CS 556 – Spring 2018 Project 1
Study and Demonstration of Computer Attacks and Security Tools

Project Due Dates:

Due on CANVAS by Tuesday, February 13, 2018

Please prepare a video of your presentation (include live demo related to point C below) and upload it together with your report on CANVAS

Description

This is an exploratory project. The purpose is to introduce you to the world of cyber-attacks and security tools. The Internet is your resource.

You have to find a concrete attack/vulnerability/exploit in a platform or application of your choice and a security tool to investigate and present in class. The report is based on your investigation and should touch on the points below. The presentation should be no more than 10 minutes.

For attack/vulnerability/exploit,

A The attack should be an interesting (high impact / complex) one. Use your judgment to decide what is an interesting attack. Explain the basic background of the attack, e.g., what it can do, how dangerous they are.

B Explain how the attack works, preferably with key pieces of code (if applicable) shown to illustrate the process.

C Make a live demo when possible. Note it is not required that you implement the attack yourself. You only need to show that it works on a live system (many of attacks have source code available online). Some attacks are not possible to demo without the proper hardware or infrastructure, in which case the concept and effect of the attack should be clearly explained in sufficient detail.

D Discuss possible defenses.

For security tool, the deliverables will be the demo during which the following questions need to be answered.

A Explain the background of the tool, e.g., what it does? Who made it? How popular it is? Mostly used in what circumstances?

B Explain how the tool works behind the scene.

C Show what the tool can do. Run the tool and demo (the tool should be demoable).

Resources: (Just suggestions – you can use your own)

1. The National Vulnerability Database (NVD) – https://nvd.nist.gov
2. Common Vulnerabilities and Exposure (CVE) – https://cve.mitre.org
3. Full Disclosure – http://seclists.org/fulldisclosure/
4. Open Vulnerability Assessment (OpenVAS) – http://www.openvas.org
5. The Exploit Database (ExploitDB) – https://www.exploit-db.com
6. Google Hacking Database – https://www.exploit-db.com/google-hacking-database/
7. Heartbleed Bug – http://heartbleed.com
8. NSA Toolbox – https://nsa.gov1.info/dni/
9. IMSI Catcher (http://www.engadget.com/2010/07/31/hacker-intercepts-phone-calls-with-homebuilt-1-500-imsi-catcher/ ; https://docs.google.com/presentation/d/11eBmGiHbYcHR9gL5nDyZChu_-lCa2GizeuOfaLU2HOU/edit?pref=2&pli=1#slide=id.g1d134dff_1_222)
10. SecTools.Org: Top 125 Network Security Tools
    a. Password audit – http://sectools.org/tag/pass-audit/
    b. Sniffers – http://sectools.org/tag/sniffers/
    c. Vulnerability scanners – http://sectools.org/tag/vuln-scanners/
    d. Web scanners – http://sectools.org/tag/web-scanners/
    e. Wireless – http://sectools.org/tag/wireless/
    f. Exploitation – http://sectools.org/tag/sploits/
    g. Packet crafters – http://sectools.org/tag/packet-crafters/