

Socket Programming

Offensive and Defensive Tool Construction

Table of Contents

[Objectives 2](#_Toc67897537)

[Background Reading 2](#_Toc67897538)

[Important Information 2](#_Toc67897539)

[Introduction 3](#_Toc67897540)

[Setup 3](#_Toc67897541)

[Questions 1 (5) 3](#_Toc67897542)

[Sanity Test (No Marks. Do not submit answers for Sanity Test!!!) 3](#_Toc67897543)

[Problem 2 (15) 4](#_Toc67897544)

[Questions 2 (5pts) 5](#_Toc67897545)

[Problem 3 (10) 6](#_Toc67897546)

[Problem 4 (35) 7](#_Toc67897547)

[Questions 4 7](#_Toc67897548)

[Problem 5 (See chapter 5 for an example) (25pts) 9](#_Toc67897549)

[Questions 5 9](#_Toc67897550)

[Problem 6 (40) 10](#_Toc67897551)

[Questions 6 11](#_Toc67897552)

Offensive and Defensive Tool Construction

Applying a Debugger for Windows

Objectives

This lab focuses on the following objectives:

* Understand the basics of Network sockets.
* Write Python code to scanner ports.
* Perform analysis on results of port scan.

Background Reading

Read chapter 2 in the ***Black*** *Hat Python* textbook. The following links are also useful:

* https://docs.python.org/3/library/socket.html/
* https://realpython.com/python-sockets
* A myriad of YouTube tutorials; use the link below:
  + https://www.youtube.com/results?search\_query=python+socket+programming
* https://en.wikipedia.org/wiki/Banner\_grabbing
* https://en.wikipedia.org/wiki/Netcat

# Important Information

* Download executable on D2L

**YOU MUST SUBMIT YOUR CODE AND IMAGES OF THE CODE EXECUTION. CREATE A BLANK DOCUMENT AND SUBMIT YOUR ANSWERS THERE.**

**YOU WILL LOSE MARKS FOR NOT FOLLOWING THE ABOVE REQUIREMENTS.**

# Introduction

The network is arguably the most sought-after attack surface. For network administrators, nightmares involve hackers penetrating their network defenses and stealing valuable information from the organization. For hackers and penetration testers they dream of being able to enumerate all the weak points or dream up scenarios to gain a foothold and eventually escalate privileges. For the hacker the final pot of gold is exfiltration of data and for the pentester to provide their clients a valuable report on what weak points to secure.

As a cyber-security analyst your task is to gain and understanding of how all of this is possible and eventually build the tools or leverage tools to provide insight into these problems.

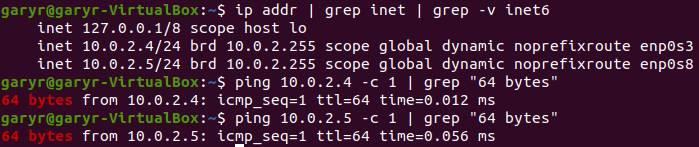
# Setup

1. You will need a Linux VM (create a new one or use an existing one).
   1. **SNAPSHOT (and|or) CLONE THE VM, in case you need to recover the VM.**
2. Before booting up the VM a few adjustments need to be made
   1. If using VirtualBox:

**File** > **Preferences** > **Network**

Add a new NatNetwork

* 1. Select the VM, open the settings for your VM
  2. Under Network Enable “**Adapter 2**”
  3. Click OK
  4. Confirm that both Networks are available and that you can ping the IP addresses associated with those interfaces.

See below for an example:

1. Copy the file **Portcreator2021**, provided on D2L, to your VM and execute it from the command line.

**CTRL+C terminates the application**.

## Questions 1 (5)

1. Name three purposes of the netcat tool?
2. Python provides a simple http(s) module, what is the name of the module?
3. Show images the module running using port 8989 and 80.

## Sanity Test (No Marks. Do not submit answers for Sanity Test!!!)

1. How can you tell if a service, that uses a port, is running on Linux?
2. What tool(s) can you use to provide information about the ports available on your Linux VM?

# Problem 2 (15)

Nmap is a powerful port scanner that allows Gray, Black and White hat hackers to enumerate the network interfaces of a system. The hope is to determine if there are soft targets as well as if open ports that should be closed are available on the system.

In this section you will build a port scanner in Python. Your job will be to enumerate all available ports on your system.

1. Run the Tool downloaded from D2L (ie **./Portcreator2021**)
   1. The Portcreator2021 is simple tool that generates open ports on your network interfaces
2. Provide screen shots showing the output of the port scanner. Only show the open ports?
   1. Generate a file with all the open ports on your 2 IP interfaces ONLY.

## Questions 2 (5pts)

1. How many possible TCP ports can there be on a system?
2. Can a regular user generate ports below 1024?
3. Do open ports automatically mean that there is a vulnerability?
4. What determines whether a port is vulnerable?
5. Name at least two services (on Windows/Linux) that you should shutdown if you find that service running.

## Submit:

1. The python files
2. The screenshots of program output
3. File containing open network ports.
4. Answers to questions.

# Problem 3 (30)

Banner Grabbing involves the process of connecting to and communicating with a server to potentially gain information about the type of server and services being provided. It can be used by White, Black and Gray hat hackers to provide useful inform that could lead to potential exploit(s).

During a user’s usual interaction of these services these bits of information are hidden from the average user. In this section we will see how it could be possible to extract useful information.

Try the following to get an idea of the tool to be built.

## Testing Ground:

1. Install openssh-server

**sudo apt install openssh-server**

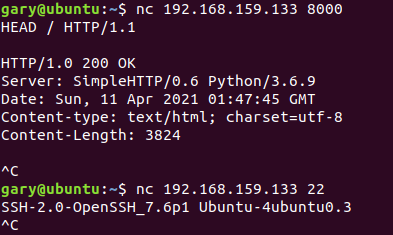
1. Run openssh-server

**sudo systemctl start ssh**

1. Start python http server

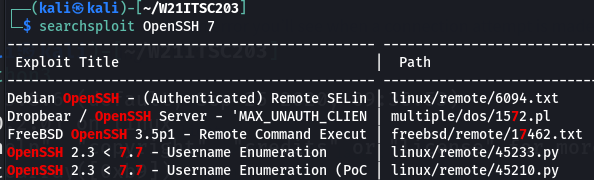
*gary@ubuntu:~$* **python3 -m http.server**

*Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...*

1. Get Banner with netcat for both services.
2. If you are not using kali for this lab you must setup **searchsploit** locally on your VM (takes about 200MB)
3. **cd ~**
4. **git clone https://github.com/offensive-security/exploit-database.git**
5. **sudo apt update**
6. **cd ./exploit-database**
7. **sudo mkdir /opt/exploitdb**
8. **sudo cp files\_\*.csv /opt/exploitdb**
9. Manually check to see if there’s an exploit using a tool like searchsploit

**./searchsploit OpenSSH**

Are there any services available for you to enumerate?



**Submit** an image of the services running on your VM and also report if either service has any known vulnerability.

## Python Banner Grabber

You will build a python Banner Grabber for the Portcreator2021.

1. The tool will go through the entire list of open ports and grab the banners
2. Find all the running services already completed in a previous Problem
3. **IMPORTANT**: If the port is an HTTP port; you will need to send the server a request before it will respond. Use the **HEAD** command.
4. Determine if the service is exploitable.
   1. This is going to be very challenging because you will need to run **searchsploit** and then parse the results. **HINT: See what happens if you search searchsploit a non-existent service.**
5. Print a list of services you found, the port and IP Address that they were found on. Example:

**10.0.2.5 – 22 - OpenSSH 7.6**

**10.0.2.5 – 2222 - OpenSSH 7.6**

**10.0.2.5 – 5543 – HTTP**

1. The output displayed on the screen should also be written into a time stamped file. Example: bannergrab\_04122021\_1551

The file represents the following information:

* 1. Filename: bannergrab
  2. Date: April 12, 2021
  3. Time: 3:51pm

## Submit:

1. The python files
2. The screenshots of program output
3. File containing open network ports.
4. Answers to questions

## Bonus (10pts)

Enhance your program so that it uses 3 Threads to scan the ports.