OSIRIS

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™***
- Vulnerability Analysis / Exploitation
- Discovery and Prevention of Hardware Trojans

* Patent pending

CSAW

Largest student-run cyber security event in the world
- November 20176
- 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

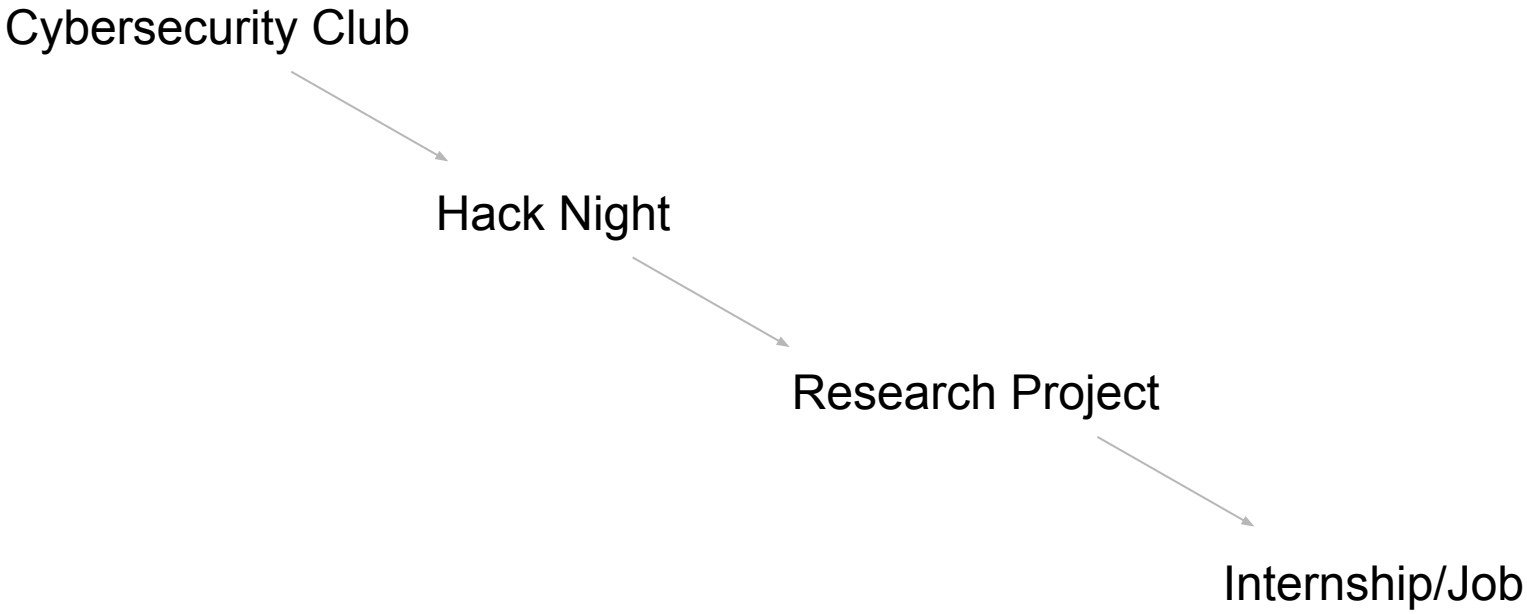
Capture the Flag

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



Hiring Partners


Questions?

Hack Night

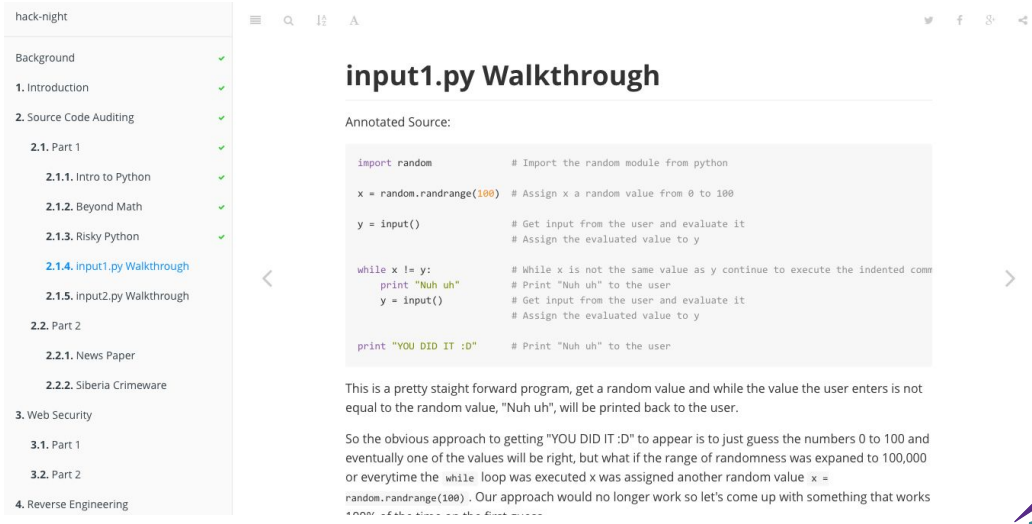
Wednesdays at 6PM in RH221!

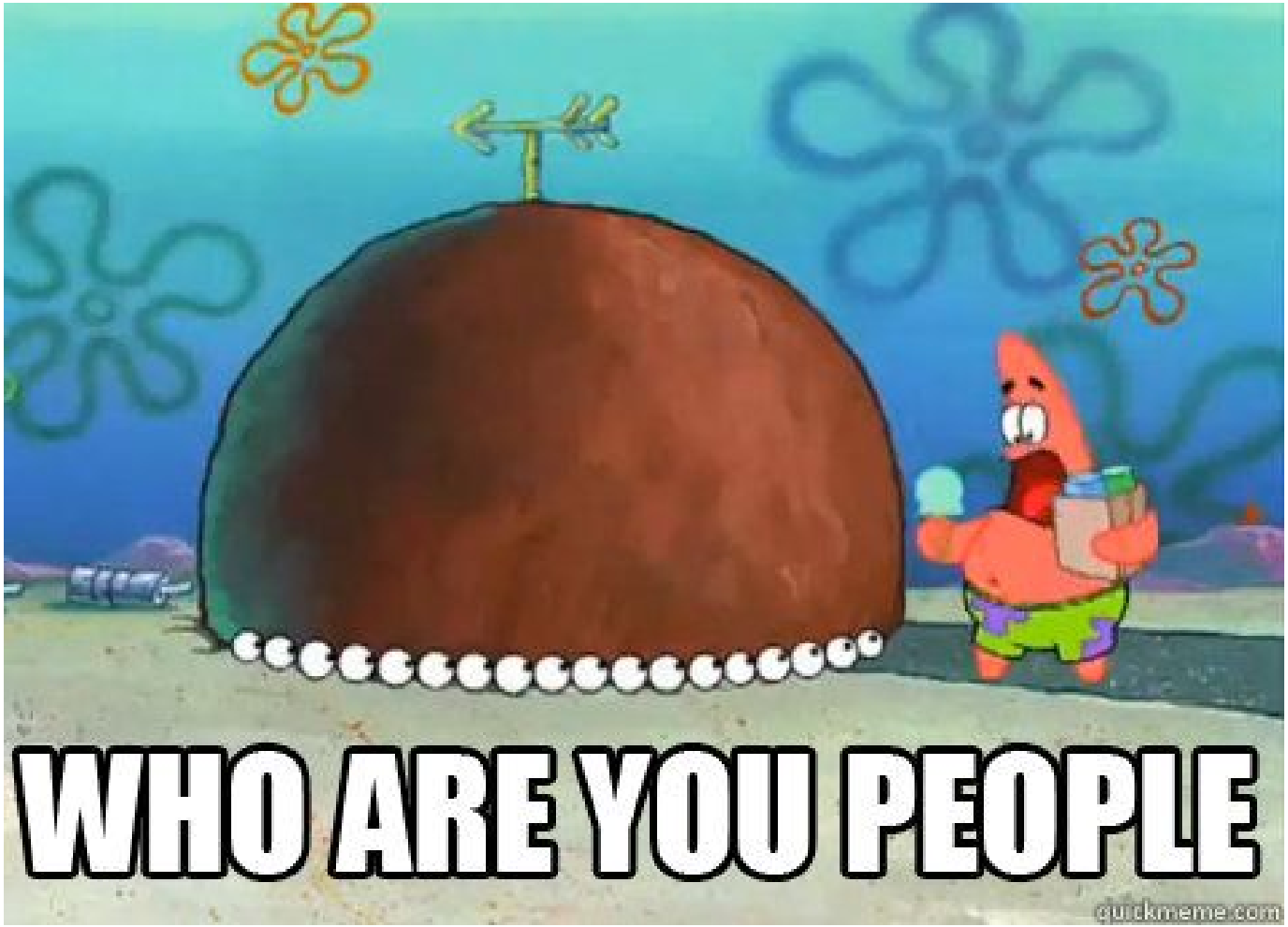
“A sobering introduction to offensive security”

Developed from Penetration Testing and Vulnerability Analysis material

Table of Contents:

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




WHO ARE YOU PEOPLE
quickmeme.com

What is H4X1N9?

Ethics

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

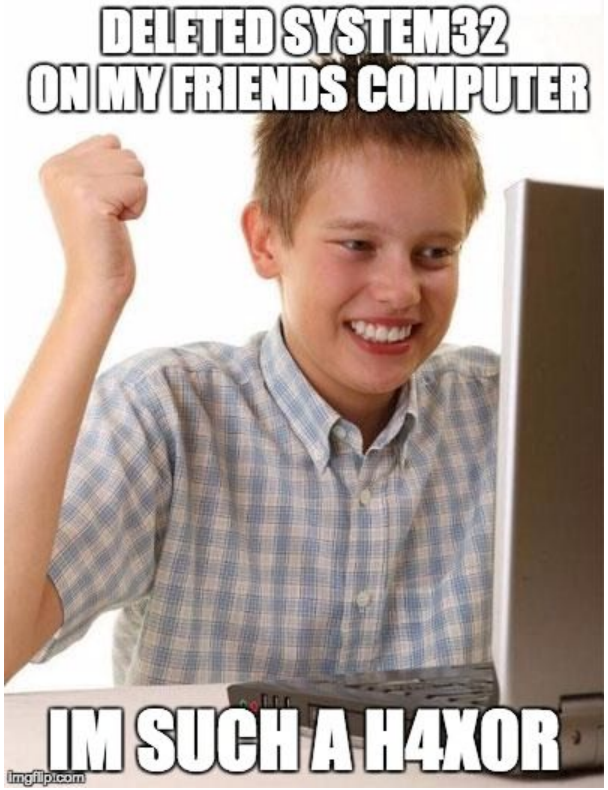
Money: Bug bounties, CTFs, consulting

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


Questions?
SONY

Let's Get Hackin

https://hn.csaw.io

Find a group and try the first challenge