PMAT Review

PMAT - TCM Security Review

This review is about the **Practical Malware Analysis and Triage** course by HuskyHacks (@HuskyHacksMK) on the TCM Security Platform. I took this course a while back and want to do my part by reviewing it. I'll keep it short, I don't like overly long reviews.

What's my background?

I read the *Practical Malware Analysis* book before taking this course and have done a lot of reverse engineering (mainly malware) prior to that. I code, pentest and do security work for a living. Malware analysis is something I do on the side and has become somewhat of a passion. I tell you this mainly to give perspective about my viewpoint. I'm not a complete beginner, but someone seeking to learn more.

Why did I take this course?

My goal was to learn more about malware analysis. In the past, I focused more on the reverse engineering side and I wanted to get a more holistic view. Also, I wanted to have a certificate I can show in case I decide to apply to a malware analysis position in the future, or some other position asking for this kind of knowledge.

Alright, now that we got that covered, let's get on with it :^)

Review

I highly recommend this course, it gives you:

- a safe environment to analyze malware in + best-practice methods you can use beyond the course
- static and dynamic analysis primers and tools, knowledge from the ground up
- analyzing malicious documents
- malware delivery (vbscript, powershell)
- writing (good) reports
- golang malware, android malware
- sandboxes, automated analysis
- analyzing full samples made for the course on your own

and much more. You get a holistic course with practical aspects covered. It pretty much doesn't get any better in my opinion. In addition, Matt is a great instructor, he's extremely proficient at explaining things. The videos are on point, they are short and concise without fillers. The tools you use in this course are free of charge. It's not showing things in IDA Pro, which costs a fortune, instead it uses Cutter and a free Windows VM.

The most important part of the course are the challenges and practical bits. It just doesn't get boring, you can follow along, gain experience and the challenges really help you to "get it" (while being fun as hell). So, to get the most out of this course **do the challenges and follow along**.

There is one thing I have to mention here: **x86 and x86_64 assembly**. I get the impression that lots of people think they can learn this from a course. In my opinion, that is not possible. While you can learn the *why* and *what* from a lecture, you can never gain experience and really get things to sink in. Expecting to learn and become proficient at any language from a course is like expecting to gain muscle by reading a book about weightlifting. It's not gonna happen, it takes time and practice. The approach taken in this course is realistic and honest. Matt clearly explains the most important aspects and gives a nice overview you can work with. With that, you are well equiped to analyze the samples in this course and beyond.

In summary, I think this course was great. A very good instructor and a well thought out course structure give you what you need to get started in malware analysis. The course is very much **beginner friendly**. In my opinion it is suitable for anyone with enough interest in the topic.

After this course, you will know the basics and you will have a **solid foundation** you can build upon. You can use this to your advantage in an interview, mainly because you can not only say "yeah, I heard about it in a lecture once" but "yeah, I did that, I worked on a challenge". As someone who has interviewed job candidates, I can tell you **practical experience** makes a huge difference. The price is also more than fair, in my opinion, you get a lot more content than you actually pay for, I mean come on: about thirty bucks for all of that content?! I think you get great value for very little money.

Last thing: Join the Discord server if you get the course, the community is very friendly (and there are lots of cat pictures).