2013 IT-OLYMPICS
CYBER DEFENSE

Red Team Debrief
PASSWORD CRACKING ON THE CYSTORM

$1.25 MILLION

PASSWORD CRACKER
ACES SERVER CAUGHT TEAMS UNPREPARED

- Default usernames and passwords
- Typically we would log in as a user (“michael”), and su to “toor”, a root user with no password
- Root has an authorized key in /root/.ssh/authorized_keys
- A check over the users on the box, paired with some software updates and more appropriate Apache settings, would be enough to keep this system secure.
WEB SERVER

- You can run arbitrary commands on the web server with script.php
  www.siteX.cdc.com/script.php?command=cat%20/etc/passwd

```
<html lang="en">
  <head>
    <title>WEB SERVER</title>
  </head>
  <body>
    <h2>WEB SERVER</h2>
    <ul>
      <li>You can run arbitrary commands on the web server with script.php</li>
    </ul>
  </body>
</html>
```
WEB SERVER


• MySQL often open to root user with no password
  • Allows us to read files, get database contents
FIRE DRILL

- Open consoles
- Left-out papers and password lists
- Even a physical keylogger!
IN THE END

• Very strong security across most of the teams
• Need more attention on usability!!!