Dan Guido – SOURCE Boston 2009

So you want to train an army of Ninjas…

Introductions

- Dan Guido
  - Last 5 years: "security researcher" in ISIS lab
  - Currently: IR for someone *really* big in NYC
- OEP
  - November 2004, Polytechnic CTF competition
- Lots of experience being a student
  - I can't stress this enough

NYU:Poly

- Infosec program started in early 2000s
  - NSF grants helped
- NSA Center of Excellence
  - Education (everyone has it, the CISSP)
  - Research (very exclusive, the NOP)
- Offers NSTISSI 4011, 4013 certs (gov specific)

- ~10 courses in Infosec

Problem

- Pentest course suffered from neglect
  - No one was qualified to teach it
- Many CS courses were/are too academic
  - Pentest course doesn't fit into this mold
- Took the course in 2006
  - Another student and I restructured the contents of the course mid-semester

Ninjas!

I* trained some!

I got these guys to help

Stephen Ridley

Dean De Beer

Mike Zusman

Dino Dai Zovi

Erik Cabetas

Thanks!

Results

- Vulnerability analysis on SHOUTcast server
- Vulnerability analysis on QNAP NAS
- ImmDBG script for buffer tracking
- Burp import script for Metasploit WMAP
- Meterpreter scripts…
- Bunch of odays

- *a lot of this work is being released *today*

- I couldn't be happier with the quality of work

Results

- How would you rate this course against others you've taken at Poly?
  - "The best course hands down"
  - "… useful in real situations…"
  - "Please make Pentest II"
  - "I learned the most in this class"
  - "The only course that's given me my value for my money"
  - "It's been 13 semesters (undergrad and grad), this is simply the BEST."
- Students couldn't be happier with the quality of the class

Results

- Continued involvement
  - ~5 NYSEC attendees
  - ~5 ShmooCon attendees
  - ~5 working on InfoSec research projects
  - One student hired into infosec consulting firm
- Huge interest in 2nd run class
- The class bred passionate students

Agenda

- Ninja training HOWTO
  - Sensei
  - Dojo
  - Equipment
  - Tactics
  - Strategies
  - Warfare
- The actual class
  - Organization
  - Grading

Sensei

Sensei

- Stay current and know where to look for help
  - You have to provide direction or the whole class will only be concerned with aircrack-ng
  - Maintain a presence in your community
    - Attend conferences, read dailydave, go to CitySec, etc.
- You don't have to know everything, only where you can go to find the answer

Sensei

- Think you can pull it off? Just do it!
  - Action was the largest roadblock in my case
- Creating a course from scratch is hard
  - I will help you with this ☺
- Many strategies for winning mindshare
  - NSA COE, NSF grant money, etc
  - Not my strong suit, remember, we already had a full program

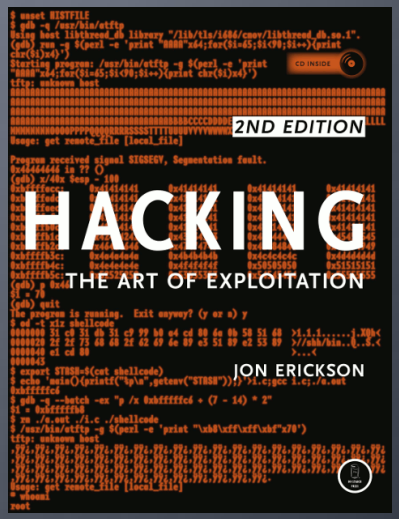
Dojo

Dojo

- Videotape your lectures
  - Not everyone could see what you did there
  - Buy a camera, hire a student, edit in iMovie
- Beware of online courses
  - Asymmetric communication is a killer
  - Presentations? Speaking skills? Hah!
  - Hard to create passionate students
    - lack of "buy-in"
  - Bottom line: teach a night class instead

Dojo

- Books? What books?
  - The best resources are all free, online, and current
  - No one book covers everything we did in our class
- Still need one?
  - Hacking: The Art of Exploitation (2nd)
    - Bonus: large size makes it look scholarly
  - Confessions of Teenage Hackers
    - Inspiration > reference material



Equipment

Equipment

- Equipment? What equipment?
  - Your students already have computers
  - VMware Player, Workstation, Server
- What about targets?
  - Use apps and devices the students have
  - RE? Offensive Computing, any Win32 binary
  - Exploitation? Securinfos, write your own
  - Web Apps? Might want to invest in your own app

Equipment

- Setup a mailing list and use it
  - Reading e-mail not considered "work" by students
  - Used to gauge skill level of class before it began
    - Props to Erik for thinking of that
  - Continues the discussion outside class
    - Students more likely to ask questions on it
    - Students will answer each others questions
- Mailing list = office hours at 4am

Tactics

Tactics

- Inspire your students (own some sh*t)
  - Create an aura of mysticism around yourself and be the uberhax4r your students hope to become
  - 1 minute of excitement is worth 1 hour of grade threats
  - Not a bunch of formulas for formulas sake
- Excitement gets better quality work
- More of an effect than a cause

Tactics

- Have a mole among your students
  - Adjust lectures, homeworks, topics on-the-fly
  - Don't wait 12 weeks for feedback
- Get more formal feedback at the end
  - Plan long-term changes in the course
  - Show your dept. you provided value
  - I'll release the simple template I used

Strategies

Strategies

- Don't put all the content together yourself
  - …or ask anyone else to
  - We chose a broad array of topics to cover
    - It's hard for someone to be an expert in all of it
    - You don't see Chris Eagle teaching Web Hacking!
  - "Steal" from people smarter than you
    - Use as much outside material as you can
    - Steal from me! ☺

Strategies

- Skip the basics and jump right in
  - CS programs don't usually cover fuzzing, RE, etc.
  - Don't let this stop you
- Introduce the topics early
  - Use the mailing list
- Keep them inspired
  - They will surprise you

Strategies

- Make your students present
  - A hacker who can't communicate is useless
  - Much better at measuring comprehension than a test
- Make your students famous
  - Encourage students to work on HW and projects that are practical and that they can release
  - They try harder, come up with better solutions, get exposure to what is actually out there

Warfare


THE PRESIDENT HAS BEEN KIDNAPPED BY NINJAS.
ARE YOU A BAD ENOUGH DUDE TO RESCUE THE PRESIDENT?

Warfare

- Ethics
  - I really didn't want to get caught up in this
    - Not a course in philosophy and law
  - Defined Hacking vs Pentesting 1st lecture
  - 30 mins on disclosure debate, legal issues
    - Current events sent to mailing list during semester
  - Reminded students mid-semester

The Class

Introducing CS6573

- Penetration Testing and Vulnerability Analysis
  - Took over the class in July 2008
- Course ran on-campus, Fall 2008
  - Thursdays 6-8:15pm (night classes)
- 22 registered students
  - Mostly 4th year CS and CE, less grad students
  - **Little to no experience in InfoSec**
  - Invited 8 other interested students to attend

Organization

- What skills do you need to be a pentester?
  - Divvy up each skill to 1 instructor

Course Section	Instructor
Source Code Analysis	Dan Guido
Reverse Engineering	Stephen Ridley
Exploitation	Dino Dai Zovi
Fuzzing	Mike Zusman
Clientsides and Post-Exploitation	Dean De Beer
Web Hacking	Erik Cabetas

Organization

- Each instructor taught 1 section for 2 weeks
  - 2 homeworks each
  - Assignments followed previous advice
    - Reverse real malware, fuzz real software, write meterp scripts, etc.
- Variety of teaching methods used
  - Labs, whiteboard, slides – all worked
  - Delivery was more important than the method
- Live demos blew students away
  - "1 minute of excitement…"
  - Students more engaged with the class and with us

Demo!

Organization

- What did I do?
  - Discussed ethics and disclosure
  - Provided extra help and solution guides
  - Moderated the mailing list (hundreds of emails!)
    - Introduced each topic 1 week beforehand
- Essentially, provided the glue
  - Made sure the class flowed week to week
  - Helped fully immerse the students in the material

Grading

- Want students to do HW – 35%
- Midterm is primarily for me – 15%
  - "Choose your own adventure" test
- Communication is essential – 15%
- Final project, true test of retention – 35%

- Extra credit available for outside work, CTFs, etc.

- Don't really care about lateness
  - oday shows up at the strangest times
  - Attackers don't have deadlines

Final Project

- Allows students to explore their interests
- Must display mastery of at least 1 skill
- Document their experience for others

- Graded via committee of instructors

- We could have done this better
  - Should have introduced it near the start
  - Single vs. group projects (do single)

Release

- Making course videos, assignments, tests, student work, feedback templates available
  - Some now, more available soon
- http://tinyurl.com/source-ninjas

EOF

- Thank you!
  - Stephen Ridley, Dino Dai Zovi, Mike Zusman, Dean De Beer, Erik Cabetas for teaching
  - Justin Prosco, Daniel Alex Finkelstein, Michael Aiello, Stephen Komal for helping with this presentation
  - Chris Eng for convincing me to talk
  - Prof. Nasir Memon for letting me take over the class

- dguido@gmail.com
- http://tinyurl.com/source-ninjas

Appendix

- Pics
  - Floppy Disk Ninja
  - Hot ninja girls 1, 2, 3
  - Ninja dudes 1, 2
  - Dr. McNinja
  - Ninja Party