Faculty of Business, IT, and Management

HACK2200 Hacking and Exploits

Lab 1: Reconnaissance, and Packet Sniffing

Answer File

**Syed Adil Ahmed Altaf Hussain**

**100841799**

# Part 1- Reconnaissance

1. Provide a screenshot of running your client domain through Maltego Company Stalker. (10 Marks)

**A screenshot of a computer

Description automatically generated**

1. Provide a screenshot of running your client domain through Maltego URL To Network And Domain Information. (10 Marks)

A screenshot of a computer

Description automatically generated

1. Provide a screenshot of running your target asn through Shodan. (10 Marks)

**Graphical user interface, text, application

Description automatically generated**

1. Enter the command you used to run your client company through sublist3r. (10 Marks)

**Sublist3r -d durhamcollege.ca -t 3 -e bing**

1. Provide a screenshot of your sublist3er findings. (10 Marks)

**A screenshot of a computer

Description automatically generated with medium confidence**

1. Enter the command you used to run your client company through theHarvester. (10 Marks)

**theHarvester -d durhamcollege.ca -l 500 -b google**

1. Provide a screenshot of your theHarvester findings. (10 Marks)

**A screenshot of a computer

Description automatically generated with medium confidence**

1. Provide a screenshot of the IP range reported in the site report generated by Netcraft. (10 Marks)

A screenshot of a computer

Description automatically generated

# Part 2 - Wireshark

1. What password you were able to read in clear text in the ftp-passwords101.pcapng file? (10 Marks)

**mickey**

**cristina**

**michael**

1. What made you believe the traffic was Internet Relay Chat (IRC) traffic? (10 Marks)

**Usually, the IRC traffic starts with NICK and USER commands and runs on TCP port 6667. On decoding the data transferred on port 18067 as text we get the result as Nick and User with which we can conclude the traffic could be IRC traffic.**

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated