Final Assignment (Graded)

Write a report about your experience with solving problems in security labs this term. The report should include and reflect on all cryptography and security related topics discussed during the lab, such as: Vigenère Cipher, RSA algorithm, cryptographic tools, security monitoring and vulnerability. The report will be graded according to the following:

This should be a short report (5-10 pages) - not an essay - and use as many tables and diagrams and code examples as you can. It is not an ESSAY! **No plagiarism:** Copy and paste is not allowed and will lead to zero marks. All used sources have to be referenced.

Implementation of Vigenère and RSA 20%

Implement the Vigenère Cipher and RSA algorithm in a programming language of your choice (see first two labs for more detailed descriptions) and document your implementation with code samples and a reflection on your own experience during the process.

Cryptographic Tools: 20%

Use Sagemath (http://doc.sagemath.org/html/en/thematic_tutorials/numtheory_rsa.html) and OpenSSL (https://www.openssl.org/docs/manmaster/man1/rsa.html) to prove that your RSA and Vigenère implementations work and reflect on the usage of the tools. Explain the options these tools give you in order to use the ciphers.

Security Monitoring and Vulnerability: 20%

Explain security monitoring with Nagios and describe how it can be used to increase security in a network. Identify ten vulnerabilities in applications, networks and protocols and find exploits that can take advantage of these vulnerabilities. Explain how the exploits work.

Kali Linux: 20%

Install Kali Linux in a virtual machine or use a live image. Use it to answer the following questions:

1. What's your computer's IP address for its current Internet connection? (How can you tell the difference between your Ethernet IP and your wireless IP if you have both connections active?)
2. How can you determine the IP address associated with a given host name?
3. How can you determine the host name(s) associated with a given IP address?

4. How can you copy a file from one computer to another? Or more to the point, if you create a file on the Kali virtual machine and you want to put it someplace where you can save it, how do you go about it from the Kali command-line interface?
5. How can you tell whether there's a process listening on a given port (e.g. port 80 or port 22) on a given host?
6. How can you tell which ports have processes listening on them on a given host?
7. How can you retrieve and save a given web page (say http://google.com/ in a file on your system?
8. How can you view the HTTP headers sent back from a specified web server when you request one of its pages?
9. [Super bonus question] Is there a command-line-only way to view the HTTP headers that *my* computer sends when I run the commands in the previous two questions?

What is the difference between Kali Linux and other linux distributions? How does it support computer security?

Discussion: 20%

Based on the contents of your report, discuss your experience with implementing cryptography algorithms, using crypto tools, security monitoring and vulnerability, and using Kali Linux. Reflect on your own experience during the labs and information you gathered while working on the report. What is your personal opinion of security after this lab and how has it changed compared to your previous impressions.