Creating a local virtual lab for hands-on cybersecurity exercises

Master di primo livello in cybersecurity organizzato
dall'Università di Pisa e dall'Istituto di Informatica e Telematica del CNR

Lab of Secure system configuration, device hardening and firewall management

Docente— Filippo LAURIA

Introduction

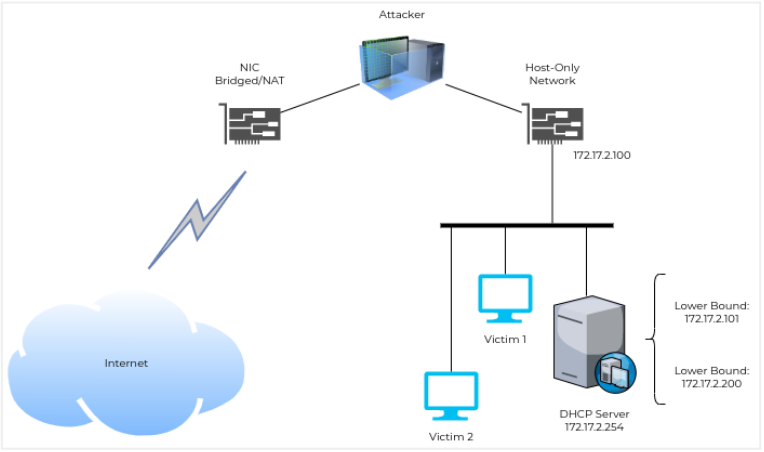
This document describes a possible way to set up a virtual lab for conducting simple security tests. The virtual lab consists of a virtual local network segment to which the virtual machine (VM) used for conducting the tests (i.e. *the attacking machine*) and, from time to time, the VMs being tested (i.e. *the victim machines*) will be connected.

We will be connecting a specific type of victim machine to our virtual training environment, called *boot2root machines*. These machines are designed to be intentionally vulnerable and, once connected to our virtual environment and started, allow you to participate in a *capture-the-flag challenge* [1]. To solve the challenge, you must "capture the flag" by exploiting the vulnerabilities of the system using your computer security skills. In this context, *pwning the system* means gaining full control over it [2], including obtaining root privileges.

To achieve this, the tester attempts to compromise the target system by gaining remote access and executing arbitrary commands, typically through an *interactive shell* [3]. With this access, we can attempt to elevate our privileges and ultimately gain full control of the compromised system.

Configuring a virtual local network segment

The logical diagram of our virtual training environment is shown in the following picture:



virtual environment diagram

To set up a virtual lab as shown in the previous picture, we will use *Oracle VM VirtualBox software* [4] to run VMs. Our first step is to create a new virtual local network segment, which is called a *Host-Only Network* in VirtualBox terminology. We can create this network using VirtualBox's *Host Network Manager* by going to *File / Host Network Manager...*.

Some possible settings are as follows:

Adapter:	DHCP Server (must be enabled):
• IPv4 Addr: `172.17.2.1` • IPv4 Netmask: `255.255.255.0` • Leave the IPv6 fields unchanged.	• Addr: `172.17.2.254` • Mask: `255.255.255.0` • Lower Address Bound: `172.17.2.101` • Upper Address Bound: `172.17.2.200`

After configuring the *Host Network Manager settings,* apply the changes, close the dialog box, and proceed to connect the attacking virtual machine to the new virtual network.

Deploying the attacking VM

To deploy the attacking VM, we recommend using Kali Linux [5], a Linux distribution specifically designed for penetration testing, security auditing, and other hacking activities. Users who prefer a virtual machine installation can download a VirtualBox image of Kali Linux (in OVA format)from [6]. However, there are other distributions available that are equally valid, such as those listed on [7].

Once we have downloaded and imported the Kali Linux OVA file using *File / Import Appliance...*, we need to configure the VM's network settings to ensure that it has two network adapters. To do this, right-click on the imported VM and select *Settings*. In the *Network* tab, check that the first adapter (i.e. *Adapter 1*) is connected in NAT mode and the second adapter (i.e. *Adapter 2*) is connected to the virtual local network that we created earlier.

When we start the attacking VM, its eth0 interface will be mapped to the virtual Adapter 1, which provides Internet access to the VM. Its eth1 interface will be mapped to the virtual Adapter 2, which connects the VM to the virtual local network.

Next, we need to configure the network settings on the attacking VM. In the network manager (*Settings / Advanced Network Configuration*), we must ensure that there are two Ethernet connections. The first connection is used to connect to the Internet via the attacking VM. We can leave the default settings but make sure that the connection name is "to Internet", and the automatic connection option is enabled. In the *Ethernet tab*, choose the eth0 interface, and in the IPv4 *Settings tab*, select the automatic addressing method (DHCP).

The second Ethernet connection connects the attacking VM to the virtual local network. We recommend using the following settings: set the connection name to "to Host-Only Network", enable the automatic connection option, choose the eth1 interface in the *Ethernet tab*, select the manual addressing method in the *IPv4 Settings tab*, and add a new address (`172.17.2.100`) with a netmask of `255.255.255.0` and a blank gateway. In the *IPv6 tab*, disable IPv6.

Deploying victim VMs

For victim VMs, we generally need to ensure that they have a single virtual network adapter connected to the local virtual network. The steps are the same as those for connecting the attacking VM to the local virtual network. VulnHub [8] is a good source for finding victim VMs.

Resources

[1] Capture the flag - https://en.wikipedia.org/wiki/Capture_the_flag_(cybersecurity)

[2] What is Linux? - https://www.linux.com/what-is-linux/

[3] “PWNED” meaning - https://www.inverse.com/gaming/pwned-meaning-definition-origins-video-games-internet-hackers

[4] What is an Interactive Shell? - https://www.gnu.org/software/bash/manual/html_node/What-is-an-Interactive-Shell_003f.html

[5] Oracle VM VirtualBox - https://www.virtualbox.org/

[6] Kali Linux - https://www.kali.org/

[7] 7 Linux Distros for Security Testing - https://securityboulevard.com/2020/03/7-linux-distros-for-security-testing/

[8] Get Kali | Kali Linux, Virtual Machines - https://www.kali.org/get-kali/#kali-virtual-machines