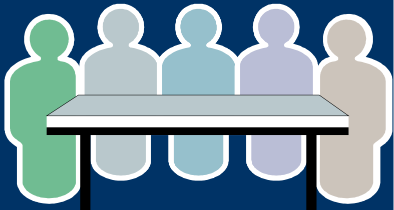
NebraskaCERT 09/2004 - CSF

MetaSploit: The Beginning of the End or the End of the beginning?

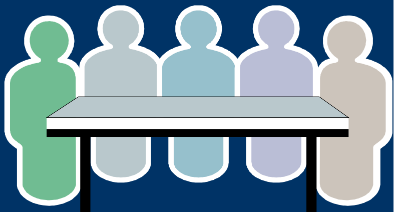
By

Aaron Grothe (CISSP)



Intro

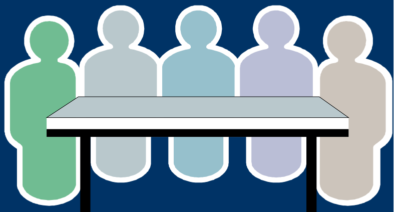
- My Background
  - Currently a DBA
  - Working for a company undergoing Sarbanes-Oxley work
  - Last round of Oracle exploits through us for a loop
  - Member of NebraskaCERT for 2+ years



Intro Quote Credit

- Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning.”

  Winston Churchill



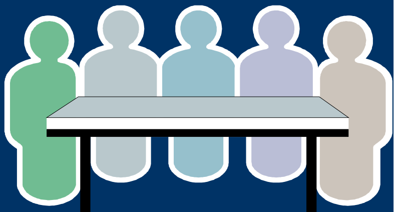
Disclaimer

- “ In some cases ... the knife can turn savagely upon the person wielding it ... You use the knife carefully, because you know it doesn't care who it cuts.”

Steven King

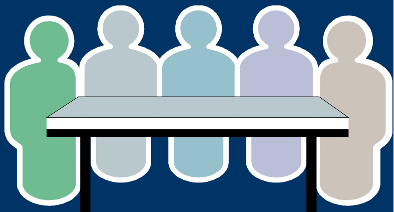
Disclaimer 2

- This speech in no way is intended to reflect the endorsement of my employer
- The views expressed reflect my personal beliefs and no one elses
- If you do something very bad with this, please don't blame me



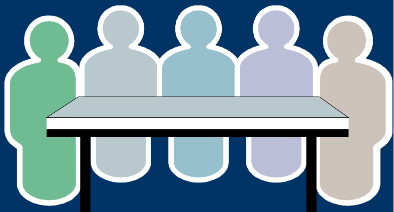
Three Things you'll Hopefully Walk away with from this talk

- Metasploit may be the standard for exploit testing in the future
- Standardized exploit testing is probably the next logical step in vulnerability assesments
- Maybe, I should try Metasploit



What Metasploit Does

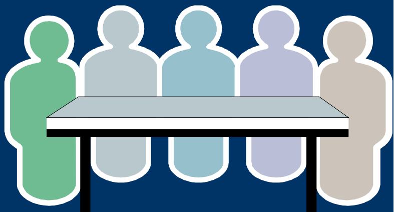
- “ Metasploit: Hacking like in the moves” - Metasploit.com site
- Metasploit brings point, click, 0wn to exploits
- Metasploit provides a standardized base for writing exploits
- Metasploit also provides some good tools for writing exploits



Problems Metasploit Solves

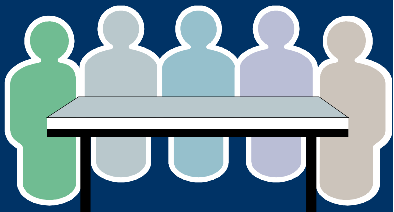
- How can I verify that the patch or workaround I applied worked?
- How can I trust exploit code written by people with l33t skillz?
- “ Trust, but verify” - Ronald Reagan

- How can I demonstrate an exploit to non-tech people (management)?



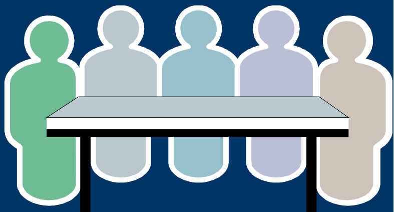
Personal Lessons Learned

- The SUN RPC exploit is very effective
- Windows XP SP2 breaks a lot of exploits by changing addresses
- Techniques such as PIE/NX make it harder to execute some exploits
- Metasploit is cool
  - Tempted to write some of the Oracle vulns into metasploit exploits



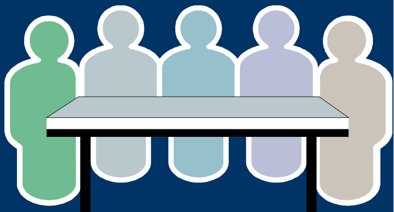
Why we need Metasploit?

- Typical Scenario at a Company
  - Run Nessus
  - Take report and drop “ may” , “ can” and “ could” from report
  - Throw fit
  - Upgrade recklessly, whether necessary or not



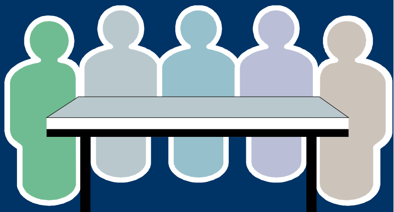
Example Fit #1

- “ You're running Apache 1.3.12. You're vulnerable to the Apache Chunk Vulnerability” - Security People
- “ No we're not we've put the patch on our system for this” - Me



Example Fit #2

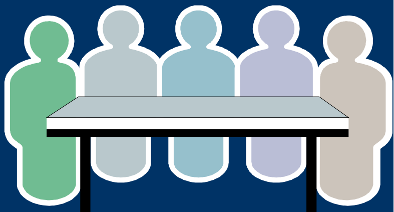
- “ You're running a vulnerable version of OpenSSH on box X. FIX IT NOW!!!” - Security People
- “ That only applies if you're running PAM. We're not using PAM. GO AWAY!!!” - Me



How does this Happen?

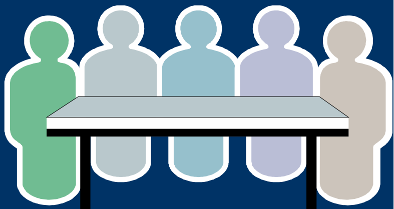
- Are security people stupid by nature?
- Is there a belief in the infalibity of the tools?
- Does anybody read a CERT advisory?

- Personal belief
  - Too many machines
  - Hard to tell if machine is really vulnerable



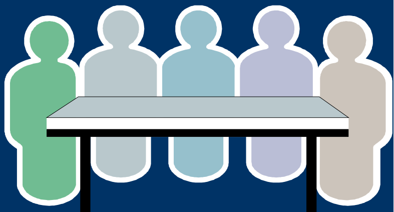
Then Now of Vuln/Pen Testing

- Then – Custom tools to do telnet to all ports
- Now – Nmap
- Then – Custom tool to telnet and grab banners on all services to get versions
- Now – Amap or Nessus



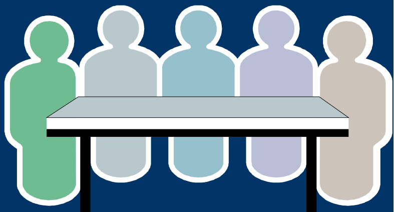
Dos and Don'ts

- Do download Metasploit
- Do read at least the Crash Course User Guide and FAQ
- Do run on your test network
- Don't run on your production network
- Do rember that some poorly written exploits can/will crash your system



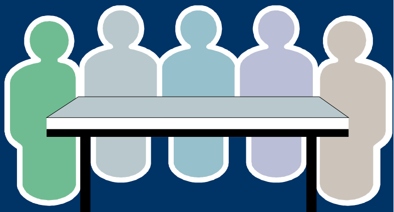
Dos and Don'ts

- Do run msfupdate to get more exploits
- Don't blindly accept new updates from untrusted 3rd parties
- Do mention me if things go well
- Do mention Matthew Marsh if things don't ;-)



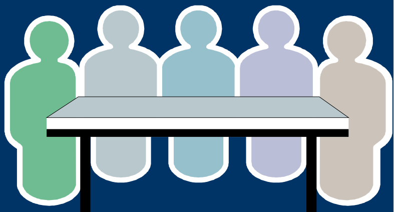
Why Metasploit Rocks

- Open Source: GPL and Artistic License
- Well written
- Written by experienced people
- Extensible
- Multiple layers of goodness
- Seperation of exploit from payload



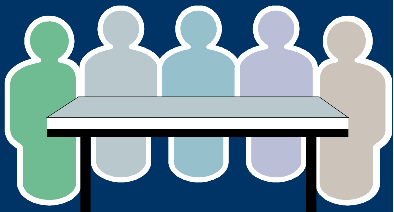
Resources

- Metasploit Home Page
  - http://www.metasploit.com
- Exploit in Action: The Apache Chunked Encoding Vulnerability
  - http://www.shrinkster.com/mf
- Sample 3rd Party Exploit
  - http://www.shrinkster.com/mb



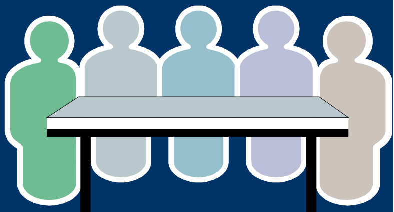
Resources

- Security Focus Metasploit Article Part 1
  - http://www.shrinkster.com/m7
- Security Focus Metasploit Article Part 2
  - http://www.shrinkster.com/m8
- Security Focus Metasploit Article Part 3
  - http://www.shrinkster.com/m9



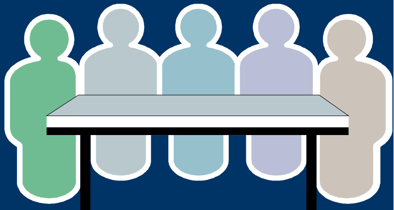
Resources

- Auditor Bootable CD-Rom Toolkit comes with Metasploit 2.1
  - http://www.shrinkster.com/ma



Contact Info

- Ajgrothe <at> yahoo.com



Semi-demo of Metasploit

- Show a couple of cool features of Metasploit
- I will be stopping before actually executing the exploit