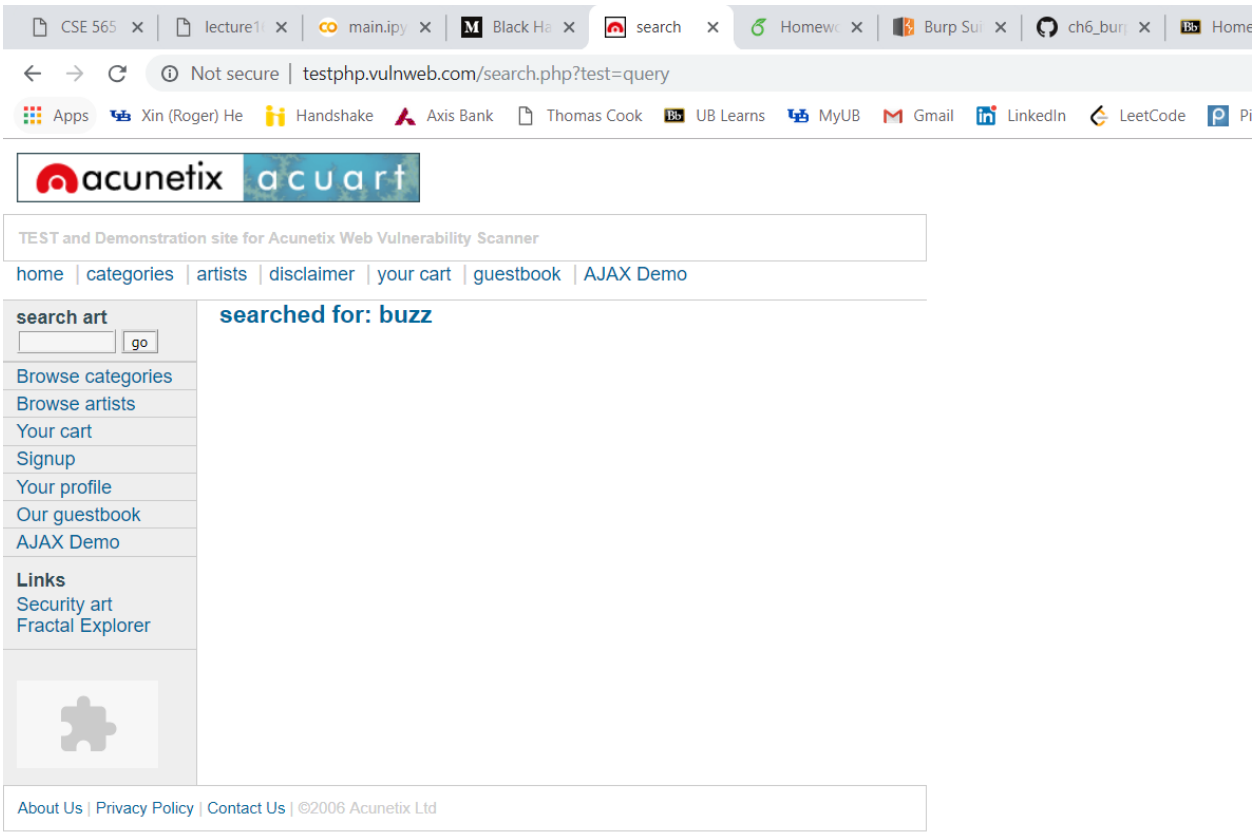

2 Question 2

2.1 Important Property of a program that reproduces itself

The two most important properties for a program to reproduce itself are as follows:

1) The program can be easily written by another program.(self-reproducing)
2) The program can contain an arbitrary amount of excess baggage that will be reproduced along with the main algorithm.

These two properties are necessary for a self replicating or a recurring program.The self replicating programs are called as Quines and in this paper a Quine has been developed in the first stage using these two properties. In the example shown in the paper even the comments are replicated.

The first point is important because only if we are able to write a program, we will be able to generate quines and hence this program must be able to to be written by another program. The second property states that the program may contain arbitrary extra baggage that can be reproduced(For example the comments in the program have no significance but still they are reproduced) along with the main algorithm.Also these quines must have the property of a recursion in the program as well.

2.2 Observations in the article and rootkits in Operating System

In the article mentioned above, he can actually log on to any remote system by using the trojan that he planted in to the system by actually making the system miscompile the login command so that it would accept either the intended encrypted password or a particular known password. Thus if this code were installed in binary and the binary were used to compile the login command, he could log into that system as any user.

Rootkits also work in the same way as the trojan mentioned above.A rootkit is a program or, more often, a collection of software tools that gives a threat actor remote access to and control over a computer or other system., a rootkit gives the remote actor access to and control over almost every aspect of the operating system (OS). Older antivirus programs often struggled to detect rootkits, but most antimalware programs today have the ability to scan for and remove rootkits hiding within a system. The rootkits developed now are the recent versions of the trojans mentioned above. One main difference though is that rootkits unlike the trojan cannot multiply itself wheras a quine can occur self-recurringly. The only similarity that one can have between the trojan mentioned here and the rootkits are both of them can go undetected.Rootkits can self reproduce and the program mentioned in the paper is also self reproducing.

3 Question 3

The problem deals with the Distributed Denial of service Attack(Ddos) and asks us to calculate the number of zombies to flood a target machine using a 0.5 Mbps,2 Mbps and 10 Mbps Link. In order to implement a classic DDoS flood attack, the attacker must generate a sufficiently large volume of packets to exceed the capacity of the link to the target organization.
Also, the attacker has compromised a number of broadband-connected residential PCs to use as zombie systems.Each zombie has an average uplink capacity of 128 kbps. The ICMP echo request packets are 500 bytes in size.

Information Obtained from the question
Capacity of each zombie = 128 kbps.
Size of each echo request packet in bytes = 500.

The formula used is as follows :
Number of packets / sec = Capacity of the link/ (Size of packet * Number of bits)