VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

CSE3501 INFORMATION SECURITY ANALYSIS AND AUDIT
EXERCISE - 2

DATE: 23.07.2020

Implement the following in Wireshark:

1. Protocol Analysis - Address Resolution Protocol (ARP)
2. TCP 3-way handshake
3. Password Cracking
   a. http site
   b. FTP Server
4. Packet Analysis – Ping packets (ICMP)
5. Implement the following filters (Create suitable traffic for each filter, so that you get response for each filter)
   a. ip.addr == 10.0.0.1
   b. tcp or dns
   c. tcp.port == 443
   d. tcp.analysis.flags
   e. !(arp or icmp or dns)
   f. follow tcp stream
   g. tcp contains facebook
   h. http.response.code == 200
   i. http.request
   j. tcp.flags.syn == 1

Note :

- In a word document, mention step by step procedure and show the screen shot for each step output.
- The IP address of your machine has to appear (ipconfig command) in each screen shot (For reliability)