Network Security

Week 1

DaeHun Nyang
nyang@ewha.ac.kr

Password cracking

- Password is stored not in a plaintext but in a hashed form.

- Hash function is oneway and you cannot inverse it.
  - Y = Hash(X), where X cannot be found easily from Y.

- You are given a file that has one million hashed passwords.
- You have to find out passwords as many as possible.
- The hash function is MD5.