Cyber Storm

PREPARE TO BE

Hacked

DEFEND ATTACK ADAPT

CYBERSTORM IS AN ANNUAL DAY-LONG CYBER SECURITY COMPETITION THAT PITS TEAMS OF STUDENTS AGAINST ONE ANOTHER IN A FIERCE CYBER BATTLE. THE TEAM WITH THE BEST NETWORK DEFENSE AND ATTACK STATEGIES WINS. WANT TO PARTICIPATE? CONTACT JGOURD@LATECH.EDU.

MAY 16, 2014

LOCATION: TECH STUDENT CENTER (Tonk)

COLLEGE OF ENGINEERING AND SCIENCE
LOUISIANA TECH UNIVERSITY

2014 Cyber Storm

Note: This document may be amended/changed at any time.

Cyber Storm is a "hacking" competition (or hackfest) that pits several teams against each other in a fierce battle to the death! Well, not really, but you get the general idea. The teams are split from Introduction to Cyber Security (CSC442) and Computer Network Security (CYEN301), and are denoted by unique colors (e.g., `Red`, `Blue`, etc). The "administrative" team (me and a few other carefully selected students) will comprise `White`. I should probably mention that this event serves as the final examination for the class. And, no, losing the competition doesn't mean failing the course. At least not in odd numbered years...

The teams will be provided with hardware and some know-how (a large part of succeeding in Cyber Storm is a desire to learn and explore on your own). This document outlines a set of requirements, goals and rules that, in part, define the competition to be held on Friday, May 16, 2014 from 9am-5pm (although you will need to set aside from 7am-7pm), in The Tonk.

In general, each team is to defend its network. But what would such a stupendous event be without the opportunity to attack! Therefore, teams are also permitted to attempt to infiltrate, compromise, disrupt, and generally take down their opponents' networks. Of course, all teams are to leave `White` alone (we'll discuss exactly what this means later) under penalty of death. Or maybe just losing 100% of your points at the time of the infraction in addition to failing the course.

You will need permission from `White` to carry out any exploit that may *irreversibly* take down an opponent's system. For example, you may not format an opponent's hard drive should you have access and the capability to do so until `White` has given the OK. However, no permission is required to take over a system. In other words, if it's something destructive, ask. And if in doubt, you might also want to ask first.

In order to "own" a server, you will need to identify your team name in some manner on the server. For HTTP, that means a connection to the HTTP server returns a web page with your team name proudly displayed somewhere. For SSH, that means a connection to the SSH daemon displays a MOTD (message of the day) with your team name somewhere in it. For FTP, that means a connection to the FTP server displays a login message with your team name somewhere in it. For MySQL, that means a connection to the MySQL server and executing the command `SHOW DATABASES;` lists a database with your team name.

A word about usernames and passwords. You will be provided a portal to specify usernames and password for all servers and services. This will create a configuration for `White` to use. It can be updated at any time throughout the competition, so you are permitted to change passwords as you see fit throughout the day.

Gryffindor

Network

Subnet:	10.1.0.0/16
Netmask:	255.255.0.0
Gateway:	10.1.0.1
Network:	10.1.0.0
Broadcast Address:	10.1.255.255
Switch:	10.1.0.2

Machines

Slackware 14.1:	10.1.192.133
FreeBSD 10.0-RELEASE:	10.1.66.66
Arch Linux 2014.04.01:	10.1.1.1

Services

FTP:	Port 21
SSH:	Port 22
HTTP:	Port 80
MySQL:	Port 3306

Hufflepuff

Network

Subnet:	10.2.0.0/16
Netmask:	255.255.0.0
Gateway:	10.2.0.1
Network:	10.2.0.0
Broadcast Address:	10.2.255.255
Switch:	10.2.0.2

Machines

Slackware 14.1:	10.2.192.133
FreeBSD 10.0-RELEASE:	10.2.66.66
Arch Linux 2014.04.01:	10.2.2.2

Services

FTP:	Port 21
SSH:	Port 22
HTTP:	Port 80
MySQL:	Port 3306

Ravenclaw

Network

Subnet:	10.3.0.0/16
Netmask:	255.255.0.0
Gateway:	10.3.0.1
Network:	10.3.0.0
Broadcast Address:	10.3.255.255
Switch:	10.3.0.2

Machines

Slackware 14.1:	10.3.192.133
FreeBSD 10.0-RELEASE:	10.3.66.66
Arch Linux 2014.04.01:	10.3.3.3

Services

FTP:	Port 21
SSH:	Port 22
HTTP:	Port 80
MySQL:	Port 3306

Slytherin

Network

Subnet:	10.4.0.0/16
Netmask:	255.255.0.0
Gateway:	10.4.0.1
Network:	10.4.0.0
Broadcast Address:	10.4.255.255
Switch:	10.4.0.2

Machines

Slackware 14.1:	10.4.192.133
FreeBSD 10.0-RELEASE:	10.4.66.66
Arch Linux 2014.04.01:	10.4.4.4

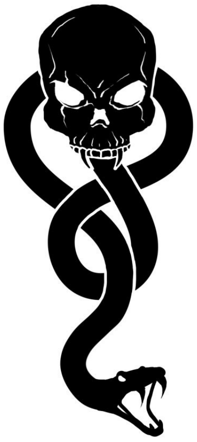
Services

FTP:	Port 21
SSH:	Port 22
HTTP:	Port 80
MySQL:	Port 3306

The Death Eaters

Network

Subnet:	10.5.0.0/16
Netmask:	255.255.0.0
Gateway:	10.5.0.1
Network:	10.5.0.0
Broadcast Address:	10.5.255.255
Switch:	10.5.0.2



Services

None

The Dementors

Network

Subnet:	10.6.0.0/16
Netmask:	255.255.0.0
Gateway:	10.6.0.1
Network:	10.6.0.0
Broadcast Address:	10.6.255.255
Switch:	10.6.0.2

Services

None

The Ministry of Magic

Network

Subnet:	`10.0.0.0/16`
Netmask:	`255.255.0.0`
Gateway:	`10.0.0.1`
Network:	`10.0.0.0`
Broadcast Address:	`10.0.255.255`

Services

Access Portal:	`https://10.x.0.1:1337/access/access.php`
Scores:	`https://10.x.0.1:1337/scores/scores.php`

Notes:

1. Add “`UseDNS no`” (without the quotes) to your `sshd_config` for all VMs;
2. No DOS or DDOS;
3. No ARP spoofing or spoofing any other team (i.e., stay within your IP subnet);
4. Don’t go after switches (`White` is using them to deliver situational awareness);
5. No destructive attacks unless you obtain permission from `White` first;
6. No simultaneous connections to the Cyber Storm network and any production network (e.g., LaTech OpenAir, etc); **unplug from the Cyber Storm network before going on the Internet!**;
7. Wireless networks within the Cyber Storm network will all relate to Harry Potter;
8. No attacking `White` on `10.0.0.0/16` or the `Muggles` on `10.8.0.0/16`; and
9. Remember that the point of Cyber Storm is **not** to try to find weaknesses in the competition itself and exploit those!