Cordelia Tan
c63tan
21112180

Question 1:
1a. Read. Software engineer is at higher clearance than intern
1b. None, Terry's clearance is not high enough and no matching categories
1c. None, since Terry cannot access finances
1d. Read. Read down is available
1e. Read and write, sensitivity and clearance levels are the same

2a. No change. Clearance level is the same
2b. No change. File is of lower clearance than Kelly
2c. Kelly downgrades to Intern level. I(kelly) = glb(I(kelly), I(file3))
2d. File4 downgrades to intern level (since Kelly is now at intern level)
2e. File5 downgrades to intern level.

Question 2:
1.
ALLOW 16.35.125.0/24 => 0.0.0.0/0 FROM PORT all TO {80,443} BY TCP {SYN}
ALLOW Kim's_IP => 16.35.125.25 FROM PORT all TO 22 BY TCP {SYN}
DROP 85.63.28.0/24 => 16.35.125.0/24 FROM PORT all TO all BY TCP
ALLOW 0.0.0.0/0 => 16.35.125.13 FROM PORT all TO {80,443} BY TCP {SYN}
ALLOW 16.35.125.0/24 => 22.95.33.101 FROM PORT [5000,5100] TO 53 BY UDP

2. There might be IP spoofing taking place, to bypass security.
To stop this, an additional rule in the firewall to block all packets with a source IP from inside but actually originating from outside can be added.

3. Could implement a Demilitarized Zone (DMZ). By placing the web server inside it will allow me to expose the web server while still keeping the rest of the network secure.
For the firewall changes, add rules that allow traffic to and from the DMZ to the internet. Block traffic from DMZ and internal network.
Only allow necessary communication from internal network to the DMZ

Question 3:
1. Rainbow table attack (and keylogger attack)
2. No. If Terry's new passwords are still weak, it could still be easily cracked with a rainbow table.
(No, since the building is unrestricted, hardware attacks such as the keylogger attack would not be prevented by changing passwords.)
3. They should use stronger hash functions that are more computationally slow/ expensive. Compared to MD5, if the attacker tries to brute force, it will take a lot more time and resources.

They should also make use of salt before hashing. By adding a unique salt each time, the same password will have a different hash which makes rainbow tables hard to use.
4. The additional pin adds a layer of security, but if too simple could still be easily discovered. (also more susceptible to other basic attack methods)
The authenticator phone app is a much more secure method, it makes use of a different device and usually has time limits as well. It would be harder for the attacker to gain access to both devices at once.
5. MD5 is susceptible to collision attacks which could be exploited. bcrypt is a good alternative as it has preimage resistance and is slower (making brute force harder)