2018 PROGRAM

Western Regional

Collegiate Cyber Defense Competition

Contact: Michelle Behne - michelle.behne@wrccdc.org

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

WELCOME!

Welcome to the Western Regional Collegiate Cyber Defense Competition (WRCCDC). Since 2008 WRCCDC has challenged and expanded the horizons of students by exposing them to new technologies and concepts. 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).

It is an honor to host this event. However, it requires the support of industry and professional association support, and our many volunteers, that allows this interesting, exciting, and inspiring competition to continue and grow. Thank you all for helping to forge future cyber security professionals!

Good luck to all our competitors!

Michelle Behne

WRCCDC Director

Contact: Michelle Behne - michelle.behne@wrccdc.org

GOOD LUCK 2018 COMPETITORS!

Arizona State University

CSU Northridge

Contact: Michelle Behne - michelle.behne@wrccdc.org

THANK YOU TO OUR SUPPORTERS!

Raytheon

workday.

paloalto NETWORKS

IBM

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

CWW
cyberwatch west

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

AIR FORCE CIVILIAN SERVICE

UNIVERSITY of WASHINGTON | BOTHELL
CYBER SECURITY ENGINEERING

Contact: Michelle Behne - michelle.behne@wrccdc.org

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

2018 Competition Schedule

All competition activities will be in the Cal Poly Pomona Bronco Center.

Friday – March 23

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 Day 1	

Saturday – March 24

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	Panel Discussion with Cyber Security Pros	England Evans
7:00 PM	Recruiting Mixer & Dinner	Ursa Minor

Sunday – March 25

Please eat breakfast at your hotel. Everyone is welcome to attend!

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

Contact: Michelle Behne - michelle.behne@wrccdc.org

Competition Set Up

The overall goal of the competition is to test the skills and knowledge of competing teams (Blue 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 may override or add to NCCDC 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 the WRCCDC Lead judge 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

Contact: Michelle Behne - michelle.behne@wrccdc.org

attend to their desires in a timely fashion. Here are 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.
- 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.

Competitor Pod Overview

Your competition pod represents a team's scope of responsibility within 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 network that will be maintained by the BLACK Team. Connections sourced from the pod networks to outside of the competition network may be filtered. Only connections using HTTP, HTTPS, and FTP will be permitted.

Contact: Michelle Behne - michelle.behne@wrccdc.org

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

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.

Note that your competition pod may be extended to include other pieces of remote infrastructure beyond the local physical stations in your designated competition area, including cloud services.

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

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 entering and leaving your environment but you must keep a vigilant watch because your pod systems are under continuous attack. Finally, you will need to try and find the perpetrators via forensic means and file reports on any suspicious activity.

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.):

Contact: Michelle Behne - michelle.behne@wrccdc.org

- Debian Linux and derivatives.
- Ubuntu Linux and derivatives.
- Arch Linux
- CentOS Linux and derivatives.
- Gentoo Linux
- MS Windows XP/Vista/7/8/10
- MS Windows Server 2003/2008/2012/2016
- Cisco IOS
- Palo Alto (PAN-OS)
- Juniper (JunOS)

FUNCTIONAL SERVICES

Certain services are expected to be operational at all times or as specified throughout the competition. Points will be continually 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, these services will be tested for function and content where appropriate. Most checks will be automated, but some service check points may be awarded via manual inspection across all teams.

Services may be added and/or removed at any point throughout the competition. The following protocols may be used for various service checks against your pod:

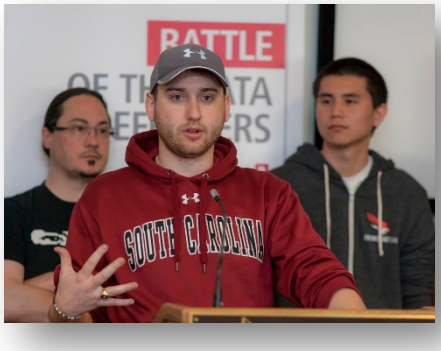
FTP – One or more files made available via an FTP server will be downloaded and checked for content and validity. Note that this service may be dependent on user accounts with known passwords, or may be accessed anonymously. File names and contents must remain intact unless otherwise instructed. Each successful connection, login, file download, and content/integrity check will be awarded points.

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.

Contact: Michelle Behne - michelle.behne@wrccdc.org

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 the POP3 protocol. 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.

Individual failed service checks have no effect on a team's service score (no points gained or lost). However, some or all services may be subject to a Service Level Agreement (SLA). The SLA indicates a point penalty for services that have failed service checks for a consecutive period of time. This period of time will be announced for each specific competition. Different services may receive different point penalties based on their level of importance to the scenario. Once a service is penalized for violating an SLA, the timer resets for a countdown to the next SLA interval.

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

Contact: Michelle Behne - michelle.behne@wrccdc.org

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)
- 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."

Contact: Michelle Behne - michelle.behne@wrccdc.org

- 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 contrac ts.
- 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. Orange Team represents the consumers of the systems, information, and services Blue Teams are managing. Meaning Orange Team can be internal users, remote users, and end users such as customers or clients. Orange Team adds the human touch to the competition environment. These are only some Orange Team activities:

- Use of any of Blue Teams systems and services such as: email systems, help desk tickets, Sharepoint, etc.
- Place phone calls as remote users, customers, clients, etc.

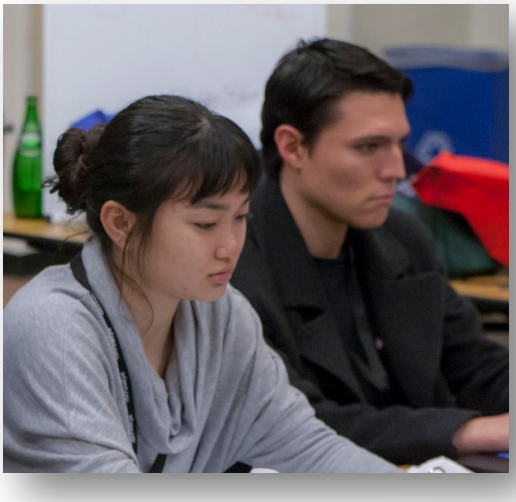
The Presentation Room

- The Presentation Room provides the opportunity for competitors to show off their soft skills through composing and presenting of 5 minute reports on a variety of topics. Presenters should assume their audience comprises powerful decision makers – like a Board of Directors or a group of managers. 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.

Contact: Michelle Behne - michelle.behne@wrccdc.org

- 25% scoring penalty on late arrivers.
- Presenters leaving presentation holding area 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: Michelle Behne - michelle.behne@wrccdc.org

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

VOLUNTEERS

These are the key 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.

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

James Schneider
A founding WRCCDC member, James is the Black Team lead, systems developer and lead tech support for events

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

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

Justin Townsend

White Team Liaison to Red Team, scenario and inject development

Tim Krugh
Develops injects, collaborates on Orange Team coordination, and scenario development.

Karoline Bednarski
Volunteer Coordinator

Anna Carlin
Resume Book coordinator and resume training developer, and some event logistics

Phil Lucas
Presentation Room Coordinator and WRCCDC alum

Contact: Michelle Behne - michelle.behne@wrccdc.org

VOLUNTEER INVOLVEMENT

It's a large volunteer effort!. Starting months before the first invitational a core group of individuals begin planning and prepping. Then number swells so at the regional event there are more volunteers than competitors. Some of those volunteers are:

- Students looking forward to competing in future WRCCDC events
- WRCCDC Alumni
- Industry professionals
- Program Supporters

It is with gratitude for all the efforts, resources, goodwill and program supporters who make the WRCCDC possible. We're pleased to be a part of forging future cyber security professionals..

GOOD LUCK, TEAMS!

Contact: Michelle Behne - michelle.behne@wrccdc.org