CS 6353
Unix and Network Security
Assignment 1
Due Monday October 7

1. Consider a worm that randomly scans IP addresses to find other vulnerable computers. Assume that there are x vulnerable systems. Assume that Successive random IP addresses generated by a machine and generated by different machines are independent and IP adresses are 32 bits long. Assume that all of the IP addresses can be assigned to computers. Answer the following based on this information.

   (a) What is the probability that a randomly generated IP address belongs to a vulnerable computer?

   (b) What is the probability of a specific vulnerable computer not being hit after y total random IP addresses are generated by the worms?

2. Suggest an efficient way to determine the IP addresses of all the computers with the following requirements

   (a) computers running a web server in the subnet 129.115.20.0/24

   (b) computers running an ftp server in the subnet 115.114.10.0/24

3. Consider an intrusion detection system with the following properties. Attack traffic is 0.1 %. The intrusion detection system is 99 % accurate. That is 99 % of the attacks raise an alarm. Assume that a valid packet causes an alarm 1 % of the time. Answer the following questions based on this information.

   (a) What is the probability that an alarm with be raised for a packet?

   (b) What is the probability that an alarm corresponds to an attack?

   (c) What is the probability that an alarm corresponds to a valid packet?

4. Assume computers c_1 and c_2 with IP address IP_1 and IP_2 and that c_1 and c_2 are in different domains. Computer c_1 can establish bidirectional communication with computer c_2. Consider IP address IP_3 in a third domain. Is it possible for computer c_1 to change its IP address to IP_3 and establish bidirectional communication with computer c_2. Assume that c_1 has a single network adapter. Explain briefly.

5. Let $H(y)$ denote a cryptographic hash function which takes string y of arbitrary length and produces m bit hash and let $H_n()$ denote the first n bits ($n < m$) of the cryptographic hash. Answer the following questions.

   (a) Given a string x what is the probability that none of the m randomly selected strings $s_1, \ldots, s_m$ have hash values with the property $H_n(s_1) = H_n(x)$?

   (b) What is the expected number of random strings necessary to find a string s with the property $H_n(s) = H_n(x)$? (Hint: Compute the probability that there is a match in k^{th} try and use the definition of expectation).