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: Classical encryption techniques, cryptographic tools, security monitoring and vulnerability and penetration testing. Use the Kali LInux you installed during lab to complete all assignments. 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. Which means, every time you use text or code from another source this must be clearly marked and the source must be included in your report (use either footnotes or a reference section at the end of the document).

Decrypting a Monoalphabetic Ciphertext 20%

Decrypt the following message and document all steps in detail (your evaluation will not only depend on the correct plaintext message, but also on the quality of documentation) using frequency analysis and general cryptanalytic techniques:

Om ol b htkogr gy eoxos cbk. Ktzts lhbetliohl, lmkoqofu ykgd b iorrtf zblt, ibxt cgf mitok yoklm xoemgka buboflm mit txos Ubsbemoe Tdhokt. Rwkofu mit zbmmst, Ktzts lhotl dbfbutr mg lmtbs ltektm hsbfl mg mit Tdhokt'l wsmodbmt ctbhgf, mit RTBMI LMBK, bf bkdgktr lhbet lmbmogf comi tfgwui hgctk mg rtlmkga bf tfmokt hsbftm. Hwklwtr za mit Tdhokt'l lofolmtk butfml, Hkofetll Stob kbetl igdt bzgbkr itk lmbklioh, ewlmgrobf gy mit lmgstf hsbfl mibm ebf lbxt itk htghst bfr ktlmgkt ykttrgd mg mit ubsbva. Om ol b rbkq modt ygk mit Ktztssogf. Bsmigwui mit Rtbmi Lmbk ibl zttf rtlmkgatr, Odhtkobs mkgghl ibxt rkoxtf mit Ktzts ygketl ykgd mitok iorrtf zblt bfr hwklwtr mitd bekgll mit ubsbva. Txbrofu mit rktbrtr Odhtkobs Lmbkysttm, b ukgwh gy ykttrgd youimtkl str za Swqt Lqacbsqtk ibl tlmbzsolitr b ftc ltektm zblt gf mit ktdgmt oet cgksr gy lgmi. Mit txos sgkr Rbkmi Xbrtk, gzltlltr comi yofrofu agwfu Lqacbsqtk, ibl rolhbmeitr migwlbfrl gy ktdgmt hkgztl ofmg mit ybk ktbeitl gy lhbet. Swqt Lqacbsqtk ibl ktmwkftr mg iol igdt hsbftm gy Mbmggoft of bf bmmtdhm mg ktlewt iol ykotfr lbf Lgsg ykgd mit eswmeitl gy mit xost ubfulmtk Pbzzb mit lwmm. Sommst rgtl Swqt qfgc mibm mit ubsbemoe tdhokt ibl ltektmsa ztuwf egflmkwemogf gf b ftc bkdgktr lhbet lmbmogf txtf dgkt hgctkyws mibf mit yoklm rktbrtr Rtbmi Lmbk. Citf egdhstmtr, miol wsmodbmt ctbhgf coss lhtss etkmbof rggd ygk mit ldbss zbfr gy ktztsl lmkwuusofu mg ktlmgkt ykttrgd mg mit ubsbva.

Include both, the plain text and a documentation of your decryption process into the report. State clearly what you did and which approach you used and don't forget to include any diagrams or pictures you produced.

Password Cracking: 20%

The website yellow-wasp-28.loca.lt/top-secret uses basic authorisation to hide content. When first visiting the site click the blue “Click to Continue” button. Use a parallelised login cracker (such as THC Hydra) to get access to the hidden content. Document the whole process with text and screenshots and reveal the secret. The evaluation includes both your documentation and the proof of a successful login. If you can’t complete the hack you can still get points for your documentation of the attempt.

Hack into a Server: 20%

Go to https://www.hackthebox.eu/home/start and pick a lab machine to hack. Document the process and explain every step in your own words. Again, your documentation and explanations will be the main part of the evaluation.

Public Key Encryption: 20%

Download my public key yellow-wasp-28.loca.lt/bojan.key and use it to decrypt the following message: yellow-wasp-28.loca.lt/picard.txt.asc. Send me a reply and submit your public key + encrypted text or add links to your report.

Kali Linux: 10%

Use your Kali Linux 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: 10%

Based on the contents of your report, discuss your experience with cryptography, using crypto tools, password cracking, penetration testing, 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.

Use the slack channel for any questions.

Good luck!