0 –Malware Lab VM Configurations

0.1 VM: MetaSploitLab

The Virtual machine is available in Download VM.

This is a OVA file that can be imported to VirtualBox or VMware. For more information check supporting material.

Configurations

The lab works with three network interfaces, Adapter 1, set as a Nat and Adapter 2 & 3 set as a Bridged.

The VM was created and tested with 2048 MB memory RAM for optimum performance. However, it can also be run with a different amount of RAM.

Suggestions

- It is recommended to deactivate the mouse integration. This configuration can be done as follows:

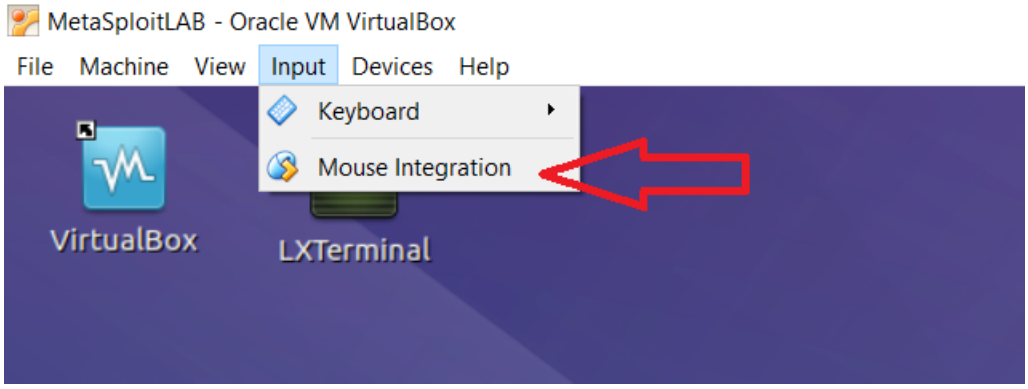

Figure 1 How to set mouse integration

- Use right-ctrl+c to enter in Scaled Mode screen.

Accounts

The user 'Lab' is an administrator account and the password is 'e2rml' which means '**e**asy **to** **r**emember **m**etasploit **l**ab'. The root access uses the same password. To test it, write 'sudo bash' in the terminal.

0.2 Starting up tools

The VM is equipped with various tools, use the following recommendations:

- Guidance-tool: double-click on the icon 'Start Guidance-tool' ▶
- Msfconsole: on the terminal, run 'msfconsole' as a root.
- Vulnerable VMs: Windows XP as much as Metasploitable OS (Linux) are configured in VirtualBox, double click on the hypervisor icon, and start the machine you want.