National Institute of Technology Calicut
Department of Computer Science and Engineering

Winter Semester 2020 – 21
CS4035D: Computer Security
(B.Tech. (VI), MCA IV, and MCA VI)

Assignment (Submission Date: 09, May.'21)

Instructions:

- The assignment will be evaluated individually.
- You can select ONLY ONE among the three questions.
- Any programming language, library, or toolkit as per the proficiency of the student can be made use of.
- The mini project topic and the selected assignment question should not be the same.
- The source code together with the README file should be uploaded. The source code should be properly commented.
- Design, Workflow, and Algorithm should be briefly documented in not more than 2-3 pages (pdf).
- Screenshots of the various stages of output should be properly named and documented in a PDF file.

Questions

Q1) Design and Develop a Secure Remote Password (SRP) that is one of the strong password protocols developed by Tom Wu. After computing the session key between the communication entities, the parties indulge in message passing. Encrypt the communication between the parties using SRP. You may refer RFC 2945.

Q2) Design and Develop the basic Lamport Hash, a one-time password scheme, developed by Leslie Lamport. You may enhance the scheme by adding salt. Illustrate the authentication with Alice authenticating with Bob using both the basic and enhanced Lamport Hash scheme.

Q3) Design and Develop a Botnet scenario with a single BotMaster and multiple Bots that get involved in DDoS attack. The BotMaster should send a command to the bots that will result in sending TCP/UDP/HTTP packets. Typical commands from BotMaster can be:

1) SEND TCP-SYN <Target-IP> 10
   The bot machine sends 10 TCP-SYN packets to the Target-IP machine
2) STOP Attack
   The bot machine stops sending packets

You can devise your own command structure. You can use Virtual Machines (bots/victim machine) to build your attack scenario. The technicalities are left to the student. However, the student in expected to document the scenario and other technical details in the report.

*****