Comp 199

Penetration Testing I

Admin

- Wednesday's current events presenters
  - Jeffrey A.
  - Greg R
- Todays presenters
  - Show details of man-in-the-middle attacks and discuss
- Project update

Penetration Testing

- Why penetration testing?

Penetration Testing

- Why penetration testing?
  - “the network is the computer”
    - Very few computers off network today.
  - Malicious Attackers regularly attacking
    - cf. the British citizen on trial for hacking
    - http://www.ibamag.com/news/one-sector-especially-at
  - Government and private computer presences must protect themselves.
  - Internal/external penetration testing schemes.
  -

What you learn here

- Penetration testing is a tool
  - Like any tool it can be used for good or bad
    - “Anti-Forensics” stuff from digital forensics
    - Guns/pepper spray/chainsaws etc in the physical world
  - As per your book, use the tools that we are learning here responsibly
  - What is used in this lab is fine.
  - Do not use them on the rest of the network. (without IT's specific permission.
  - If contacted by IT I will tell them I told you this.
    - Story from a few years ago.

First in any Penetration Test

- The first thing you do as a security professional in a Pen test
  - Get Authorization
    - Company management authorizes the pen text
  - Establish scope
    - Which machines are fair game
    - Which does the company want to keep out of the test
    - <<Set up possible scenario>>
  - Now actually carry out the test

Phases of Penetration Test

- Reconnaissance
- Scanning
  - Port Scanning
  - Vulnerability Scanning
- Exploitation
- Maintaining Access.

Reconnaissance

- Figure out what the systems are
  - Find the raw IP addresses.
  - Whois
  - Host lookup
  - Is the hostname spread over several actual machines?

Scanning

- Port scanning
  - Use tools to find open ports
  - Figure out what services are running
  - Explain this
- Vulnerability testing
  - What services are on the machine – how are they configured

Exploitation

- Gain unauthorized access

Maintain Access

- Install backdoors to allow you back in

Tools

- You need tools for this
  - Backtack linux
  - Linux is standard for pen testing as windows was for digital forensics.

Reading

- Read chapter 1 in Engebretson