3.1 Maximum number of packets by a single zombie if byte size is 500 per second

Here the capacity of the link is 128 kbps. The packet size as mentioned is 500 bytes. Substituting in the formula above we get,

Maximum no. packets with the specified configuration =

$$\frac{128 * 1000}{500 * 8}$$

Calculating the values we get the answer as 32 packets. Hence, a maximum of 32 packets per second can be sent by a single zombie is capacity is 128 kbps and the byte size is 500.

3.2 Number of Zombies to flood a target organization using 0.5 Mbps

Here the capacity of the link is 128 kbps. As stated in the question the target organization is using 0.5 Mbps Link and we have to flood that link by sending in more packets by using the zombies. In order to predict the number of zombies we will have to divide the target organization link and our average uplink capacity of each zombie.By doing so, we will be able to figure out the required number of zombies.

Number of zombies required =

$$\frac{0.5 * 1000000}{128 * 1000}$$

Calculating the values we get the answer as 3.90 zombies which is ceiled to 4 zombies. Hence, In order to flood a 0.5 Mbps link with the specified configuration we need 4 zombies.

3.3 Number of Zombies to flood a target organization using 2 Mbps

Here the capacity of the link is 128 kbps. As stated in the question the target organization is using 2 Mbps Link and we have to flood that link by sending in more packets by using the zombies. In order to predict the number of zombies we will have to divide the target organization link and our average uplink capacity of each zombie.By doing so, we will be able to figure out the required number of zombies.

Number of zombies required =

$$\frac{2 * 1000000}{128 * 1000}$$

Calculating the values we get the answer as 15.60 zombies which is ceiled to 16 zombies. Hence, In order to flood a 2 Mbps link with the specified configuration we need 16 zombies.

3.4 Number of Zombies to flood a target organization using 10 Mbps

Here the capacity of the link is 128 kbps. As stated in the question the target organization is using 10 Mbps Link and we have to flood that link by sending in more packets by using the zombies. In order to predict the number of zombies we will have to divide the target organization link and our average uplink capacity of each zombie.By doing so, we will be able to figure out the required number of zombies.

Number of zombies required =

$$\frac{10 * 1000000}{128 * 1000}$$

Calculating the values we get the answer as 78.1 zombies which is ceiled to 79 zombies. Hence, In order to flood a 10 Mbps link with the specified configuration we need 79 zombies.

3.5 Thousands of Zombie Systems on a large organization

When an attacker has a 1000's of such zombies, it will be very difficult for a larger organization to protect from such botnets. Each zombie was capable of sending 32 packets of size 500 per second.The average capacity is 128 kbps which when multiplied by 1000 gives 128000 kbps which when converted to Mbps is 125. Hence the target organization must have a link that is greater than 125 Mbps to avoid a Ddos Attack.

4 Question 4

4.1 Firewall Rules

The IP addresses of a corporate network is 219.33.*.*
Allowing all incoming and outgoing connections to the web servers with IP addresses 219.33.12.2 and 219.33.3.4 for both HTTP and HTTPS

- allow TCP *:*/out -> 219.33.12.2:80/in
- allow TCP *:*/in -> *:*/out
- allow TCP *:*/out -> *:*/in (if ACK bit set)

- allow TCP *:*/out -> 219.33.12.2:443/in
- allow TCP *:*/in -> *:*/out
- allow TCP *:*/out -> *:*/in (if ACK bit set)