Practical Malware Analysis & Triage

Arm yourself with knowledge and bring the fight to the bad guys. Learn the state of the art of malware analysis and reverse engineering.

Course Overview

Arm yourself with knowledge and bring the fight to the bad guys! Practical Malware Analysis & Triage (PMAT) brings the state of the art of malware analysis to you in engaging instructional videos and custom-made, practical labs.

Welcome to Practical Malware Analysis & Triage. I'm Matt, aka HuskyHacks, and I'm excited

to be your instructor for this course. I had a blast putting it together and I hope that you will come along with me and learn the art of splicing, slicing, inspecting, and dissecting malware samples.

Featuring two malware analysis lab build options: local virtual machines and a rapid-deployable cloud malware analysis network! Learn how to spin up a malware analysis network on AWS from anywhere in the world!

Skill Level

Basic-Plus to Intermediate. The course includes a selection of advanced topics. All concepts are taught in an accessible, foundational manner.

Why Take the Practical Malware Analysis & Triage Course?

This course is centered on practical labs that bring malware samples to bear in a safe, controlled environment.

First, you will learn to handle malware safely and construct an isolated lab environment. Then, you will learn the basics of malware analysis on samples designed to teach you the core analysis concepts. As the labs progress, the level of offensive tradecraft employed by these samples grows.

By the end of the course, you'll be using automated workflows and advanced analysis to extract key facts about real-world specimens.

Finally, and most importantly, you'll learn the keys to writing detection rules and triage reports to tell the world what you have learned.

What Will I Receive from this Course?

- Access to the student-only channel on Discord to receive support from the instructor and other students.
- Access to 9+ hours of engaging, instructional video content.
- Access to the PMAT Lab repository containing dozens of malware samples designed to teach you the fundamentals.
- Course completion certificate.

System Requirements

- Basic IT knowledge.
- Knowledge of the general classes of malware (virus, trojan, worm, etc). Knowledge of how these malware classes function on the technical level is **not** required.
- Comfort in the command line of Linux and Windows. All tools and techniques taught in the course are explained step-by-step but working knowledge of Bash and the Windows command prompt is recommended.
- For a local lab build, you need:
    - A computer that:
        - Has at least 6GB of available RAM.
        - Has at least 40GB of available storage.
        - Can run Oracle VirtualBox and host two lab virtual machines at the same time (with the option to host a third for additional development).
        - Has an internet connection.
- For a cloud malware analysis lab, you need:
    - An AWS account and a way to pay for AWS resource utilization.
- Knowledge of x86 Assembly and other low level computer programming concepts is **not** required.

Recommendations

- Familiarity with programming concepts is recommended but not required.
- Familiarity with offensive cybersecurity Tactics, Techniques & Procedures (TTPs) will be helpful but is not required.

Practical Malware Analysis and Triage Course Objectives

Course Topics

1. **Safety Always!** Build good habits for handling malware safely and create an analysis lab.
2. **Safe Malware Sourcing**. Learn where to source malware samples safely (no need for the dark web!).
3. **Basic Analysis.** Learn basic analysis methodology, including interpreting strings, inspecting Windows API calls, identifying packed malware, and discovering host-based signatures. Then, detonate malware to collect network signatures and identify malicious domains and second-stage payloads!

4. **Intro to the x86 Assembly Language.** Dip your toes into the low-level world of Assembly Language! Learn the foundations of x86 Assembly and use it to perform advanced analysis.
5. **Advanced Analysis.** Use sophisticated tools like Cutter and x32dbg to discover key insights about malware samples at the lowest possible level. Control the execution flow of a program and manipulate its low-level instructions in a debugger.
6. **Patch It Out: Binary Patching & Anti-analysis**. Learn the crafty practice of patching binaries at the ASM level to alter the flow of their programs. Then, learn to identify and defeat anti-analysis techniques.
7. **Gone Phishing.** Learn to analyze malicious documents and document-delivered malware, including malicious macros and remote template injections.
8. **What the Shell?** Learn to identify and carve out embedded shellcode.
9. **Off Script.** Identify scripted, obfuscated malware delivery techniques that use PowerShell and Visual Basic Script.
10. **Stay Sharp.** Decompile and reverse engineer C# assemblies and learn about reverse engineering the .NET Framework! Then, reverse engineer an encrypted malware C2 dropper back to near-perfect original source code with DNSpy!
11. **Go Time.** Learn the analysis considerations of malware written in Go.
12. **Get Mobile!** Use MobSF to reverse engineer malicious Android applications.
13. **The Bossfight!** Use everything you have learned to do a full analysis of one of the most infamous malware samples in history.
14. **Automating the Process.** Use Jupyter Notebooks and malware sandboxes to automate the analysis process.
15. **Tell the World!** Write YARA rules to aid in the detection of malware samples and learn how to write effective analysis reports to publish findings.
16. **Course Final.** Apply everything you've learned to display your mastery of the art and science of malware analysis!

Who Should Take the Practical Malware Analysis & Triage Course?

- **IT professionals** of all skill levels who are looking to gain foundational knowledge of malware analysis.
- **Network defenders** looking to deepen their knowledge of the state of the art of malware analysis.
- **Penetration Testers/Red Teamers** looking to pick up the skill of malware analysis to increase tradecraft/provide higher threat emulation fidelity.
- **Anyone** who wants to learn an in-demand skill set and bring the fight to the bad guys!

Student Reviews:

https://syedhasan010.medium.com/honest-review-of-tcm-securitys-practical-malware-analysis-and-triage-e0285e773523

https://squiblydoo.blog/2021/11/26/review-practical-malware-analysis-and-triage-pmat

https://www.domedion.com/2021/11/24/practical-malware-analysis-triage-review/

https://www.youtube.com/watch?v=Y2Bb8BPEycc&ab_channel=WireDogSec

Cyril H., Cybersec Padawan

"Practical Malware Analysis and Triage, another WAY-beyond-expectation installment in the TCM Academy library! The course progression is excellent, with practical, walk-along exercises in a majority of the videos. I particularly enjoy the rate-of-flow from Husky's pedagogical style -- it has a pristine blend of step-by-step instruction alongside a pace that deters distraction or boredom. Thanks Husky!"

David R., Cybersecurity Student

“It's a fantastic course packed to the brim with information. Everything is explained in a way that makes it very easy to understand. Instead of just spitting information at you, there are built-in challenges that give you an opportunity to put your understanding to the test. This is one if the highest quality courses I've taken in a while, and I couldn't be happier with it.”

Syed H., Security Engineer, DFIR

“The course curriculum is properly designed to take an analyst from the start till the end. I loved how Matt explained concepts to ensure everyone could be on the same playing field.... Should you get it? YES.”

Practical Malware Analysis & Triage Course Curriculum - 10+ Hours

Course Introduction

- Hey, thanks!(0:14)
- Whoami & Course Overview(5:55)
- Course Discord Information

Safety Always! Building Your Malware Analysis Lab & Malware Safety

- Lab Network Options: Local VMs vs. AWS Cloud Lab
- Downloading VirtualBox(2:29)
- Downloading Windows 10(2:05)
- Setting Up the Windows 10 VM(8:12)
- Downloading REMnux(1:10)
- Installing REMnux(2:05)
- Installing FLARE-VM(16:45)
- Analysis Network Setup(7:26)
- INetSim Setup(13:16)
- Host-only Safety & Internal Networks
- Lab VM Repo Link
- Rapid-deployable Cloud Malware Analysis Lab Setup
- Course Lab Repo Link

Course Lab Repo Download & Lab Orientation(4:00)

Taking a Snapshot Before First Detonation(1:29)

Detonating Our First Sample(5:57)

Tool Troubleshooting(5:05)

Course Tool List & Resources

Basic Malware Handling(8:52)

Safe Malware Sourcing & Additional Resources(6:50)

Basic Static Analysis

Hashing Malware Samples(3:45)

Malware Repositories: VirusTotal(2:49)

Strings & FLOSS: Static String Analysis(8:03)

Analyzing the Import Address Table(7:36)

Introduction to the Windows API(6:00)

MalAPI.io(4:08)

To Pack Or Not To Pack: Packed Malware Analysis(9:42)

Combining Analysis Methods: PEStudio(6:45)

Identifying Malware Capabilities & Intro to MITRE ATT&CK

Note Review(1:59)

Basic Dynamic Analysis

Basic Dynamic Analysis Intro: Host and Network Indicators(3:39)

Initial Detonation & Triage: Hunting for Network Signatures(8:44)

- Host-Based Indicators: Procmon Part I(7:44)
- Host-Based Indicators: Procmon Part II(6:06)
- Dynamic Analysis of Unknown Binaries Part I: Analyzing Wireshark(13:02)
- Dynamic Analysis of Unknown Binaries Part II: Host-Based Indicators(21:19)
- Analyzing a Reverse Shell Part I: Correlating IOCs(18:12)
- Analyzing a Reverse Shell Part II: Parent-Child Process Analysis(6:43)

Challenge 1: SillyPutty

- Challenge 1: SillyPutty Intro(1:43)
- Challenge 1: SillyPutty Walkthrough(18:21)

Advanced Static Analysis: Assembly Language, Decompiling, & Disassembling Malware

- Intro to Advanced Analysis & Assembly Language(10:01)
- Disassembling & Decompiling a Malware Dropper: Intro to Cutter(8:46)
- x86 CPU Instructions, Memory Registers, & the Stack: A Closer Look(13:06)
- Revisiting the Dropper: Assembly Instructions and the Windows API(8:17)
- Hello, World! Under a Microscope Part I(18:31)
- Advanced Analysis of a Process Injector(16:56)

Advanced Dynamic Analysis: Debugging Malware

- Getting Comfortable in x32dbg: Flow Control & Breakpoints(12:59)
- Debugging the Dropper: Dynamic Analysis of x86 Instructions & API Calls(17:49)
- Hello, World! Under a Microscope Part II(14:27)

Challenge 2: SikoMode

Challenge 2: SikoMode Intro(1:37)

Challenge 2: SikoMode Walkthrough(20:18)

Bonus Lecture: Live Analysis of Challenge 2 SikoMode Twitch Stream with Taggart

Binary Patching & Anti-analysis

Patch it out: Patching x86 Binaries

Identifying & Defeating Anti-analysis Techniques

Specialty Malware Classes

Specialty Malware Classes

Gone Phishing: Maldoc Analysis

Analyzing Excel Maldocs: OLEdump(10:55)

Analyzing Word Maldocs: Remote Template Macro Injection(7:35)

What The Shell? Shellcode Analysis

Analyzing Shellcode: Carving Shellcode & scdbg(14:29)

Carving Shellcode from Memory(13:00)

Off-Script: Scripted Malware Delivery Mechanisms

PowerShell: Analyzing Obfuscated Scripts(12:25)

VBScript: Analyzing a Multi-Stage MSBuild Dropper(13:58)

HTML Applications (HTA): Wrapped Payloads, Scripted Delivery, & WMI

Stay Sharp: Reversing C# Malware

Intro to Reversing C# & the .NET Framework(8:24)

Reversing an Encrypted C2 Dropper DLL with dnSpy(13:37)

Go Time: Analyzing Go Malware

Programming Language Recognition & Analyzing a Go Service Backdoor(9:33)

Get Mobile! Mobile Malware Analysis

Lab Update: Installing MobSF(4:54)

Intro to MobSF(7:58)

The Bossfight! Analyzing Real-World Malware Samples

WannaCry.exe Introduction(1:29)

WannaCry.exe Walkthrough(28:33)

Automation: Sandboxes & Pipelines

BlueJupyter: Automating Triage with Jupyter Notebooks(17:04)

Any.Run: Malware Sandboxing(5:17)

Advanced Script Analysis with ChatGPT(15:45)

Tell The World: Rule Writing & Report Publishing

Writing YARA Rules(16:59)

Detecting Malware with YARA(7:33)

Writing & Publishing a Malware Analysis Report(10:06)

Course Final

Course Final(1:45)

Course Conclusion

- Congrats! Course Outro(2:05)
- Learning Objectives
- A new challenger approaches... PMRP!
- Feedback Form

By the end of the course, you will be prepared to tackle the Practical Malware Researcher Professional certification exam!

This unique exam experience will put the student in the shoes of an enterprise-level malware researcher who must identify, report on, and remediate malware. Students will have five (5) full days to complete the assessment and an additional two (2) days to write a professional report.

About the Instructor: Matt Kiely

Matt Kiely (HuskyHacks) is a seasoned practitioner with 10 years of experience in IT and cybersecurity. Matt has worked as a Lead Cybersecurity Analyst at the Massachusetts Institute of Technology Lincoln Laboratory Space Research Division, Red Team Operator & Exploit Developer at a large financial institution, Principal Cybersecurity Content Architect & Instructor at SimSpace, and served as a United States Marine.

Matt holds a Bachelor of Science in Information Technology from Northeastern University and a Graduate Certificate in Cybersecurity from the Rochester Institute of Technology. Some of Matt's professional certifications include OSCP, eCPPT, eCPTX, CRTO, and CRTP.

Follow Matt on Social Media:

GitHub - https://github.com/HuskyHacks

Twitter - https://twitter.com/HuskyHacksMK

YouTube - https://www.youtube.com/channel/UCtJgZIyoZ0wIKEzctj_8pZQ

Blog - https://huskyhacks.dev