Introduction to Penetration Testing

CS6573

Meet Instructor #1

- Dan Guido, dguido@gmail.com
  - Skype: danguido
  - GTalk: dguido@gmail.com
- Former Student researcher at ISIS Lab
- Experience in InfoSec at IBank, .gov, .com

Questions

- before I taint your minds...
- What does Pentesting mean to you?
- What do you want out of this class?
- What related work have you done?

Pentesting

- 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.
- Vulnerability Assessment vs Penetration Test

Pentesting?

- Hacking vs. Pentesting?
  - PERMISSION!
  - Oregon/Intel vs. Randal Schwartz
- Legal Issues/Regulations
- Scope – are you limited in what you can do and when you can do it?
  - 0-days? Client-sides? Aggressiveness?
- Internal Team vs. Consultants vs. Attackers

Rules of Engagement

- Impact & Consequences
  - Inform the Client/Dept/BU/Etc.
  - Incident Response
- Cover Your @$$ Agreement
  - Define the Scope
  - Stick to it (can't stress this enough)

Methodology

- Reconnaissance
- Scanning
- Fingerprinting/Enumeration
- Exploitation
- Escalation/Post Exploitation
- Covering Tracks
- Reporting

Course Philosophy

- "The Fundamentals of Hacking"
- We teach core technical skills
- People tend to specialize in certain areas
- Less focus on business issues and reporting
  - Still important though!

What we will cover

- 5 industry experts + me, 2 classes each
- Me! - Source code analysis
- Stephen A. Ridley - Reverse engineering
- Dino Dai Zovi - Memory corruption
- Mike Zusman - Fuzzing
- Dean De Beer - Client-side attacks
- Erik Cabetas - Web hacking

What you'll work on

- each section will have at least one HW
- due the week after w/discussion of solution
- best homework entries go up on the blog
- take home midterm, project final
  - we'll discuss these later
- use the mailing list for help on assignments

Extra Credit

- I'm flexible, only want you to be good hackers
- You can compete in a Capture the Flag competition for extra credit
- outside projects - give me 0day :-D