Cabrillo College

CIS 76 Linux Lab Exercise

Lab 2: Network Fundamentals
Fall 2016

Lab 2: Network Fundamentals

This lab gives you some practice using Netlab+ using Wireshark and tcpdump. In addition, you can try out Mac and ARP spoofing using macchanger and Cain.

Warning and Permission

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

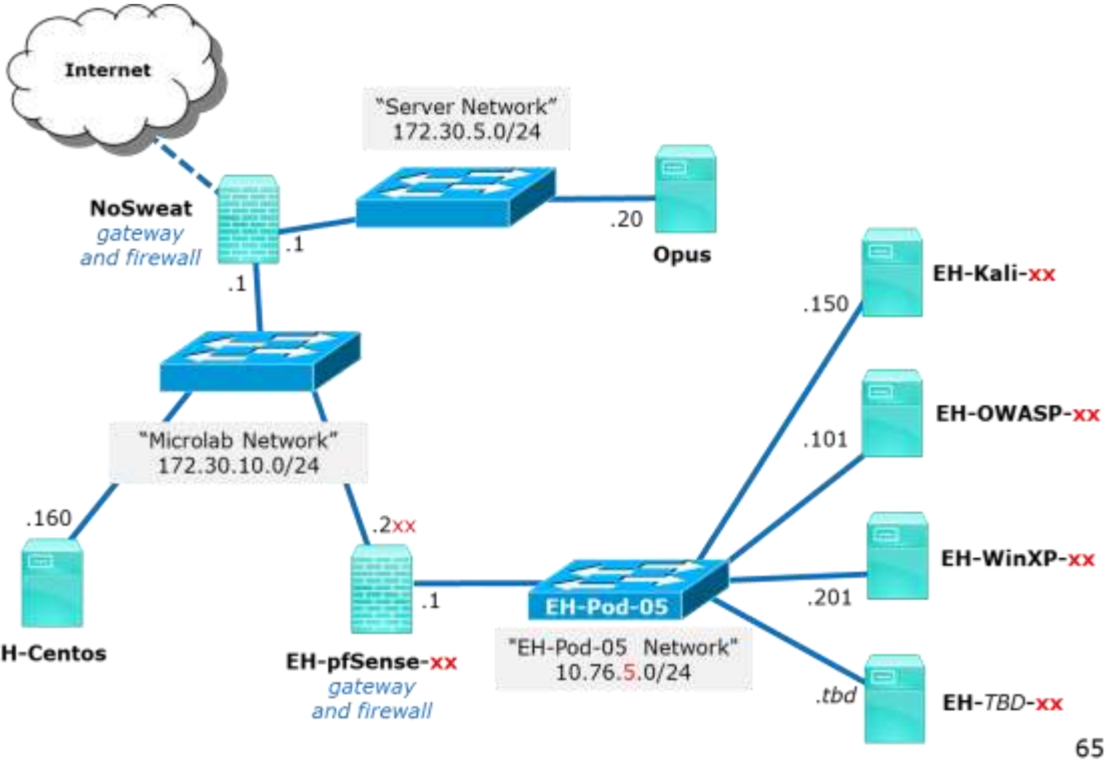
For this lab you have authorization to hack the VMs in the VLab pod assigned to you.

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.

Network Overview



Part 1 – Pod configuration

1) Set up your OWASP VM pod by following the instructions in the Pod Setup document: https://simms-teach.com/docs/cis76/cis76-podSetup.pdf

Part 2 – MAC Spoofing

1) Come up with a "new" vendor for your Kali VM and spoof the MAC address to match this new vendor. Do this by replicating the MAC spoofing example here: https://simms-teach.com/docs/cis76/cis76-MAC-spoofing.pdf
When finished restore your original MAC address.

Part 3 – ARP Poisoning

1) Poison the arp caches of your OWASP and pfSense VMs by replicating the example here: https://simms-teach.com/docs/cis76/cis76-MITM-arp-poison.pdf

Part 4 – Netlab+

1) Log into Netlab+, schedule a time slot and do the NDG Ethical Hacking Lab 11 "Network Analysis".

Part 5 – 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 Part 1 include a screenshot showing:
     - **cat /etc/network/interfaces** output
     - **ifconfig eth0** or **ip addr show eth0** output
   - For Part 2 (MAC Spoofing) include screenshots of:
     - A portion of your Kali command line session showing how to use macchanger to spoof a MAC address.
     - Wireshark capture showing your Kali pinging your pfSense VM and with the spoofed MAC address.
   - For Part 3 (ARP Poisoning) include screenshots of:
     - Cain showing successful ARP poisoning of OWASP and pfSense VMs.
     - WinXP Wireshark capture showing the poison ARP flooding.
     - On OWASP, output from **cat admonition**
   - For Part 4 (Netlab+) include screenshots of:
     - Any command line tcpdump output from Part 1.
     - Any interesting Wireshark output from Part 2.
     - Extra credit Any useful Xplico output for Part 3. “Useful” means clearly showing the benefit of using this forensics tool to analyze packet captures.

   As an example you can see Benji’s report for Pod 5 here:
   https://simms-teach.com/docs/cis76/cis76-lab02-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)

6 points for correct OWASP VM configuration.
6 points for correct MAC spoofing.
6 points for correct ARP poisoning.
6 points for correct (Netlab+ NDG Lab 11) tcpdump output.
6 points for correct (Netlab+ NDG Lab 11) Wireshark output.

Extra Credit (3 points)

3 points - Screen shot showing useful Xplico output you create in NetLab+.