CSCI 345 – Computer & Network security
Spring 2019
Semester Project

Goals:
1. Students will apply the knowledge from the course, such as vulnerability analysis, pen testing, and software security testing.
2. Students will:
   a. Develop or replicate a tool for security, or
   b. Discover or replicate a protocol or system vulnerability, or
   c. Perform pen testing for a system or software suite.
3. Students will write a 4-6 page, workshop style publication and present their work in class.

Teams:
The project will be completed in teams of up to three students. If you would like to work on an idea individually you will need to discuss this with me.

Topics:
Your topic may be pen testing a target, creating a cyber security education lab, or extending/creating a tool for security. Please choose one of the suggested topics and avoid suggesting your own. I am not trying to stifle innovation. On the other hand, I would like to be realistic with this semester project. My recommendations fit within your knowledge and the timeframe of a semester. If you would like to suggest your own topic, you will need to discuss with me before the first deadline to get my approval.

Milestones:
There will be several presentations in the form of lightning talks or short presentations. If you do not know what a lightning talk is, please read the information in the link above. It is important to fit your presentation within the time limit. You will receive feedback from me on all presentations. I will grade the final project product, not the intermediate presentations. The presentations and dates are:
1. **Project proposal**: short presentation (up to 10 mins) will be performed on Feb. 2. Depending on my feedback, you may change the proposal. The presentation will include:
   a. Title, team members, team name (optional)
   b. Motivation: why is what you are doing important.
   c. What you are proposing: Description of the system or network protocol that you are planning to analyze or implement, or the tool that you intend to build or extend. Description of security properties you intend to investigate. Tools and/or analysis techniques you are planning to use. Clear description of project deliverables. Possible deliverables are a software product, a substantial case study, or, a network topology and scripts to run an experiment.
2. **Project progress report 1**: lighting talk on your progress on March 23. What has worked, what needs to be refined, and what did not work and why?
3. **Project progress report 2:** lighting talk on your progress on **April 13.** What has worked, what needs to be refined, and what did not work and why?

4. **Project final presentation:** conference style presentation with duration 15 mins on the last week of classes. A demo can be included in the presentation in the form of live demo or video demo.

**Evaluation:**
You will be evaluated on all the presentations and final products at the end of the semester. Parts of the evaluation include:

1. Your preparedness and timely delivery of the 3 presentations. *Project points: 15*
2. The completeness and originality of your final products. If you have fulfilled at least one of the following: created a new security lab, or replicated a conference paper completely with coding and testing, or performed security assessment thoroughly on a system or product you may receive full points on originality. The completeness of your deliverables, i.e., code, documentation of the hack and testing, as well as suggestions for resolution, will be evaluated. *Project points: 50*
3. Final presentation and paper: a professional presentation with a well written scientific paper that can be presented at a conference or workshop. *Project points: 35*

**Project topics**
You may choose one of the options: security assessment, lab generation, or tools.

**Security assessment**
This project requires you to:

1. **Understand** a specific networking or communication protocol, software or hardware device (running software).
   1. You should feel free to limit your research to specific aspects of the target if it is very complicated.
   2. If a project requires the purchase of software or hardware, do not spend too much money! Throwing money at a problem should be a last resort, and it can reduce the value of the project.
2. **Analyze** the target for security vulnerabilities. You might want to limit yourself to a particular implementation (say, in a particular operating system). If possible, suggest methods of improving the security. The less you can change (and improve security), the better.
3. **Present**
   1. *Your own* understanding of the target's operation.
   2. A security analysis of the protocol's vulnerabilities and suggested security improvements.
   3. A live exercise for the class demonstrating an interesting (but legal and ethical!) misuse of the target.

**Suggested targets:**

1. Protocols:
- Network Time Protocol (NTP): reproduce the known **NTP buffer overflow vulnerability** using scapy. Explore if you can create a new variation of a buffer overflow for NTP.
- HTML 5: Study the OWASP HTML 5 Security Cheat Sheet. Write your own website that uses at least two of the listed vulnerabilities and pen test it to prove that it is secure.
- Tor: prove that anonymity can be compromised with a Tor network. First, complete the following lab on anonymous traffic using Tor on GENI. Then intercept the traffic and consider methods that anonymity can be compromised. Install a DNS server and check this resource on how DNS affects Tor’s anonymity. Reproduce the result on GENI.
- Simple Message Transfer Protocol: Setup a topology with an SMTP server and clients on GENI. Test for at least 10 known SMTP vulnerabilities. You may use this source or others of your choice.
- Internet Message Access Protocol: Create an IMAP server on GENI and test it for injection and at least two more known vulnerabilities.
- Bitcoin: First follow the instructions in the following GENI lab: [https://witestlab.poly.edu/blog/get-rich-on-fake-bitcoins/](https://witestlab.poly.edu/blog/get-rich-on-fake-bitcoins/). Then reproduce the potential bitcoin vulnerability described in [MIT Technology Review](https://mitreview.mit.edu/).  

2. **Software**: for this topic you will need to reverse engineer and test the software for known vulnerabilities and replicate at least three software vulnerabilities such as data theft, unauthorized access, or data sniffing. Again a proof of concept is needed, such as data logs, personal data compromised, etc.
   - Android contacts app (or e-mail or calendar)
   - Google maps
   - Apache httpd

3. **For all the hardware devices you need to exploit at least one known vulnerability, show a good proof of concept that may include wireshark traces, video or live demo of the exploit, other data from the exploit such as**
   - **Hardware1**: The following items Can be found at the XLab and the makers lab. You may borrow these in a FCFS basis. system logs, etc.
     1. Smart light
     2. Parrot AR.Drone 2.0 quadcopter:
     3. Wireless security camera
     4. Amazon Echo
     5. Google Home
     6. Trusted Execution Environments such as ARM Trustzone
     7. Electronic Locking System (e.g. from Onity)
     8. Router
   - **Hardware2**: Currently we do not have these items in the XLab. Please, do not hesitate to ask early in the semester for a purchase. The earlier you ask, the sooner I can buy these. Please, first look for potential known vulnerabilities, then request to buy:
     1. WiFi-Enabled Programmable Thermostat (e.g. Nest)
     2. Point of Sale (Square etc.)
     3. Smart plug
4. Smart clothing  
5. Smart toys

Lab generation

The objective of this project is to:

- Learn in detail a popular penetration tool.
- Give a presentation about the tool to the class.
- Design a lab/tutorial making use of the tool, to be performed by all other students in the course.

You will have to provide a solution manual for your lab/tutorial.

Suggested lab topics:

- Penetration testing lab on GENI: create one vulnerable VM with at least ten different exploits.
- Cyber range on GENI: create a large topology (at least 30 VMs) with at least ten different VMs that are vulnerable to known exploits.
- Cyber defense on GENI: create a lab similar to the Snort IDS lab of your homework, where students will have to configure a firewall to reflect a set of at least ten different known network attacks.
- IoT Lab: build a lab with inexpensive IoT such as IP cameras, routers, etc. where students are discovering known vulnerabilities. Your lab should include at least three different IoTs.
- IoT Search Lab: build a lab on detective work and searches with Shodan or Censys. The lab should include at least one IoT that you have locally in your ownership and then the students can test it for different known vulnerabilities. The lab should also include students using the Shodan/Censys API, build interesting reports, and data analytics.
- Vulnerable app lab: create a software application in a high-level language (Java, PHP, C++, etc.) or a mobile app (Android preferred). Include at least ten different known vulnerabilities in your application.

Suggested tools

Create a similar tool or extend the following:

- Snort, Suricata, Bro: you may improve these IDSs by adding to the code base.
- Recon-ng
- Nikto
- Nmap for IoT
- Honeynet: create your own IoT honeypot with off the shelf tools. You may use a set of unsecured IP addresses in the XLab for your experimentation.
- Simulation: create a simulation or emulation tool for the following topics:
  - Worm propagation – you may use the Mirai worm as a sample.
  - Adversary behavior – use the Mitre ATT&CK website for tactics and behavior samples.
  - Defender behavior – implement simulation of basic defense techniques against specific attacks.