Hacking in Online Games:
bypassing security to gain an unfair advantage

What I have done: in-depth analysis of the following topics:

**Memory address scanning (dark souls/POE)**
- Explanation of client – server model and why it’s a bad idea to store things client side
- delve a little into how this is actually done
- vulnerable online games: DARK SOULS!!

**DLL Injection (maple story/APB)**
- Talk about what this is, explain how it works and why
- Explain its potential in hacking games
- Demonstrate on a game/explain how a specific one works

**Use of VMs in hacking**
- talk about cheat engine’s DBVM and what it does, how it is useful

**Hacking in online games on Consoles**
- Discussion of how hacking online games changes on consoles, why DS people thought they were secure
- Examples from real life: D3 hacking on consoles more prevalent than on computers

**Countermeasures (punkbuster/onlineonly/other services)**
- Discussion of different methods to prevent hacking/history
- Ways these services protect a game
- Segway into next two sections: even the best protection can be circumvented

**Botting (D3/POE)**
- Bots give players unfair advantages in a way that is very difficult to detect from the game makers side
- Discussion of different bots, how they work, how they are detected

**Exploits and Glitching in Online Games**
- Breaking the intended use of the game without the assistance of code: exploits in game,
  Discuss gunz, assassination of lord british

**Hacker Utilities/Sites**
- wrap up with a discussion of hacker resources, tools, and sites

Questions:
Demo- is it worthwhile to write an address scanner/find a hack myself?
Length of the meeting next week- what will we talk about for 40 minutes?
My results will be powerpoint + word doc for slides + demo code if I have it. Is this good? Should I write a page on the wiki?
Overlap with botting project: I have a section on botting, is this okay?

Details on: http://cs166.cs.brown.edu/mediawiki/index.php/Online_Game_Hacks