|  |  |
| --- | --- |
| Course | INFT1201 Hacking and Exploits |
| Lab | Lab 1- Reconnaissance, & packet sniffing |
| Name of the Student | Maisha Khatoon |
| Student ID | 100899259 |

INFT1201 Hacking and Exploits

Lab 1: Reconnaissance, and Packet Sniffing

Answer File

# Part 1- Reconnaissance

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

**{Insert Screenshot Here}**

A picture containing text, software, screenshot, computer icon

Description automatically generated

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

**{Insert Screenshot Here}**

A picture containing text, software, screenshot, multimedia software

Description automatically generated

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

**{Insert Screenshot Here}**

A screenshot of a computer

Description automatically generated with medium confidence

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

**{Insert command Here}**

**Ans: sublist3r -v -d durhamcollege.ca -e google, ask, yahoo -b**

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

**{Insert Screenshot Here}**

**A screenshot of a computer

Description automatically generated**

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

**{Insert command Here}**

Ans: **theHarvester -b all -d dc-uoit.ca**

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

**{Insert Screenshot Here}**

**A screenshot of a computer screen

Description automatically generated with medium confidence**

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

**{Insert Screenshot Here}**

**A screenshot of a computer

Description automatically generated with medium confidence**

# Part 2 - Wireshark

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

**{Insert password Here}**

Ans: The following are some of the passwords that I was able to read:

nyquist

oceanography

nutritition

nuclear

orca

osiris

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

**{Insert your answer here, shouldn’t exceed one line}**

**Ans:** The JOIN command in the TCP stream stands for Internet Relay Traffic (IRC).