Welcome to Malware Development for Red Team Operator Training

Skill Level: Beginner to Intermediate

Track: Technical Focus

Duration: 2 Days

Program Overview:

A comprehensive, training malware development that offers knowledge ranging from beginner to intermediate levels on becoming a better ethical hacker, penetration tester, and red team member by learning offensive security tool development in cross-platform operating system.

Are you a penetration tester with some experience using Metasploit or Cobalt Strike? Or maybe you're just starting out as an ethical hacker and want to learn more about how these malware development work? Or are you a blue team member or threat hunter looking to better understand how malware internal operates?

This training is designed to equip participants with essential knowledge and practical skills in malware development, specifically for Windows environments. While the program is capable of running cross-platform, this training will be conducted using a Windows environment. However, you are welcome to customize the setup based on your own environment as needed. Covering topics from **building your own custom working dropper and downloader** for the latest cross platform operating system (Microsoft Windows, Linux, MacOS). This includes building a dropper for any payload you choose, such as Metasploit meterpreter, Cobalt Strike beacons, or Empire. Including techniques to **protect your binary** from analysis and reverse engineering. This training provides a thorough foundation for anyone aspiring to be an malware analyst or developer, making it essential for security professionals to understand its development and mitigation. Being able to create malware helps red teams enhance an organization's detection and prevention capabilities.

You'll receive a virtual machine with a **complete environment** for developing and testing your software, along with source code templates. This will help you focus on understanding the key mechanisms rather than getting bogged down by less important technical details.

Modules

Day 1: Introduction for Malware Development

1. **Introduction: Malware Development**
    - Short introduction to malware development.
2. **Basics of Binaries Development**
    - Code Understanding, Tools, and Techniques.
3. **Malware Development Hands-On Scenario**
    - Practical labs and exercises to enhance your development skills.

Day 2: Practical Malware Development

Developing the following malicious software:

- **Dropper and Downloader**
    - Learn how to write custom droppers and downloader.
- **Obfuscation and Hiding**
    - Discover how to hide your code from static analysis.
- **Software Protection**
    - Learn how to safeguard your binary and make the program harder for analyst to reverse engineering.

Learning Objective

- To understand malware development in practical approach.
- To enhance offensive security skills.
- Explore new tools and development techniques.
- Discover realistic attack simulation.
- To understand malware ethical principles.

Target Audience

- Red teamers and penetration testers looking to enhance their malware development skills should take this training.
- Blue teamers who want to understand the approach and techniques of adversaries.
- All security engineers/professionals wanting to learn beginner to intermediate offensive tactics.

Knowledge Prerequisites

- Be familiar with using Windows and Linux operating environments and be able to troubleshoot general OS connectivity and setup issues.
- Be familiar with VMware and be able to import and configure virtual machines.
- Have a general idea about core programming concepts such as variables, loops, and functions in order to quickly grasp the relevant concepts in this area.

Hardware Requirements

- A working laptop capable of running virtual machines.
- Each participant required to Download and install VMware Workstation Player (Free) or VMware Workstation Pro 16.2.X+ (for Windows 10 hosts), VMware Workstation Pro 17.0.0+ (for Windows 11 hosts), or VMWare Fusion Pro 12.2+ (for macOS hosts) prior to class beginning in order to run the given VM image. If you do not own a licensed copy of VMware Workstation Pro or VMware Fusion Pro, you can download a free 30-day trial copy from VMware. VMware will send you a time-limited serial number if you register for the trial at their website. Trainer will not spend much time on setting up and troubleshoot the environment.
- 8GB RAM required, at a minimum or more is required and dual core processors.
- Reserved at least 150GB of hard disk space on your host machine for the VM image to run and to copy the given material.
- Administrator / root access MANDATORY.
- At least one available USB 3.0 Type-A port. A Type-C to Type-A adapter may be necessary for newer laptops. Some endpoint protection software prevents the use of USB devices, so test your system with a USB drive before class.
- Wireless networking is required.

Your course media is delivered via download. The media files for class can be large. Many are in the 40-50GB range, with some over 100GB. You need to allow plenty of time for the download to complete. Internet connections and speed vary greatly and are dependent on many different factors. Therefore, it is not possible to give an estimate of the length of time it will take to download your materials.

Participants will need to download the course materials during the early training begins. The materials will be provided in a zipped folder, and the password to unzip the folder will be shared during the class. As a backup, the course materials will also be provided on a pre-loaded USB drive, which will be distributed on the day of the training.

YOUR INSTRUCTORS: Fatah Hashim

Fatah Hashim is a member of the VX Engineering Security Research Group. He served in the cyber military sector in Malaysia Ministry of Defence (MINDEF) during his previous work and is now employed as a malware analyst in the national cybersecurity specialist agency. Specializing in offensive and defensive security software research, analysis, and development. His professional career and research interests focus on countering adversaries, malware research, reverse code engineering, and Red-Blue Teaming.