CYBERCRIME DETECTION
AND FORENSICS
CIS 4930-01
Syllabus, lectures, and other materials — Spring 2010

Spring 2010: Syllabus for CIS-4930r-01

Final Paper Requirements

Assignments

Assigned 2010-01-07:

- Required reading: WFA, pp. 1-61; MF, pp. 1-91; all articles linked below in the "Other Material".
- Suggested reading: DECC, pp. 1-85; FCC, pp. 1-80.

Assigned 2010-01-28:

- Required reading: MF, pp. 91-120.
- Assignment 1. Assigned on 2010-01-28, due 2010-02-04.

Assigned 2010-02-04:

- Required reading: Chapter 2 of WFA, pp. 63-86, chapter 3 of WFA, pp. 89-124, and chapter 3 of MF, pp. 121-192 of MF.
- Assignment 2. Assigned on 2010-02-04, due 2010-02-11.

Assigned 2010-02-16:

- Assignment 3. due 2010-02-18.

Assigned 2010-02-23:

- Required reading: MF, pp. 193-253.
- FYI: There is a campus IT security meeting today, February 23, in 242 Sliger at 3:30pm. The agenda for the meeting.
- FYI: There will be a "viewing party" of the broadcast of the webcast *Emerging Trends and Threats for 2010* tomorrow, February 24, in 150 Shaw (RSB) at 2:00pm. Announcement

Assigned 2010-03-18:

- If you haven't already, please read WFA Chapter 4, pp. 125-189.
- Also, please read MF Chapter 6 (pp. 253-281). I won't lecture much (if at all) on the material, but I will expect you to be familiar with it for the midterm on March 25th.
- The midterm on March 25th is comprehensive, and will cover (1) MF Chapters 1-6 and (2) WFA

Chapters 1-4, and all additional material referenced on the class webpage or referenced in the class notes.

Class Notes

Introduction

Technical Introduction to Windows

Technical Introduction to Linux

Memory Analysis, Part 1

Memory Analysis, Part 2

Malware Post-Mortem

The Windows Registry

File Analysis, part 1

File Analysis, part 2

Live Analysis: Executables and Execution

Rootkits and Blue Pill

Basics of static analysis

Other Material

2008-08-11: Plastic Keys to Physical Locks: *Researchers Crack Medeco High-Security Locks With Plastic Keys*

2008-08-22: An Email about an intrusion at Redhat's Fedora: Infrastructure report, 2008-08-22 UTC 1200

2009-02-10: Data breach at FAA: *FAA reports 45,000 data records pilfered from server*

2009-04-01: *Spam Back to 94% of All E-Mail*

2009-05-12: Berkeley data break-in: *Hackers attack campus databases, steal Social Security numbers, other data*

2009-05-15: Backup woes at Avsim: *Hackers 'destroy' flight sim site*

2009-07-23: Adobe Flash woes: *New attacks exploit vuln in (fully-patched) Adobe Flash*

2009-10-16: *Big-Box Breach: The Inside Story of Wal-Mart's Hacker Attack*

2009-10-22: *FBI and SOCA plot cybercrime smackdown: White hats get proactive on e-crime*

2010-01-20: *Fearing Hackers Who Leave No Trace*

2010-01-20: *More Researchers Going On The Offensive To Kill Botnets*

2010-02-04: *Identifying almost identical files using context triggered piecewise hashing*

2010-02-04: *Using Every Part of the Buffalo in Windows Memory Analysis*

2010-02-04: *Using Hashing to Improve Volatile Memory Forensic Analysis*

2010-02-05: *Hacking for Fun and Profit in China's Underworld*

2010-02-05: *US oil industry hit by cyberattacks: Was China involved?*

2010-02-06: *FATKit: A Framework for the Extraction and Analysis of Digital Forensic Data from Volatile System Memory*.

2010-02-19: *Modern banker malware undermines two-factor authentication*

2010-02-19: *Broad New Hacking Attack Detected*.

2010-02-19: *The Kneber botnet - FAQ*.

2010-02-19: As mentioned in class yesterday, the creation of a rogue CA certificate via an MD5 collision story: MD5 considered harmful today: Creating a rogue CA certificate.

2010-02-19: *Why the Windows Registry sucks... technically*

2010-02-23: Keyloggers: *Churchill High grade scheme may involve half-dozen students*; apparently, from other stories on this incident, the students may have picked this up from Youtube, which hosts videos on install keyloggers, including ones showing how to create trojans to install keyloggers (search Youtube for "Ardamax", for instance.)

2010-03-02: Big botnet: *Authorities bust 3 in infection of 13M computers*

2010-03-08: A classic: *No Stone Unturned*

2010-03-16: *What we know (and learned) from the Waledac takedown*

2010-04-01: Another classic on the Linux ELF format: *A Whirlwind Tutorial on Creating Really Teensy ELF Executables for Linux*.

2010-04-08: *Older work on analyzing a binary*

Suggested Mailing Lists

I also highly recommend reading comp.risks (you can read it in rdf format at http://catless.ncl.ac.uk/rdigest.rdf, or via email — instructions are at http://www.csl.sri.com/users/risko/risksinfo.html) or adding its RSS feed at http://catless.ncl.ac.uk/risksatom.xml to your feed browser.