Malware Lab Setup: Resource & Verification Checklist

Section 1: Host System Preparation

[ ] Confirm hardware virtualization

Resource: Hardware manual

Note: Check for Intel VT-x or AMD-V in BIOS/UEFI. Usually under "CPU", "Advanced", or "Security".

[ ] Enable virtualization in BIOS/UEFI

Resource: BIOS/UEFI menu

Note: CRITICAL: The lab will not function if disabled.

[ ] Create a dedicated downloads folder

Resource: Your computer

Note: Name it clearly (e.g., Malware_Lab_Setup_June2025).

Section 2: Required Software & Operating Systems

[ ] Download VirtualBox installer

Resource: https://www.virtualbox.org/wiki/Downloads

Note: Always use the official site for the latest version.

[ ] Download VirtualBox Extension Pack

Resource: https://www.virtualbox.org/wiki/Downloads

Note: The version must match your VirtualBox installer.

[ ] Download 7-Zip

Resource: https://www.7-zip.org/

Note: For file extraction and local checksums.

[ ] Download Python 2.6.6

Resource: https://www.python.org/downloads/release/python-266/

Note: Required only for running legacy tools inside XP VM.

[ ] Download PyWin32 (Build 212)

Resource: https://github.com/mhammond/pywin32/releases/tag/b212

Note: Download pywin32-212.win32-py2.6.exe for XP.

[ ] Obtain Windows XP 32-bit ISO

Resource: Legal sources (archive.org, MSDN)

Note: CRITICAL: Never use untrusted sites. Verify hashes.

[ ] Obtain Windows 7 SP1 ISO

Resource: Legal sources (MS, archive.org)

Note: Use "unpatched" version for exploit testing.

Section 3: File Verification and Backup

[ ] Verify SHA-256 checksums of all files

Malware Lab Setup: Resource & Verification Checklist

Resource: 7-Zip (Right-click > CRC SHA > SHA-256)

Note: Use a local tool; compare to trusted hash lists (vendor or Reddit).

[ ] Search file hashes on VirusTotal

Resource: https://www.virustotal.com/

Note: Paste the SHA-256 hash in the SEARCH bar. CRITICAL: Never upload live ISOs or malware!

[ ] Back up all verified files

Resource: External drive

Note: Create a clean, trusted backup now.

Section 4: Optional (But Recommended) Analysis Tools

[ ] Download HxD Hex Editor

Resource: https://mh-nexus.de/en/hxd/

Note: Safely view file contents without execution.

[ ] Download Ghidra SRE

Resource: https://ghidra-sre.org/

Note: NSA reverse engineering suite; run only in an isolated lab.

Section 5: Reference & Community Resources

[ ] Review "Lost in Translation" Megathread

Resource: https://www.reddit.com/r/netsec/comments/65sy6f/the_shadow_brokers_equation_group_mega_thread/

Note: Invaluable for context and trusted hashes.

[ ] Read foundational analysis

Resource: https://securelist.com/lost-in-translation/78294/ / https://blog.talosintelligence.com/shadow-brokers

Note: Understand tool background and risk.

[ ] Bookmark VirtualBox documentation

Resource: https://www.virtualbox.org/manual/UserManual.html

Note: Essential for troubleshooting and VM setup.

Section 6: General Tips & Student Notes

- CRITICAL: Never run, mount, or extract any suspicious file on your main computer. Only perform these actions inside your verified, isolated lab.
- Always confirm download links before clicking; watch out for scam or typo URLs.
- Keep a simple log (text file or spreadsheet) of every file: source, date, and verified SHA-256 hash.
- Take screenshots during your setup process for documentation or rebuilding later.

Student Notes:

Malware Lab Setup: Resource & Verification Checklist

> Use this space for download issues, checksum notes, link changes, or your own reminders.

> For every file, record: date, exact source, and SHA-256 hash.