# Module 07: Malware Threats - Practical Guide

This guide covers the essential tools and step-by-step hands-on sessions for analyzing and understanding malware threats as defined in the CEH v13 curriculum.

## 1. Comprehensive Malware Toolset

### Static Analysis Tools (Code Analysis)

These tools help you inspect a file without executing it.

* **Strings:** Extracts human-readable text from binary files to find IPs, URLs, or function names.
* **PE Explorer:** Analyzes the structure of Windows Executable (PE) files, including headers and resources.
* **Dependency Walker:** Lists all the DLLs and functions a program requires to run.
* **BinText:** A fast, advanced strings-gathering tool.

### Dynamic Analysis Tools (Behavioral Analysis)

These tools monitor the system while the malware is actually running in a sandbox.

* **Process Monitor (ProcMon):** Real-time monitoring of file system, Registry, and process activity.
* **Regshot:** Takes "before" and "after" snapshots of the Windows Registry to identify changes made by malware.
* **Wireshark:** Captures network traffic to identify Command & Control (C2) communication.
* **TCPView:** Shows active socket connections (similar to netstat but with a GUI).

### Online & Automated Analysis

* **Any.Run:** An interactive online sandbox where you can watch malware execute in real-time.
* **VirusTotal:** Scans files against over 70 antivirus engines and provides community comments.
* **Cuckoo Sandbox:** An open-source automated malware analysis system.

## 2. Hands-On Lab Sessions

### Lab 1: Performing Static Analysis (Strings & PE Headers)

**Goal:** Identify hardcoded indicators of compromise (IOCs) without running the file.

1. **Extract Strings:** Open your terminal and run strings malware\_sample.exe > output.txt.
2. **Search for IPs:** Search output.txt for IP addresses or domain names.
3. **Inspect PE structure:** Open malware\_sample.exe in **PE Explorer**.
4. **Check Imports:** Look at the "Import Table" to see if the file uses suspicious functions like CreateRemoteThread or WriteProcessMemory (common in process injection).

### Lab 2: Behavioral Analysis with Regshot

**Goal:** Identify where malware hides in the Windows Registry for persistence.

1. **First Shot:** Open **Regshot** and click "1st Shot" followed by "Shot".
2. **Execute Malware:** Run the malware sample in an isolated VM.
3. **Second Shot:** After a few minutes, click "2nd Shot" followed by "Shot".
4. **Compare:** Click "Compare". A text file will open showing exactly which registry keys were added (often in HKLM\Software\Microsoft\Windows\CurrentVersion\Run).

### Lab 3: Monitoring Activity with Process Monitor

**Goal:** Watch file system and process creation in real-time.

1. **Set Filter:** Open **ProcMon**. Set a filter for Process Name is malware\_sample.exe.
2. **Run Sample:** Execute the malware.
3. **Analyze Events:** Look for "Process Create" events (indicates a secondary payload being dropped) and "WriteFile" events (indicates data encryption or exfiltration).

### Lab 4: Online Interactive Analysis (Any.Run)

**Goal:** Use a safe cloud environment to verify malware behavior.

1. **Upload:** Go to Any.Run and upload a suspicious file (or use a public sample).
2. **Interact:** Once the VM boots, watch the process tree.
3. **Identify C2:** Look at the "Network" tab to see if the malware attempts to reach out to a specific IP or download additional files.

### Lab 5: Trojan Construction (Educational Wrapper Concept)

**Goal:** Understand how attackers bundle malware with legitimate tools.

1. **Tool:** Use a binder like **IExpress** (built into Windows) or **SfxBar**.
2. **Selection:** Select a legitimate file (e.g., calc.exe) and a "payload" (e.g., a simple Netcat listener).
3. **Binding:** Bundle them into a single .exe.
4. **Verification:** Run the new file. Note that the calculator opens, but the Netcat listener starts silently in the background.

## 3. Defensive Countermeasures Summary

* **Sandboxing:** Always run suspicious files in a isolated environment (VM) with no network access to the host.
* **Hashing:** Calculate the MD5/SHA256 hash of every sample and search for it on **VirusTotal**.
* **Egress Filtering:** Block all outbound traffic from servers except for specifically approved ports and IPs.