Dan Guido – CS6573 Fall 2010

Class Logistics, Background

Who we are

- Dan Guido – dguido@gmail.com
  - Application Security consultant
  - Incident Response at a large financial
  - Student in the ISIS lab
- Brandon Edwards is co-teaching with me
- We don't have office hours, please use e-mail!

Tell us about yourselves

- Majors? CS? CE? Anything else?
- Poly? NYU?
- Prereqs? Exploits? Languages?
- What do you expect to learn in this course?

What we actually teach you

- 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 *try* to make you to think like and simulate malicious attackers

8 categories of skills

1st half:

- Architecture security and threat modeling
- Source code auditing
- Reverse engineering
- Exploitation

2nd half:

- Fuzzing
- Web hacking
- Client-side exploitation
- Post-exploitation

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
- I oversee everything with Brandon to keep the course consistent

Meet the instructors

- Architecture, threat modeling, code auditing
  - Brandon Edwards – McAfee
- Reverse Engineering
  - Aaron Portnoy – Tipping Point ZDI
  - Peter Silberman – Mandiant
- Exploitation
  - Dino Dai Zovi – The Mac Hacking Handbook

Who is teaching you?

- Fuzzing
  - Myself and Brandon
  - Rajendra Umadas – Intrepidus Group
- Web Hacking
  - Joe Hemler – Gotham Digital Science
- Client-sides and Post-Exploitation
  - Myself and Brandon
  - Dean De Beer – zero(day)solutions
  - Colin Ames – Attack Research

Phew!

- This course is very fast-paced
- If you want to simulate a real attacker, you have a lot of catching up to do!
- If you make it through, you will have the basic skills necessary to exploit almost anything
- Let me show you a demo or two…

Demos

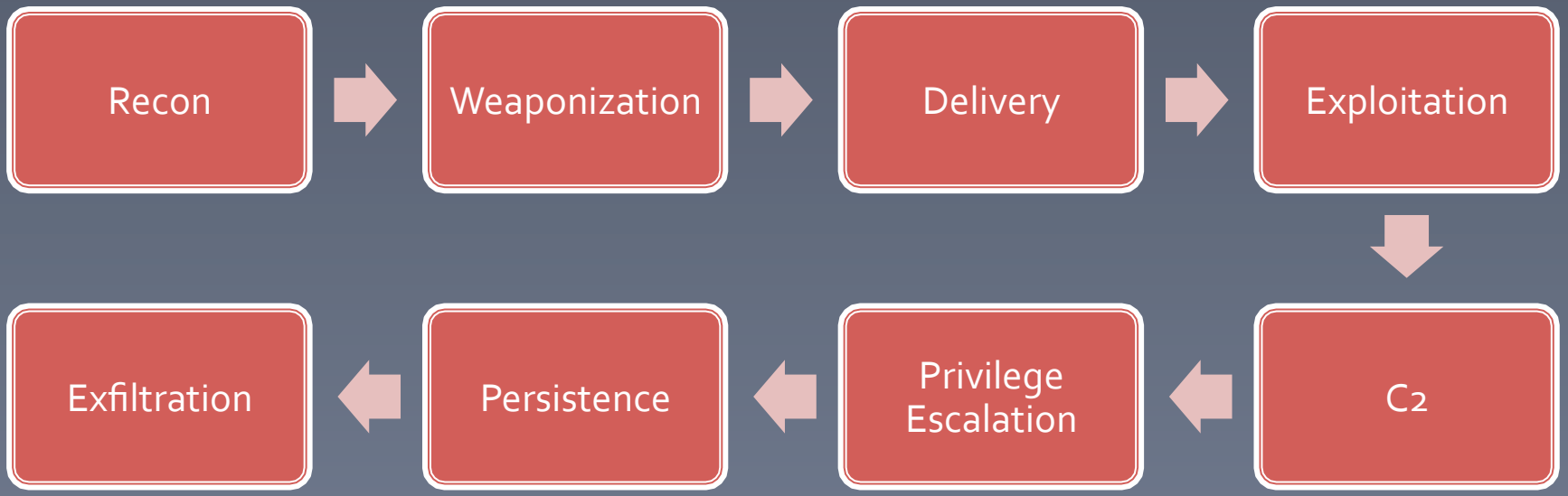
- 1st demo: web exploitation
- 2nd demo: clientside exploitation
- These will take all the skills we try to teach from start to finish and then some
- DEMO TIME!

Whiteboard time

- Name all the vulns I exploited in demo #1
- Name all the vulns I exploited in demo #2

Exploitation Lifecycle

- Attacks follow a natural progression
- Each step exploits a *vulnerability* of some kind
- We simulate this, in whole or in parts, to make it harder for someone else to do



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!

People pay for this!?

- Why?
  - Identify and understand impact of vulnerabilities
  - Are my defenses working properly? IR?
  - Regulations?
- Replicate sophisticated, modern attacks that people are using to compromise your apps and your organization
  - If you're on this Internet, you get this for free!

Whiteboard time again

- Refer back to the vuln lists from before
- Who might care that each of them were found and fixed?
- Who might pay for that service?

Logistics

- Each topic lasts about two weeks
  - One homework each week
  - These are hard, require new skills each week
  - Use the mailing list for help on assignments
- 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 Policy

- 35% - Homeworks & Final Project
  - Do your homework every week!
- 15% - Midterm & Discussions

- Extra Credit
  - Any involvement in CSAW
  - Any (legal) outside application of course material
  - I take any excuse to give away extra credit, *use it*

Career Day

- The midterm is a takehome, so we will have a career day on Nov 1st instead of class
- Have friends show up, talk about their companies, and help you find internships

Questions?

- Language?
  - C and x86 assembly and one scripting language
- Textbook?
  - Gray Hat Hacking, 2nd Edition
  - I will be sending out readings each week
- Are you excited yet?

Homework

- Scenario: you find a bug in an app you use
  - Why is it good to publish it online?
  - Why is it good to report it and keep it secret?
  - Find one real vuln that affected your app and describe where it came from and who found it
  - Find out how that app accepts security reports
- 1 paragraph each
- Adobe Reader is a good example app

Next steps

- Brandon is going to teach you about Architecture now
- Everyone can take a 10 minute break while we get set up