

Preparing Malware Testbed

Note: Prior to starting the preparation of malware testbed, Section 1 and Section 2 must be filled with required information.

Section 1: Details of the Organization

Organization Name:	
Contact Number:	
Website:	
Address:	
<i>Additional Contact Information:</i>	

Section 2: Details of the Incident Responder

Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			

Section 3: Steps to be Followed to Prepare Malware Testbed	
Actions	Completed
Step 1: Allocate a physical system for the analysis lab	<input type="checkbox"/>
Step 2: Install virtual machine (VMware, Hyper-V, etc.) on the system	<input type="checkbox"/>
Step 3: Install guest OS in the Virtual machine(s)	<input type="checkbox"/>
Step 4: Isolate the system from the network by ensuring that the NIC card is in "host only" mode	<input type="checkbox"/>
Step 5: Simulate Internet services using tools such as iNetSim (https://www.inetsim.org)	<input type="checkbox"/>
Step 6: Disable "shared folders" and "guest isolation"	<input type="checkbox"/>
Step 7: Install malware analysis tools	<input type="checkbox"/>
Step 8: Generate hash value of each OS and tool	<input type="checkbox"/>
Step 9: Copy the malware to the guest OS	<input type="checkbox"/>