Lab 3: Cryptography, FTP Server

Objective:

The objective of this lab is to manipulate the mechanisms adopted to apply FTP installation and configuration, enumeration and attack, system security and precaution.

1. Use Linux Centos terminal to install and Configure VSFTPD as FTP server under *NIX.
2. Use Linux Kali machine terminal to execute a network scanning to check if the FTP server is up and running on the Centos machine. (Hint: Port 21).
3. Use Linux Kali machine Msf Server (Metasploit) to search for anonymous login permission.
4. Use Windows machine to connect to FTP server as anonymous user. (Try Filezilla software).
5. Disable the anonymous login inside the config file and try it again in Filezilla.
6. Open Wireshark in Kali machine and try to capture the TCP stream while connecting from Filezilla to VSFTPD server. We will be able to capture the username/password of the FTP authentication because the FTP over port 21 sends the credentials and the data as plain text.
7. Use SSL Certificate to prevent Credential stealing.
8. After restarting the server, try to reconnect to your FTP server via Filezilla while opening Wireshark on Kali machine.
9. Use Linux Kali machine Msf Server (Metasploit) to steal credential with Brute force attack on FTP Server.