CS 290
Host-based Security and Malware

Christopher Kruegel
chris@cs.ucsb.edu

Administration

- Where do you get your information?
  - class web page
    http://www.cs.ucsb.edu/~chris/teaching/cs290/index.html
  - mailing list (public, for all students)
    cs290g@lists.cs.ucsb.edu
    I will subscribe you if you are registered for this class
    if you are not officially registered, please send mail to me
  - mail to instructor (for private matters)
    chris@cs.ucsb.edu

Administration

- What material will we be using?
  - unfortunately, there is no good book on systems security
  - you should use the slides that I will post on the web site
  - related research papers and online material (links will be posted)

Administration

- What are the requirements to get a grade?
  - Two exams (midterm and final) – 50% of grade
  - Eight challenges (small projects) – 50% of grade
    roughly one per week
    done with auto-grading (can retry multiple times)

Topics

- What are we covering in this class?
  - idea is that this class is complementary to Giovanni's class but some overlap can probably not be avoided
- Overview of areas
  - operating system security (both Unix and Windows)
  - forensics
  - reverse engineering
  - malware and botnets
  - social network security
  - (advanced) memory exploits
  - (practical) cryptanalysis

Challenges

- You will receive mail with account information!
- You can log into our environment or do most of the work on your own machine
- In the end, use our submit program to turn in solution
- Then, you get feedback mail and see update on a web page
  - uses auto grading – make good use of this