2012 Western Regional
Collegiate Cyber Defense Competition

Team Packet

Version 1.6

Friday Lunch Keynote Speaker:

Mahvash Yazdi, CIO
Southern California Edison

Friday Dinner Keynote Speaker:

Laura Chappell, Founder
Protocol Analysis Institute

For more information:

Dr. Dan Manson
dmanson@csupomona.edu

Western Regional CCDC
http://www.wrccdc.org

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 (CCDC). 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 fifth Western Regional CCDC and this year we will host 10 teams. We've had several "National Virtual" competitions and in other parts of the country 9 regional competitions are expected. 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.
Director
Center for Information Assurance

2012 COMPETITION SCHEDULE

Friday – March 23

8:00 AM	Registration opens inside Convention Center next to Exposition Hall
9:00 AM	Competition Instructions and Brief-In (Exposition Hall)
10:00 AM	Competition Begins (Exposition Hall)
12:00 PM	BREAK: Lunch and Opening Keynote (Sonoma Room) – *Competition Suspended*
1:30 PM	Competition Resumes (Exposition Hall)
5:30 PM	BREAK: Dinner and Evening Keynote (Sonoma Room) – *Competition Suspended*
7:00 PM	Competition Resumes
12:00 AM	Competition ends for the day

Saturday – March 24

8:00 AM	Competition Resumes
12:00 PM	Lunch available (Sonoma Room) - Competition Continues
6:00 PM	BREAK: Dinner (Sonoma Room) - *Competition Suspended*
7:00 PM	Recruiting Banquet (Exposition Hall)
9:00 PM	Competition Resumes (Exposition Hall)
12:00 AM	Competition ends for Saturday

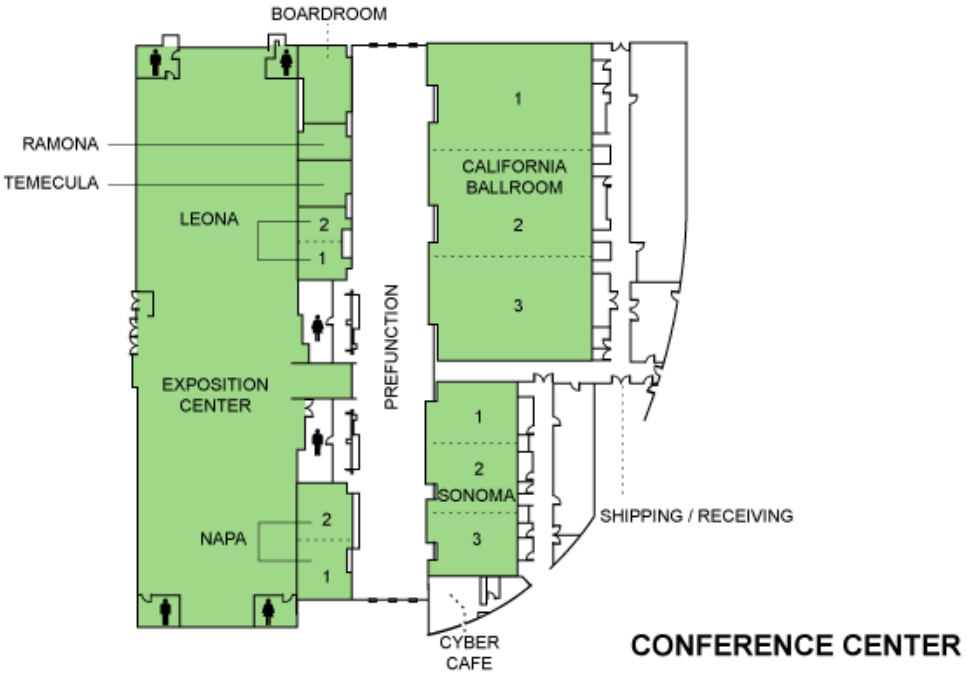
Sunday – March 25

9:00 AM	Competition Continues (Exposition Hall)
11:00 AM	Competition Ends - Clean Up Begins
11:30 AM	Feedback Session (Red, Black, & Blue Teams)
12:30 PM	Lunch (Sonoma Room)
1:30 PM	Award Ceremony (Sonoma Room)

LOCATION & LODGING

We're pleased to host this year's competition at the Pomona Fairplex Conference Center right next to our lodging at the Pomona Sheraton Fairplex.

You will park in the guest parking next to the hotel, go through the lobby of the hotel and out the back. The Conference Center is behind and to the right of the hotel. Competition Registration is inside the Conference Center next to the Exposition Center.



The address for our lodging is:

Pomona Sheraton Fairplex Hotel
601 West McKinley Avenue,
Pomona, California, 91768
Phone: (909) 622-2220.

Please contact Dr. Dan Manson at dmanson@csupomona.edu or (909) 455-2403 regarding lodging needs.

WRCCDC GOAL

The overall goal of this competition is to challenge and expand the skills of competing teams. This is done by attempting to provide a fair and equal playing field for all Blue Teams. The following measures have been instituted to provide the same opportunity for all Blue Teams:

1. Blue Teams are assigned their own pods during the competition.
2. Begin the competition with identical sets of hardware and software.
3. Are located on a dedicated internal network, connected to a competition network allowing equal bandwidth and access for scoring and Red Team operations.
4. Must adhere to corporate standards while performing injects and mitigating any resulting security threat.
5. Are challenged with identical business injects (tasks) at the same time during the course of the competition.
6. During the 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 the WRCCDC coordinator.

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.

COMPETITION SCENARIO & SCORING

This year's competition scenario is set in the medical field. Your organization is a medical integrator, basically a translator, for a large medical office to its medical billing service. The previous IT team has been fired for running a music and video file sharing service on company systems. It has also been reported that your predecessors were grossly incompetent.

As the replacement IT team, you must look for system vulnerabilities, and if one is discovered, you have an obligation to correct it. If your environment is exploited, it must be reported. When Management makes demands, you must attend to their requests.

Here are the ways your IT team might gain or lose favor with Management.

Teams gain points by:

1. Keeping required services up
2. Controlling/preventing un-authorized access
3. Completing business tasks (injects)
4. Completing accurate Business Incident Reports

Teams lose points by:

1. Violating service level agreements
2. Usage of recovery services provided by the Black Team
3. Successful penetrations by the Red Team
4. Not following Competition Rules

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.

THE PRESENTATION ROOM

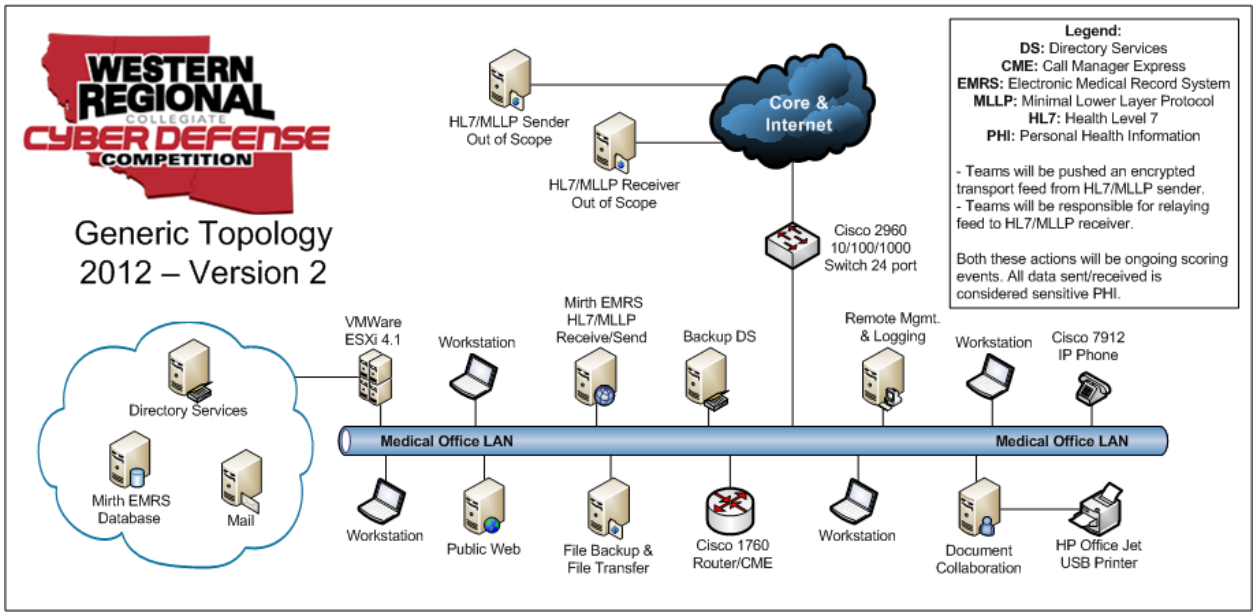
This year's Presentation Room schedule will be extremely busy since there are 10 teams participating. Here are this year's rules:

1. All presenters for the same topic will be collected at the same time.
2. A presenter can present again ONLY after all team members have presented.
3. Presentations should be no longer than 5 minutes.
4. A team can have more than 1 presenter, however, there can only be 1 lead presenter who must present at least 70% of the time.
   A caution: Presenters will be gone for more than 1 hour.
5. All presenters must remain in the waiting area until all presentations have finished.
6. Teams will not be allowed to contact the presenters during the period they are out of the pods.

NETWORK & TOPOLOGY

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.

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



Each team network will be connected via their central layer 2/3 switch into the Black team's layer 2/3 switch. Please note, Internet access will be monitored through a proxy and any unethical, unlawful, or restricted access will be subject to the Blue Team in question being disqualified. 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. Note that both the 32Bit and 64Bit versions of the operating system may be used, along with any variants (i.e. Standard, Enterprise, etc.):

- MS Windows XP
- MS Windows Vista
- MS Windows 7
- MS Windows 2003
- MS Windows 2008
- Debian Linux
- Ubuntu Linux
- Mint Linux
- Arch Linux
- CentOS Linux
- Gentoo Linux
- Fedora Linux
- Open-WRT
- Cisco IOS 15
- Cisco IOS 12.4

FUNCTIONAL SERVICES

Certain services are expected to be operational at all times or as specified throughout the competition. In addition to being up and accepting connections, the services must be 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 "Managed Services Provider". 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 of this attack via forensic means.

Protocols allowed into your network include but are not limited to:

HTTP If requests for specific services are made, you will need to stand them up as quickly as possible. Once the request is made, the result will be stored in a file and compared to the expected result. The returned page must match the expected content for points to be awarded.

HTTPS A request for a page over SSL will be made. Again, the request will be made, the result stored in a file, and the result compared to the expected result. The returned page needs to match the expected file for points to be awarded.

SMTP/POP3 Email will be sent and received through a valid email account via SMTP. This will simulate an employee in the field using their email. 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. Each successful login and log check will be awarded points.

SQL An SQL request will be made to the database server. The result will be stored and compared against an expected result. Each successfully served SQL request will be awarded points.

DNS DNS lookups will be performed against the DNS server. Each successfully served request will be awarded points.

HIPPA, HL7, AND MLLP CONSIDERATIONS

As part of the scenario this year, each team will be required to maintain one or more service dependencies with neutral third-party systems. The transport protocol used to communicate between the teams and this third-party is MLLP (Minimal Lower Layer Protocol), operating over TCP (Transmission Control Protocol). The data contained within the MLLP packets is formatted according to HL7 (Health Level 7) standards. This data is comprised of sensitive medical patient information, and should be protected in all capacities within the team's scope of control.

There will be 2 service checks used during the competition. One check will monitor transmissions sent from one or more neutral third-party systems. The other check will monitor data sent from the team system back to one or more third-party systems. Note that for each service check round, a single set of data will be sent to each team, and the return data should match the most recent data sent to the teams during the same service check round.

Note that these are functional service checks similar to the other checks listed above. This means that a full transmission of the data will need to complete successfully in order to consider the operation successful, just as if a client in a business environment would expect the service to behave.

The service engine has been configured to always attempt to send new data to the teams before performing a check to determine if that data was properly received.

While these two checks are independent, teams WILL FAIL a check on the received data back from the teams if the initial data could not be sent successfully. The scoring system will only verify the data received matches the data sent earlier in the same check round.

It is possible for a team to fail a check on the data received back from the teams if that data was successfully sent to the teams. However, if the team did not successfully receive the data for that round, the check for the received data back from the teams will always fail.

Also note that the Mirth system used to send and receive the HL7 information may keep transactional records as the competition progresses. This data needs to be kept intact and accessible, as it may play a role in delivered injects further into the competition. If patient data is contained within these records, it will be considered Personal Health Information, and should be protected appropriately.

Good Luck, Teams!