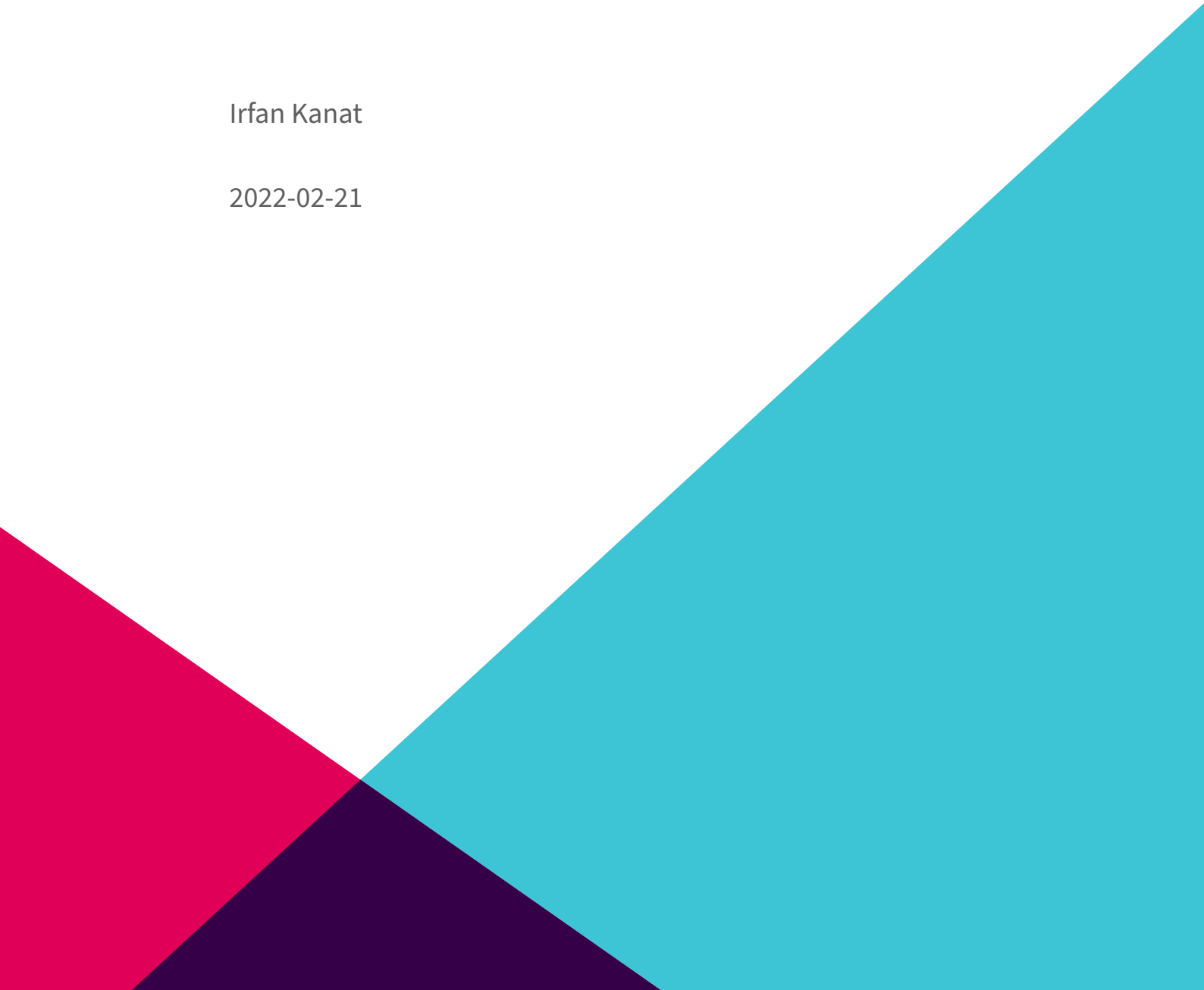# Cybersecurity Foundations

Irfan Kanat

2022-02-21

Cybersecurity Foundations

This course is designed to introduce the technical aspects of the foundations of cybersecurity to a non-technical audience.

Many of the modules here can be carried out without any prior experience with computer science topics. Yet, we still have included activities that more technically inclined students can still enjoy.

In module 2 (computer networks) and module 6 (cryptography) we included two activities each, one more technical, the other less technical. The more technical activities are noted in each modules readme file.

Modules 4 and 5 (the most technical) require access to a computer with unix like shell (Linux or Mac). We used Haaukins platform for these modules. You may be able to use Mac computers or live boot from a Linux usb. If your students are not technically inclined, you may also choose to skip these two modules.

Below is a list of modules included in this course.

01 Threat Landscape

This module introduces the students to various threat actors, and common methods threat actors employ to gain access.

02 Computer Networks

This module introduces students to TCP/IP protocol stack and routing for the internet. We recommend two class sessions be dedicated to this module.

04 Operating Systems and Commandline

This module introduces the students to the unix command line and shell scripting.

06 Cryptography

This module introduces the students to cryptography and how it can be used to achieve authentication, confidentiality, and integrity online.