CS 458/658
Assignment 2
Hanzhang Chen
ID: 20574275

Q1.

a. A salted hash can defend against those dictionary guessing attacks. A random or user-specific salt will avoid the situation that the same password will lead to the same hashes.
b. 1: 8-bit salt maybe a bit short, so that an attacker can build a lookup table for every possible salt. Any longer bit salt will be better.
   2: SHA-1 hash is relatively cheap to compute (in microseconds). Should use other cryptographic hash other than SHA-1 or SHA-512
   3: H-S will not be equal to SHA1(P*). Should check if SHA1(P*+S) == H

Q2.

a. D101: r
   D102: neither
   D103: neither
   D104: r
   D105: w

b. D201-> (Secret, {D, E})
   Carol-> (Secret, {B, D})
   Eve-> (Unclassified, {B, C})
   Eve-> (Confidential, {C, D})
   Carol-> (Secret, {D})

Q3.

a. smurf attack/ personal firewall
b. CPU/memory resources being used up; TCP initializes state by having the two end nodes exchange three packets (SYN, SYN-ACK, ACK), Server queues SYN from client and removes it when corresponding ACK is received, attacker sends many SYNs, but no ACKs. Then this would make the server being attacked half-connected, and keep sending the second syn+ack packet.
c. There is no client and server model for stateful inspection firewalls.