Network Security
Assignment 06
(IDS)

Distribution date: May 22nd , 2011 Due date: May 29th, 2011, at 23:59 pm.

Note Carefully:

- Send your assignment by email at asimrasheed@mcs.edu.pk only. Submission to any other address is not accepted.
- There is a 25% penalty on late assignments, up to half an hour. More than half an hour late assignments will NOT be accepted, what so ever is the reason.
- Total points for this assignment are 50, which will be scaled down as per plan.
- Important for Email Submission:
- The subject field of your email must be "Assignxx_full_name_Regno". For example, Assign04_Asim_Rasheed_123456.
- The name of the solution document file must also be AssignxxfullnameRegno.pdf. For example, Assign04Asim_Rasheed_123456.pdf.
- Only.pdf formats are accepted.
- At most ONE attachment will be accepted. Multiple attachments will not be entertained.
- You MUST NOT send your assignment to the course mailing list: it will NOT be accepted, and you may get discredit.
- Submission time is NOT the time when you email your assignment; rather it is the time BEFORE which we must receive your email.
- We encourage you to send your assignment two hour before the deadline ends.

Important for Cheating Cases:
This is an individual assignment. Cheating is strictly prohibited. Students found involved in the cheating/copying (irrespective of doing or allowing) will be marked simply as ZERO.

Important for all questions: Use your own wording to explain the answers. Just copy / paste / edit from the research paper will not receive the credit.

Be brief and to the point. Do not write more than 8 lines for each part. (10 x 5)

Q-1 Briefly describe the intrusion detection approaches?

Q-2 Differentiate between external intruders and internal intruders with suitable examples?

Q-3 What are the assumptions made by the system designers to limit the scope of the problem of detecting intrusions?

Q-4 What are the limitations of rule based intrusion detection systems?

Q-5 What metrics are useful for profile based intrusion detection and why?