Malware Learning Path for Authorized Penetration Testers

1. Fundamentals of Malware

- Types of Malware: Deepen your understanding of viruses, worms, Trojans, ransomware, etc.
- How Malware Works: Study infection vectors, persistence mechanisms, and evasion techniques.
- Malware Lifecycle: From development to deployment, execution, and cleanup.

2. Malware Analysis

- Static Analysis
- File Inspection: Examine metadata, strings, and headers using tools like file, strings, PEview (for Windows executables), ExifTool (for metadata).
- Disassembly: Use tools like Ghidra, IDA Pro, or Radare2 to analyze binary code.
- YARA Rules: Learn to write rules for malware detection.
- Dynamic Analysis
- Sandboxing: Use tools like Cuckoo Sandbox, Any.Run, or Hybrid Analysis to observe malware behavior in a controlled environment.
- Debugging: Tools like x64dbg or OllyDbg to step through malware execution.
- API Monitoring: Tools like Process Monitor or Frida to track system calls.

3. Reverse Engineering

- Assembly Language: Basics of x86/x64 assembly to understand disassembled code.
- Decompilation: Use tools like Ghidra or Binary Ninja to decompile binaries.
- Unpacking: Learn techniques to unpack obfuscated or packed malware.

4. Writing Custom Malware (For Ethical Testing)

- Simple Payloads: Start with basic scripts (e.g., Python or PowerShell) to simulate malware behavior.
- Shellcode: Learn to write and execute shellcode for exploits.
- Evasion Techniques: Study how malware bypasses AV (e.g., obfuscation, encryption, process injection).

5. Defensive Techniques

- Signature Detection: Understand how AVs detect malware and how to bypass them.
- Behavioral Analysis: Learn how EDR (Endpoint Detection and Response) tools detect malicious activity.
- Memory Forensics: Use tools like Volatility to analyze malware in memory.

6. Practical Labs and Resources

- Hands-On Labs: Malware Analysis Challenges, FLARE VM for a pre-configured malware analysis environment.

- Books: Practical Malware Analysis by Michael Sikorski and Andrew Honig; The Art of Memory Forensics by Michael Hale Ligh et al.
- Courses: SANS FOR610 (Reverse-Engineering Malware); Offensive Security’s Malware Development courses.

7. Legal and Ethical Considerations

- Ensure you have explicit permission for any testing involving malware.
- Document your findings and actions clearly for reporting.

Next Steps

- If you're just starting, focus on static and dynamic analysis first.
- Once comfortable, move to reverse engineering and writing custom payloads.