

Real-World Scenario 4-1: Securing a Virtual Machine

Scenario: You have been tasked with securing a Type 2 virtual machine that was created by one of the developers in your organization.

You are required to

- Secure the network connection
- Change the BIOS boot order
- Disable unnecessary devices
- Add encryption
- In general, secure the VM as much as possible

Virtual machines that are contained within a Type 2 host are sort of like a computer within a computer. Consider writing down exactly what you are configuring. Try to do this in an illustrative way, or consider using a network documentation program such as Visio. As you progress in the virtual world, you will be using more and more virtual computers, and you will connect to them in a variety of remote ways. The more you document what you are doing, the better you will understand your virtual environments.

Real-World Scenario 4-1 Solution

Virtualization security is vital. VMs should be secured in the same way that a regular operating system is secured; however, the VM itself (and the virtual hosting software) can be further secured by disabling virtual hardware.

This solution utilizes a Windows 10 computer running Hyper-V with a virtual machine that has Ubuntu Linux installed.

NOTE Other software manufacturers, such as Virtual Box, will have similar settings.

At the minimum, the solution should include the following:

1. Within Hyper-V, configure the virtual switch in a secure manner. The most secure way would be to use a private virtual switch, which means that VMs within the host can communicate with each other but not with any other systems. A less secure option would be to use an internal virtual switch, where VMs can talk to each other and the host. The least secure option would be to use an external virtual switch, where the VMs can communicate with systems beyond the host.
2. Create a network connection for the VM. To make it more secure (especially if you're using an external virtual switch) consider using a VLAN or a separate IP subnet.
3. Change the BIOS boot order so that the hard drive is first, not optical discs or USB drives.
4. Disable unnecessary devices such as COM ports, USB devices, even diskette drives!
5. Add a key storage drive and encryption within Hyper-V.

Video Solution: Watch the video solution "4-1: Securing a Virtual Machine" for each of the steps listed and much more.