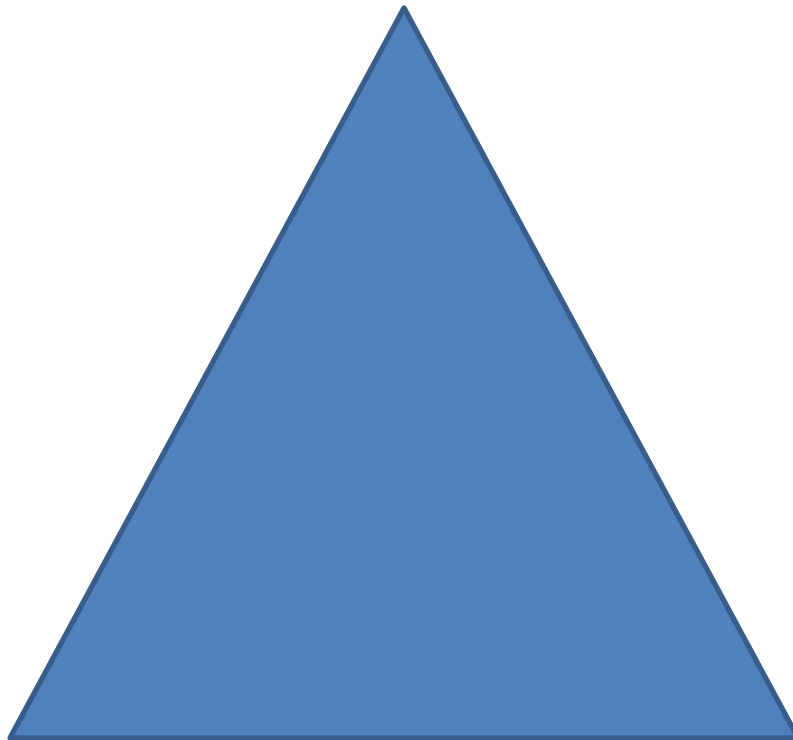


WCC Cybercamp Competition

Winter 2012

Cyberdyne



The Cake is a Lie

Table of Contents

Required Tools.....	3
Competition Schedule.....	4
Competition Overview.....	5
Scenario.....	6
Competition Rules.....	6
Network Description.....	8
Inject 1.....	10
Inject 2.....	11
Inject 3.....	12
Inject 4.....	13
Inject 5.....	14
Inject 6.....	15
Inject 7.....	16
Inject 8.....	17
Inject 9.....	18
Inject 10.....	19

Required Tools

Switch: Catalyst 2950 series

Cables: Straight through cat 5

PC: Four PC's

VMWare Player Version 4.0.2

Ubuntu Version 10.10 Running WordPress

Ubuntu Version 10.10 Running Zencart

Windows XP

Windows 2008 Server

Competition Schedule

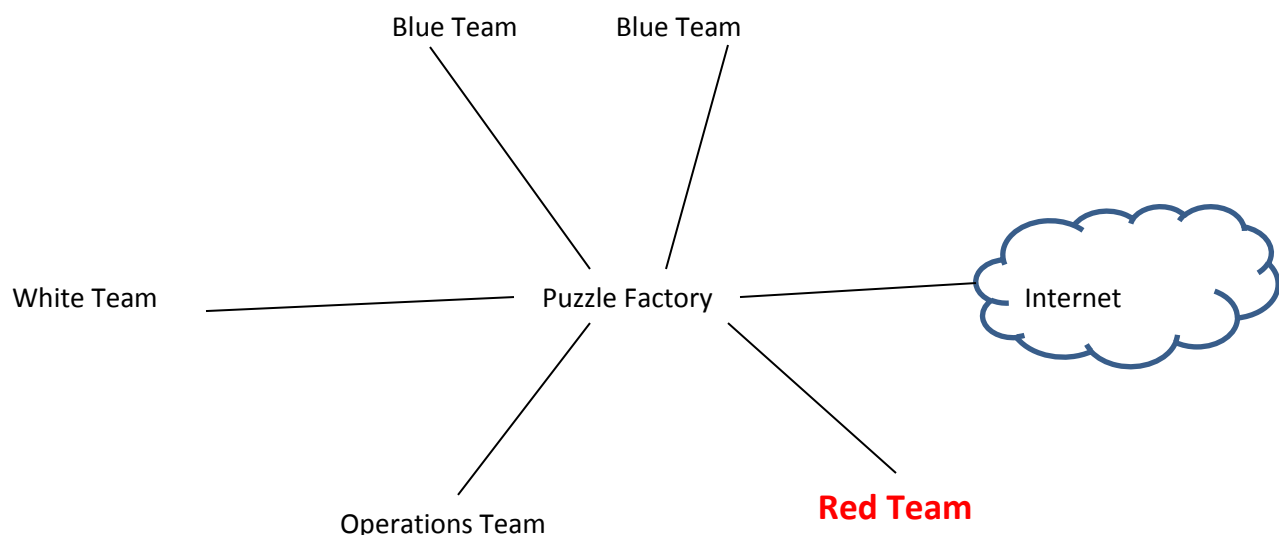
Time	Place	Topic
10:00 - 10:15	Baker 102 and 103	Teams get situated Packets handed out, questions answered
10:15 – 10:45	Baker 101	Cybercamp Competition phase 1
10:45 – 11:00	Baker 101	Break
11:00 – 12:00	Baker 101	Cybercamp Competition phase 2
12:00 - 12:30	Baker 101	Lunch Guest Speaker Dennis Skaar
12:30 – 2:00	Baker 102 and Baker 103	Cybercamp Competition phase 3
2:00 – 2:15	Baker 101,102,103	Break
2:15 - 2:30	Baker 102, 103	Log into Angel and do post, debriefing by red team
2:30	Baker 101	Awards Ceremony

Competition Overview

The WCC Cybercamp competition takes place over a period of 5 hours. Each team is comprised of 4 high school students and one mentor (acting as advisor).

Participants in the competition have the following designations:

- Operations Team - competition officials that organize, run, and manage the competition.
- White Team - judges
- Red Team – pen testers (hackers).
- Blue Team – network defenders.
- Team Captain – Blue team member acting as lead for team.
- Blue teams will be provided with a complete unsecured network. All teams will have identical networks. The computers will run various operating systems and a variety of services.



Scenario

Cyberdyne Company is a puzzle factory that produces puzzles for various audiences. Recently, the IT Director (Arnold) was found to be posting walkthroughs on the Internet and was terminated. Arnold did not take this well and declared “I’ll be back” while he was escorted out the door. The IT staff also was under a cloud of suspicion and management decided to clean house and terminate everyone.

Because the IT department spent all of its time playing games, the network (fondly referred to as SKYNET) is in total disarray.

It is your job to secure the network and keep the business running.

Objective

Defend your network from the army of attackers Arnold has assembled. Keep the network running and perform any tasks assigned to you by management.

Competition Rules

- Each team will consist of (4) members and a mentor.
- Each team will designate a Team Captain (not the mentor) for the duration of the competition.
- The team captain is responsible for all communication between the team and the competition staff.
- Each team may have one mentor present at the competition, who will assist and advise at the request of the captain.
- Team members must perform all tasks; the mentor is not allowed to complete any task for the team.
- No electronic equipment is allowed in the competition rooms. This includes usb flash drives, laptops, cellphones, tablets, peripheral devices. Printed

material is allowed. Any violations will result in **disqualification of the team.**

- Teams may only work on the vms that are part of the competition network. DO NOT change any settings on the host machine or change the network infrastructure (cables and switch).
- All team members will wear badges identifying team affiliation at all times during competition hours.
- Each student team will start the competition with identically configured systems.
- A Red Team will attempt to infiltrate or disrupt each team's daily operations throughout the competition.
- Team members will not be allowed to communicate with the Red team members throughout the competition unless requested by the chief judge.
- Points will be awarded based on whether tasks (injects) were successfully completed and whether network services remained up.
- Points will be subtracted for successful compromises by the Red Team.
- Teams may earn back points by filing a complete incident report within 30 minutes of a compromise.
- Teams **may not** counterattack the red team. Any participant found to be doing this will **be dismissed from the camp** and the team disqualified.
- Teams must abide by all rules and directions issued by competition staff during the competition. Failure to do so will result in **dismissal from the camp.**

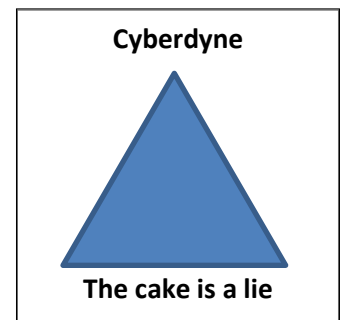
Network Description

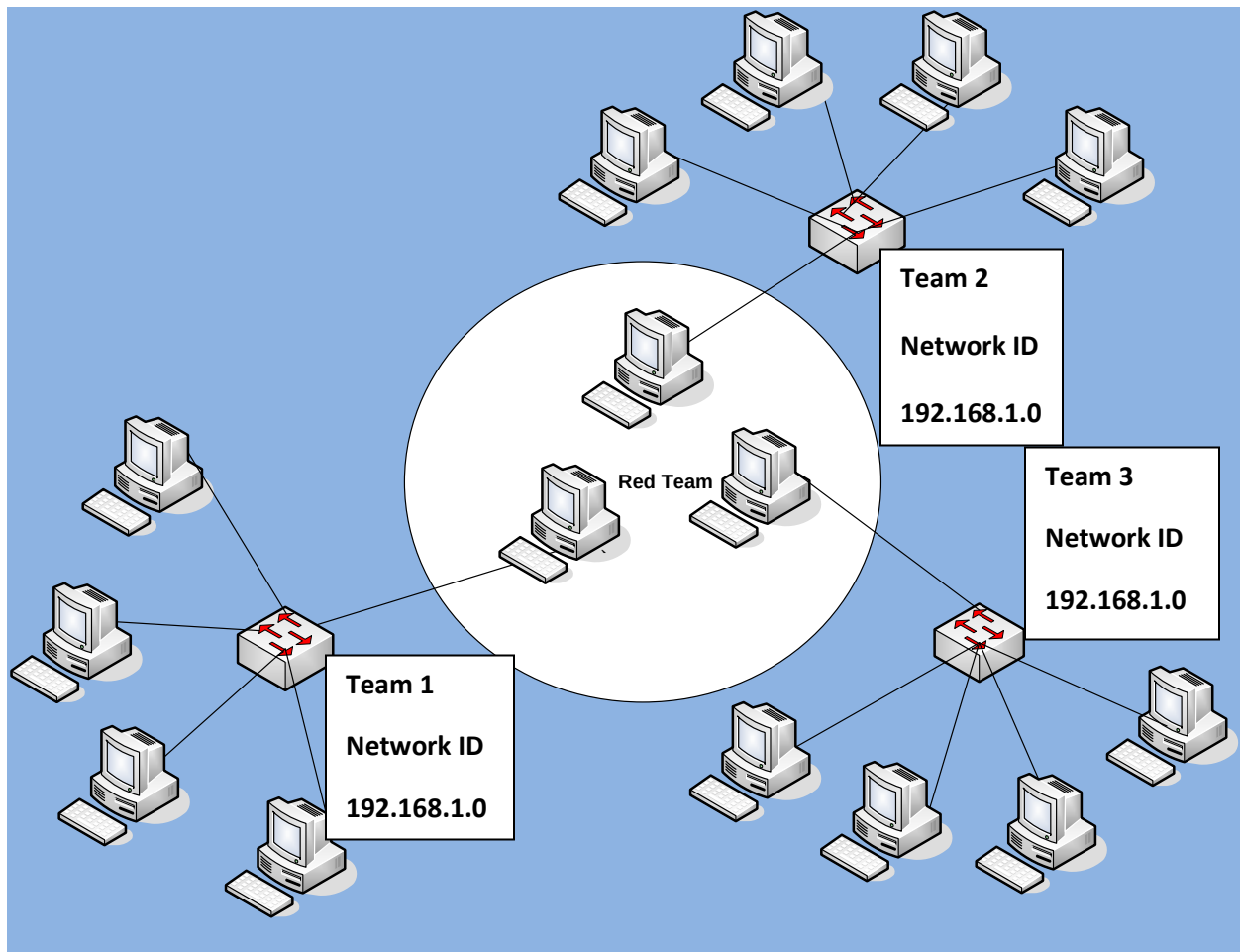
The competition network will be completely standalone with no external connectivity. Blue team members will have access to an internet machine to look up information. Scores will be based on periodic tests of services running and whether injects are completed in the time allowed.

Network Topology:

Team networks consist of:

- Windows 2008 Domain Controller
- Zencart
- Word Press
- Work station







Cyberdyne



The cake is a lie

From: IT Director (interim)

To: STAFF

CC:

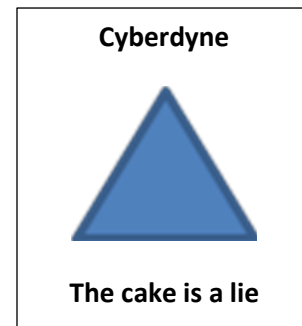
Subject: New IT Director

IT Staff,

Good news! A new IT Director has been hired. Her name is Sarah Conner and she needs an account with full administrator access. Please make sure you supply her with an account and initial password. You should be able to log in to the domain from the Windows XP machine. Get this done in the next 30 minutes.

Thanks,

IT Director (interim)



From: Sarah Conner

To: STAFF

CC:

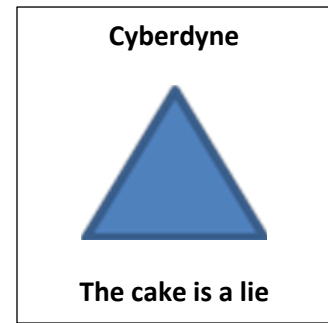
Subject:Recent change in IT Personnel

IT Staff,

As you know, we recently replaced all IT personnel and are in the process of changing procedures in the company. Please add yourselves as users in Active Directory. All users in your group should be able to log in to the domain from the Windows XP machine. You have 20 minutes to accomplish this task.

Thanks,

Sarah Conner



From: Sarah Conner

To: STAFF

CC:

Subject:T101 Division

IT Staff,

We need a new OU created for our T101 division. Please create an OU and name it T101. Add the following users:

Kyle Reese

Ed Traxler

Hal Vukovich

Linda Hamilton

Give these users an initial password of Password01

These users are in two groups: Engineering and Esthetics.

Please create these groups and add Hal and Linda to the Engineering group and Kyle and Ed to the Esthetics group. Please prevent the Esthetics users from having access to the control panel. This needs to be done within the next 30 minutes.

Thanks,

Sarah Conner



Cyberdyne



The cake is a lie

From: Sarah Conner

To: STAFF

CC:

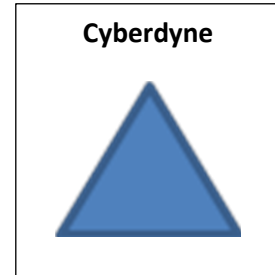
Subject: Wordpress

IT Staff,

Please customize the wordpress site to more accurately reflect the nature of our business. At a minimum we need another theme, the name of our business on the site, and an updated front page blog. Please get this done in the next 20 minutes.

Thanks,

Sarah Conner



From: Sarah Conner
To: STAFF
CC:
Subject: Zencart

IT Staff,

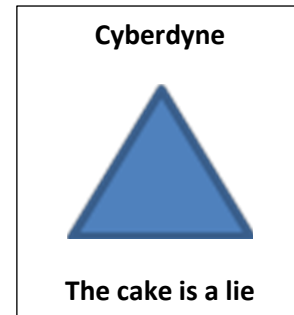
The Zencart front page is appalling! We need to update this with the products we sell. Please edit the Zencart page to list the following items and descriptions:

ITEM	DESCRIPTION
Hydraulic press	Super crushing ability!
Mototerminators	Great for high speed chases!
Hydrobot	Swarming Bot for all your aquatic needs!
T-1000	Vast improvement over the T-800! All new parts! Improved memory!!

Also please make sure the Cyberdyne name is prominently displayed on the front. Please have this done in 25 minutes.

Thanks,

Sarah Conner



From: Sarah Conner

To: STAFF

CC:

Subject: Presentation to Management

IT Staff,

Management at Cyberdyne does not seem to understand how this network works. Please prepare a short presentation explaining what wordpress, zencart, and windows 2008 are and the role they play in our company. Your presentation should be about 3 minutes long. Please select someone from your group to do the presentation to our top management.

Thanks,

Sarah Conner



Cyberdyne



The cake is a lie

From: Sarah Conner

To: STAFF

CC:

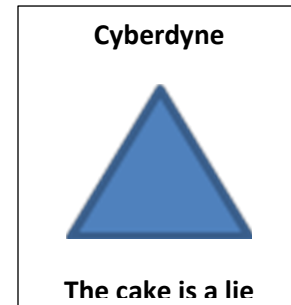
Subject: Security Audit

IT Staff,

As you know, there were issues with our previous IT Staff. I am concerned about the security of our network. Please perform a security audit and identify all open ports running and identify any suspicious connections on the network. I have heard that netstat works well for this. We need to know about all machines on the network. You have 15 minutes to complete this task.

Thanks,

Sarah Conner



From: Sarah Conner

To: STAFF

CC:

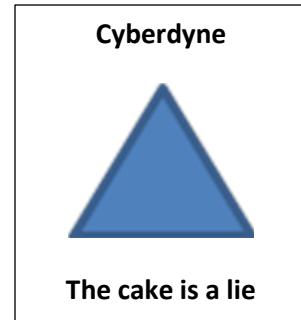
Subject: Internet Access

IT Staff,

I have been monitoring network usage and it looks like the engineering staff is wasting a lot of time on the internet instead of work. This explains the delay in production for our new T-1001 model. Please create a gpo that prevents the engineers from accessing the internet. You have 10 minutes to complete this.

Thanks,

Sarah Conner



From: Sarah Conner

To: STAFF

CC:

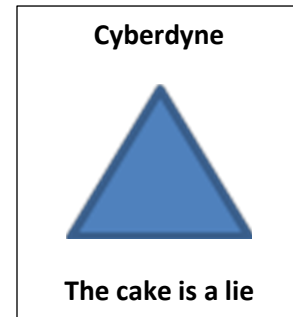
Subject: Network Map

IT Staff,

I am having a hard time visualizing how everything is connected on our network. Please provide me with a network map, with the ip addresses, operating systems, and services clearly labeled for each machine. Please show how these machines are connected (what are they plugged into and what are the port numbers). You have 15 minutes to complete this.

Thanks,

Sarah Conner



From: Sarah Conner

To: STAFF

CC:

Subject: Incident Report

IT Staff,

As you know, our previous IT Director (Arnold) was very disgruntled when he was dismissed from Cyberdyne. I'm afraid he might try something. Please make sure nothing unusual is running on the network. Also, please be prepared to file an incident report if anything should happen. This must be filed within 30 minutes of an incident occurring. The report should include:

What happened?

How did they get in?

What measures need to be taken to prevent this from happening again?

Thanks,

Sarah Conner

Partial support for this work was provided by the National Science Foundation's Advanced Technological Education (ATE) program under Award No. 1104192. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

