A(X) Probability of guessing the correct address

P(X) Probability of guessing the correct port

N1 Average number of attempts needed to guess address

N2 Average number of attempts needed to guess port

n Number of addresses in address space

m Number of ports in port range

I Shuffling interval in sec

S Scanning rate per seconds

**Without MTD**

**(To find ports, IPs should be found.)**

N1 = n/2

N2 = N1 + m/2

**IP**

Average case time: N1/S

Worst case: n/S

**Port**

Average case time: N2/S

Worst case: n/S + m/S

**With IP MTD**

z = S\*I/n

P(X) = ∑ z (1-z)y (y goes from 0 to infinity) (Here is the logic: Consider n=100 and I\*S=20. Hence there are 5 shuffling for a complete scan. Attacker starts from 1. In the first round, the success probability is 20/100=0.2 since shuffled IP should be between 1-20. For a second round, first round should be unsuccessful. Hence the probability is 1-0.2=0.8. Besides, again the shuffled IP should be between 21-40. Hence probability of the finding the IP in the second shuffling becomes 0.8\*0.2. The third one similar like 0.8\*0.8\*0.2 and so on.)

N1 = n/P(X) = n since P(X) =1

N2 = N1 + m/2

**IP**

Average case time: N1/S

Worst case: Never

**Port**

Average case time: N2/S

Worst case: Never

**With IP and Port MTD**

N1 = n

N2 = N1 + m

**IP**

Average case time: N1/S

Worst case: Never

**Port**

Average case time: N2/S

Worst case: Never