Assignment 2

Subject: Information Security

Due date: 3 April 2023

Teacher Name: Dr. Qaisar Javaid

Question 1.

(a) Compare switched vs broadcast media LANS from security point of view; briefly explain which one is more advantageous and why?

(b) Is it possible to sniff network traffic on both these types of LANs; if yes how?

(c) How can a hacker who has got a machine connected to a network, determine whether he is on a switched or a broadcast media LAN?

(d) To what extent can we provide protection against traffic analysis attacks and how?

Question 2.

(a) How can the routing information be exploited for launching any security attack?

(b) How can RIP spoofing be avoided?

(c) What kinds of local/remote attacks can be launched by an attacker on a host to become an Illegal User and an Illegal Root on the said host?

Question 3.

Consider two networks, each with its own DNS server running. A host on one network wants to get certain information from a specific site on the Internet. Using DNS spoofing, how can the hacker intercept the host's communication with the site? Give step by step procedure for the following scenarios:-

(a) When the hacker and the host are both on the same network?

(b) Describe two ways the hacker may carry out DNS spoofing if the host and the hacker are on separate networks.

Question 4.

Consider an attacker on the same local network as a host (client). How can the attacker employ ICMP re-direct message to trick the host into sending all his outbound traffic (destined for a remote server) to itself (the attacker) instead of to the default router (gateway)? Describe the sequence of messages exchanged between the attacker, the host and the default router?

Question 5.

Consider an e-commerce company, where customers connect to the company web site over internet and provide a user name and password for a private account that is used later for placing orders. Users have to choose their own passwords for the account. Assume that you are the security consultant for the company and are tasked to determine the password selection criteria for these customer accounts. In this regard, you can consider the relative effectiveness of longer versus short passwords, enforcing randomness of password characters compared to permitting the users to choose any characters they like, and whether forcing password changes every six months is a good idea. Briefly discuss (about half a page) the advantages/disadvantages of these password selection schemes to help in deciding the password selection criteria.