Cabrillo College

Lab 1: Getting Started

We will be using VLAB and NETLAB+ this term to get hands-on ethical hacking practice. VLab is a homegrown collection of VMware ESXi and vCenter servers. In this lab you will configure your pod of VMs (Virtual Machines) and then practice using nmap and Metasploit to exploit a vulnerability in Windows XP.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this lab you have authorization to hack the VMs in the VLab pod assigned to you.

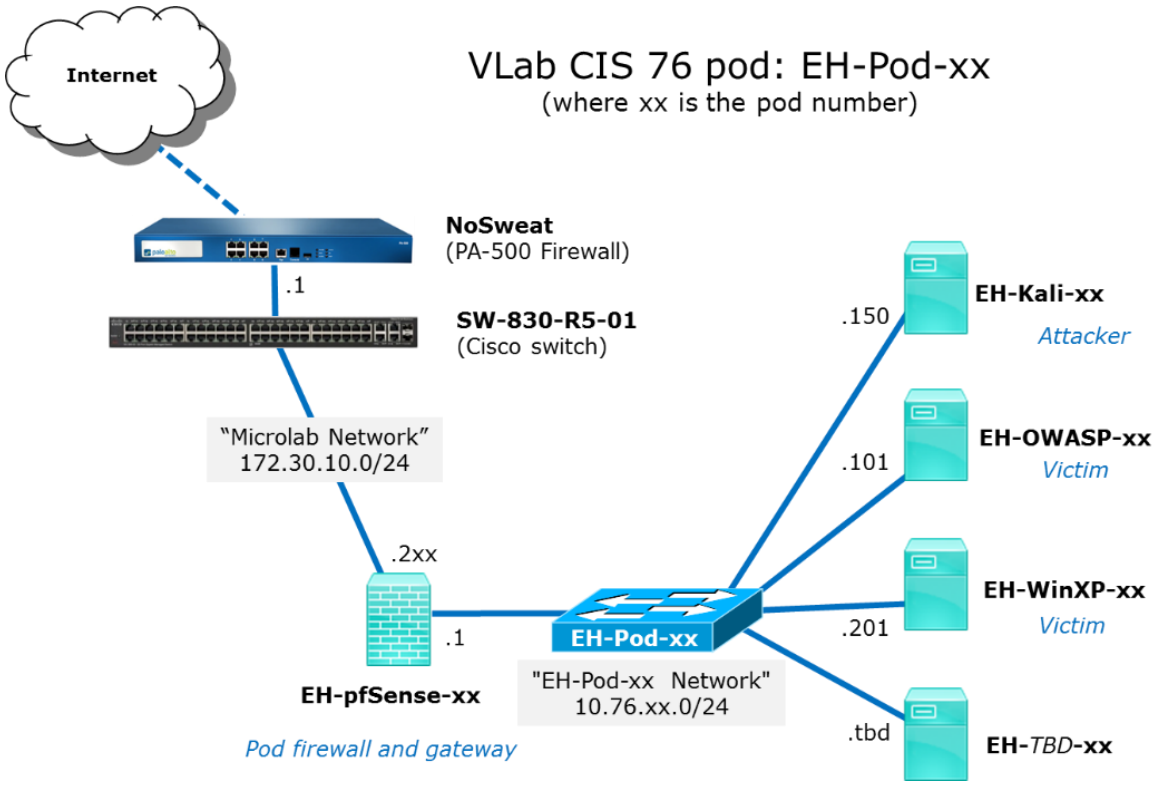
Preparation

- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.

- Determine which VLab pod number you were assigned. See the link on the left panel of the class website.

Overview

Each student has been assigned a pod of VLab VMs for the term to safely practice their new ethical hacking skills. In this lab we will configure three of the VMs (Virtual Machines). The pfSense VM is a FreeBSD based firewall. The Kali VM will be the "attacker" and the Windows XP VM will be the "victim".



Each pod has been populated with an initial set of VMs but they have not been fully configured yet. In the diagram above the "xx" represents the pod number. We need to configure the VMs in your pod so they are cabled into your own pod network, have unique hostnames and IP addresses and some backup snapshots made.

Part 1 – Set up your VLab Pod

1) Set up your pod by following these Instructions: https://simms-teach.com/docs/cis76/cis76-podSetup.pdf
2) If you run into issues you can watch the recorded Lesson 1 to watch the instructor do the pod setup.
3) The forum is an excellent place to ask and answer each other's questions.

Part 2 – Attack the Windows PC from Kali

1) Create a file named confidential.txt on the desktop of your Windows XP VM. Edit the file and add some text containing your first name and your favorite color.
2) On Kali, exploit the MS08-067 vulnerability on the Windows VM and display the contents of the confidential.txt file using the Meterpreter shell command.
3) For step-by-step instructions see: https://simms-teach.com/docs/cis76/cis76-CVE-2008-4250.pdf

Part 3 – Submit your work

1) Prepare a report using the word processor and formatting of your choice. Your report should contain the following:

   - Course name, lab assignment name, your name, and date.
   - For the Kali VM:
     - **ifconfig eth0** command output.
     - **route -n** command output.
     - **hostname** command output.
     - **ping -c2 google.com**
   - For the pfSense VM:
     - Sscreen shot of main menu (showing hostname, network settings and menu).
   - For the Windows VM:
     - **ipconfig** command output.
     - **hostname** command output.
     - **ping google.com** command output.
   - For your VM backup snapshots:
     - Screen shots of the Snapshot Manager dialog boxes for each VM
   - For the exploit of the Windows VM:
     - **meterpreter** session showing use of the shell command to display the contents of the confidential.txt file on the Windows PC.

   As an example you can see Benji's report for Pod 5 here: https://simms-teach.com/docs/cis76/cis76-lab01-simben76.pdf

2) Email your report to: **risimms@cabrillo.edu**

Remember **late work is not accepted.** If you can't finish the lab by the deadline submit what you have completed for partial credit.

Grading Rubric (30 points)

5 points for 100% correct pfSense VM configuration.
5 points for 100% correct Kali VM configuration.
5 points for 100% correct Windows XP VM configuration.
5 points for 100% correct cabling of the three VMs.
5 points for making snapshots named Pristine and Baseline of each of the three VMs.
5 points for hacking the Windows XP system.

Note: 100% correct means they are configured exactly (hostnames, IP settings, virtual LAN cabling) as shown on the network map above.

Extra Credit (3 points)

1 point - Screen shot showing modified and correct hostname for your pfSense VM.
2 points - Configure port forwarding on your pfSense VM so you can ssh from Opus to your Kali VM and include screenshot showing Kali ssh session from Opus.