1 Culminating project

The project is meant for you to delve into a specific topic of computer security that interests you. Projects are meant to be instructive and fun. We encourage and expect you to apply yourself. We want you to find a project that you are *passionate* about, some topic you really hungered to sink your teeth into. You can take chances: Failure is OK as long as you fail well and deservedly.

What is important is that you use your creativity, your knowledge, your intuition and your energy to grapple with an aspect of computer security.

You are encouraged to work in pairs, but you do have the option to work alone, if you prefer.

1.1 Timetable

Here are the critical dates in the project:

Ongoing : Bounce ideas off Daniel and Lyn

Nov. 1st : Proposal due Comments will be returned by November 7th.

Nov. 17th : Progress report Hand in in a description of the work you have done on your project so far.

Dec. 1st – 12th : 30 minute group presentation in class.

Please refer to http://cs.wellesley.edu/~cs342/TechnicalPresentations.pdf on how to give a technical presentation.

Dec. 12th : First draft of your final report Draft is returned by Friday Dec. 15th

Dec. 21st : Final reports due

1.2 Proposal

One page long, due Wednesday, November 1st, e-mailed and in hardcopy, with both your names and containing the following sections:

1. **Introduction and motivation**: What you want to do and why it is worthwhile doing

2. **Deliverable**: What will be the result of your project (research paper, survey paper, computer program, proof-of-concept, data results, step-by-step guide, etc)

3. **Methodology**: How are you going to produce the deliverables (implement something, design the prototype, do a survey, test its functionality etc)
4. **Sources**: Where you will find what you need to know to do this?
5. **Milestones**: This is your insurance policy with us if your project fails (which can happen). We would like 4 or 5 milestones (that includes the final deliverable) on the way to the end result. It is also for your benefit so that you can track your progress.

1.3 Final Report

Due December 21^{st}, your reports should thoroughly cover your topic and work that you have done. Somewhere between 12-20 pages long (please not 10 pages of screenshots) and have the following sections:

1. **Introduction**: Include a problem statement here
2. **Background** : Some background research on the state of the art in this area
3. **Statement of Work**: What you did and how you did it
4. **Results** : What tentative conclusions you have reached? If you have negative results, discuss them, too.
5. **Conclusions** : Recap and forward-looking, including recommendations for other work in this area.
6. **How-to guide**: If other people want to do what you did or you wanted to reproduce your work , how would one go about it? Include tips/caveats

You will also make a presentation (30 minutes) in class beginning of December.

2 Appendix

2.1 Sample proposals

2.1.1 Some ideas

- Evaluate the security measures for one or more of the electronic systems you use at Wellesley: the CWIS, FirstClass, puma, wilbur, on-line course registration, and on-line SEQs.

- Implement a honeypot and report on what you find.
- Research security holes that have been fixed since Fedora 9 and write exploits that take advantage of the security holes in Fedora
- Design and possibly implement a security protocol for a problem of interest to you.
- Report on issues in electronic voting.
- Study information warfare (how vulnerable are companies and countries?)
- Write your own rootkit or experiment with an existing one.
- Study denial of service attacks and countermeasures.
- Experiment with firewalls.
- Report on the security features/holes of a chosen programming language
- Study/implement security features for e-commerce.
- Experiment with cryptographic protocols.
- Investigate the security issues in Microsoft's Next-Generation Secure Computing Base architecture.
- Study/evaluate biometric authentication.
- Report on video surveillance.
- Study security issues associated with wireless systems.
- Study security issues associated with radio frequency identification (RFID) systems.
- Study watermarking and/or steganography.
- Study systems for prevent digital piracy and means for circumventing these systems.
- Study viruses and/or virus protection programs.

- Evaluate an existing virus protection program.
- Study a class of viruses/worms in depth.
- Study spyware and/or spyware protection programs.
- Evaluate and compare security tools: e.g. tools for hardening Linux (Bastille, LIDS, Openwall patches), scan detectors, etc.
- Report on electronic money.
- Report on zero-knowledge proofs.
- Experiment with Linux exploits/tools not covered in class.
- Study MULTICS and compare its security features to LINUX.
- Investigate the benets/drawbacks of smart cards.

2.1.2 Excerpts from Proposals

These are excerpts from some sample proposal introductions from prior years:

HyperPacket

An experiment in anomaly detection, HyperPacket is a framework and a tool for modeling and analyzing network activity, for finding and characterizing malicious attack-traffic amongst the good and benign. A good anomaly detection based network intrusion detection system has been a holy grail of the security world. In theory, a good anomaly detection based system has the potential to identify new attacks before the security community has been able to research the attacks and identify its fingerprints, an feature which is fundamentally impossible for traditional rule based intrusion detection systems. However, anomaly detection schemes need to be able to accurately build a model of normal network traffic. This is indeed a tricky problem. Solutions generally involve complex theoretical mathematical modeling techniques. In general, these models have proven to be sensitive and tend to flag new benign network usage as suspiscious behaviour.

Auditing Wireless Linksys Router

The goal of our project was to learn about the process of discovering and exploiting vulnerabilities in network devices. A compromised network device could be used to mount a DDoS attack or as a tool in a further attack against the network on which it is located. The network devices that we chose to explore for security holes, or ”pen test”, are wireless routers made by Linksys (a Cisco subsidiary). The choice of Linksys devices was made because of their widespread use in homes and small businesses in the US today. The process of finding and exploiting vulnerabilities on these devices started with researching the devices themselves. We were able to find the source code for one of our routers. This allowed us to do a static analysis of the code to try and find an exploitable buffer overflow. The other router did not run on publicly available code, so it was tested for vulnerabilities using a ”black box” approach. This included researching the device on the Internet and then performing a number of attacks and closely observing the results.

Cyberlaw

So, you’ve just taken cs398 and you have a whole toolbelt of skills on your trousers. Now, you’ve told Dr. Bilar that you won’t do anything illegal with these new skills. But if you can’t do anything illegal, what the hell can you do with them? We will look deeply into the policies and laws of the cyber world to try to find what you can do legally, and what the consequences might be if for some reason you used your skills for bad, naughty purposes.

Computer Forensic Techniques

Computer Forensics is the use of specialized techniques for recovery, authentication, and analysis of electronic data. These techniques are used when a case involves issues relating to reconstruction of computer usage, examination of residual data, or explanation of technical features of data and computer usage. Forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel.

It also includes the analysis of data processing equipment– typically a home computer, laptop, server, or office workstation– to determine if the equipment has been used for illegal, unauthorized, or unusual activities. It can also include monitoring a network for the same purpose. Forensics is used to do data recovery, data hiding, email recovery, and password recovery. All of the above fall under the general scope of incident response.

SecSysD–An Exploration into IDS

A centralized analyzer and console manager that could potentially pool the alerts from various independent IDSs, analyze the alerts centrally, from which a global view of the state of the network could potentially be visually displayed. As a specific implementation of our idea, we targeted snort for Linux machines, though theoretically any number of IDSs could be implemented simultaneously.

Implementing GPG

GNUPG is the GNU projects free replacement for Pretty Good Privacy developed by Philip Zimmerman in the early 90s. GNUPG implements the OpenPGP Internet standard as described in RFC 2440. As such it is compatible with most other public key cryptoapps out there. GNUPG provides all of the desirable functionality that was discussed above in a very neat package. My project was to implement this software on the local machines, and incorporate it into the two most popular mail programs, Pine and Mutt.

LaBrea Tarpit: Implementation and Analysis

Worms and crackers are quite possibly the most difficult part of a network administrator's job. A recent development in the area of network security has facilitated the process of stopping, or at least slowing, the progress of these sources of traffic. Honeypots listen on a network for types of traffic which, when detected, can only be bad. They then can take action based on the traffic that was detected. Our project was the installation, configuration, and testing of LaBrea, a tarpit, or sticky honeypot. In the words of its creator, "LaBrea takes over unused IP addresses on a network and creates 'virtual machines' that answer to connection attempts. The program answers connection attempts in such a way that the machine at the other end gets 'stuck', sometimes for a very long time."