Part 04 – Download & Import Vulnerable OVA's

This tutorial covers downloading vulnerable OVA files and importing them in Virtual-box for ethical hacking purposes.

It is assumed that Part 1, Part 2, Part 3 are completed.

As with any course introducing students to ethical hacking. Having a clearly stated ethical hacking statement is a must have. Below is one such statement.

Ethical Hacking Statement:

The need for well-trained Cybersecurity specialists continues to grow at an exponential rate. Training to become a Cybersecurity specialist requires in depth understanding and exposure to how Cyber attacks occur, as well as how they are detected and prevented. These skills will naturally also include learning the techniques that threat actors use to circumvent data, privacy, and computer and network security.

In this course, learners will use tools and techniques in a "sandboxed", virtual machine environment that allows them to create, implement, monitor, and detect various types of Cyber attacks. The hands-on training is performed in this environment so that students can gain the necessary skills and knowledge needed to thwart these and future Cyber attacks. Security holes and vulnerabilities that are created in this course should only be used in an ethical manner and only in this "sandboxed" virtual environment. Experimentation with these tools, techniques, and resources outside of the provided sandboxed virtual environment is at the discretion of the instructor and/or local institution. If the learner has any doubt about which computer systems and networks are part of the sandboxed virtual environment, they should contact their instructor prior to any experimentation.

Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

The instructor is NOT responsible for any un-ethical and/or unlawful actions of the student should they use the tools and techniques learned in this course in a malicious manner.

1) Before we start hacking, we need a few vulnerable machines to get started. Below I have compiled a list of sites offering VM for free download. Note, since we are using virtual box, download VM's that are packaged a OVA files. While you get covert other VM files, it is easiest to start with VM's purpose built for Virtual-box and its container format, OVA files.

Popular sites for downloading vulnerable VM's: https://www.vulnhub.com/

Some additional sites with popular vulnerable VM's:

- OWASP Broken Web Apps: https://sourceforge.net/projects/owaspbwa/files/1.2/
- OWASP WebGoat: https://www.vulnhub.com/entry/webgoat-1,365/
- DVWA: https://www.vulnhub.com/entry/damn-vulnerable-web-application-dvwa-107,43/
- DVL: https://www.vulnhub.com/entry/damn-vulnerable-linux-dvl-11-blackhat-edition,5/
- Metasploitable 1: https://www.vulnhub.com/entry/metasploitable-1,28/
- Metasploitable 2: https://www.vulnhub.com/entry/metasploitable-2,29/
- Metasploitable 3: https://github.com/rapid7/metasploitable3
- OWASP Juice Shop: https://github.com/juice-shop/juice-shop#vagrant

Some additional pre-selected, easy/beginner vulnerable VM's:

- Basic Pentesting 1: https://www.vulnhub.com/entry/basic-pentesting-1,216/
- Basic Pentesting 2: https://www.vulnhub.com/entry/basic-pentesting-2,241/
- Rickdiculouslyeasy: https://www.vulnhub.com/entry/rickdiculouslyeasy-1,207/
  - Rick and Morty Themed box, may not be suitable for younger age groups
- Escalate My Privileges: https://www.vulnhub.com/entry/escalate-my-privileges-1,448/
- So Simple: https://www.vulnhub.com/entry/so-simple-1,515/
- Tenderfoot: https://www.vulnhub.com/entry/tenderfoot-1,581/

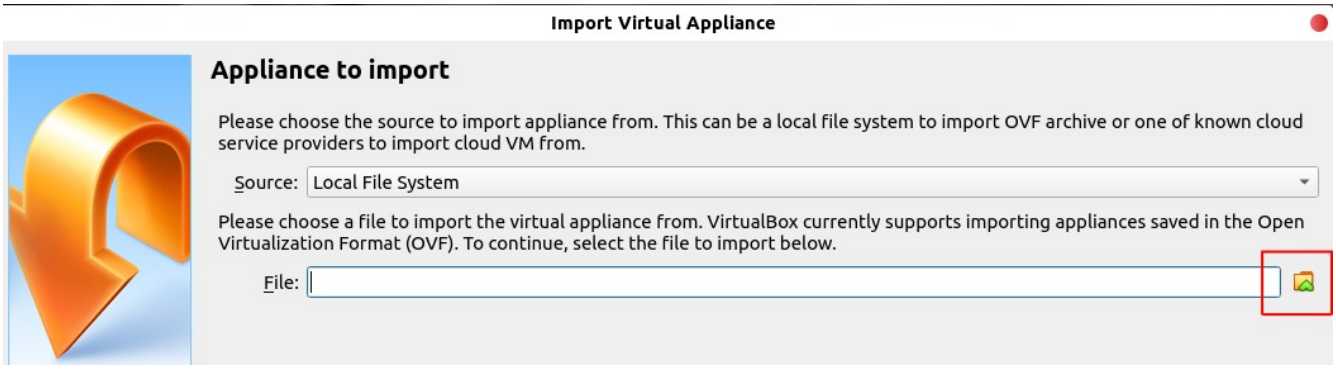
****Note** These VM's are free/fan made. Sometimes explicit language may exist by the creator. It always advised to complete the whole VM hacking challenge first, before deploying to a classroom.**

2) Lets start out with and easy one. Start my downloading the OVA for Metasploitable 2.

3) Make sure that your OpnSense VM and your Kali Linux VM are running.

4) We are going to import the OVA file into virtual box. Select "File" in Virtual-box. In the drop down menu you will see and option for "Import Appliance".

5) Select the folder icon on the Import Appliance screen to select the OVA file that you downloaded for import.



6) On the next screen, you will see and overview of the import. Select the option to import the OVA file/VM.

7) Once the import is complete, we need to adjust one final setting, that is to change the network adapter. Go into the VM's settings, and select the network options. There set/change the network adapter to "Internal Network".

8) With the VM adjusted, start up the vulnerable VM.

9) You will need to find the vulnerable VM on the network. Nmap might help with that...