Dan Guido – CS6573 Fall 2009

Introduction to Penetration Testing

Meet Instructor #1

- Dan Guido, dan@isis.poly.edu
  - GTalk: dguido@gmail.com
- Former student researcher at ISIS lab
- Experience in InfoSec at IBank, .gov, .com
- You can google stalk me later

Questions

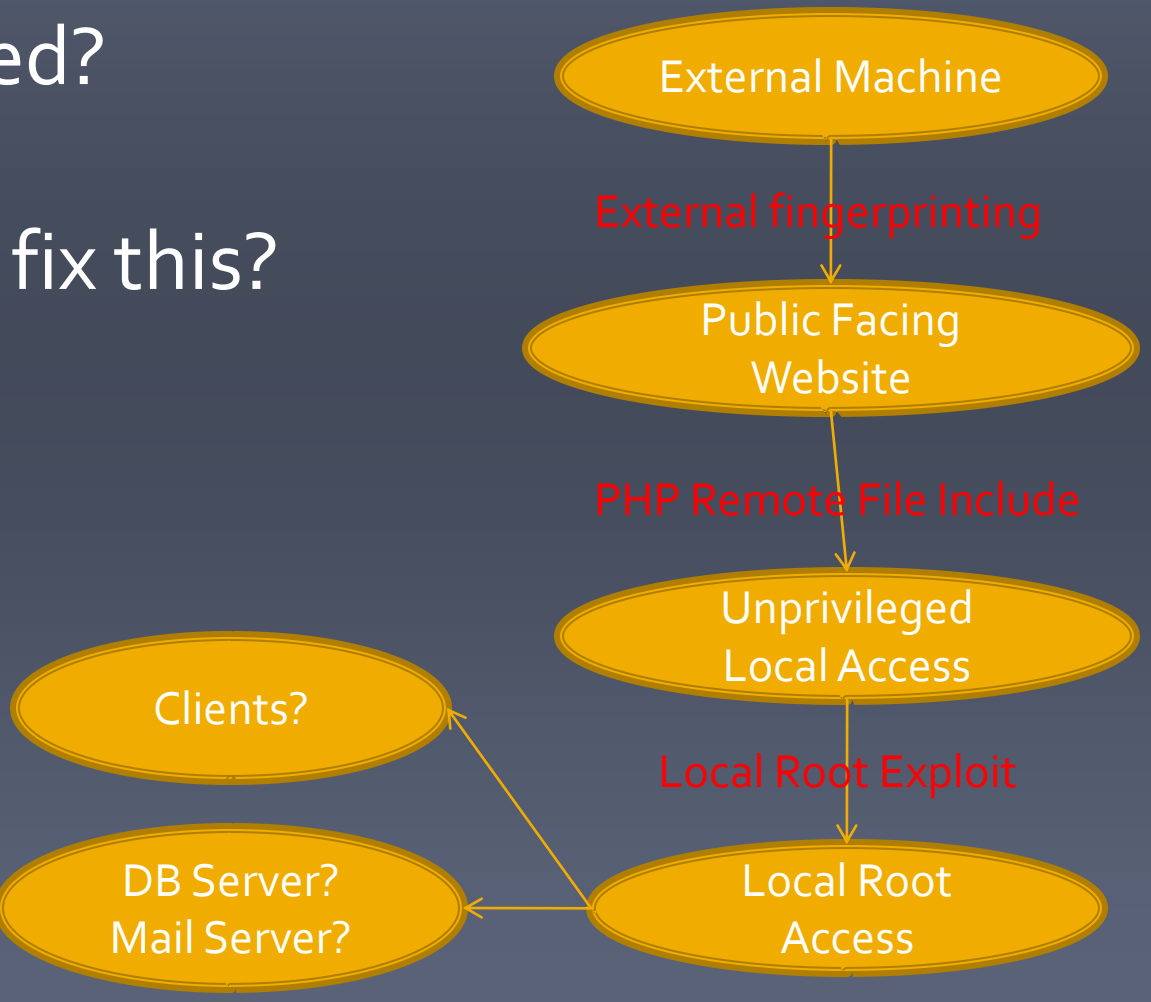
- Majors? CS? CE? Anything else?
- Poly? NYU?
- What do you expect to learn in this course?

Thought Experiment

- Beta Two Labs
- Public facing website
  - CentOS 5.3
  - HTTP
  - Blog
- Let's own^H^H^H simulate a sophisticated attack against it!

Break it down

- Skills required?
- How do you fix this?



What are we really teaching you?

- Source Code Audits
  - *Access to source = access to vulnerabilities*
- Reverse Engineering
  - *How does this compiled app work?*
  - *Modify it to do what you want*
  - *Identify vulnerabilities in compiled code*

What are we really teaching you?

- Binary Exploitation
  - *Take advantage of memory corruption*
- Fuzz Testing
  - *Negative testing you never learned about*
- Client-side Exploits
  - *Users are the weakest link*
  - *Internal attack surface to explore*

What are we really teaching you?

- Web Application Exploitation
  - *Knock down the front door*
  - *Public website = public attack surface*
- Fundamental technical skills
  - *Identify*
  - *Analyze*
  - *Exploit [anything, by the end of the course]*

Who is teaching you?

- Brandon Edwards – Code Auditing
  - Security Researcher at McAfee
- Aaron Portnoy, Peter Silberman – Reversing
  - Security Researcher at Tipping Point
  - Security Researcher at Mandiant
- Dino Dai Zovi – Binary Exploitation
  - Author, The Mac Hacking Handbook

Who is teaching you?

- Mike Zusman, Stephen Ridley – Fuzz Testing
  - Security Researcher at Intrepidus Group
  - Security Researcher at Matasano
- Dean De Beer, Colin Ames – Client-sides
  - Dean – Principal at zero(day)solutions
  - Colin – Security Consultant at Attack Research
- Joe Hemler – Webapp Exploitation
  - Co-Founder, Gotham Digital Science

Penetration Testing

- You can combine these skills for use in 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!

Business Issues

- Legal issues and regulations
- Scope – are you limited in what you can do and when you can do it?
  - odays? Client-sides? Aggressiveness?
- Impact and consequences
  - Inform the Client/Dept/BU/etc.
  - Incident Response
- Internal team vs. Consultants vs. Attackers
- *We won't focus on this part of pentesting*

What should you get out of this?

- Identify and understand vulnerabilities
- Assess impact, what are the ramifications?
- Are my defenses working properly?
- What systems and data are at risk?
- Incident response procedures working?

- Replicate sophisticated, modern attacks that people are using to compromise your applications and your organization

How we are teaching this?

- Each major topic lasts two weeks
  - One homework each week
  - Interesting HW entries will be posted online
  - These are hard, require new skills each week
- Mailing list for help on assignments
- Takehome midterm – it's easy if you ask me
- Final Project
  - We can talk about this later

Class Presentations

- Each class will start with one or two 10-minute presentations from students
- Review any security tool
  - *What it is, how to use it, what it's best at*
- Volunteers for next week?
  - I can help you get started

Grading Policy

- 15% - Discussions and Presentations
- 35% - Homeworks
- 15% - Midterm
- 35% - Final Project

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

Questions?

- Language?
  - Ruby, Python, Perl are best to know (pick one)
  - x86 assembly and C come in handy too
- Textbook?
  - I will be sending out readings each week
  - If you bought 'Hacking' 2nd edition, keep it
- Are you excited yet?
- 5 minute break while Brandon gets set up