Purple Team Playbook: Threat Modeling for Security Testing

Felisha Mouchous

Technical Report

RHUL–ISG–2020–7

22 June 2020

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

ABSTRACT

The reality with information security is that we cannot completely mitigate the threat of an attacker getting into our networks. Organisations can, however, control how they prepare and react to attackers by understanding how they operate. Threat modeling and security testing provide a way to first identify the threats and then simulate how an attack can take hold. In order to fully understand the threats, employees need to have the right information at the right time so that they are fully equipped to match the attacker's capabilities. To do this, the red and the blue team in an organisation must work together to simulate attacks and test their defences.

In this thesis we first explore the available threat models and how they can apply to security testing in an organisation. Based on the research we have conducted and our own knowledge on security testing, we have created a Purple Team Playbook Framework. The purpose of this framework is to allow organisations to leverage existing data on threats, attack techniques, defences and asset data so that they can get the red and the blue team working together. By using this framework, organisations can effectively identify where they have gaps in their defences and how they can simulate threat actor behaviour, in order to assess how they can address these security gaps. To this end, we have formulated proof of concept scenarios to show how this framework can be used in an organisation and how it helps address the challenges with threat modeling and security testing.