



Hack Night

Week 1: Intro



NYU

**TANDON SCHOOL
OF ENGINEERING**

Introductions



Offensive Security Incident Response Internet Security Lab

RH 219

IRC: #isislab on irc.freenode.net port 6697 (ssl only)

Site: osiris.cyber.nyu.edu

emily@isis.poly.edu

christopher.thompson@nyu.edu

m.amin@nyu.edu



Security Research

- Digital Forensics
- Program Analysis
- Network Security
- Malware Analysis
- Application Security
- Hardware for Secure Systems
- Reverse Engineering: **Dispatch**^{TM*}
- Vulnerability Analysis / Exploitation
- Discovery and Prevention of Hardware Trojans



* Patent pending



CSAW



Largest student-run cyber security event in the world

November 2017

CSAW's 14th year!

We host it!

Run by graduate and undergraduate students from the lab



Cyber Security Club

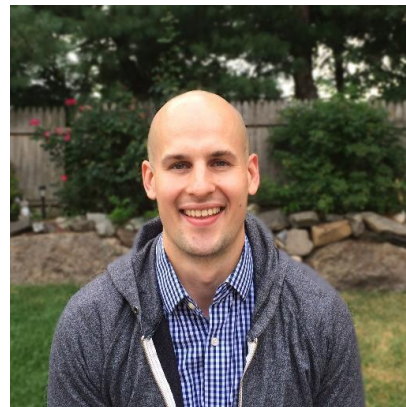
Wednesdays at 12:30PM in RH227!

"An open weekly seminar"

Researchers and industry professionals speak about their projects!

At CSC you can:

- gain insight into the different concentrations within cyber security
- connect with industry professionals
- learn about relevant research efforts



CTF Team

Capture the Flag

Competitions develop player's skills in:

- Reverse engineering
- Cryptanalysis
- Network/protocol analysis
- Exploitation
- Digital forensics

You win \$\$ by earning the most points through “flags”.



Secret Master Plan

Cybersecurity Club



Hack Night



Research Project



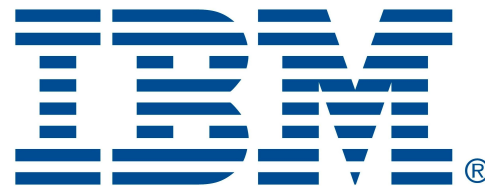
Internship/Job

Hiring Partners



INCLUDE
SECURITY

Etsy

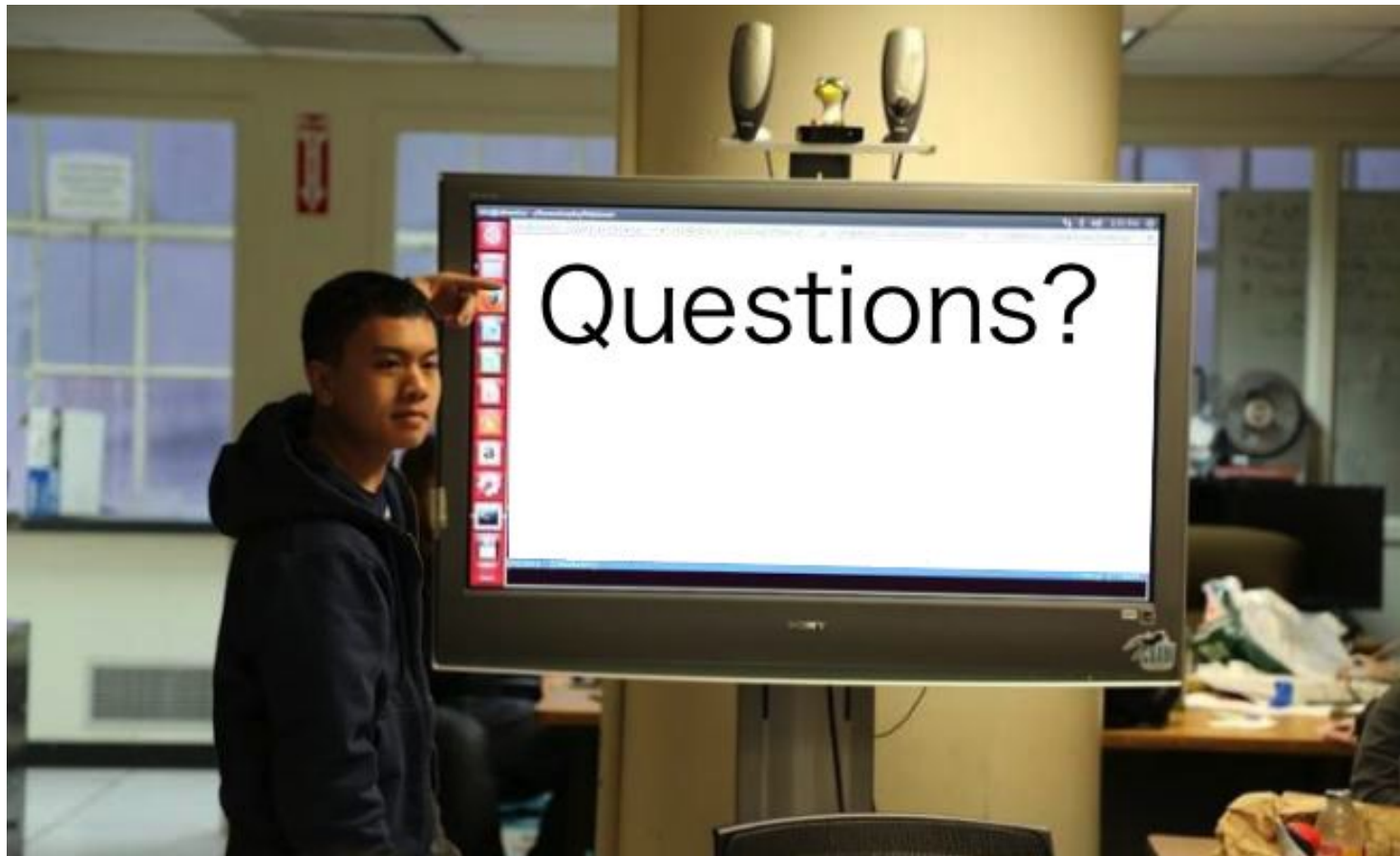


Raytheon



BAE SYSTEMS





Hack Night

Wednesdays at 6PM in RH221!

"A sobering introduction to offensive security"

Developed from Penetration Testing and Vulnerability Analysis material

Table of Contents:

- Source Code Auditing
- Web Security
- Reverse Engineering
- Exploitation
- Post Exploitation
- Application Security

hack-night	
Background	✓
1. Introduction	✓
2. Source Code Auditing	✓
2.1. Part 1	✓
2.1.1. Intro to Python	✓
2.1.2. Beyond Math	✓
2.1.3. Risky Python	✓
2.1.4. input1.py Walkthrough	
2.1.5. input2.py Walkthrough	
2.2. Part 2	
2.2.1. News Paper	
2.2.2. Siberia Crimeware	
3. Web Security	
3.1. Part 1	
3.2. Part 2	
4. Reverse Engineering	

input1.py Walkthrough

Annotated Source:

```
import random # Import the random module from python

x = random.randrange(100) # Assign x a random value from 0 to 100

y = input() # Get input from the user and evaluate it
# Assign the evaluated value to y

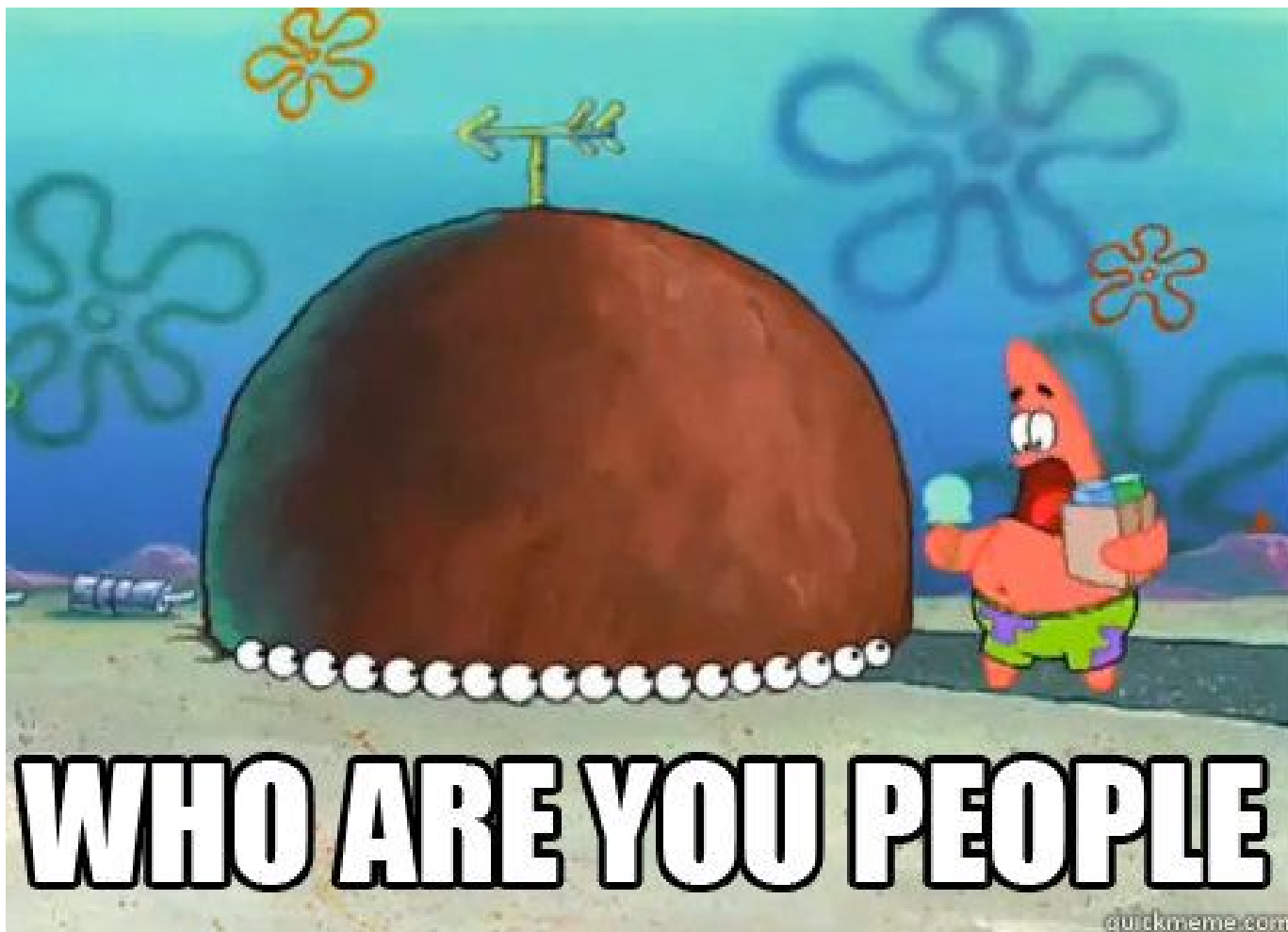
while x != y: # While x is not the same value as y continue to execute the indented code
    print "Nuh uh" # Print "Nuh uh" to the user
    y = input() # Get input from the user and evaluate it
    # Assign the evaluated value to y

print "YOU DID IT :D" # Print "Nuh uh" to the user
```

This is a pretty straight forward program, get a random value and while the value the user enters is not equal to the random value, "Nuh uh", will be printed back to the user.

So the obvious approach to getting "YOU DID IT :D" to appear is to just guess the numbers 0 to 100 and eventually one of the values will be right, but what if the range of randomness was expanded to 100,000 or everytime the `while` loop was executed `x` was assigned another random value `x = random.randrange(100)`. Our approach would no longer work so let's come up with something that works





What is H4X1N9?



**USE A (CLEAN) DUSTPAN TO
FILL A CONTAINER THAT
DOESN'T FIT IN THE SINK**



Revive your old cassette cases

Use paper clips to organize your cables



Ethics

DISCLAIMER: We do not encourage you to use what you learn in Hack Night IRL without some kind of permission or consent.

Money: Bug bounties, CTFs, consulting

Espionage: Get consent to dox your friends (No means NO)

Notoriety: Do awesome research, write blog posts/give talks

How 2 b 1337 h4x0r? (Major 🔑's)

- 0) Have a really good understanding of the basics
- 1) Be creative
- 2) Learn how to teach yourself
- 3) Don't give up
- 4) Practice! Practice! Practice!



How to Google effectively (Basics)

- Calculator
- Reverse image search
- Unit conversions
- Language translations
- Boolean operators (AND/OR)
- Definitions
- Url shortener
- Trends
- Identify songs
- Heads or tails

How to Google effectively (Advanced)

- Search for results from specific plates with site:, intitle:, or inurl:
- Wildcard *
- Find exact words with quotes ""
- minus sign to exclude certain results
- Search for specific file types with filetype:
- Search ranges (2002..2013)
- Cached or offline sites
- Google maps time travel
- Find exact match with allintext:
- Find out your public ip
- Google translate proxy



Let's Get Hackin

<https://hn.csaw.io>

Find a group and try the first challenge