Lessons from Training Ninjas

W. Owen Redwood - redwood@cs.fsu.edu
Prof. Xiuwen Liu - liux@cs.fsu.edu
Florida State University
Or:
How to revamp your security curriculum
Before we start

● The purpose of this talk is to provide others with wisdom/insight/tricks/resources to teach their own
  ○ Appsec Course
  ○ Pentesting Course
  ○ Incident Response Course

● Target Audience:
  ○ Educators / Professors / Instructors
  ○ Graduate Students
    ■ Cyber Security Club Leaders?
  ○ Professionals who want more skilled graduates
  ○ Anyone who wants to learn security more efficiently
#whoami

W. Owen Redwood

- Vulnerability Researcher
- PhD Student at FSU - Research area: Counterintelligence tools and stuff
- Director of SAIT Research Lab
- Founded N0L3ptr CTF team
- Sandia Internship
  - Briefed Obama’s Chief Science Advisor
  - Invited member of Sandia Summer Institute (like a think tank) 2012
- Cyber 9/12 student challenge “Most Creative” award
  - How I met one of the BSIDES DC organizers
- Created from scratch and taught Offensive Security at the graduate level:
  - [http://offsec.noleptr.com](http://offsec.noleptr.com)

- LOTS of experience as a student...
Why You Should Listen

Student Feedback:

- “Thank you for a great semester and possibly the most interesting/helpful class I have ever enrolled in”
- “I want to also take this time to say that this class was awesome! I learned more in this class than in any class and that I used skilled in this class to help me with some other classes. This class should be mandatory for all Comp. Crim majors. Thanks for a ridiculously challenging and awesome learning experience!”
- “Very applied/hands on. Tests/Homework correlated very with with actual skills (felt useful)”
- “Cutting edge and state-of-the-art content. Well organized and greatly informative”
- “Excellent skeleton for the type of course the NSA would love.”

Top or /r/netsec, all over other forums, and tons of community support
Why a new class?

- Generic security classes at most major universities usually...
  - A survey of topics and degrade from neglect
  - Focus heavily on crypto
  - Produce students who usually can't "do" security

  ■ Thats why we have all these certs + training programs
Related Work

Dan Guido, 2009 - "So You Want To Train An Army Of Ninjas"  [http://www.youtube.com/watch?v=-MNpNrARTFU]

- Application Security and Vulnerability Analysis [http://pentest.cryptocity.net/]
CIS-5930 "Offensive Security"

http://offsec.noleptr.com

DISCLAIMER: No affiliation with http://www.offensive-security.com/

A hands-on, in-depth survey of:

- Process Memory layout (Stack, Heap, .text)
- Reverse Engineering (x86)
- Exploit Development / Mitigation
  - How to write shellcode, ret2libc, ROP
  - Stack Cookies NX/DEP, ASLR, SafeSEH, SEHOP
- Network Hacking, Web Application Hacking
  - SQLi, XSS, SSL, ...
- Metasploit, Meterpreter, Volatility, IDA, Wireshark ...
- "Cyber warfare", lockpicking, physical security

In summary:
- Teaches security SKILLS from a red-team heavy perspective
NINJAS

I trained some (with help)
The Help (many thanks!)

Mitch Adair

Professor Xiuwen Liu

Joshua Lawrence

And many others for moral and mental support...
Results

- Mockdroid port to latest Android kernel
- Security Context--sensitive File--system for Android (Extension of FUSE)
- Volatility plugins to export PE's better to IDA
- Post Exploitation Forensic tool(s) / Meterpreter script(s)
- Vulnerability analysis on PHPBB
- PDF fuzzers
- ASLR randomness analysis
- custom x86 Payload encoder
- ...
Challenges

● Create a brand new class from scratch
● Getting support from faculty
  ○ NSA CoE - Cyber Ops, InfoSec, Research ...
  ○ NSF Grant Money
  ○ SFS / CyberCorps
● Organizing the topics
  ○ Picking textbook(s)
● Bridging the knowledge gaps
  ○ Producing students who can do pen testing
  ○ Most software development courses don't touch security
  ○ Many security classes may be copies of each other...
The knowledge gap
Outline of this Talk

● Soul Searching
  ○ 8 key aspects to guide success

● HOWTO
  ○ Sensei
  ○ Setup
  ○ Tactics
  ○ Strategy
  ○ The Campaign
    ■ Organization
    ■ Assignments
    ■ Grading
Planning (soul searching)

1) How many core areas do you want to cover?
   - Stick to the book(s)? Go your own way???
   - Crypto?
   - Reversing?
   - Code Auditing?
   - Exploit Development?
   - Malware Analysis?
   - Network Analysis?
   - Web App?

2) What advanced topics do you want to reach?
   - ROP?
   - Reversing packed malware?
   - Building custom encoders?
   - Cryptanalysis?
Planning (soul searching)

3) What should you expect the students to already know?

- PKI?
- Crypto?
- Secure Software Development?
- Code Auditing?
- Assembly? x86? MIPS?
- General security?
- Networking?
- Web dev?

4) Can you establish pre-requisite classes?

- I found out at the last second:
  - NO - NOT FOR ELECTIVES
    - threw a wrench in things
Planning (soul searching)

5) What is the best way to assess the grasshoppers' progress?
   - Homeworks?
     - High level?
     - Hands on?
   - Projects?
   - Presentations?

6) Exams?
   - How many? 2? 3?
   - Take home?
     - Can further assess their ability to DO the material. Higher cheating risk
   - In class?
     - Can only assess their ability to critically think about the topics and their nuances.
Planning (soul searching)

7) How well do you know the material overall?

- 100%?
  - BS
- >75%?
  - You sure? Ok... go for it!
- >50%?
  - Very difficult to do all of it alone
- >25%?
  - Better have outside help
  - Still totally doable
  - NYU's pentest class taught by 5
Planning (soul searching)

8) How well can you DO the material?
   - 100%?
     ○ total BS
   - >75%?
     ○ Probably BS, but go for it
   - >50%?
     ○ Ok go for it!
   - >25%?
     ○ Might want to reconsider being the lead instructor, delegate perhaps?
Now, how to proceed
The Sensei

● Must be current
  ○ Attend conferences, read daily security news
    ■ /r/netsec, darkreading.com, or whatever ...
  ○ CTFs help keep skills sharp
    ■ http://ctftime.org/

● Need not know everything, just where/how to guide students
The Sensei

- Need not be a great public speaker
  - I'm not!
  - Hadn't taught before

- Should have a teaching method appropriate for the aggressiveness of the class agenda
  - Socratic method won't work for highly aggressive agendas
    - Better Slower paced - b/c more engaging
  - Fast-paced, Demo heavy works well for aggressive agendas
    - Requires heavy prep-work
Setup

VMware, Virtual Box
- MSDNAA (free windows)
- Linux distros - Ubuntu / Backtrack

LiveCD from textbook
- Dated debian distro with ASLR off by default
- Lots of useful code samples
Setup

Students: (30 at first)
  ● 19 grads
  ● 8 undergrads

75 minute lectures, twice a week
  ● Deserves to be a lab-course

Video taped every lecture (when possible)
  ● I used Microsoft Expression Encoder (free!)
Tactics

- Demo topics frequently
  - Students seem to learn best when they witness an exploit work
  - Have backup plans for demo-failures!
- Have a mole / Get feedback
  - Ask on homeworks (for minimal extra credit) how they think they are doing, and what they don't understand.
- Talk about news / current events
  - Important to give them perspective
- Make things due earlier than you expect
  - When you extend the deadline frequently - they think you are the most caring teacher ever!
Tactics

● Hands on Workshops
  ○ Proved very successful & rewarding
  ○ Reinforces cognitive processes
  ○ Tons of resources out there
    ■ Practical Malware Analysis textbook labs
    ■ Labs from http://pentest.cryptocity.net/
    ■ Labs from http://www.opensecuritytraining.info/Training.html
    ■ Exploit tutorials from http://www.corelan.be/
    ■ Level-based CTF exercises make good labs!
      ● http://exploit-exercises.com/
      ● http://smashthestack.org/
      ● ...
Tactics

● Term Project
  ○ Individual work?
  ○ Open ended vs Narrow Scope?
  ○ Provide sample projects
  ○ Provide detailed rubrics so they know how to **earn** the A
    ■ Especially with open ended projects

● [Project] Presentations?
  ○ Communication is important!
    ■ Easy to see BSers vs students who know the subject
  ○ Means less weeks for you to lecture
[War] Strategy

● Blitzkrieg into the thick of it!
  Week 3: Diving into the deep end (x86 RE)
  Week 4: Fuzzing + exploit dev
  Week 5: Exploit dev
  Week 6: Network Hacking + exploit dev
  Week 7: Web Application Hacking + exploit dev
  ...

● Remember to go up for air (cover big picture)
● Continue teaching on assignments
  ○ At least 20% of each HW is new stuff usually
● Keep them inspired
The Campaign
Organization

As the lead instructor I:

- Discussed ethics
  - Disclosure debate (day 1)
- Provided external tutorials, extra help, hw solutions
- Discussed importance of news and events

Coordinated:

- Other lecturers'
  - Their expectations
  - Their goals
Organization

In 15 weeks:

● 23 High content, fast paced lectures
  ○ less than 50% material done up front
● Very high attendance rate
● 8 CTF-style homeworks
● 2 exams (In class midterm, take-home final)
● Individual-work, open-ended term project
● Took newbs and painstakingly made them 1337
Organization

Advanced topics I wanted to teach:

- **ROP**
  - Found it was best to cover SEH exploits and ret2libc first

- **Memory Analysis of Running Exploits (for IR)**
  - Found it was best to cover all of exploit development first, along with tools like metasploit and meterpreter
    - Students already understood shellcode, encoders, exploits, payloads, and post-exploitation tricks.

- **UAV drone hacking WORKSHOP**
  - Failed - Parts never came in from China :(

- **Lockpicking**
Grading

- Homeworks - 40%
  - primarily for the students
- Midterm - 15%
  - primarily for instructor
- Communication - 10%
- Term Project - 20%
- Final Exam - 15%

Didn't care about lateness, as long as they had their work turned in before I released the solutions
The Results?

NATURAL 20
Because no matter how unlikely, with the right skills, ANYTHING is possible.
Results

● Students asked for:
  ○ More classes like this
  ○ "Offensive Security II"
  ○ "Advanced Exploitation"

● Graduating student(s) have job(s) at high profile IR team(s)

● Many more students going to DEFCON and other future cons/conferences
  ○ Some here at BSIDES
Results

● I modified / reused a lot of CTF questions on students
  ○ Our CTF team solved some that no one else did (zero writeups on the web)
    ■ So I reused these as extra credit problems :D

● Reused an unpatched anti-RE n-day against the students
  ○ made them binary patch it out

● Students loved the homeworks
  ○ This shocked me

● Inspired the students to do term projects that have REAL VALUE!
Results

What I did:

- 78% of the lectures on my own (18/23)
- 100% of the grading (for ~27 students)
  - 8 homeworks, 2 exams, individual term projects...
- 81% of the homeworks:
  - Created 6.5 of the 8 homeworks
- Created most of the midterm and final

Results:

- Constantly swamped
- Zero freetime, gallons of coffee
- Always behind on grading

GET A TA TO GRADE

The Lesson Learned?
Other... results

- "Sandals on the moon"
- people using the course material all over the world
- Have a big stick to beat up the other faculty now
  - Did I say stick? I meant class.
Overall Suggestions / Observations

● If you think you can do it still?
  ○ GO FOR IT
  ○ Hugely rewarding

● Get a TA to grade

● Find guest lecturers for your weak areas

● Use existing material
  ○ Reuse from me! From others!

● Keep the bar high & inspire the students
  ○ They WILL surprise you!

● You will learn from your students & teaching
  ○ *Teaching is the best way to learn*
Big Lessons

● Video Tape Lectures
  ○ IMMORTALIZE YOUR MISTAKES! (it's fun)
  ○ Put them online quickly
  ○ Allows you to pack more content in each lecture
    ■ faster pace; supports aggressive curriculum(s)

● Stay Current, Stay Sharp & Network, network, network
  ○ Find future guest lecturers for next time
  ○ Find like-minded people, for support, advice..

● CTFs are a huge untapped educational resource!!!!!!!

● Regularly revisit ethics/disclosure debate
An After-Semester Lessons

Posted everything online but:

- Lower than expected amount of independent study students getting through it all
  - Similar to Khan academy
  - This seems to be common in study-at-your-own-pace online courses

However,

- Still very useful as training material for organizations
Future plans

- Teaching again in the spring, and each year for as long as I can.
- [http://opensecuritytraining.info](http://opensecuritytraining.info)
- More guest lecturers (friends & industry professionals who have offered help)
- Lab based future.
  - Flip the lecture (Khan academy’s Salman Khan TED Talk)
- Starting a tradition among SFS for helping teach this subject.
HOW YOU CAN HELP

Have ties to your alma mater or a local university?? See if they are interested in this type of course, or club!!

● Show support
  ○ state recruiting interests,
  ○ demonstrate how others are teaching this ethically.

● Offer help
  ○ Homework exercise or two
    ■ find the packet, reversing challenge, malware reversing
    ● make sure to provide solutions!
  ○ Offer to do a guest lecture
HOW YOU CAN HELP

- Help them research existing FREE material. Finding material you can use to build a class with is hard research!
  - This course http://offsec.noleptr.com,
  - http://pentest.cryptocity.net,
  - http://opensecuritytraining.info,
  - and more!
Questions?
Course URL: http://offsec.noleptr.com
Contact info: redwood@cs.fsu.edu
Thanks!

- Xiuwen Liu, Mike Burmester, Mitch Adair, Joshua Lawrence for help/teaching/guidance
- FSU CS Department for letting me teach black magic
- and big thanks to the community
  - too many to list