olproof Protocol for Building an Isolated VirtualBox Malware Analysis

Prepared by: Derek Mckiernan

Date: June 2025

For Educational and Research Use Only

[SHIELD]

(Insert your logo or icon here for the final version.)

Executive Summary

Executive Summary

This protocol is the gold standard for constructing a secure, isolated malware analysis lab using Oracle VirtualBox. Each step is designed to enforce safety, operational discipline, and clarity, making it accessible for both seasoned analysts and students.

This guide provides the methodology to safely analyse live exploits and malware samples with confidence that your host computer and local network will remain uncompromised. Each phase explains the rationale ("the why") behind critical actions, while tips, mandatory checkpoints, and notes sections reinforce learning and ensure reproducible results.

PHASE 1: Preparation and Host System Setup

[Illustration Placeholder: BIOS/UEFI setup screen with virtualization toggle]

Instructions

- Reboot your laptop and enter the BIOS/UEFI setup utility.
- [CRITICAL] Enable the hardware virtualization setting ('Intel VT-x' or 'AMD-V').
- Save and reboot.
- Download the latest VirtualBox installer for your OS.
- Download the matching Extension Pack.
- Obtain legal ISOs for: Windows XP (32-bit) and Windows 7 SP1 (unpatched, 32/64-bit).
- Store all files in a dedicated folder.

Tips & Notes

* BIOS/UEFI menus vary by device. Check documentation if unsure.
* Only use trusted, legal sources for ISOs.

Student Notes:

____

____

CHECKPOINT 1:

[ ] Virtualization enabled   [ ] VB installer/pack downloaded   [ ] ISOs accessible

[Review the above. Illustrations to be added.]

PHASE 2: VirtualBox Installation and Global Configuration

[Illustration Placeholder: VirtualBox window and Preferences]

Instructions

- Install VirtualBox with defaults. Allow network interfaces.
- Install Extension Pack. Check in Preferences > Extensions.
- Set Default Machine Folder to a fast SSD location.

Tips & Notes

* Extension Pack must match VirtualBox version.
* SSDs greatly improve VM performance.

Student Notes:

____

____

CHECKPOINT 2:

[ ] VB runs error-free   [ ] Extension Pack listed in Preferences

[Review the above. Illustrations to be added.]

PHASE 3: Creating the Isolated Lab Network

[Illustration Placeholder: Two shielded VMs inside 'Internal Network']

Instructions

- Set Adapter 1 to 'Internal Network' with identical name (e.g. malware-lab-net) for all VMs.
- [CRITICAL] Do not use NAT/Bridged adapters.

Tips & Notes

* Name is case-sensitive; all VMs must match.
* Network isolation is the #1 safety step.

Student Notes:

____

____

CHECKPOINT 3:

[ ] Internal network configured and understood

[Review the above. Illustrations to be added.]

PHASE 4: Building the 'Attacker' VM (Windows XP)

[Illustration Placeholder: XP VM, tool icons, network cable, 'No Shared Folders']

Instructions

- Name: EQ-ATTACKER | OS: Windows XP 32-bit | RAM: 1024 MB | CPU: 1 | Disk: 20 GB.
- Network: Internal Network (malware-lab-net).
- Shared Folders/Clipboard/Drag'n'Drop: Disabled. Audio: Disabled.
- Mount XP ISO. Install Windows XP.
- Install Guest Additions, Python 2.6.6, PyWin32 v212.
- Transfer tools via read-only ISO only. Take a snapshot: '[1] Clean Install - Ready to Attack'.

Tips & Notes

* Disabling sharing prevents malware escape.
* Snapshots are your instant recovery tool.

Student Notes:

____

____

CHECKPOINT 4:

[ ] Network internal only   [ ] No sharing   [ ] Snapshot taken

[Review the above. Illustrations to be added.]

PHASE 5: Building the 'Victim' VM (Windows 7)

[Illustration Placeholder: Win7 VM, network cable, Firewall Off]

Instructions

- Name: VICTIM-WIN7 | OS: Windows 7 | RAM: 2048 MB | CPU: 2 | Disk: 30 GB.
- Network: Internal Network (malware-lab-net).
- Shared Folders/Clipboard/Drag'n'Drop: Disabled.
- Mount Win7 ISO. Install Windows 7. No updates or internet.
- Install Guest Additions. Disable Firewall inside VM.
- Take a snapshot: '[1] Clean Install - Ready to be Attacked'.

Tips & Notes

* Never let this VM online. It's vulnerable on purpose.
* Firewall off is for lab only-never on a real machine!

Student Notes:

____

____

CHECKPOINT 5:

[ ] Network internal only   [ ] No sharing   [ ] Snapshot taken

[Review the above. Illustrations to be added.]

PHASE 6: Final Lab Verification

[Illustration Placeholder: Two VMs pinging; host ping blocked]

Instructions

- Start both VMs. Use ipconfig in each to find their IPs.
- From EQ-ATTACKER, ping VICTIM-WIN7 (should work).
- From host, ping either VM's IP (must fail: 'Request timed out').

Tips & Notes

* Do not continue if host can ping VMs-fix isolation first.
* This proves your lab is secure for research.

Student Notes:

____

____

CHECKPOINT 6:

[ ] VMs ping each other   [ ] Host cannot ping VMs

[Review the above. Illustrations to be added.]

Ongoing Usage and Safety Protocol

[Illustration Placeholder: Shield, checklist, backup drive]

Rules

- Always revert to a clean snapshot before every new experiment.
- Never change network from Internal. Never enable sharing after setup.
- Only use read-only ISOs for file transfer.
- Always shut down VMs from inside guest OS before closing VirtualBox.
- Regularly export backup appliances.
- Never leave lab VMs running unattended.

[Review the above. Illustrations to be added.]