SENG8030

Testing Tools

Assignment #4 – Penetration Testing

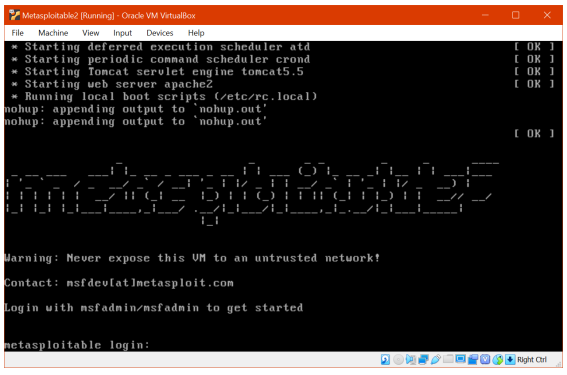
75 Marks – worth 7.5%

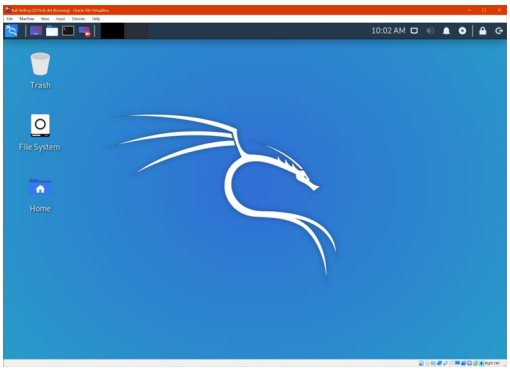
This is an individual assignment. Do your own work and do not share your work with others. Sharing work is an Academic Offense and is subject to a penalty. Be aware that all source code and other documentation is automatically checked by eConestoga upon submission.

The purpose of this assignment is to explore the Reconnaissance and Scanning stages of a Penetration Test. As a result, 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.

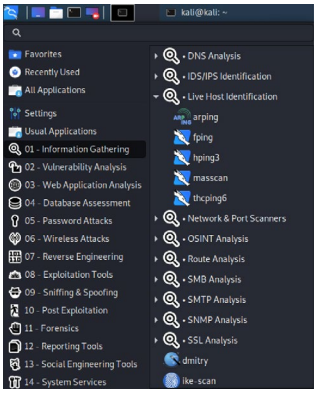
You are to treat this Assignment as if you were hired by a company to perform a Penetration Test on their systems.

In this assignment, we will be attempting to exploit the Metasploitable2 Virtual Machine. Instructions for running this Virtual Machine are available in eConestoga along with this Assignment. 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 for more information. Ensure that both VMs are operational as shown below:





The first step is to find the IP address of the Metasploitable2 VM – that is on the same network as our Kali attacking VM. Find the IP Address of ONLY your Kali VM by issuing the `ifconfig` or `ip a` command – this will give you the network address portion which you can then use to find the exact IP Address of the Metasploitable2 VM. Now, we will use the Kali Linux command tool "fping". You can access fping from the Kali application menu as shown below or simply from the Terminal prompt by typing in `fping -h`



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

- scanning all of the IP addresses on the network on which both the VMs are on
- and showing the final stats

Issue this command and capture the screenshots of this command executing and showing all the IP addresses that are alive as well as those that are not reachable and the final stats. (There may be several screenshots that you will have to capture from this output).

Based on the results of the fping command, you may have found some IP addresses that are alive, while finding a majority of the IP addresses are not alive. Discuss a bit about how you would go about to find the exact IP address of the Metasploitable2 VM – in this discussion, talk about what the other IP addresses that are alive are as well. Do not use the `ifconfig` or `ip a` commands on the Metasploitable2 VM as this will not simulate the finding of an IP Address in a live environment! Now, use the `nbtscan` tool in Kali on each of the live IP Addresses to get more information about them – take a screenshot of these outputs – ensure to use the correct options if required.

Once you've determined the correct IP address of the Metaspoitable2 VM, use NMAP (again from within your Kali Linux VM Terminal or application menu) and perform a single scan with the following options: TCP SYN, OS detection, version detection, and verbose output.

Performing multiple scans of each option here will result in a loss of marks! Only perform one NMAP scan that encompasses all of the required options.

Capture all of the NMAP output (again, you may have to capture using multiple screenshots) from this command and highlight the open ports and services on these screenshots.

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.**
- **Again, describe in your own words, what would you do with this information as part of completing the Penetration Test on this system. Demonstrate the next steps to help explain your points by using the appropriate commands in Kali and provide a brief recommendation on your findings as well as the next steps that a client can do to safeguard their systems from your chosen attack type.**

For the above portion, provide the correct APA Referencing to all sources that you used.

DO NOT COPY THE TEXT OF THE QUESTIONS
DO NOT COPY WORD FOR WORD FROM ANY SOURCE.

Submissions

The format for submitting the assignment is as follows:

1. eConestoga submissions:

   A single MS Word document named:

   FirstName_LastName_StudentID_Assignment4.docx that contains:

   i. Assignment Title Page with your name, student ID, "Assignment #4" in the title and date; INCLUDE CLEAR NUMBERS FOR YOUR ANSWERS
   ii. A screen shot showing the setup of Kali on your VM (show your machine name, and show Kali in nested windows, make cure to include date/time)
      - [**25 Marks**]
   iii. The correct output from fping showing the correct options used as well as the results of all responses and stats
      - **[5 Marks]**
   iv. Answers and screenshots from nbtscan provided regarding the finding of the correct IP Address
      - **[10 Marks]**
   v. NMAP output is correctly shown with the correct options being used and properly showing the highlighted service being researched upon
      - **[10 Marks]**
   vi. Answers regarding the research about the highlighted service as well as the next steps in completing the pen test and recommendations.
      - **[25 Marks]**
   vii. References Used

Please submit to the **"Assignment #4"** assignment folder in eConestoga.
Late penalties will apply for any late submissions.
A -50% 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.