University of Dar es Salaam, College of ICT
IS364: Principles of Systems Security
Semester 2, 2024

Lab 2: Cryptography | Instructor: Dr. Hellen Maziku

Lab Reference;

1. Hands-On INFORMATION SECURITY Lab Manual, Fourth Edition, Michael E. Whitman, Cengage Learning
2. TryHackMe: https://tryhackme.com/

Due Date: 19th April 2024 – utilize this week's lab sessions to complete the lab

In the first lab, you were introduced to the key concepts of cybersecurity including three fundamental tools we can use to address a wide range of security vulnerabilities and threats that aim to compromise security goals. This lab focusses on cryptography, which is one of the tools.

NOTE: This lab is completed individually.

I assume we have all completed the lab preparation step:

Navigate to https://tryhackme.com/ and register. Make sure your username is as follows = surname+groupnumber+coict. For example, maziku5coict. Make sure you follow this username creation guideline, otherwise, you will not be graded.

Tasks:

Search the following rooms to complete the concepts covered within the rooms;

1. Introduction to Cryptography

In this rooms, complete all the 9 tasks; Introduction, Symmetric encryption, asymmetric encryption, Diffie-hellman key exchange, hashing, PKI and SSL/TLS, authentication with passwords, cryptography and data – example and conclusion. You should answer all the questions in each task. After you have completed, the room should show, 100% completed.

Note: To complete this lab, you will have to download, install and configure OpenVPN so that you can connect to TryHackMe machines and execute the labs for tasks 2 to 6. Your lab will be considered incomplete and not graded if you will not have OpenVPN working in either Linux or windows. The lab instructor will cross-check your terminal to see that you are indeed **connecting to the machine using your username, e.g., "maziku5coict@TryHackMe$",** and that you have successfully completed the tasks.

2. Encrypting HTTP using SSL/TLS

Navigate to this blogpost: How does HTTPS actually work?

Link: https://robertheaton.com/2014/03/27/how-does-https-actually-work/ Read all the five sections to understand how HTTPS works, how SSL/TLS works, concept of certificates and digital

signatures and some cool real-life scenarios. Click on all the shared links and summarize the content on the external links shared in the blog.

3. Breaking RSA encryptions

Pre-requisite: Visit the RSA Wikipedia page to understand in detail the math behind RSA encryption (you will require to summarize this in your presentation).

Now consider the RsaCtfTool tool, which is a utility designed to decrypt data from weak public keys and attempt to recover the corresponding private key. This tool also offers a comprehensive range of attack options, enabling users to apply various strategies to crack the encryption. The RSA security, at its core, relies on the complexity of the integer factorization problem. The RsaCtf project (Link: https://github.com/RsaCtfTool/RsaCtfTool) serves as a valuable resource by combining multiple integer factorization algorithms, effectively enhancing the overall decryption capabilities. Please note that this tool is primarily intended for educational purposes. Follow through the following links as tutorials on Cracking Weak RSA Keys using RsaCtf tool

Link: https://www.youtube.com/watch?v=ki29gJbtlvs

Then solve the following RSA decryption challenges:

a. https://infosecwriteups.com/synkcon-ctf-2021-not-hot-dog-writeup-90b0f9d027f0
b. https://stackoverflow.com/questions/76728134/rsa-ctf-encrypt-and-decrypt

Show clear workings and the step-by-step guide how you captured the flags.

Added resource: You can also find a collection of such challenges here:

https://medium.com/@hva314/some-basic-rsa-challenges-in-ctf-part-1-some-basic-math-on-rsa-5663fa337c27

Submission:

i. Each individual must complete all lab sections individually, especially lab tasks 1 and 3 that require individual practice. Submit to your team evidence that you have completed the practicals. This will be attached to the end of the slides and submitted together with the team presentation.
ii. For tasks 1 to 3, all materials including room contents, questions, scenarios, blogpost content, and notes on breaking RSAs should be summarized in a presentation which will be presented during lecture sessions. The presentations should be prepared and submitted in groups; HOWEVER, each individual should complete practical tasks individually to answer room questions and obtain a certificate. Also, evidence on catching flags should be submitted. Each group should include in the presentation evidence that each member completed every room and the practice on RSA encryption.
iii. Note that the practical and lecture sessions in class will be used to assess and grade each individual as they complete the rooms. Therefore, for each class, you must come with a laptop and ability to access the tryhackme account