Preface

It was just another day at work, as usual we were supposed to configure some scans, validate some results, and perform some manual tests. We have been working with our team on some pentesting projects. Unlike many other jobs pentesting is not that boring, honestly who doesn't enjoy finding flaws in someone's work and get paid for it. So following the process we did some recon and found some interesting information about the target. We started digging deeper and soon we had enough information to compromise the target. We finished the rest of the process and send out the reports to the clients, who were more than happy with the results.

Later that evening we were discussing about the tests and realized that most of the information, which allowed us to get a foothold in the target was actually public information. The target has already revealed too much about itself and it was just a matter of connecting the dots. It ended here and we almost forgot about it. Another fine day we were working on some other project and the same thing happened again. So we decided to document all the tools and techniques we were aware of and create a shared document, which we both could contribute to. Anytime we encountered some new method to discover public information, we added it to the document. Soon we realized that the document has grown too long and we need to categorize and filter it.

Though the topic has been known and utilized in pentesting and red team exercises widely yet when we tried to find documented work on it, we didn't find anything substantial. This is where we started thinking of converting our document into a book.

While researching about the topic we understood that there is too much public information, which is easily accessible. Most of it might not seem very useful at first glance but once collected and correlated, it can bring phenomenal results. We also realized that it is not just pentesting where it is of prime importance to collect information about the target, but there are many other professions, which utilize similar methods, such as sales reps find information about prospective client, marketing professionals collect information related to market and competition. Keeping that in mind we have tried to keep the tone and flow of the book easy to follow, without compromising on the technical details. The book moves from defining the basics to learning more about the tools we are already familiar with and finally toward more technical stuff.

WHAT THIS BOOK COVERS

Hacking Web Intelligence has been divided into different sections according to the complexity and mutual dependency. The first few chapters are about the basics and dive deep into topics most of us are already familiar with. The middle section talks

about the advanced tools and techniques and in the later portion we will talk about actually utilizing and implementing what we discuss in previous sections.

While following the book it is suggested to not just read it but practice it. The examples and illustrations are included to understand how things work and what to expect as a result. It is not just about using a tool but also understanding how it does so as well as what to do with the information collected. Most of the tools will be able to collect information but to complete the picture we need to connect these dots. On the other hand like any tool, the ones we will be using might be updated, modified, or even depreciated and new once might show up with different functionality, so stay updated.

HOW DO YOU PRACTICE

A desktop/laptop with any operating system. Different browsers such as Mozilla Firefox, Chrome or Chromium, and internet connectivity. Readers will be assisted to download and install tools and dependencies based on the requirement of the chapter.

TO WHOM THIS BOOK IS FOR

The book would focus mainly on professionals related to information security/intelligence/risk management/consulting but unlike "from Hackers to the Hackers" books it would also be helpful and understandable to laymen who require information gathering as a part of their daily job such as marketing, sales, journalism, etc.

The book can be used in any intermediate level information security course for reconnaissance phase of the security assessment.

We hope that as a reader you learn something new which you could practice in your daily life to make it easier and more fruitful like we did while creating it.

Sudhanshu Chauhan
Principal Consultant, Noida, India

Nutan Kumar Panda
Information Security Engineer, Bangalore, India