Indian Institute of Information Technology, Allahabad
Department of Information Technology

Program Code & Semester: B.Tech (IT)- 5th Semester.

Paper Title: Network Security
Tutorial and Practical Assignment - 2 (Component 1)

Important Note: The group members have to prepare the report and presentation

1. **Tutorial: RSA** - Working and proof of Correctness using Fermat's Little Theorem.
2. **Practical: DES** - Implementation of DES algorithm
3. **Tutorial: Merkle Damgard and Sponge Construction** - How Length Extension attack is related to Merkle Damgard and Sponge Construction?
4. **Tutorial: Stream Control Transmission Protocol (SCTP)** - As we have discussed, TCP is vulnerable to SYN flood attack. If so, how TCP overcomes it?
5. **Practical: TCP SYN flood** - How TCP SYN flooding is possible? Trace the location of TCP file in the Linux/Windows and analyze.
6. **Tutorial: Spoofing** - Discuss the methods of controlling the IP Spoofing.
7. **Tutorial: IPSec Tunnel Mode** - Is there any advantage of using the new IP header in the IPSec tunnel mode?
8. **Tutorial: Network** - Differentiate Gateway and Router. Justify the need.
9. **Tutorial: IPSec** - Why the AH with NAT is not possible when ESP with NAT is possible?
10. **Tutorial: IPSec and SSL** - Analyze in detail, the need of IPSec and SSL. Why not only SSL (TLS) is sufficient?
11. **Tutorial: Active Attack** - Choose the relevant existing protocols and analyze with respect to replay attack, impersonation attack, man-in-the-middle attack and meet-in-the-middle attack. Also, find the solution [nonce, timestamp, etc.] to overcome these attacks.
12. **Practical: Active Attack** - Implement the man-in-the-middle attack using any of the key establishment protocol.
13. **Tutorial: SSL and SSH** - a) Can Eavesdropping possible if we use SCP/SSH/SSL, b) Analyse SSH with Telnet.
14. **Practical: SSL and SSH** - Capture and analyse the SSL and SSH packets using Wireshark
15. **Practical: Length Extension Attack** - Implement the Length extension attack in Merkle-Damgård construction.
16. **Practical: Penetration Testing** - According to the available infrastructure, perform the penetration testing.
17. **Common Assignment for all groups** - virus, worm, threat, advanced persistent threat, bomb, adware, malware, vulnerability, zero day vulnerability, penetration testing, zero-day attack, Shoulder surfing, keylogger, spyware, Trojan, spear phishing, Social engineering attack, ransomware, rootkit