**PROG8190**

**Computer and Application Security \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Assignment #4 – Scanning – due at the date/time specified in eConestoga**

**Marks: / 25**

**Weight: 5%**

*This is an individual assignment. Do your own work and do not share your work with others. Sharing work is an Academic Offense and is subject to a penalty. Be aware that all source code and other documentation is automatically checked by eConestoga upon submission.*

The purpose of this assignment is to explore the Scanning stage of Penetration Testing. We must be able to discover open IP addresses, discover open ports and what services run on those ports, and then finally discover vulnerabilities on those services. We will use some scanning tools to help find some vulnerabilities in this application.

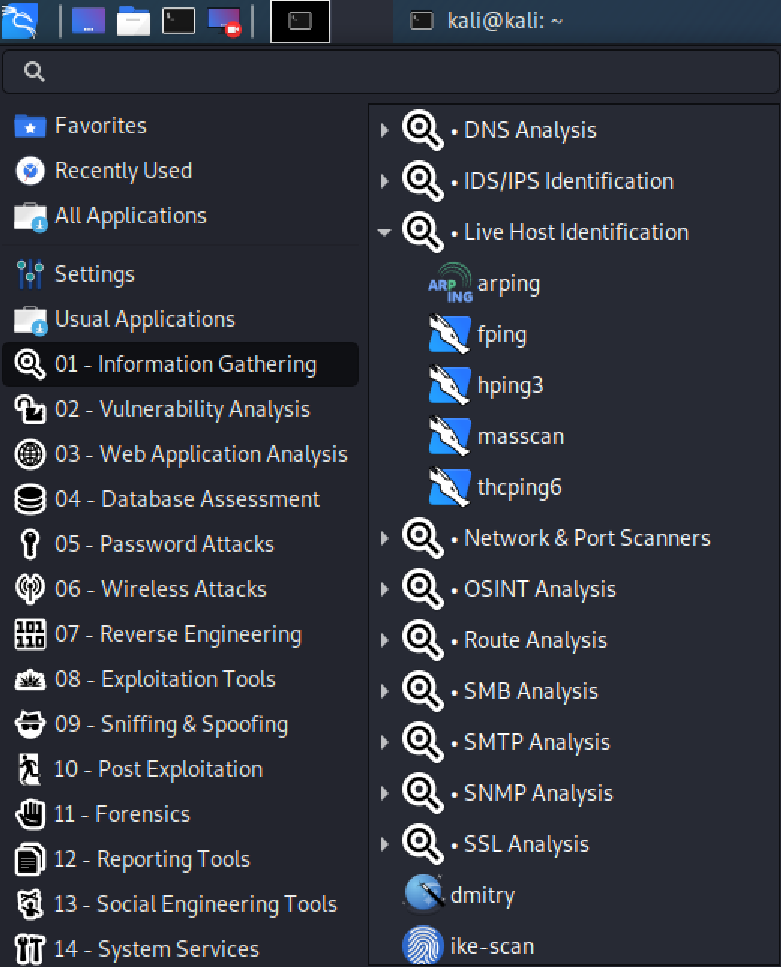
**This assignment is to be completed individually.** You are to treat this as if you were hired by a company to perform a Penetration Test on their systems.

In this assignment, we will be attempting to exploit the Metasploitable2 Virtual Machine. Instructions for running this Virtual Machine are available [here](https://www.youtube.com/watch?v=-45OU0shOrk). You will also require your Kali Linux VM (as the attacker). You may also need to adjust your Network Settings in the Virtual Machine to be using a Host-Only connection to have both of your VMs on the same network as your physical PC – link [here](https://www.vmware.com/support/ws4/doc/network_configure_ws.html) for more information.

**Task 1**

The first step is to find the IP address of the Metasploitable2 VM **without** using the ifconfig command as such, leave your Metasploitable2 VM up and running and perform the remaining tasks on only your Kali VM.

On your Kali VM, we will use the Linux command tool fping.



When fping starts, read the options presented for fping and determine the correct option(s) required for:

* Showing systems that are alive
* Generating a target list from a supplied IP network
* Printing the cumulative statistics upon exit

Issue this command and capture the screenshots of this command executing. In these screenshots, be sure to show the command used and the final output (that includes the statistics). You will need multiple screenshots for this – include them in your MS Word document.

Re-issue the command, but this time, use the appropriate settings to pipe your results to a text file. Save this text file as you will need to include this as part of your submission. Take a screenshot of this and include it in your MS Word document.

Based on the results of the fping command, you may have found some IP addresses that are alive, while finding most of the IP addresses are not alive. Now, using the **nbtscan** tool on each of the alive IP Address, confirm the correct IP Address of your Metasploitable2 VM. Provide screenshots of using this tool with the commands used and all of the outputs and include them in your MS Word document.

**Task 2**

Once you’ve determined the correct IP address of the Metaspoitable2 VM from Task1, use NMAP (again from within your Kali Linux VM) and perform a single NMAP scan with the following options: TCP SYN, OS detection, version detection, and verbose output (you need to use four (4) distinct options here).

**DO NOT PERFORM MULTIPLE SCANS (ONE FOR EACH OPTION)!**

Capture all of the NMAP output (you may have to capture using multiple screenshots) from this command and highlight the open ports and services on these screenshots. Include these in your MS Word document.

This should detect several services. You are to search the output and select one service (other than VSFTPD 234) on an open port. You must then search for vulnerabilities manually. Google is a good way to do this. **Provide the entire NMAP output as a screenshot, highlighting the section that you have selected to investigate for vulnerabilities. Research this version of the service.**

# When was it released?

* **Is it the newest version? If not, when was it updated?**
* **Is there a known vulnerability for this service? If so, describe *in your own words* how this version is vulnerable and what the vulnerability allows an attacker to do. DO NOT COPY WORD FOR WORD FROM ANY SOURCE.**

**NOT PROVIDING THE PROPER APA REFERENCES FOR THIS SECTION WILL CAUSE A SIGNIFICANT LOSS OF MARKS AND/OR AN ACADEMIC OFFENSE/WARNING BEING FILED.**

**Submissions:**

eConestoga submissions –

* An MS Word document named:

**FirstName\_LastName\_StudentID\_Assignment4.docx**

Where FirstName, LastName and StudentID (seven-digit student ID) are your particulars.

that contains:

* + 1. Assignment Title Page with your name, student ID, “Assignment #4” in the title and date
    2. Answers to the above questions, along with accompanying screen shots
    3. References
  + Text file of your raw fping output, named as:

**FirstName\_LastName\_StudentID\_Assignment4.txt**

Where FirstName, LastName and StudentID (seven-digit student ID) are your particulars.

Late penalties will apply for any/all submissions submitted past the due date.

A -10% penalty will be applied for any files that are zipped up or not using the correct naming format.

As this is a technical report, proper spelling and grammar will also be required and marks may be lost for reports that have poor spelling and / or grammar. A more detailed marking scheme is shown in the Rubric associated with the Assignment Folder in eConestoga.