First Objective

Penetration test tools

- Hardware-based:
  - http://www.mudynamics.com/products/overview.html
  - >$50,000
- Software-based:
  - Commercial products
    - Core impact: http://www.coresecurity.com/content/core-impact-overview
    - Immunity canvas: http://www.immunitysec.com/products-canvas.shtml
  - Open-source
    - Metasploit: http://framework.metasploit.com/
    - Linux: knoppix, backtrack
  - Free tools
    - Vulnerability Exploitation Tools: http://sectools.org/sploits.html
    - Packet Crafting Tools: http://sectools.org/packet-crafters.html
    - Web Vulnerability Scanners: http://sectools.org/web-scanners.html
    - x-Scan: http://www.xfocus.net/tools/200507/1057.html
    - Hack Tools, Utilities and Exploits: http://www.darknet.org.uk/hack-tools-exploits-feeds/

Resources (1)

- "white markets" - set up by VeriSign, TippingPoint, Google
  - where they buy zero-day flaws and alert the companies so that they can patch their products before the vulnerabilities can be taken advantage of
- NSS Labs: https://www.nsslabs.com/research/research-subscriptions.html
  - ExploitHub is the first legitimate marketplace for validated, non-zero-day exploits: https://www.exploithub.com/
  - Bounty System, ExploitHub has initially placed bounties on twelve client-side exploits https://www.exploithub.com/request/index/developmentrequests
- WSL lab: http://www.wslabi.com/
- TippingPoint Zero Day Initiative: The amount we offer to a researcher for a particular vulnerability depends on the following criteria.... http://www.zerodayinitiative.com/about/benefits/
  - Pedram Amini of TippingPoint says that when governments are involved, a vulnerability can sometimes yield as much as $1 million to the skillful researcher.

Resources (2)

- Vulnerability Contributor Program
  - iDefense Labs, http://labs.idefense.com/vcp/
- CORE IMPACT, from Core Security Technologies
  - a tool that aims to help in the process by automating as much of it as possible. CORE IMPACT allows the user to safely exploit vulnerabilities in the network, replicating the kinds of access an intruder could achieve, and proving actual paths of attacks that must be eliminated. www.coresecurity.com
- Packet filtering security devices including firewalls, routers, and intrusion detection and prevention systems. www.idappcom.com
- Explore new attack vectors before they are exploited maliciously. www.mudynamics.com

RESOURCES (3)

- Rapid7/Metasploit
  - The Metasploit Framework is both a penetration testing system and a development platform for creating security tools and exploits. www.rapid7.com
- The Vulnerability Research Service (VRS) from TELUS provides security product vendors with timely, in-depth engineering analysis on the top five to eight security vulnerabilities that emerge each week. www.telus.com

US guidelines

- Special Publication 800-42, Guideline on Network Security Testing
- Special Publication 800-115, Technical Guide to Information Security Testing and Assessment, September 2008 (replaces SP800-42)

Commercial reports

- J M. Fossi, T. Mark, D. Turner, D. Mazurek, G. Egan, T. Adams, D. McKinney, K. Haley, J. Blackbird, P. Wood, E. Johnson, and M. Low, *Symantec Internet Security Threat Report–Trends for 2010*, Technical Report XVI, Symantec Corporation, 2011.
- Muttik, "Russia: Economics, not Mafia, Fuel Malware," in McaFee Sage Report http://www.mcafee.com/us/local_content/reports/sage_2008.pdf.
- Similar reports from McAfee, Trend Micro, Cisco, IBM, Microsoft, HP, Verizon, etc.
  - Google's browser security report
  - Verizon data breach report: www.verizonbusiness.com/resources/security/databreachreport.pdf
  - Symantec: J. Blackbird, S. Entwise, M. K. Low, D. McKinney, and C. Wueest, "Internet Security Threat Report, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf.
  - McAfee: Muttik, "Russia: Economics, not Mafia, Fuel Malware," in McaFee Sage Report http://www.mcafee.com/us/local_content/reports/sage_2008.pdf.
  - Trend Micro: "Trend Micro Threat Roundup and Forecast," http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/1h_2008_threat_report_final.pdf.
  - Cisco's security report: www.cisco.com/web/go/securityreport
- Google's browser security handbook: http://code.google.com/p/browsersec/wiki/Main

Main targets

- Web browser attacks
  - Cross site scripting
  - Encrypted scripts
- SQL injection
- Mutating malware
  - Polymorphic
  - Metamorphic
- Youtube has many demos
- Malware collection by surfing to dangerous sites
  - Need a PC without anything important to you
  - Unplug power or battery when the PC is not used

Assignments (1)

- Read previous report by David Rose @sftp://scp.eng.auburn.edu/home/eewu/wuchwan/Teachings/Senior+Design
  - You need to use SFTP client (Winscp or cyberduck)
- Read all commercial reports
- Read my slides: 5220 + 4000
  - 5220: Ch 1, 2, 3
  - 4000: Ch 17, 25, 26
- Surf BitTorrant and other sites using Rose’s report as the guide
- Log at least 10 hours per week for reading and surfing
- Logs are part of the final submission at the end of the semester

Assignments (2)

- The logs needs to contain
  - screen shots of your surfing
  - Time: starting time and ending time of each survey
  - Summary of the discovery of each survey
  - Format: Word .docx
- It is mandatory to upload your logs at least once every week
- First report needs to contain the logs
- Use the Internet to find ideas and tools
- Hardware Equipment for attack and victim needs to be ready

Shared site

- Leader: one letter grade
- Set up site and folders for sharing logs and discovery
  - Or emails
- Coordinate attacks and defense
- Coordinate hardware sharing
- Lab in 312 Broun

Q&A

- Lecture session: 1/11, 2 – 2:50 PM @ 107 Broun
- Lecture session: 1/18, 2 – 2:50 PM @ 107 Broun
- Group forming session: 1/23, 2 – 2:50 PM @ 107 Broun
- Group session: 1/30, 2 – 2:50 PM @ 107 Broun
- Schedule for review meeting: @324 Broun