Class Logistics and Background

Penetration Testing and Vulnerability Analysis

Dan Guido

Fall 2011

Introductions

Who we are

- Dan Guido – dan@isis.poly.edu
  - Current: Application Security Consultant, iSEC
  - Former: Incident Responder, Federal Reserve System
  - Former: Student in the ISIS lab
- Brandon Edwards – brandon@isis.poly.edu
  - Current: Independent Consultant
  - Former: Application Security Engineer, McAfee
  - Former: Security Consultant, Neohapsis
- We don’t have office hours, please use e-mail!
  - Mailing List: pentest@isis.poly.edu

Outside Instructors

- Bring in a local expert to teach each subject
  - Different viewpoints
  - Up-to-the-second accurate
  - Meet people doing real work in the industry
  - It’s fun, and we like you guys

- Brandon and I oversee the course as it progresses

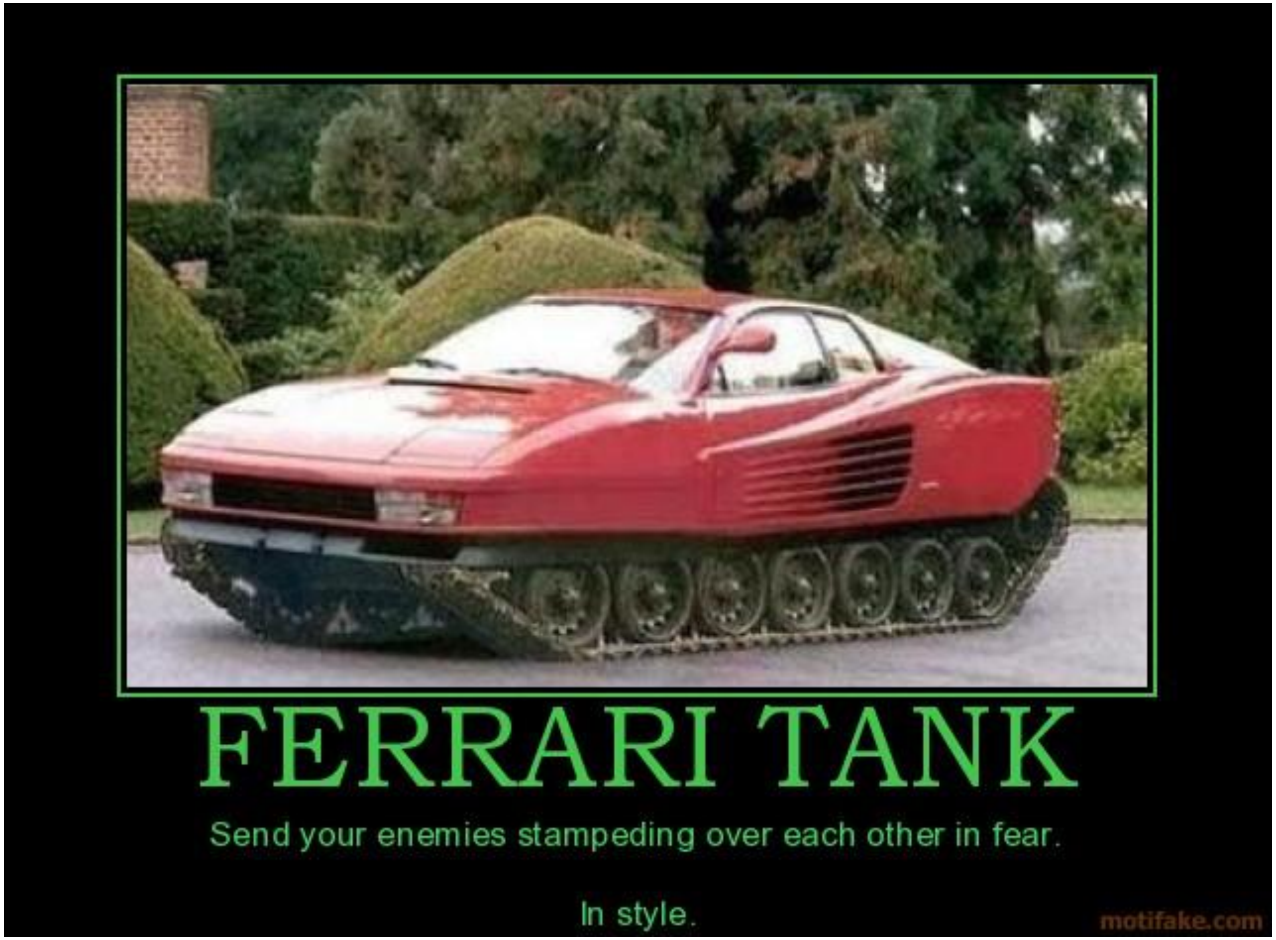
Meet the Instructors

- Alex Sotirov – Independent Consultant
  - www.phreedom.org
- Aaron Portnoy – HP TippingPoint ZDI
  - www.zerodayinitiative.com
- Dino Dai Zovi – Independent Consultant
  - www.trailofbits.com
- Joe Hemler – Gotham Digital Science
  - www.gdssecurity.com
- Colin Ames – Attack Research
  - www.attackresearch.com

Who are you guys?

- Majors? CS? CE? Anything else?
- Poly? NYU?
- Prereqs? Exploits? Languages?

Course Background



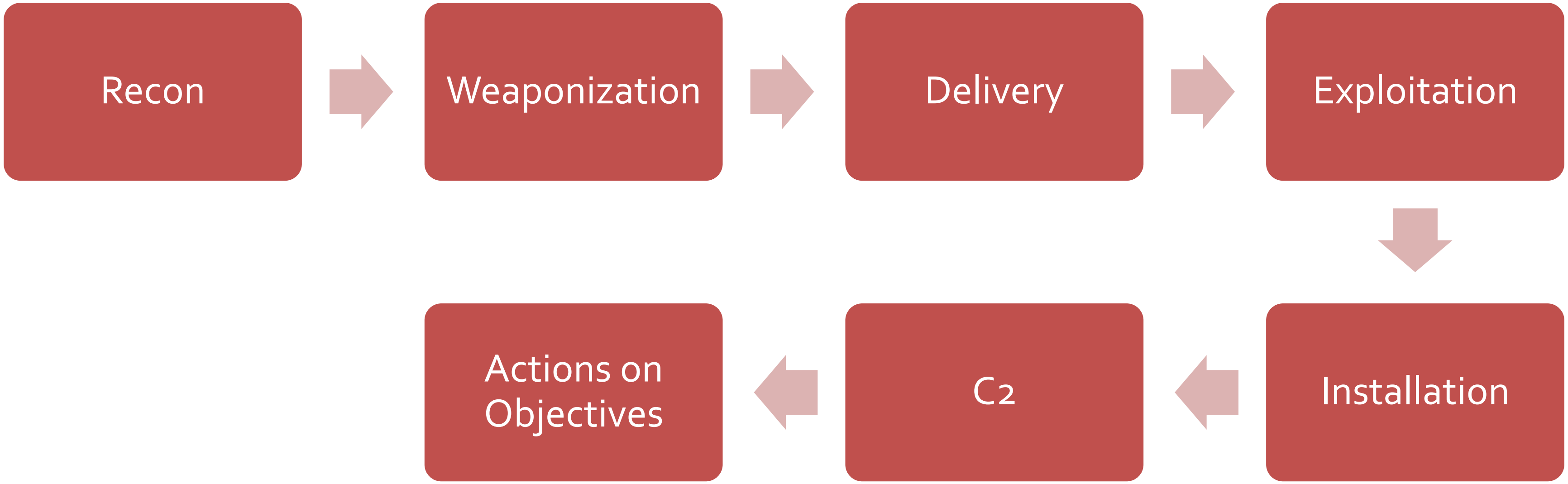
Penetration Testing

- When we use these skills to help secure a client, it’s called a penetration test
  - “A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user, commonly known as a hacker.”

- Hacking vs Pentesting?
  - PERMISSION!

Intrusion Kill Chain

- Systematic process that an intrusion must follow
- Penetration tests simulate this, in whole or in parts…
  - Why? To make it harder for someone else to do,
  - To identify weak links and ineffective defenses,
  - To test response, comply with regulations, etc.



Semester Goal

- This class prepares you to identify, analyze, and exploit software vulnerabilities
  - How to find them
  - How to understand their impact
  - How to take advantage of them

- We walk you through the process of simulating an attacker, across as much of the kill chain as we can

Categories of Skill

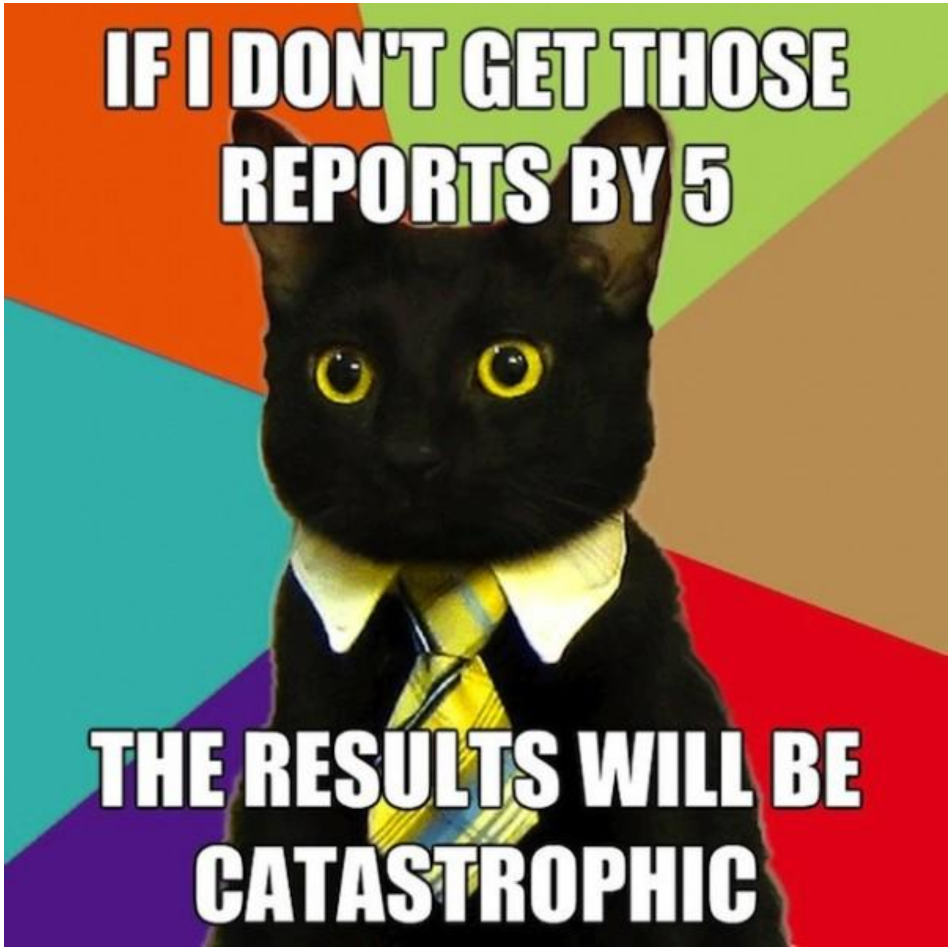
Part 1:

- Architecture
- Code Audits
- Reverse Engineering

Part 2:

- Exploitation
- Web hacking
- Network Pentests
  - Initial Compromise
  - Additional Vectors
  - Post-Exploitation

Logistics


IF I DON'T GET THOSE REPORTS BY 5
THE RESULTS WILL BE CATASTROPHIC

Assignments

- Homeworks and Readings
  - One per week (allowed two late homeworks)
  - These are hard, each requires new skills
  - Use the mailing list and IRC for help

- Takehome Midterm
  - It’s easy, do well on it

- Individual Final Projects
  - These are small, fun, and useful
  - These can count as SFS projects

Grading

- 30% - Homeworks
  - Do your homework every week!
- 20% - Midterm
  - Not heavily weighted in this class
- 50% - Final Project
  - Don’t wait until the last minute!

- Extra Credit
  - Involvement in CSAW
  - Any (legal) outside application of course material

Midterm / Class Party

- The midterm is a take-home
  - You have 1 week to complete 2/3 of it

- If you come to class on 10/17…
  - I'll have food and drinks
  - Short presentation on careers in infosec
  - Representatives from iSEC Partners, Gotham Digital Science, Matasano, Intrepidus Group, and others
    - Find an internship
    - Ask questions about your midterm

- http://pentest.cryptocity.net/careers/

FAQ

- Language?
  - C and x86 assembly and one scripting language

- Textbook?
  - Gray Hat Hacking, 3rd Edition
  - Metasploit, 1st Edition
  - Readings go out each week on the mailing list

Get More Involved

- NYU:Poly Hack Night
  - Tuesdays from 6-8pm in RH219

- NYU:Poly Cyber Security Club
  - Wednesdays from 12-2pm in RH227

- NYU:Poly CSAW
  - http://www.poly.edu/csaw

- NYSEC
  - 3rd Tuesday of the month, 6-9pm at Swift NYC
  - 34 E 4th St, New York, NY
  - http://twitter.com/nysecsec