

CIS 76 Ethical Hacking Lab Exercise

Lab 6: Enumeration
Fall 2017

Lab 6: Enumeration

This lab introduces the use of various enumeration tools.

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.
- If you haven't already configured your pod in the previous labs, then follow the instructions here: <https://simms-teach.com/docs/cis76/cis76-podSetup.pdf>

Part 1 – Zenmap

- 1) Review the corresponding module in Lesson 7.
- 2) Do the first activity (install SearchDiggety/Zenmap).
- 3) Do the second activity (“intense” scan) and answer the “black bomb” question.
- 4) Get a screen shot of your EH-WinXP desktop showing Zenmap with the “Host Details” view showing a black bomb icon.

Part 2 – Global Network Inventory

- 1) Review the corresponding module in Lesson 7.
- 2) Install Global Network Inventory on your EH-WinXP VM.
- 3) Conduct an inventory of your EH-WinXP VM and answer the BIOS question.
- 4) Get a screen shot of your EH-WinXP desktop showing the “BIOS” tab information as well as the related quick report of the BIOS details.

Part 3 – NBTSTAT and NET VIEW commands

- 1) Review the corresponding module in Lesson 7.
- 2) Do the activity (list workgroup systems and get a MAC address) and answer the question.
- 3) Get a screen shot of your EH-WinXP (or Kali) desktop showing the remote desktop connection and the output from the net view and nbtstat commands.

Part 4 – SuperScan

- 1) Review the corresponding module in Lesson 7.
- 2) Do the first activity (run SuperScan).
- 3) Do both the second activity (enumerate Windows VM) and answer the question about users.
- 4) Get screen shots of your EH-WinXP desktop showing the both local users and their last logins.

Part 5 – Hyena

- 1) Review the corresponding module in Lesson 7.
- 2) Do the activity at the end (run Hyena) and answer the question.
- 3) Get a screen shot of your EH-WinXP (or Kali) desktop showing the remote desktop connection and Hyena showing your group membership.

Part 6 – enum4linux

- 1) Review the corresponding module in Lesson 7.
- 2) Do the activity at the end (run enum4linux) and answer the shares question.
- 3) Get a screen shot of enum4linux showing the two *-pics file shares.

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.
- Part 1 screen shot including the answer to the module question.
- Part 2 screen shot including the answer to the module question.
- Part 3 screen shot including the answer to the module question.
- Part 4 screen shot including the answer to the module question.
- Part 5 screen shot including the answer to the module question.
- Part 6 screen shot including the answer to the module question.

As an example you can see Benji Simms' report here:

<https://simms-teach.com/docs/cis76/cis76-lab06-simben76.pdf>

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

Remember **late work is not accepted**. If you run out of time submit what you have completed for partial credit.

Grading Rubric (30 points)

- 3 points for Part 1 screen shot.
- 2 points for Part 1 answer to question.
- 3 points for Part 2 screen shot.
- 2 points for Part 2 answer to question.
- 3 points for Part 3 screen shot.
- 2 points for Part 3 answer to question.
- 3 points for Part 4 screen shot.
- 2 points for Part 4 answer to question.
- 3 points for Part 5 screen shot.
- 2 points for Part 5 answer to question.
- 3 points for Part 6 screen shot.
- 2 points for Part 6 answer to question.