor

Sunday – March 26

Please eat breakfast at your hotel.

9:30 AM	Keynote Speakers & Debriefs	Ursa Minor
11:30 AM	Awards	

Contact: Dr. Dan Manson at dmanson@cpp.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://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 ways your IT team might gain or lose favor with Management.

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

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.
- 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

A 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.

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.

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

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
- Ubuntu Linux
- Mint Linux
- Arch Linux
- CentOS Linux
- Gentoo Linux
- Fedora Linux
- Cisco IOS 15
- Cisco IOS 12.4
- MS Windows 7
- MS Windows 8
- MS Windows XP
- MS Windows Vista
- MS Windows Server 2012
- MS Windows Server 2003
- MS Windows Server 2008
- Palo Alto (PAN-OS)
- Juniper (JunOS)
- MS Windows Server 2016

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:

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

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

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 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.

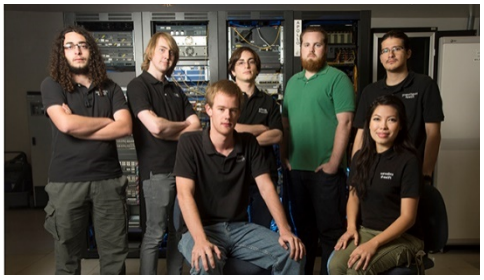
SSH - An SSH session will be initiated to simulate a vendor account logging in on a regular basis to check error logs. Note that this service is dependent on user accounts with known passwords. Each successful login and command execution will be awarded points.

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.

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

COMPETITION SCENARIO

Backstory - Meeseeks Service Provider



Meeseeks Service Provider operates as a Managed Service Provider (MSP) serving small and medium businesses. Working for an MSP certainly isn't for everyone, so welcome to the ranks of the Technology Elite!

Technology drives businesses and, when properly deployed and managed, have a significant competitive edge. Email, databases, accounting, customer management, and similar technology systems have become very important to small and medium businesses. This dependency creates significant vulnerability, and frustration, when key services fail. Smaller businesses often lack the in-house IT skill and expertise to proactively manage critical systems or rapidly restore services when something fails.

As an MSP, Meeseeks offers to remotely manage their customer's IT infrastructure, end-user systems under a subscription model. For a flat monthly fee, Meeseeks offers small and medium businesses a contractual arrangement for proactive IT management and reactive IT services. Everything is spelled out in a service level agreement. This arrangement relieves customer partners of IT responsibilities and provides them cost effective access to IT skills and expertise.

Meeseeks, as all successful MSPs, provides far more than break-fix service. Meeseeks offers a full suite of IT solutions and virtual CIO services with the promise to find and correct problems before a disruption of business occurs and handling of user support and training.

With its "Never Say No" motto, Meeseeks is capable of managing all technology services for their clients including:

- Help Desk and Support for client endpoint users via chat, email, and telephone
- HaaS, IaaS, SaaS, DPaaS
- Recommend, Coordinate, and Manage 3rd party and vendor relationships
- IT Hardware, Software, and License acquisition
- Network and Security monitoring (audits available on request)

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

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

- Disaster Planning and Business Continuity
- Project Management of IT implementations, upgrades, etc.

Client firms purchase solutions packages at a fixed monthly cost in exchange for guaranteed response and issue resolution. System availability, customer service metrics, and proactive handling of failures are clearly spelled out in SLA agreements and failing to fulfill promises is quite costly.

Your Team immediately assumes all current IT operations for hardware and services within your pod and any remote systems indicated by the BLACK or WHITE teams."

- Support existing hosted services and provide support to clients until additional staff can be hired and trained.
- Ensure there are no violations to existing service level agreements and contracts.
- Provide IT support functions and helpdesk operations for administrative staff until additional staff can be hired and trained.
- Bring up new hosted environments and services as new clients are needed.
- Be ready to assist current Meeseeks clients who wish to migrate from the current east coast data center.
- Take charge of rebranding Meeseeks' servers (web pages, email, all public facing documents, etc.).

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 customers or clients. Orange Team adds the human touch to the competition environment. These are only some Orange Team activities:

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

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

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

THE PRESENTATION ROOM

The Presentation Room provides the opportunity for competitors to polish their communication skills through the composing and presenting of 5 minute reports on current topics. Presenters should assume their audience comprises powerful decision makers. 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:

- Presentations should 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.
- 50% scoring penalty on late arrivers.
- Presenters leaving early will receive a zero score.
- A team can have more than 1 presenter but must identify the lead presenter who handles 70% of the presentation.
- Presenters are not allowed to contact with their team while in a presentation session.

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

VOLUNTEERS

These are the people who make the WRCCDC and its many activities happen. They hold regular jobs but because of their passion for what CCDC offers future information security professionals they sacrifice a multitude of hours to make WRCCDC what it is.

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 & Tim Krugh
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

Karoline Bednarski
Volunteer Coordinator

Tobi West
Orange Team Lead

Contact: Dr. Dan Manson at dmanson@cpp.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, resources, goodwill and sponsors who make the WRCCDC possible so future cyber security professionals can experience a taste of reality during one intense but stressful and fun weekend.

GOOD LUCK, TEAMS!

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

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