Methods of Attack Detection
Final Project

Requirements

1. The students can choose one topic from the list below according to the student interest.
2. The project may be done by a single student, by a pair of students or by thirds.
3. The output of the project is a theoretical research with an obligatory presentation (around 10-15 minutes) for a group, or software and its obligatory demonstration.
4. The topics are not limited by the list and may be chosen on behalf of a student (with a lecturer's permission only!).
5. If you choose a topic not listed below, send an e-mail to the lecturer (alonhkoz@ac.sce.ac.il) for approval. Please state that you are from TCB college in the subject!

Topics

1. DNS and DNSEC
2. IP and IPSEC.
3. NAT, use, motivation, security
4. Social Engineering: What is it, how it is done, known examples on social engineering attacks
5. Adware, Spyware, Malware. What are they, types, examples and security defense mechanisms.
6. PAM (Pluggable Authentication Model), its operation, configuration and uses.
7. NIS (Network Information Service): its operation, configuration and uses.
8. Kerberos , Kerberos Authentication and Authorization (Needham Schroeder Protocol)
9. LDAP: its servers, infrastructure, operations.
10. RFID and NFC. Advantages and Disadvantages. Uses in Security.
11. Secure Multi party communication.
12. Phishing and other Farming attacks
13. Backdoors
14. ARP Spoofing
15. IP Spoofing
16. Sniffing
17. DNS Cache Poisoning
18. SQL Injection
19. Cross-Site Scripting (XSS)
20. Session and Cookies in HTTP - privacy issue

References:
[1] C. Kaufman, R. Perlman, M. Speciner, “Network Security. Private Communication in a Public World”, 2-d edition, Prentice Hall, 2002.
[2] W. Stallings, “Cryptography and Network Security. Principles and Practices”, 4-th edition, Prentice Hall, 2006.

Good Luck!
Alona