Q1

1. a) r access: no
   w access: no

   b) r access: yes
   w access: no

   c) r access: no
   w access: no

   d) r access: no
   w access: yes

   e) r access: yes
   w access: yes

2. a) i) admin, {attendance, employee record, equipment}
   ii) (admin, {attendance, employee record, equipment})

   b) i) admin, {attendance, employee record, equipment}
   ii) (support staff, {attendance, equipment})

   c) i) student, {equipment}
   ii) (student, {equipment})

   d) i) student, {equipment}
   ii) (student, {equipment})

   e) i) student, {equipment}
   ii) (student, {equipment})

Q2

1. A. Allow 15.5.5.0/25 => *
   from port * to 80,443 by tcp

   B. Allow * => 15.5.5.31
   from port * to 443 by tcp

   C. Allow * => 15.5.5.0/25
   from port * to 22 by tcp

   D. Allow 15.5.5.0/25 => 14.19.21.22
   from port 6556 to 1552 by both

   E. Allow 10.16.21.21 => 15.5.5.81
   from port * to 3221 by tcp

   F. Allow * => 15.5.5.21
   from port [1024, 65535] to port 25 by tcp

   Allow 15.5.5.21 => *
   from port [1024, 65535] to port 25 by tcp

6. deny list approach

drop * => 15.5.5.0/25

from port * to port != 22 by both

allow all other rules.

2.

IP spoofing

filter packets from outside services such that IP with 15.5.5.0/25 can not enter internal network.

3.

a) The SMTP Mail Server and webpage host would go in the DMZ. All other machines (A-C) and the IRC server go in the internal network zone. This gives extra layer of defence for IRC and machines and if any of the other servers are compromised it will be harder to compromise the machines and IRC Additionally the machines will still be able to access the servers.

b) The internal network zone.

Q3.

a) There are 2^8 possible salts in total. For each password, x, Eve can get the hash, H(x), and xor each possible salt. Then look up this result in the fingerprint file for a match.

There are 500,000 entries in the dictionary and 2^8 possible salts for each entry. Hence, $500,000 \cdot 2^8$ operations, excluding look up time.

b) 1. increase salt size so there is at least a unique one for each password

2. use multiple salts and xor each one to increase possibilities

3. use a single private salt and store it in another file elsewhere