Faculty of Business, IT, and Management
HACK2200 Hacking and Exploits
Lab 1: Reconnaissance and Packet Sniffing

Instructions

- This lab should be completed individually.
- This lab is designed for the purpose of education and training, but not for any illegal activities including hacking. Beware to only use these exploits on hosts that you have permission to hack.
- When a question asks for screenshots, your screenshots must:
  - Include the full window (the application window, or the terminal window, etc.),
  - have the PROMPT setup as per the instructions, including the date and time in the same format provided in the instructions. Screenshots without the prompt setup will receive zero credit,
  - be clearly readable,
  - include all the information required by the question, and
  - not include extra commands, failed attempts, and/or error messages. When you run into errors, troubleshoot them, clear the screen, and rerun the commands to capture a screenshot clear of any error messages.
- Failure to follow submission instructions will result in marks deduction. There will be marks deduction for including more than what is required in the instructions. Do not provide any screenshots that are not required in the instructions.
- The below instructions are guidelines, you are expected to troubleshoot any errors you run into.
- Read and complete the lab instructions below and finish all the tasks. Once completed, submit your answer file on DC Connect.

Part 1- Reconnaissance

This lab is limited to collecting publicly available information. You are expected to do passive information collection **only** with publicly available information. You do not have permission to perform any active network scanning, enumeration, or vulnerability assessment in this lab.
We will perform some passive reconnaissance tasks using Durham College as our client.

1. On your KaliVM, use Maltego free edition to find information about your client organization. Provide 2 screenshots of your most important findings (e.g., Company Stalker, and URL To Network And Domain Information).
2. Find the asn (Autonomous System Number) of the client organization, and run it through Shodan. Provide 1 screenshot of your most important findings.

3. Use sublist3r to collect information on your client organization, and provide 1 screenshot of your findings. Include the command you ran in sublist3r.
4. Use theHarvester to find collect information about your client organization. Provide 1 screenshot of the most important findings. Include the command you ran in theHarvester.
5. Use Netcraft to generate a site report of your client organization's website. Provide 1 screenshot of the generated report showing the organization's IP range.

Part 2 - Wireshark

1. Watch the Wireshark tutorial posted on DC Connect. Note that if you are familiar with the use of Wireshark, you can skip this step.
2. Read the below article:
   Top 10 Uses of Wireshark for Hackers Part I
   https://www.ethicalhacker.net/columns/chappell/top-10-uses-of-wireshark-for-hackers-part-i/
3. Follow the steps under Hack#2, and map the network as per the shown diagram.
4. Follow the steps under Hack#3, use the file ftp-passwords101.pcapng. What is one password you were able to read in clear text?
5. Follow and understand Hack#4 and Hack#5 using sec-sickclient.pcapng file.
6. What made you believe the traffic was Internet Relay Chat (IRC) traffic?
7. Follow Hack#6 in this article: Top 10 Uses of Wireshark for Hackers Part II https://www.ethicalhacker.net/columns/chappell/top-10-uses-of-wireshark-for-hackers-part-ii/ to decode the traffic as IRC.