Name : Shivam Agarwal
Roll No. : 2020123

Ans 3.a,b) I have used selenium to automate the process(tried using bs4 but search queries don't change its web address, weird)

So first we open the webpage of dnsdumpster using selenium
Then find its search bar and then enter the domain we want to search for and the send the enter key

Then we filter using css_selector and store all the tables in the var ‘data’
The Host records are then moved to var ‘host’
The values in the first column(filtered using css_selector) are stored in the var ‘names’ and the values in the second column are stored in the var ‘ips’
We iterate over all rows in names and ips and store the first line in each row after splitting the records
All the subdomains and ips are then combined to form a list of tuples called ‘submission’ which is the printed

Ans 3.c) There are many ways to leverage this:

1. Say the attacker doesn't want to attack the entire network of iiitd but only some part of it, say a particular ip or subdomain, this allows them to ddos that subdomain with a lot less resources as compared to the entire network.

2. Some subdomains might be older and not up to date in terms of security making it easier for attackers to find vulnerabilities. And there is a good chance that these vulnerabilities are also present

in other subdomains as they are usually programmed by same the people or using the same method

3. Increase in chances of CSRF attacks :
   The attacker might succeed in infiltrating a particular subdomain or send a malicious object to that subdomain server that then tries to infiltrate other servers and domains as it bypasses the network firewall