BISHOP FOX®

So You Want to be a Hacker?

WHITEHAT GROUP

CAL POLY
SAN LUIS OBISPO

November 10, 2014

whoami

THE PRESENTERS

Bishop Fox

- Vinnie Liu
  Partner

- Joe DeMesy
  Security Associate

- Jasmeen Broome
  Recruiter – University Outreach

whoami

THE PRESENTERS

Bishop Fox

- Vinnie Liu
  Partner
- Joe DeMesy
  Security Associate
- Jasmeen Broome
  Recruiter – University Outreach

whoami

THE PRESENTERS

Bishop Fox

- Vinnie Liu
  Partner

- Joe DeMesy
  Security Associate

- Jasmeen Broome
  Recruiter – University Outreach

SO YOU WANT TO BE A HACKER?

A STEP BY STEP GUIDE

Hackers

FINAL FORM

Step #1

SKI MASK SELECTION

Step #2

IRC & LEET SPEAK

Hackers IRL

LOOK LIKE NORMAL WEIRDOS

Hacker Skill Levels

KNOWLEDGE OF THE FORCE

Novice

Advanced

Apprentice

Expert

Master

The Novice

SECURITY INDUSTRY PROFESSIONAL

70%

The Novice

SECURITY INDUSTRY PROFESSIONAL

- **Tools** – Reliant
  - Knows enough to run a tool or script
- **Programming** – None
  - No experience with programming or computer science
- **Methodology** – Checklists
  - Generated reports

The Advanced

SECURITY INDUSTRY PROFESSIONAL

15%

The Advanced

SECURITY INDUSTRY PROFESSIONAL

- **Tools** – Effective
  - Targeted use of various tools
- **Programming** – Basic
  - Familiarity with a one or two languages
  - No personal research
- **Methodology** – Exploratory
  - Basic Exploits

The Apprentice

HACKER

10%

The Apprentice

HACKER

- **Few Years Experience**
  - Always learning more
- **Tools** – Effective
  - Target use of various tools
  - Understands limitations
- **Programming** – Proficient
  - Knowledge of CS or EE
  - Almost full stack knowledge
  - Various languages
  - Spends personal time hacking
- **Methodology** – Exploratory
  - Basic Exploit Chains

The Expert

HACKER

5%

The Expert

HACKER

- **Decade+ of Experience**
  - Leverages past experiences
- **Tools** – Effective
  - Understands limitations
- **Programming** – Expert
  - Full stack knowledge
  - CS and/or EE
  - Pickup up new platforms quickly
- **Methodology** – Attack Avenues
  - Exploit Chains
  - Attack visualization

The Master

HACKER

1% >

The Master

HACKER

- These are Born
- Tools – Effective
  - Never limited by them
- Programming – Savant
  - Expert programmers
- Methodology –

No art, however minor, demands less than total dedication if you want to excel in it.

— Leon Battista Alberti

What Makes a Good Hacker?

KNOWLEDGE OF THE FORCE

UNDERSTAND THE SYSTEM

DOWN THE RABBIT HOLE

Fun Times with PHP

REAL WORLD EXAMPLE

```php
<?php

$correct_password = "aSKJDkjawierui342!@3";

if (strcmp($correct_password, $_GET["pass"]) ) {

        … is authorized …

} else {

        … not authorized …
}
```

More Fun Times with PHP

REAL WORLD EXAMPLE

```
<?php

$correct_password = "aSKJDkjawierui342!@3";

if (strcmp($correct_password, $_GET["pass"]) == 0 ) {

        … is authorized …

} else {

        … not authorized …
}
```

PHP’s strcmp

PHP YOU SO SILLY

WAT

Memory Management Fun

REAL WORLD EXAMPLE

```
const int bufferSize = 64;

int length = int(elem.end - elem.start);
if (length <= bufferSize)
{
    char buffer[bufferSize + 1];
    memcpy(buffer, elem.start, length);
    buffer[length] = ‘\0’;
```

Two’s Compliment

SIGNED INTEGER STORAGE

Flip the bits and add one, so representing -2:

0000 0010
1111 1101 +*1*
1111 1110

8 Bit Number	Unsigned Value	Two’s Complement Value
0111 1111	127	127
0000 0000	0	0
1111 1111	255	-1
1111 1110	254	-2
1111 1101	253	-3

Memory Management Fun

REAL WORLD EXAMPLE

```
const int bufferSize = 64;

int length = int(elem.end - elem.start);
if (length <= bufferSize)
{
    char buffer[bufferSize + 1];
    memcpy(buffer, elem.start, length);
    buffer[length] = ‘\0’;
```

Memory Management Fun

REAL WORLD EXAMPLE

```
void* memcpy(void *dst0, const void *src0, size_t length)
```

```
const int bufferSize = 32;

int length = int(elem.end - elem.start);
if (length <= bufferSize)
{
    char buffer[bufferSize + 1];
    memcpy(buffer, elem.start, length);
    buffer[length] = ‘\0’;
```

EXPLOITATION CHAINS

FORCE MULTIPLIERS

Exploit Chains

MAXIMUM IMPACT

Exploit Chains

BY EXAMPLE

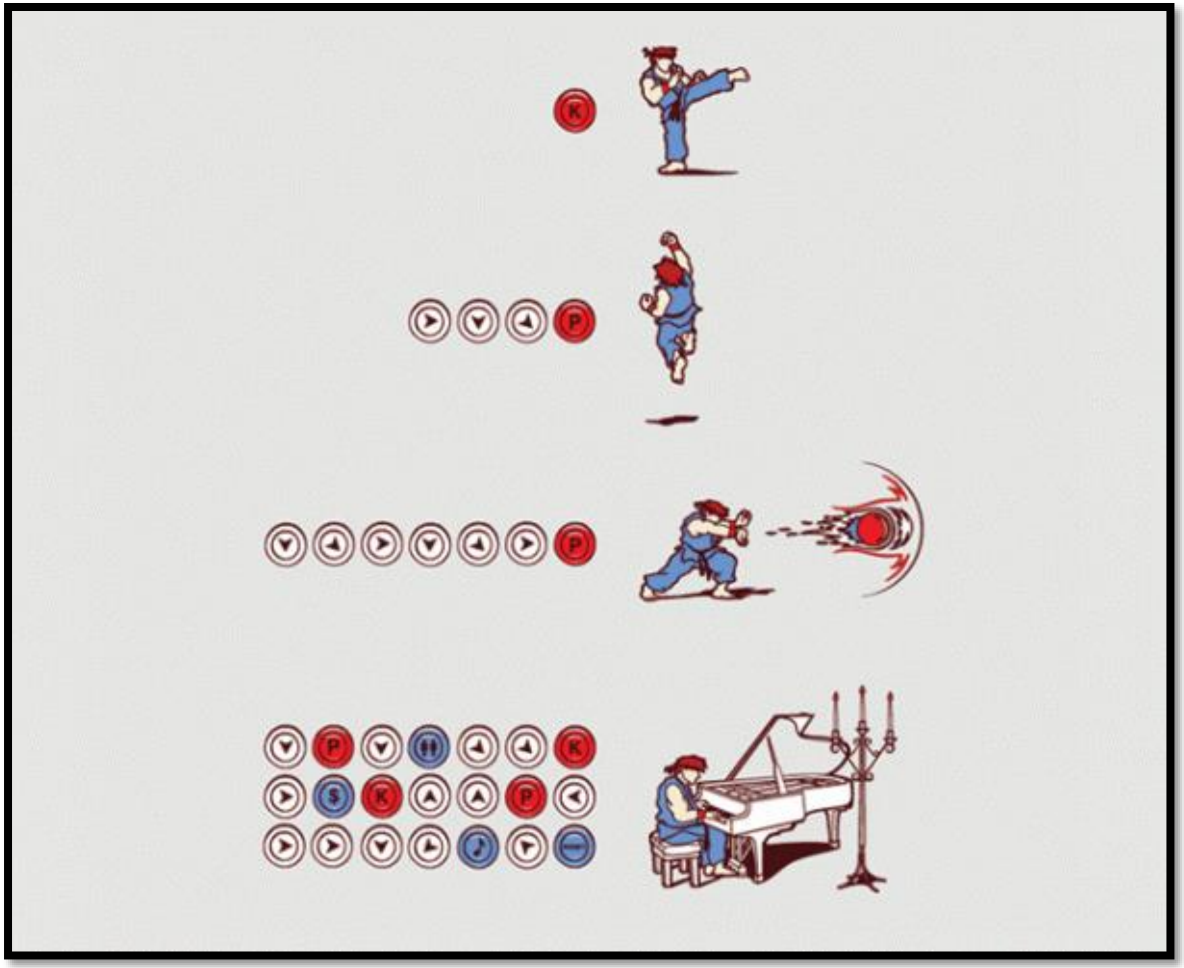
```
<?php

if (isAutenticated())
{
  $dbpass = $_GET['dbpass'];
  if (isset($_GET['dbname']))
  {
    $output = shell_exec("./dbtest.sh $dbname $dbpass 1");
    echo "<pre>$output</pre>";
  }
}

?>
```

Exploit Chains

CCCCOOOOOMMMMBBBOOOO



LEVEL UP

HACKING EXPERIENCE

Leveling Up

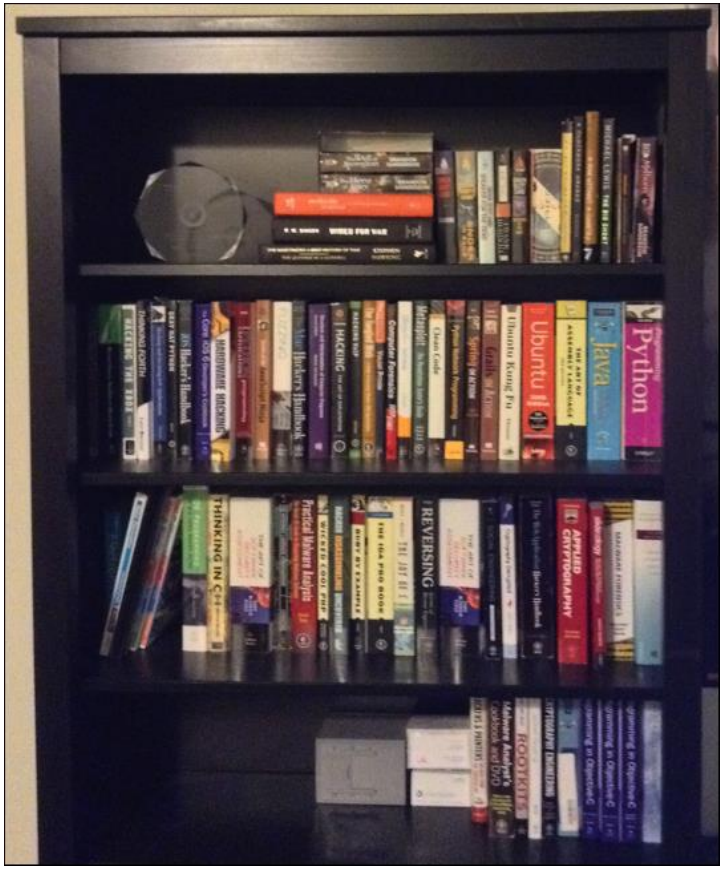
KNOWLEDGE OF THE FORCE

Book Learn You Good

BOOKS CAN ONLY GET YOU SO FAR

Favorite Books

- The Tangled Web
- Web Application Hacker's Handbook 2nd Ed.
- Cryptography Engineering
- Hacking the Xbox: An Introduction to Reverse Engineering *(Free!)*
- Hacking and Securing iOS Applications
- The Art of Software Security Assessment



Practice Every Day

10,000+ HOURS

Find a Mentor

LEARN FROM AN EXPERT OR MASTER

Team Work

PUSH EACH OTHER FURTHER

Capture the Flag

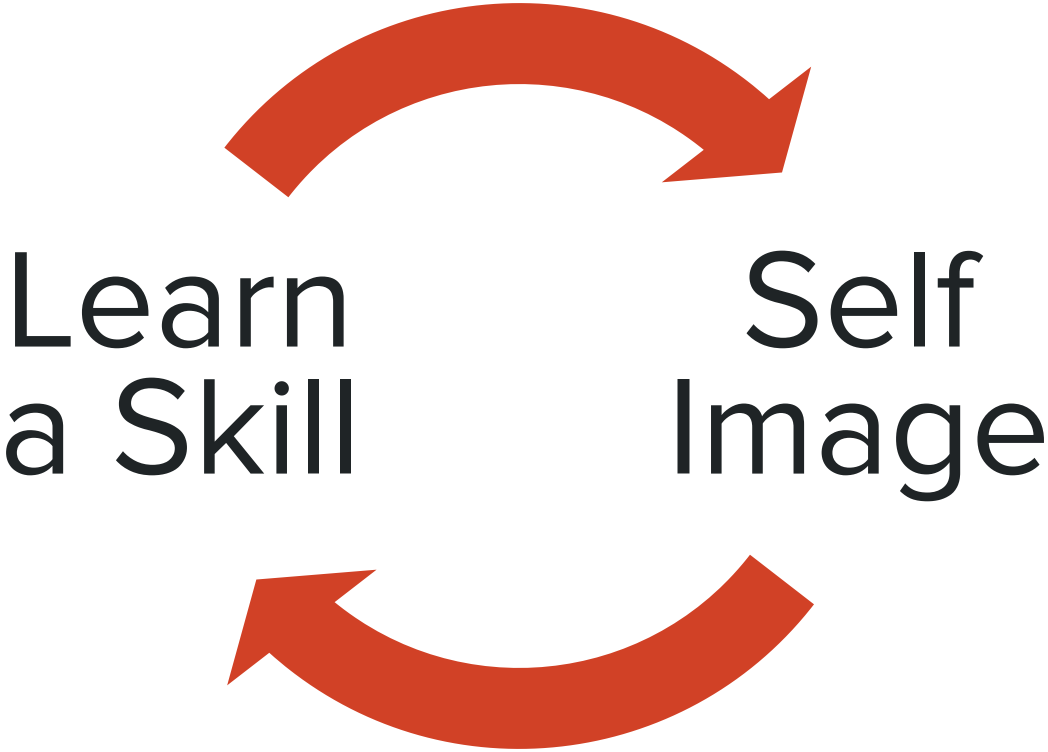
ROOT THE BOX ;-)

CTFs

- Root The Box
- CCDC
- Smash The Stack (online)
- CSAW
- Etc.

The Learning Cycle

HACKING YOUR BRAIN



Learn a Skill

Self Image

We’re Hiring!

@BISHOPFOX

FACEBOOK.COM/BISHOPFOXCONSULTING

LINKEDIN.COM/COMPANY/BISHOP-FOX

GOOGLE.COM/+BISHOPFOX

Thank you

CAL POLY

SAN LUIS OBISPO

BISHOP FOX®