Assignment 2

1. Investigate and read up on a tool called Maltego. Use whatever resources you see fit. Maltego is included in Kali Linux. Make use of this tool to search for 1. yourself and 2. a favorite actor or sports figure. Provide a screenshot.

2. Use Maltego to search for information about South Dakota University (SDSU). Note: This is not DSU. You were explicitly instructed to use only this tool to discover information about the target, so do not use any other tools. Do not use any active scanning against the target—no port scanning or exploitation. This is just information gathering. Show a few screenshots showing your results.

**Google Dorks**

*Note: Do not “try your best” or guess. Use the correct Google directives.*

3. Using Google, how do you find PowerPoint files that are on SDSU? Provide search term and

screenshot of results.

4. Using Google, how do you find PowerPoint files with the word cats in the title? Provide search term and screenshot of results.

5. Using Google, how do find Microsoft Access files about marking data analysis? Provide search term and screenshot of results.

6. Using Google, use in title directive to find sites that have "index of" in the title.

7. What benefit does “index of” have for us as penetration testers?

8. Using Google, make use of a directive to show all sites that linked to sdbor.edu.

9. Using Google, make use of a directive to show all sites that are similar to Walmart.

10. Use Kali Linux to do a whois on SDSU. Provide a screenshot and include it in the same Word/PDF.

11. Run Netcraft on SDSU and show a couple screenshots of your results. Anything stand out to you as interesting?

12. How can you defend against whois being misused against your organization?

13. What is the difference between these Google directives: allintext:[term] and intext:[term]. Explain and give an example with screenshots.

Note: Maltego is available in Kali under Information Gathering.

