PL506 Network Security Lab

Prerequisites: PL106, PL 206, CS 302, PL 406

List of suggested Assignments:

1. Implement an iterative TCP client and server application to transfer file.
2. Implement a concurrent TCP client and server application to transfer file.
3. Implement UDP client and server application to reverse the given input sentence.
4. Using basic networking command like ping, traceroute, nslookup, netstat and ipconfig (linux platform). Understanding How basic network enumeration is performed. Using whois command
5. Using port scanning to identify open ports and vulnerability detection. Using nmap command.
6. Using Network protocol analyzer tool like ethereal or tcpdump to analyze network traffic
7. Study of vulnerability exploitation techniques like
   a. Code injection using buffer overflow
   b. SQL injection
   c. Cross site scripting
   d. DNS spoofing & Denial of Service
   e. ARP poisoning
   Safeguarding against above attacks.
8. Securing(hardning) a Linux or a Windows system
9. Installing and configuring a Firewall.
10. Installing and configuring Intrusion detection system.
11. Cracking passwords and password management
12. X.509 certificate management (OpenSSL framework can be used for this purpose).
13. Securing network services. i.e. Apache HTTP server.
14. Creating secure tunnels using IPsec.