

Prerequisites

Setting Up Your Local Lab Environment

Instructor Prof. Sara Khanchi
Email skhanchi@nyit.edu
Section VA1 Tuesday 9:00AM to 12:00PM
Due Date May 27, 2025 (Tuesday)
Support TA: Parthsinh Arunsinh Jadeja (Email: pjadeja@nyit.edu)

Introduction

First of all, welcome to INCS 745: Intrusion Detection and Hacker Exploits!

Get ready to dive into the world of ethical hacking and intrusion detection with hands-on experience using industry tools and techniques. To kick things off, you'll need to set up your lab environment. This guide will walk you through installing VirtualBox, importing the VM images, and tweaking the network settings.

Make sure to complete the setup before our next class so you're ready to roll. If things don't go as planned, the TA and professor are here to help!

A Quick Overview of Our Tools

Throughout this course, you will use various tools to perform tasks specified in your lab manual. Here's a brief introduction to some of the key tools you will be using:

VirtualBox

VirtualBox is a free, open-source virtualization software that lets you run multiple operating systems on your computer at the same time, without needing a second machine. It's an essential tool for setting up and managing the virtual environments you'll use for your lab exercises, giving you a safe space to experiment without breaking your actual system.

Student Machine (Student.ova)

This virtual machine is your digital playground, loaded with all the essential tools and environments you'll need to conquer your lab exercises. You've got full control to tweak, configure, and run tasks as outlined in upcoming labs.

Server Machine (Server.ova)

Think of the server virtual machine as a mysterious black box that you'll be poking and prodding throughout the course. It's packed with various services and applications, all carefully set up to mimic real-world attack scenarios. Your mission: analyze, interact, and uncover its secrets as part of your lab assignments. Here direct access is restricted, keeping things as realistic (and frustrating) as actual penetration testing.

Step 1: Download and Install VirtualBox

1. Go to <https://www.virtualbox.org/wiki/Downloads>.
2. Here you will see a list of VirtualBox installation packages, please select the one that corresponds to the operating system and hardware architecture that you are working with.

VirtualBox 7.0.20 platform packages

- ➞ Windows hosts
- ➞ macOS / Intel hosts
- Linux distributions
- ➞ Solaris hosts
- ➞ Solaris 11 IPS hosts

3. Proceed with the installation

Step 2: Download OVA (Open Virtual Appliance) Files

Our virtual machines are packaged as OVA files, preconfigured and ready to use. Please download them to your computer before proceeding with the setup. Please verify the file size after downloading the files.



1. Server: [Download](#) (8.70 GB)
2. Student: [Download](#) (9.76 GB)

Important:

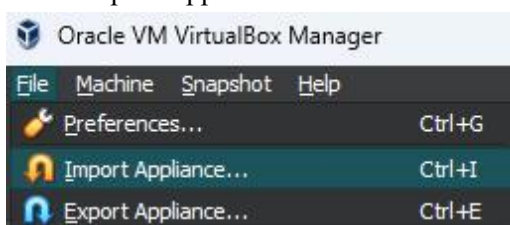
These files are quite large, so it's best to download them at home to avoid overloading the classroom WiFi. If you encounter any issues, try using a Chromium-based browser like Chrome or Edge for a smoother download experience.

Step 3: Importing OVAs to VirtualBox

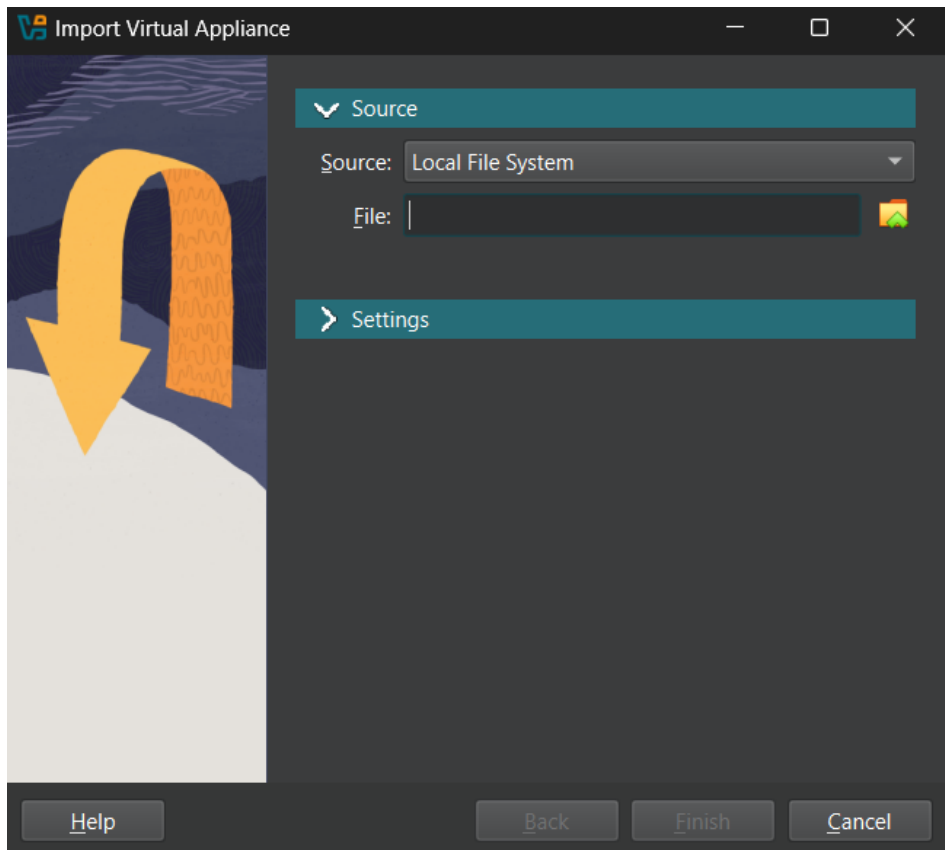
1. By now, you should have both OVA files stored in your designated folder. Proceed with the following setup steps for each file to properly configure your virtual environment.

 Server.ova	21-05-2025 19:33	Open Virtualizatio...	91,25,000 ...
 Student.ova	21-05-2025 19:16	Open Virtualizatio...	1,02,42,802...

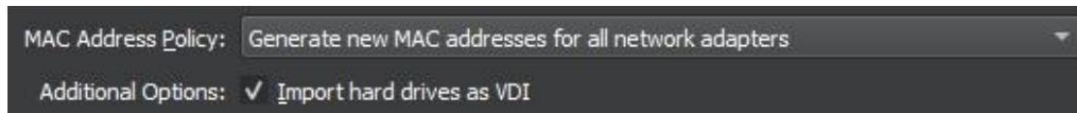
2. Run VirtualBox and go to File → Import Appliance.



3. Choose one of the OVA files from your downloaded files to begin the setup process.



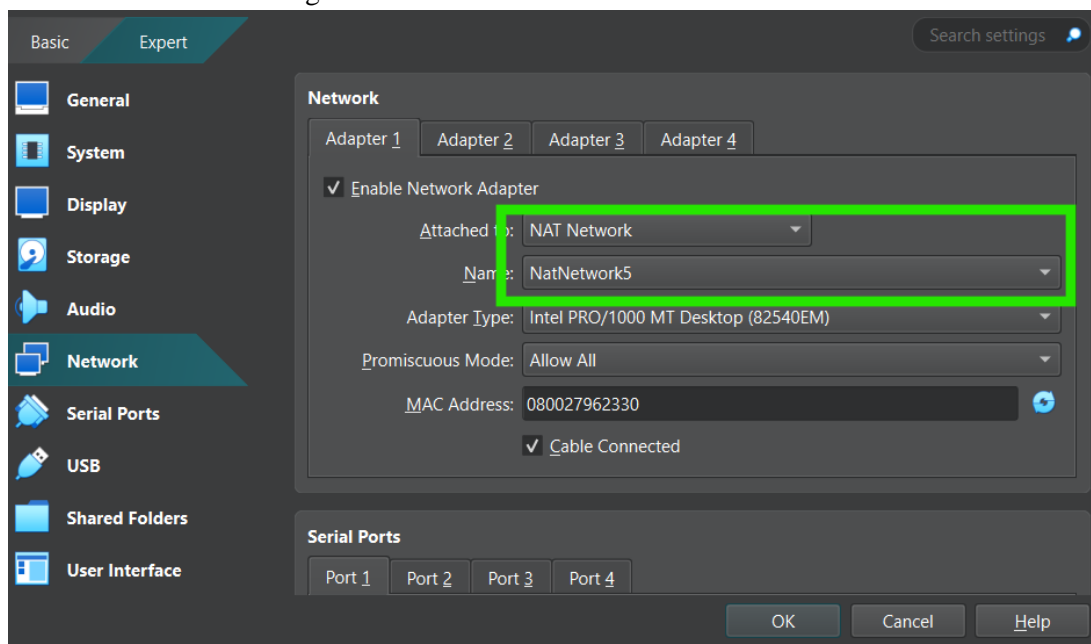
4. Ensure the virtual machine is allocated at least 2 CPUs and 2 GB of RAM for optimal performance. Configure VirtualBox to generate new MAC addresses for all network adapters to avoid potential conflicts.



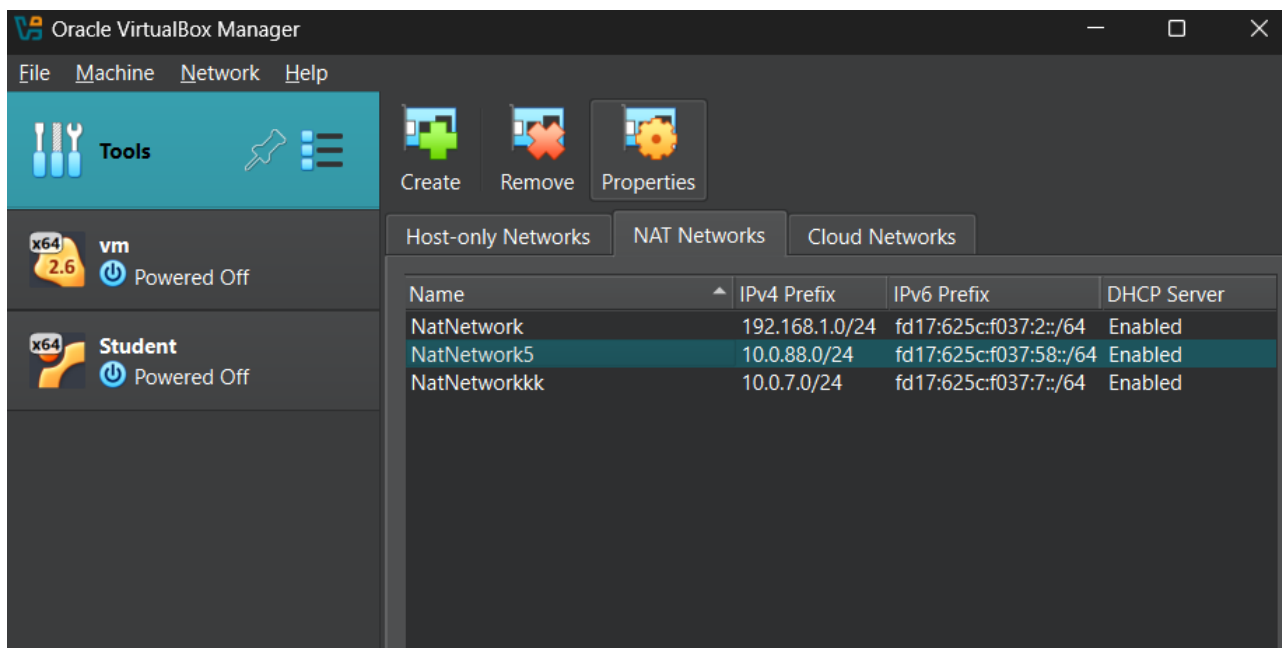
5. Click Finish and allow VirtualBox to complete the import process. This may take a few minutes, depending on your system's performance.

Step 4: Connecting to a NAT Network

1. In the Settings menu under Network for both imported virtual machines (student and server), ensure they are connected to the same NAT Network. This configuration allows them to communicate with each other while maintaining external internet access.



2. If a bridged network option isn't available, navigate to File → Tools → Network Manager in VirtualBox and click Create. You can leave all settings at their default values to set up a new NAT Network.



Important:

Even though the vulnerable services on the server virtual machine are containerized, it's important to avoid exposing the VM directly to the internet. Keeping it isolated within a controlled network environment minimizes security risks and ensures a safer testing setup.

Step 5: Powering On Virtual Machines

1. Start both virtual machines in VirtualBox to confirm your environment is set up correctly. In some labs, the server VM should run in the background while you work on tasks in the student VM, whereas in others, only the student VM will be required.
2. Log in to the student VM with password **745User!**
3. (Optional): Open the Terminal in the student VM and run a quick Nmap scan to verify the setup. The scan should detect two hosts on the NAT network you configured. Don't worry if you're unfamiliar with Nmap yet—we'll cover it in detail in Lab 2.

```

Nmap scan report for INCS-745-Lab-Student (10.0.7.10)
Host is up (0.000054s latency).
Nmap scan report for 10.0.7.11
Host is up (0.0012s latency).

```

Submission

That's all for now. Ensure your virtual machines are set up before the next class. See you then!